

## Änderung in gemSpec\_VZD\_FHIR\_Directory und gemSpec\_VZD

---

## 1 Aktualisierung Signatur-Algorithmen

---

### Es wird in gemSpec\_VZD\_FHIR\_Directory Kapitel 4.2.3 wie folgt angepasst

...

Die Föderationsliste MUSS mit einer JWS gemäß RFC7797 signiert werden. Der zu verwendende Signatur-Algorithmus MUSS "ES256" in der Liste der zulässigen Algorithmen enthalten "BP256R1" sein. Dazu MUSS ein Signatur-Zertifikat der Komponenten-PKI der TI (C.FD.SIG) verwendet werden. Das Signatur-Zertifikat MUSS im Signatur-Header enthalten sein. Der Signatur-Header hat folgende Struktur:

```
"ES256" "BP256R1", "x5c": [ "" ] }
```

### Es wird in gemSpec\_VZD\_FHIR\_Directory Kapitel 4.2.3 wie folgt angepasst

...

#### ML-142894 - AF\_10037 TIM Registrierungsdienst id\_token Prüfung (VZD-FHIR-Directory)

Die vom Registrierungsdienst ausgestellten id\_token müssen vom VZD-FHIR-Directory geprüft werden:

- Validierung der gemäß [ [RFC7519 # section-7.1](#)] vorgeschriebenen Struktur der id\_token gemäß [ [RFC7519 # section-7.2](#)].
- Prüfung Signatur des id\_token gemäß RFC7515 (das verwendete Zertifikat muss aus der Komponenten-PKI der TI stammen)
  - Zertifikatstyp: C.FD.SIG
  - technische Rolle: oid\_tim
- Die telematikID muss im Token Attribut idNummer enthalten sein.

Optional und verpflichtend ab FHIR VZD 1.2:

- Prüfung des id\_token Signatur-Zertifikats (oder sein Hash) gegen das bei der Beantragung der Credentials für die Schnittstelle I\_VZD\_TIM\_Provider\_Services übergebene Signatur-Zertifikat.
  - OCSP Prüfung des id\_token Signatur-Zertifikats
  - Prüfung Algorithmus: "alg":"ES256" "BP256R1"
  - Prüfung des Signaturzertifikats gegen das X.509-Root-CA Zertifikat der TI.
- Prüfung der zeitlichen Gültigkeit des id\_token für den Zugriff auf den VZD-FHIR-Directory: Das VZD-FHIR-Directory muss sicherstellen, dass der Zeitraum der Verwendung des Tokens zwischen den im Token mitgelieferten Werten der Attribute iat und exp liegt.
- Das VZD-FHIR-Directory muss die im id\_token übertragenen Attribute mit denen vergleichen, die mit dem Registrierungsdienst vereinbart wurden und alle mit dem id\_token in Verbindung stehenden Vorgänge abrechnen, wenn dem id\_token für die Verarbeitung notwendige Claims fehlen oder aber andere als die mit dem IDP-Dienst vereinbarten personenbezogenen Attribute vorhanden sind.

- Hinweis: Als unerwartete personenbezogene Attribute gelten gemäß Tabelle: [gemSpec\_IDP\_FD#TAB\_IDP\_DIENST\_0005] die Claims given\_name, family\_name, und organizationName
- Audience: "aud": URL der Schnittstelle z.B. "<https://fhir-directory.vzd.ti-dienste.de/owner-authenticate>"
- Die TelematikID aus dem Token Attribut idNummer muss in der Föderationsliste enthalten sein und der Föderationslisten-Eintrag muss vom gleichen TIM-Provider eingetragen worden sein der auch das Token ausgestellt hat.

[&lt;=]

...

**ML-142895 - AF\_10037 TI-Provider-Access-Token Prüfung (VZD-FHIR-Directory)**

Die TI-Provider-Access-Token müssen vom VZD-FHIR-Directory für den Endpunkt /tim-provider-services geprüft werden:

- Validierung der gemäß [ [RFC7519 # section-7.1](#)] vorgeschriebenen Struktur der ACCESS\_TOKEN gemäß [ [RFC7519 # section-7.2](#)].
- Sicherstellung der korrekten Signatur des Tokens gemäß RFC7515:
  - Zertifikatstyp: C.FD.SIG
  - technische Rolle: oid\_vzd\_ti
  - OCSP Prüfung des Signatur-Zertifikats: Nein
- Zeitliche Gültigkeit: Das VZD-FHIR-Directory muss sicherstellen, dass der Zeitraum der Verwendung des Tokens zwischen den im Token mitgelieferten Werten der Attribute iat und exp liegt.
- Die telematikID muss im Token "sub" claim enthalten sein.

Optional und verpflichtend ab FHIR VZD 1.2:

- Das VZD-FHIR-Directory muss die im ACCESS\_TOKEN übertragenen Attribute mit denen vergleichen, die vereinbart wurden und alle mit dem ACCESS\_TOKEN in Verbindung stehenden Vorgänge abbrechen, wenn dem ID\_TOKEN für die Verarbeitung notwendige Claims fehlen oder aber andere als die vereinbarten personenbezogenen Attribute vorhanden sind.
  - Prüfung Audience "aud" aus dem Token (muss der /tim-provider-services Schnittstelle entsprechen, z.B. <https://fhir-directory.vzd.ti-dienste.de/tim-provider-services>)
  - Hinweis: Als unerwartete personenbezogene Attribute gelten gemäß Tabelle: [gemSpec\_IDP\_FD#TAB\_IDP\_DIENST\_0005] die Claims given\_name, family\_name, und organizationName
- Sicherstellung der korrekten Signatur des Tokens gemäß RFC7515:
  - Prüfung Algorithmus: "alg":**"ES256"** **"BP256R1"**

[&lt;=]

## 2 Zusammenführung mehrerer TelematikID´s zu einer Organisation

Es wird in gemSpec\_VZD Kapitel 4.6.1.2.3 wie folgt ergänzt

### A\_18450-04 - VZD, I\_Directory\_Administration, modify\_Directory\_Entry

Der VZD MUSS Operation „modify\_Directory\_Entry“ gemäß Tabelle Tab\_VZD „modify\_Directory\_Entry“ umsetzen.

**Tabelle 1: Tab\_VZD „modify\_Directory\_Entry“**

<b>Name</b>	modify_Directory_Entry	
<b>Beschreibung</b>	Diese Operation ermöglicht die Aktualisierung von Verzeichniseinträgen im LDAP-Verzeichnis.	
<b>Eingangsdaten</b>	REST-Request PUT /DirectoryEntries/{uid}/baseDirectoryEntries operationId: modify_Directory_Entry Parameter: (siehe DirectoryAdministration.yaml)	
	<b>Parameter</b>	<b>Beschreibung</b>
	uid	Die „uid“ identifiziert den Verzeichnisdienst_Eintrag (Abb_VZD_logisches_Datenmodell) welcher aktualisiert wird.
	displayName	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	otherName	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	streetAddress	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	postalCode	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	localityName	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.

	<b>stateOrProvinceName</b>	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	<b>title</b>	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	<b>organization</b>	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	<b>specialization</b>	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	<b>domainID</b>	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	<b>holder</b>	Kann optional angegeben werden. Durch setzen des "holder" kann ein Verzeichniseintrag an einen anderen Eigentümer weitergegeben werden. Die Weitergabe kann nur durch den aktuellen Eigentümer/holder erfolgen.
	<b>maxKOMLEadr</b>	Kann optional angegeben werden. Durch setzen von "maxKOMLEadr" wird die maximale Anzahl von mail Adressen in den KOM-LE Fachdaten festgelegt.
<b>Komponenten</b>	Nutzer der Schnittstelle, Verzeichnisdienst	
<b>Ausgangsdaten</b>	REST-Response mit dem Distinguished Name (dn) von dem aktualisierten Verzeichnisdienst_Eintrag.	
<b>Ablauf</b>	Der VZD aktualisiert im LDAP-Verzeichnis den über Parameter „uid“ identifizierten Verzeichniseintrag mit den übergebenen Parametern. Der VZD setzt das LDAP-Directory-Attribut dataFromAuthority auf den Wert TRUE.	
<b>Fehlerfälle</b>	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

[&lt;=]

Es wird in gemSpec\_VZD Kapitel 4.6.3 wie folgt aufgenommen

#### 4.6.3 Zusammenführung mehrerer TelematikID´s zu einer Organisation

Im LDAP VZD existieren Einträge, die in der Realität eine Organisation darstellen, als einzelne Datensätze. Es haben z.B. Krankenhäuser unterschiedliche Einträge für ihre einzelnen Abteilungen im LDAP VZD. Für jeden dieser LDAP Einträge wird im FHIR VZD eine eigene Organisation generiert.

Entsprechende LDAP Einträge sollen als eine Organisation im VZD FHIR zusammengeführt werden. Damit sollen den VZD Nutzern die zusammengehörenden LDAP VZD Einträge im FHIR VZD als eine Organisation angezeigt werden.

Die Administration zusammengehörender Einträge erfolgt über Schnittstelle I\_Directory\_Administration.

Dafür wird das Attribut "providedBy" genutzt:

- Ist Attribut "providedBy" im LDAP VZD Eintrag nicht gesetzt, wird für den LDAP Eintrag im FHIR VZD eine Organisation generiert.
- Wird in Attribut "providedBy" im LDAP VZD Eintrag eine TelematikID eingetragen, wird für den LDAP Eintrag im FHIR VZD ein HealthcareService unter der - mit der TelematikID - referenzierten Organisation generiert.

#### **A\_24058 - VZD, I\_Directory\_Administration, providedBy**

Der VZD MUSS für die Administration von Attribut "providedBy" gewährleisten:

- Es wird nur eine Hierarchieebene unterstützt. Das Attribut "providedBy" im referenzierten LDAP Datensatz muss deshalb leer sein. In allen anderen Fälle MUSS der VZD mit einem Fehler antworten.
- Der VZD MUSS bei Löschung eines LDAP VZD Eintrags prüfen, ob dieser Eintrag über Attribut "providedBy" von einem anderen Datensatz referenziert wird. Ist dies der Fall, MUSS der VZD die Löschoperation mit einem Fehler ablehnen.
- Das Attribut "providedBy" darf nur eine TelematikID enthalten.
- Wenn Attribut providedBy gesetzt wurde, kann es nur zurückgesetzt (Inhalt auf leer gesetzt) werden. Eine Änderung auf einen anderen Wert wird nicht unterstützt.
- Der VZD MUSS vor dem Setzen von Attribut "providedBy" prüfen, ob der Client auch für den referenzierten LDAP Datensatz als Holder eingetragen ist. Ist dies nicht der Fall, MUSS der VZD die Operation mit einem Fehler ablehnen.

[<=]

#### **A\_24059 - VZD, I\_Directory\_Administration, Synchronisationsregeln für verlinkte LDAP Datensätze**

Der VZD MUSS für verlinkte LDAP Datensätze - mit einer TelematikID in Attribut "providedBy" - bei der Synchronisation der LDAP Daten in den FHIR VZD - abweichend von den normalen Synchronisationsregeln - das Mapping der Attribute entsprechend Tab\_VZD\_Datenmapping\_linked durchführen.

**Tabelle 2: Tab\_VZD\_Datenmapping\_linked**

LDAP Attribut	FHIR HealthcareServices Attribut	Bemerkung
displayName	name	Wird für normale Einträge in organization.name gemappt, hier auf HealthcareService.name.

organization	-	Kann einen alternativen Namen enthalten. Wird nicht synchronisiert, da es im HCS kein korrespondierendes Attribut gibt. Falls es in LDAP sinnvolle Informationen enthält, könnte man in FHR das HCS Attribut "comment" dafür nutzen.
specialization	speciality	Mapping auf HealthcareServices.specialty
domainID	identifizier	Wird normalerweise auf Organization.identifizier gemappt. Mapping erfolgt hier auf HealthcareService.identifizier. Das muss bei der Suche im FHIR VZD beachtet werden.
streetAddress, postalCode, countryCode, localityName, stateOrProvinceName	Location	Normales Mapping auf Location Attribute und Verlinkung der Location mit dem HealthcareService.
holder	-	Wird nicht in den HealthcareService gemappt. Der VZD stellt bei der Verlinkung von zwei Datensätzen sicher, dass der Client als Holder für beide Datensätze eingetragen ist. Die Zugriffsrechte für den generierten HealthcareService werden aus den Zugriffsrechten der Organisation abgeleitet (wie für alle HealthcareServices).
telematikID	identifizier	Wird normalerweise auf Organization.identifizier gemappt. Mapping erfolgt hier auf HealthcareService.identifizier. Das muss bei der Suche im FHIR VZD und bei der Authentisierung am Owner Interface beachtet werden. Der OrgAdmin des Haupteintrags kann damit auch alle untergeordneten HealthcareServices bearbeiten. Bei der Authentisierung mit der telematikID eines untergeordneten HealthcareServices darf der FHIR VZD nur das Bearbeiten dieses HealthcareService und untergeordneter Ressourcen erlauben.
professionOID	type	Wird für normalerweise in Organization.type abgelegt. Mapping erfolgt hier auf HealthcareService.type.
active	-	Wird nicht in den HealthcareService gemappt. Der Status für den generierten HealthcareService ergibt sich aus dem "active" Status der Organisation (wie für alle

		<p>HealthcareServices).</p> <p>Wenn der untergeordnete LDAP Datensatz über das "active" Attribut deaktiviert wird, hat das keine Auswirkungen auf den FHIR HealthcareService.</p> <p>Wenn der übergeordnete LDAP Datensatz über das "active" Attribut deaktiviert wird, hat dies im FHIR VZD Auswirkungen auf alle verlinkten HealthcareService.</p>
--	--	--

[<=]

**Es wird in gemSpec\_VZD Kapitel 5. wie folgt ergänzt**

**TIP1-A\_5607-11 - VZD, logisches Datenmodell**

Der VZD MUSS das logische Datenmodell nach Abb\_VZD\_logisches\_Datenmodell und Tab\_VZD\_Datenbeschreibung implementieren. Es wird keine Vorgabe an die technische Ausprägung des Datenmodells gemacht.

Der VZD MUSS sicherstellen, dass ein Eintrag nur Zertifikate aus dem Vertrauensraum der TI mit gleicher Telematik-ID enthält.

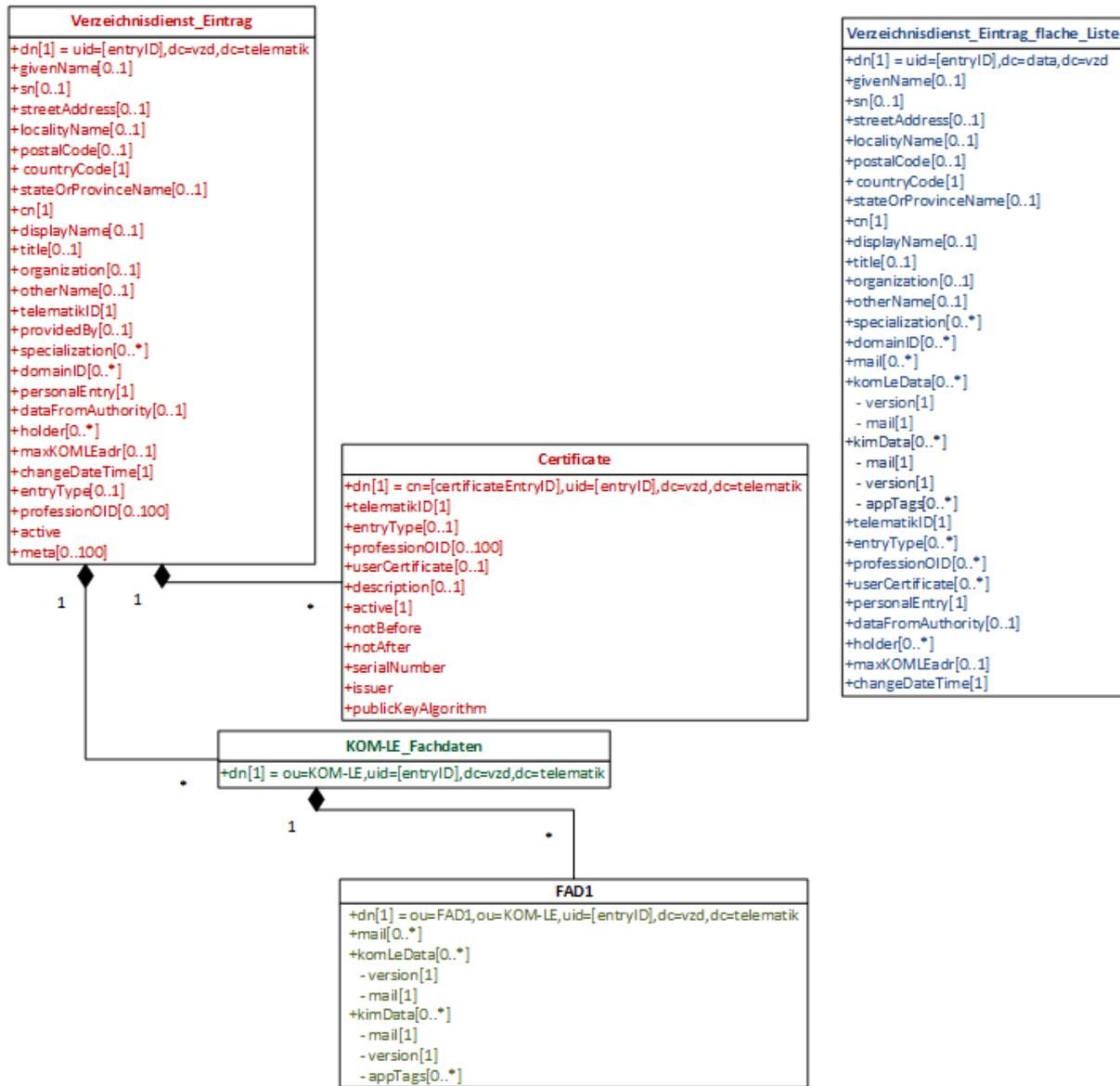


Abbildung 1: Abb\_VZD\_logisches\_Datenmodell

Tabelle 3: Tab\_VZD\_Datenbeschreibung

LDAP-Directory Attribut	Pflichtfeld?	Erläuterung
givenName	optional	HBA-Eintrag: Bezeichner: Vorname, Wird vom VZD aus dem Zertifikatsattribut givenName übernommen, wenn der Client von Schnittstelle I_Directory_Administration keinen Wert angibt. Wird über die Schreiboperationen von Schnittstelle I_Directory_Administration für givenName ein Inhalt geliefert, so wird dieser Wert für das Attribut gesetzt. Wird dem Verzeichniseintrag ein neues Zertifikat hinzu gefügt, wird der aktuelle Wert des Attributs durch der Wert aus Zertifikatsattribut givenName überschrieben.

		SMC-B-Eintrag: wird nicht verwendet
sn	optional	<p>Wird von E-Mail-Clients für die Suche nach Einträgen und die Anzeige von gefundenen Einträgen verwendet.</p> <p>HBA-Eintrag: Bezeichner: Nachname Verhalten der Befüllung des Attributs bei Nutzung der Operationen</p> <ul style="list-style-type: none"> <li>• add_Directory_Entry: <ul style="list-style-type: none"> <li>• Wird sn als Parameter übergeben, wird der angegebene Wert übernommen.</li> <li>• Wird sn nicht als Parameter übergeben, wird sn als Kopie von Parameter displayName gesetzt.</li> <li>• Wird sn und displayName nicht als Parameter übergeben und ein Zertifikat übergeben, wird sn mit dem Inhalt von Attribut surName aus dem Zertifikat gefüllt.</li> </ul> </li> <li>• modify_Directory_Entry: <ul style="list-style-type: none"> <li>• Wird sn als Parameter übergeben, wird der angegebene Wert übernommen.</li> <li>• Wird sn nicht als Parameter übergeben, wird sn als Kopie von Parameter displayName gesetzt.</li> </ul> </li> <li>• add_Directory_Entry_Certificate <ul style="list-style-type: none"> <li>• Bei dem Hinzufügen eines Zertifikats wird sn mit dem Inhalt von Attribut surName aus dem Zertifikat gefüllt/überschrieben.</li> </ul> </li> </ul> <p>SMC-B Eintrag: Verhalten der Befüllung des Attributs bei Nutzung der Operationen</p> <ul style="list-style-type: none"> <li>• add_Directory_Entry: <ul style="list-style-type: none"> <li>• Wird sn als Parameter übergeben, wird der angegebene Wert übernommen.</li> <li>• Wird sn nicht als Parameter übergeben, wird sn als Kopie von Parameter displayName gesetzt.</li> <li>• Wird sn und displayName nicht als Parameter übergeben, wird sn auf einen leeren Wert gesetzt ("- " im LDAP-View).</li> </ul> </li> <li>• modify_Directory_Entry: <ul style="list-style-type: none"> <li>• Wird sn als Parameter übergeben, wird der angegebene Wert übernommen.</li> <li>• Wird sn nicht als Parameter übergeben, wird sn gelöscht ("- " im LDAP-View).</li> </ul> </li> <li>• add_Directory_Entry_Certificate <ul style="list-style-type: none"> <li>• Hat keine Auswirkungen auf das sn Attribut.</li> </ul> </li> </ul>

cn	obligatorisch	<p>Wird von E-Mail Clients für die Suche nach Einträgen und die Anzeige von gefundenen Einträgen verwendet</p> <p>HBA: Eintrag: Bezeichner: Nachname, Vorname</p> <p>SMC-B Eintrag: Bezeichner: Name</p> <p>Unabhängig vom Kartentyp wird bei Nutzung der Schreiboperationen von Schnittstelle I_Directory_Administration cn als Kopie von Attribut displayName gesetzt, wenn cn nicht als Parameter übergeben wird. Wird cn als Parameter übergeben, wird der angegebene Wert übernommen.</p>
displayName	optional	<p>Bezeichner: Anzeigename, Name, nach dem der Eintrag von Nutzern gesucht wird, und unter dem gefundene Einträge angezeigt werden.</p> <p>HBA: Konvention für HBA Einträge: Name, Vorname Dieses Attribut wird genutzt, um den Namen der Person gegenüber dem Anwender darzustellen (Verwendung als Filter-Attribut, um die Suche einzuschränken, und bei der Darstellung des Ergebnisses).</p> <p>SMC-B: Dieses Attribut wird genutzt, um den Namen der Betriebsstätte gegenüber dem Anwender darzustellen (Verwendung als Filter-Attribut, um die Suche einzuschränken, und bei der Darstellung des Ergebnisses).</p> <p>Unabhängig vom Kartentyp: Dieses Attribut wird durch den VZD nicht automatisch aus dem Zertifikat ermittelt. Es kann über die Schreiboperationen von Schnittstelle I_Directory_Administration gesetzt werden. Wird über die Operation add_Directory_Entry von Schnittstelle I_Directory_Administration für displayName kein Inhalt geliefert, so wird in displayName der Wert "-" gesetzt.</p>
streetAddress	optional	<p>Bezeichner: Straße und Hausnummer</p> <p>Alias: street (wird vom VZD in der Response zu einer LDAP Query verwendet)</p>
postalCode	optional	<p>Bezeichner: Postleitzahl</p>
countryCode	obligatorisch	<p>Kann beim Anlegen des Datensatzes und beim Ändern gesetzt werden (falls nicht gesetzt, ergänzt der VZD den Defaultwert für Deutschland).</p>
localityName	optional	<p>Bezeichner: Ort</p> <p>Alias: l (wird vom VZD in der Response zu einer LDAP Query verwendet)</p>
stateOrProvinceName	optional	<p>Bezeichner: Bundesland oder Region</p> <p>Alias: st (wird vom VZD in der Response zu einer LDAP Query verwendet)</p>

title	optional	HBA: Bezeichner: Titel SMC-B: nicht verwendet
organization	optional	HBA: Bezeichner: Name der Organisation oder Name der Betriebsstätte SMC-B: Alternativer Name, nach dem der Eintrag von Nutzern gesucht wird, und unter dem gefundene Einträge angezeigt werden
otherName	optional	Bezeichner: Anderer Name Veraltet: Wird für die Suche nach Einträgen und die Anzeige von gefundenen Einträgen nicht benötigt (siehe displayName und organization)
specialization	optional	Bezeichner: Fachgebiet Kann mehrfach vorkommen (1..100).  <b>Für Einträge der Leistungserbringerorganisationen (SMC-B Eintrag)</b> Der Wertebereich entspricht den in hl7 definierten und für ePA festgelegten Werten ( <a href="https://wiki.hl7.de/index.php?title=IG:Value_Sets_f%C3%BCr_XDS#DocumentEntry_practiceSettingCode">https://wiki.hl7.de/index.php?title=IG:Value_Sets_f%C3%BCr_XDS#DocumentEntry_practiceSettingCode</a> ). urn:psc:<OID Codesystem:Code> Beispiel für Allgemeinmedizin: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.4:ALLG Beispiel für Zahnmedizin: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.4:MKZH Beispiel für Apotheke: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.5:PHZ Beispiel für Krankenhaus: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.4:GESU  <b>Für Einträge der Leistungserbringer (HBA-Eintrag)</b> Der Wertebereich entspricht den in hl7 definierten Werten ( <a href="https://wiki.hl7.de/index.php?title=IG:Value_Sets_f%C3%BCr_XDS#DocumentEntry_authorSpecialty">https://wiki.hl7.de/index.php?title=IG:Value_Sets_f%C3%BCr_XDS#DocumentEntry_authorSpecialty</a> ). urn:as:<OID Codesystem:Code> Psychologischer Psychotherapeut: urn:as:1.3.6.1.4.1.19376.3.276.1.5.11:82 Psychotherapeut: urn:as:1.3.6.1.4.1.19376.3.276.1.5.11:183 Fachpsychotherapeut für Kinder und Jugendliche: urn:as:1.3.6.1.4.1.19376.3.276.1.5.11:184 Fachpsychotherapeut für Erwachsene: urn:as:1.3.6.1.4.1.19376.3.276.1.5.11:185 Beispiel für FA Allgemeinmedizin: urn:as:1.2.276.0.76.5.514:011001 Beispiel für Zahnarzt: urn:as:1.2.276.0.76.5.492:1
domainID	optional	Bezeichner: domänenspezifisches Kennzeichen des Eintrags. kann mehrfach vorkommen (0..100)
holder	optional	Legt fest, wer Änderungen an den Basisdaten des Eintrags vornehmen darf. Hat keinen Einfluss auf Fachdaten und Zertifikatsdaten.
maxKOMLEadr	optional	Maximale Anzahl von mail Adressen in den KOM-LE-Fachdaten. Falls kein Wert eingetragen wurde, können beliebig viele mail Adressen in den KOM-LE Fachdaten eingetragen werden. Falls ein Wert eingetragen wurde, können maximal so viele mail Adressen in den KOM-LE Fachdaten eingetragen werden.

personalEntry	obligatorisch	Wird vom VZD eingetragen Wert == TRUE, wenn baseDirectoryEntry.entryType 1 hat (Berufsgruppe), Wert == FALSE sonst. Nach Löschung aller Zertifikate bleibt der Wert dieses Attributs `personalEntry` erhalten.
dataFromAutho- rity	optional	Wird vom VZD eingetragen Wert == TRUE, wenn der Verzeichnisdienst_Eintrag von dem Kartenherausgeber geschrieben wurde, Wert == FALSE sonst
active	obligatorisch	Mit diesem Attribut im Basiseintrag (Verzeichnisdienst_Eintrag in Abb_VZD_logisches_Datenmodell) kann der Client (Kartenherausgeber, TSP) die Aufnahme des VZD-Eintrags in die flache Liste steuern. Wenn das Attribut beim Anlegen eines VZD-Eintrags mit Zertifikat nicht angegeben wird, setzt der VZD das Attribut active auf TRUE (Default-Wert). Bei FALSE wird der Eintrag vom VZD aus der flachen Liste entfernt bzw. nicht übertragen. Dieses Attribut ist nicht in der flachen Liste enthalten. Wenn der VZD beim zeitlichen Ablauf des letzten Zertifikats einen VZD-Eintrag aus der flachen Liste entfernt, bleibt das Attribut active unverändert. Beim erneuten Hinzufügen eines Zertifikats wird der VZD-Eintrag also wieder in die flache Liste übernommen, wenn dieses Attribut den Wert "true" enthält.
meta	optional	Kann von den pflegenden Clients zur Abstimmung der Prozesse zwischen z. B. Kartenherausgeber und TSP genutzt werden. Dieses Attribut wird durch den VZD nicht ausgewertet. Die Werte für dieses Attribut müssen von den pflegenden Organisationen festgelegt und abgestimmt werden. Array von Strings (wird in LDAP auf <String, String> gemappt). Dieses Attribut ist nicht in der flachen Liste enthalten. Kann mehrfach vorkommen (0..100).
userCertificate	optional	Bezeichner: Enc-Zertifikat kann mehrfach vorkommen (0..50) Das Zertifikat wird gelöscht, wenn es ungültig geworden ist. Wenn kein Zertifikat vorliegt, dann kann der Eintrag nicht mittels LDAP-Abfrage gefunden werden. Format: DER, Base64-kodiert
notBefore	obligatorisch	Wird vom VZD bei Eintrag eines Zertifikats aus dem Zertifikat entnommen und ist nicht änderbar. Wird vom VZD zur Ermittlung der zeitlich gültigen Zertifikate genutzt. Dieses Attribut ist nicht in der flachen Liste enthalten.
userCertificate. active	obligatorisch	Wird vom VZD eingetragen. Wert == TRUE, wenn das userCertificate gemäß OCSP gültig ist (OCSP Response Status "good"), Wert == FALSE bei Zertifikaten von noch nicht freigeschalteten Karten (OCSP Response Status "unknown"). Wenn das Attribut den Wert FALSE enthält, wird der Zertifikatseintrag nicht in die flache Liste übernommen.
notAfter	obligatorisch	Wird vom VZD bei Eintrag eines Zertifikats aus dem Zertifikat entnommen und ist nicht änderbar. Wird vom VZD zur Ermittlung der zeitlich gültigen Zertifikate genutzt. Dieses Attribut ist nicht in der flachen Liste enthalten.

serialNumber	obligatorisch	Wird vom VZD bei Eintrag eines Zertifikats aus dem Zertifikat entnommen und ist nicht änderbar. Kann zur Suche nach Zertifikaten genutzt werden. Dieses Attribut ist nicht in der flachen Liste enthalten.
issuer	obligatorisch	Wird vom VZD bei Eintrag eines Zertifikats aus dem Zertifikat entnommen und ist nicht änderbar. Kann zur Suche nach Zertifikaten genutzt werden. Dieses Attribut ist nicht in der flachen Liste enthalten.
publicKeyAlgorithm	obligatorisch	Wird vom VZD bei Eintrag eines Zertifikats aus dem Zertifikat entnommen und ist nicht änderbar. Kann zur Suche nach Zertifikaten genutzt werden. Dieses Attribut ist nicht in der flachen Liste enthalten.
entryType	optional	<p>Bezeichner: Eintragstyp</p> <p>Wird vom VZD anhand der im Zertifikat enthaltenen OID (Extension Admission, Attribut ProfessionOID) und der Spalte Eintragstyp in Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID automatisch eingetragen. Siehe auch [gemSpecOID]# Tab_PKI_402 und Tab_PKI_403.</p> <p>entryType kann über Operationen add_Directory_Entry und modify_Directory_Entry gesetzt werden.</p> <p>Wird in Operation add_Directory_Entry ein Zertifikat angegeben wird, muss ein eventuell angegebener Parameter entryType mit dem Wert aus dem Zertifikat übereinstimmen. Bei nicht angegebenem Parameter entryType wird das Attribut entryType entsprechend dem Zertifikat gesetzt.</p> <p>Mit Operation modify_Directory_Entry kann über Request Parameter entryType das Attribut im VZD geändert werden, solange kein Zertifikat im VZD enthalten ist (welches dann einen abweichenden Wert gegenüber dem Request Parameter entryType enthalten würde).</p> <p>Wenn mit Operation add_Directory_Entry_Certificate ein neues Zertifikat hinzugefügt wird - welches in Bezug auf Attribut entryType vom Basisdatensatz abweicht - dann führt das zum Abbruch der Operation mit einem Fehler.</p>
telematikID	obligatorisch	<p>Bezeichner: TelematikID</p> <p>Wird vom VZD anhand der im jeweiligen Zertifikat enthaltenen Telematik-ID (Feld registrationNumber der Extension Admission) übernommen.</p> <p>Ist in den Basisdaten und in den Zertifikatsdaten enthalten.</p>
providedBy	optional	Zusammenhängende Einträge können über das Attribut providedBy gekennzeichnet werden. Siehe Kapitel 4.6.3 Zusammenführung mehrerer TelematikID's zu einer Organisation
professionOID	optional	<p>Bezeichner: Profession OID</p> <p>Wird vom VZD anhand der im Zertifikat enthaltenen OID (Extension Admission, Attribut ProfessionOID) und dem Mapping in Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID automatisch eingetragen. Siehe [gemSpecOID#Tab_PKI_402 und Tab_PKI_403]. kann mehrfach vorkommen (0..100)</p>

description	optional	<p>Bezeichner: Beschreibung Dieses Attribut ermöglicht das Zertifikat zu beschreiben, um die Administration des VZD-Eintrags zu vereinfachen. Hinweis: wird aktuell nicht verwendet.</p>
mail	optional	<p>Bezeichner: KOM-LE-Mail-Adresse kann mehrfach vorkommen (0..1000) Wird vom KOM-LE-Fachdienst-Anbieter eingetragen.</p>
komLeData	optional	<p>Bezeichner: komLeData kann mehrfach vorkommen (0..1000) Enthält die KOM-LE-Version des Clientmoduls der angegebenen "mail" Adresse im Attribut "version". Anhand dieser Version erkennt das sendende Clientmodul, welche KOM-LE-Version vom Empfänger-Clientmodul unterstützt wird und in welchem Format die Mail an diesen Empfänger versandt wird. Wenn zu einer KOM-LE-Mail-Adresse aus Attribut Mail kein korrespondierender Eintrag (mit gleicher KOM-LE-Mail-Adresse) im komLeData Attribut enthalten ist, muss KOM-LE-Version 1.0 angenommen werden. Jeder Datensatz - bestehend aus Version und KOM-LE-Mail-Adresse - muss vollständig sein (beide Attribute sind obligatorisch). Zu beachten ist bei der Auswertung bzw. Pflege dieser Daten:</p> <ul style="list-style-type: none"> <li>• Ein komLeData Eintrag setzt sich zusammen aus der Mail Adresse (Attribut "mail") und der zugehörigen KOM-LE Version (Attribut "version").</li> <li>• Für jede Mail Adresse aus dem "mail" Attribut darf es nur einen Eintrag in Datenstruktur komLeData geben. Es dürfen in komLeData keine Mail Adressen referenziert werden, die nicht im übergeordneten "mail" Attribut enthalten sind.</li> <li>• Wenn eine Mail Adresse gelöscht wird, muss auch ihr komLeData Eintrag gelöscht werden. Geschrieben wird immer die gesamte Liste. Für Änderungen muss erst der aktuelle Eintrag gelesen werden und nach Änderung in der Liste der gesamte Eintrag wieder geschrieben werden.</li> <li>• Beispiel für den Wert eines komLeData Eintrags in der flachen Liste (Ausgabe einer LDAP Suche):  <pre> komLeData: 1.0,mc_smcb_za@dom1.komle.telematik-test komLeData: 1.0,mz_smcb_za@dom2.kim.telematik-test komLeData: 1.0,mz_smcb_za@dom1.kim.telematik-test komLeData: 1.0,mb_secu_sm@dom3.kim.telematik-test komLeData: 1.0,mb_secu_sm@dom4.kim.telematik-test komLeData: 1.5,ak_secu_102@dom5.kim.telematik-test </pre> </li> </ul>
kimData	optional	<p>Bezeichner: kimData kann mehrfach vorkommen (0..1000) Enthält die KOM-LE-Version des Clientmoduls der angegebenen "mail" Adresse im Attribut "version". Zusätzlich kann zur KOM-LE-Version ein "+" angegeben sein. Anhand dieser Version erkennt das sendende Clientmodul, welche KOM-LE-Version vom Empfänger-Clientmodul unterstützt wird und in welchem Format die Mail an diesen Empfänger versandt wird. Wenn ein</p>

	<p>zusätzliches "+" angegeben ist, dann können mit dieser "mail" Adresse Nachrichten größer 15MiB verarbeitet werden. Jeder Datensatz MUSS die Attribute KOM-LE-Mail-Adresse und Version enthalten (beide Attribute sind obligatorisch). Wenn noch keine Version zu einer KOM-LE-Mail-Adresse angegeben wurde, dann wird vom VZD die Version 1.0 eingetragen.</p> <p>Jeder Datensatz kann zusätzlich ein oder mehrere Anwendungskennzeichen der angegebenen "mail" Adresse im Attribut "appTags" enthalten. Anhand dieser Anwendungskennzeichen erkennt das sendende Clientmodul, welche KIM Anwendungen vom Empfänger verarbeitet werden können.</p> <p>Das Attribut Anwendungskennzeichen (appTags) ist optional. Wenn zu einer KOM-LE-Mail-Adresse kein Anwendungskennzeichen enthalten ist, können alle KIM Anwendungen an diesen Empfänger versendet werden.</p> <p>Die Bestandteile KOM-LE-Mail-Adresse, KOM-LE-Version und Anwendungskennzeichen sind jeweils durch das Zeichen "," getrennt.</p> <p>Wenn mehrere Anwendungskennzeichen angegeben sind, dann sind diese durch das Zeichen " " getrennt.</p> <p>Zu beachten ist bei der Auswertung bzw. Pflege dieser Daten:</p> <ul style="list-style-type: none"> <li>• Ein kimData Eintrag setzt sich zusammen aus der Mail Adresse (Attribut "mail"), der zugehörigen KOM-LE Version (Attribut "version") inklusive dem optionalen "+" und optional einem oder mehreren Anwendungskennzeichen (Attribut "appTags").</li> <li>• Bei Angabe von mehreren Anwendungskennzeichen werden sie im LDAP Attribut durch das ' ' Zeichen getrennt (siehe Beispiel unten).</li> <li>• Für jede Mail Adresse darf es nur einen Eintrag in der Datenstruktur kimData geben.</li> <li>• Wenn eine Mail Adresse gelöscht wird, muss auch ihr kimData Eintrag gelöscht werden. Geschrieben wird immer der gesamte kimData Eintrag inklusive aller enthaltenen Attribute mit ihren Werten (für alle Mail Adressen). Für Änderungen muss erst der aktuelle Eintrag gelesen werden und nach Änderung der gesamte Eintrag wieder geschrieben werden.</li> <li>• Beispiel für den Wert eines kimData Eintrags in der flachen Liste (Ausgabe einer LDAP Suche):</li> </ul> <pre>kimData: mc_smcb_za@dom1.komle.telematik- test,1.0,eEB;V1.0 kimData: mz_smcb_za@dom2.kim.telematik-test,1.0,DALE- UV;Einsendung;V1.0 eEB;V1.0 kimData: mz_smcb_za@dom1.kim.telematik-test,1.0 kimData: mb_secu_sm@dom3.kim.telematik-test,1.0</pre>
--	---

		kimData: mb_secu_sm@dom4.kim.telematik-test,1.0 kimData: ak_secu_102@dom5.kim.telematik-test,1.5
changeDateTime	obligatorisch	Der VZD setzt dieses Attribut bei jeder Schreiboperation für den Datensatz (Basisdaten und Zertifikate) auf die aktuelle Zeit. Format entsprechend RFC 3339, section 5.6.

[&lt;=]

---

### 3 TI-Messenger Authentifizierung mit dem gematik Authenticator - Anbieten eines Polling Endpunktes

---

Es wird in gemSpec\_VZD\_FHIR\_Directory Kapitel 5.2 am Kapitelende wie folgt ergänzt

#### TI-Messenger Authentifizierung mit dem gematik Authenticator - Anbieten eines Polling Endpunktes

Wenn der Authenticator der gematik von Clients genutzt wird, um eine Authentifizierung auf Basis von Smartcards zu realisieren, dann ist es notwendig am Ende des Prozesses, die Kontrolle wieder an den Client zu übergeben und diesen mit den notwendigen Informationen für die weiteren Prozessschritte zu versorgen. Im folgenden werden die Anpassungen am Auth-Service des VZD-FHIR Directories beschrieben, die notwendig sind, um eine Anmeldung unter Verwendung des gematik Authenticators zu realisieren. Beim Anmeldevorgang verwendet der User eine Smartcard als Authentifizierungsmittel. Der Ablauf orientiert sich hierbei an den OIDC-Vorgaben zur Client initiated backchannel authentication. Um die Kollisionen mit standard OAuth2 Grants zu vermeiden, definiert die gematik einen eigenen Grant `urn:telematik:params:grant-type:decoupled` als Extension.

Der Standard kann nicht zu 100% umgesetzt werden, da hierfür ebenfalls noch eine Anpassung des gematik Authenticators und des IDP der gematik notwendig sind. Als Übergangslösung wird der Client den Aufruf des Authenticators übernehmen und das VZD-FHIR Directory einen Endpunkt bereitstellen über den der Status des Authentifizierungsvorgangs abgefragt werden kann. OIDC Konformität und Abweichungen werden im Anschluss an das Sequenzdiagramm im Rahmen der Erläuterung der einzelnen Schritte hervorgehoben.

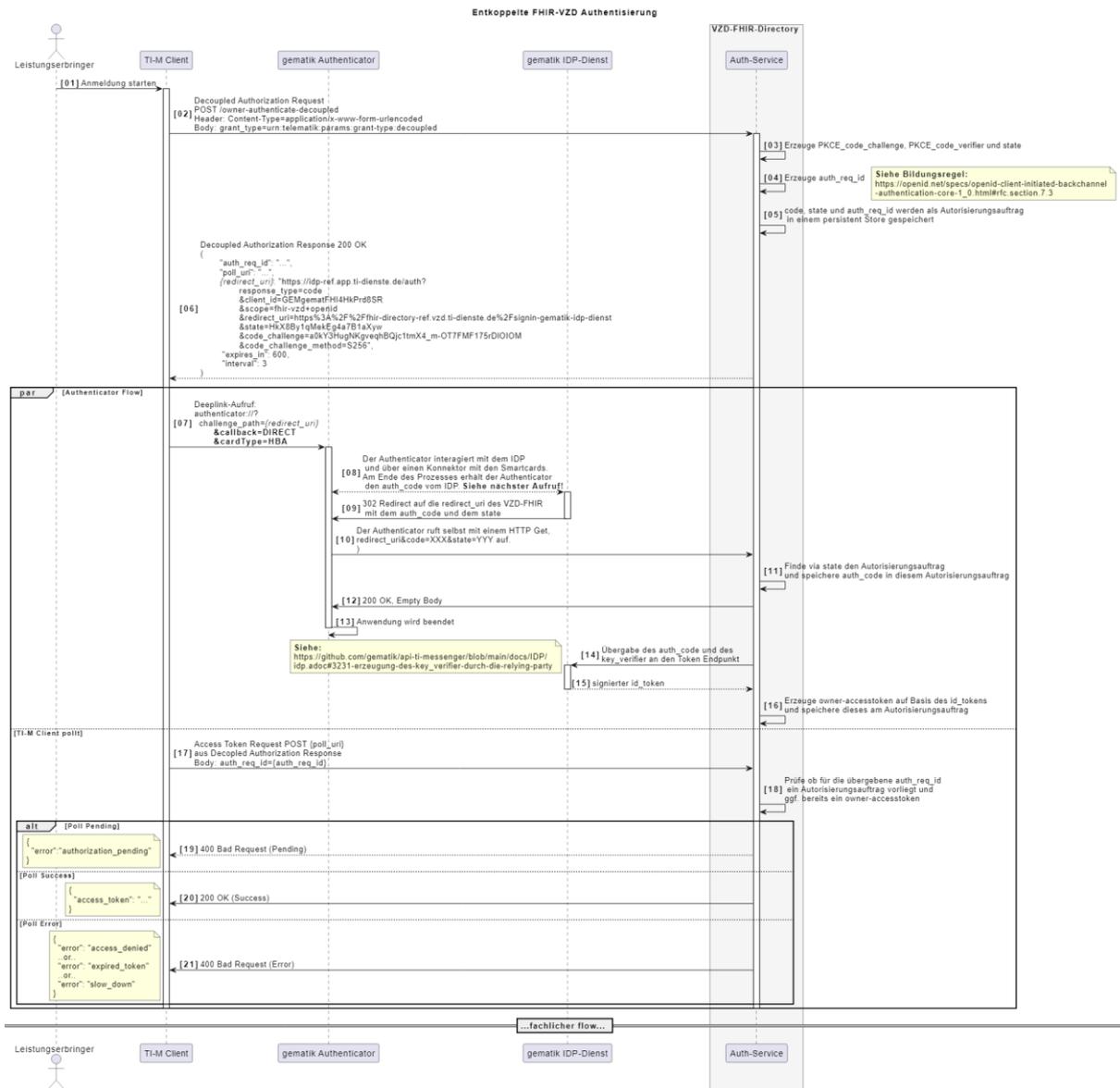


Abbildung 2: Sequence diagram - Authentifizierung mit dem gematik Authenticator

Der FHIR VZD muss für diese Authentifizierung folgende Funktionalitäten bereitstellen

Funktionalität	Anforderung
Bereitstellung des initialen authenticate Endpunkt am Auth-Service	<p>Das VZD-FHIR Directory muss einen /owner-authenticate-decoupled Endpunkt anbieten der POST Request mit dem übergebene grant_type urn:telematik:params:grant-type:decoupled akzeptiert.</p> <ul style="list-style-type: none"> <li>neuer owner Endpunkt</li> </ul>

	<p>Erhält das VZD-FHIR Directory eine derartige Anfrage wird ein Autorisierungsauftrag mit den Werten:</p> <ul style="list-style-type: none"> <li>• auth_reg_id</li> <li>• state</li> <li>• owner-accesstoken (in diesem Moment noch unbefüllt)</li> <li>• code_challenge</li> </ul> <p>erstellt und es werden folgende Daten an den Client im Response zurück geliefert:</p> <ul style="list-style-type: none"> <li>• owner Response <ul style="list-style-type: none"> <li>• expires_in: definiert die Zeit, die die auth_reg_id gültig ist und genutzt werden kann in Sekunden</li> <li>• interval: definiert das Mindestwarteintervall zwischen 2 Pollinganfragen</li> </ul> </li> </ul>
<p>Bereitstellung eines neuen polling Endpunktes am Auth-Service</p>	<p>Das VZD-FHIR Directory muss einen Endpunkt anbieten, der von Clients genutzt werden kann, um den Status eines Autorisierungsauftrages abzufragen. Dazu übergibt ein anfragender Client die folgenden Werte (wobei ist durch VZD festgelegter Endpoint, welcher im Schritt 06 dem Client über poll_uri mitgeteilt wird)</p> <ul style="list-style-type: none"> <li>• Token Request <pre>POST /oauth/v2/oauth-token HTTP/1.1 Host: idsvr.example.com Content-Type: application/x-www-form-urlencoded  grant_type=urn%3Atelematik%3Aparams%3Agrant-type%3Adecoupled auth_req_id=bspuw6ea-scst-u5hn-p3nt-37khzwY4g</pre> <p>Es wird geprüft, ob für die auth_req_id noch gültig ist und bereits ein owner-accesstoken vorliegt:</p> <p>a) Es liegt ein passendes Token vor: Dann antwortet der Auth-Service in seinem Response mit dem entsprechenden owner-accesstoken:</p> </li> <li>• Token Response Success <pre>HTTP/1.1 200 OK Content-Type: application/json Cache-Control: no-store  {   "access_token": "G5kXH2wHvUra0sHIDy1iTkDJgsgUO1bN"   "token_typ": "Bearer"   "expires_in": "86400"</pre> </li> </ul>

	<pre> } </pre> <p>b) liegt kein passendes Token vor dann antwortet der Server mit:</p> <ul style="list-style-type: none"> <li>• Token Response Error       <ul style="list-style-type: none"> <li>HTTP/1.1 400 Bad Request</li> <li>Content-Type: application/json</li> <li>Cache-Control: no-cache, no-store</li> </ul> </li> </ul> <pre> {   "error": [ERROR_REASON] } </pre> <p>Die ERROR_REASON kann die folgenden Werte annehmen:</p> <ul style="list-style-type: none"> <li>• authorization_pending - Der Authentifizierungsprozess ist noch nicht abgeschlossen</li> <li>• slow_down - Wenn der Token Request noch nicht abgeschlossen ist und der Client hat den Request schneller als 3 Sekunden gestellt.</li> <li>• access_denied - Der Authentifizierungsprozess konnte im Hintergrund nicht erfolgreich durchgeführt werden. Das minimal erlaubte Polling-Intervall wird auf 3 Sekunden festgelegt. Das VZD speichert den Zeitstempel der letzten Polling-Anfrage, sodass bei der nächsten Anfrage mit dem gleichen auth_req_id der letzte Zeitstempel abgerufen werden kann (z.B. in der gleichen Datenbanktabelle). Der Zeitunterschied des aktuellen Zeitstempel und den letzten Zeitstempel muss im Minimum 3 Sekunden betragen.</li> </ul>
Bereitstellung einer neuen Redirect_uri	Aktuell liefert die vom VZD-FHIR Directory verwendete Redirect_uri (/signin-gematik-idp-dienst) bei Übergabe des Auth_code und des state einen owner-accesstoken zurück. Diese Rückgabe ist nicht notwendig, wenn der Authenticator die Redirect_uri direkt aufruft.

---

## 4 Verlinkung von Personen und Organisationen

---

Es wird in gemSpec\_VZD\_FHIR\_Directory Kapitel 4.1.4 wie folgt ergänzt

### 4.1.4 Verlinkung von Personen und Organisationen in FHIR

Im FHIR VZD kann die Zugehörigkeit von Personen (Practitioner) zu Organisationen (Organization) hinterlegt werden. Das Eintragen dieser Verlinkung erfolgt im beidseitigen Einverständnis zwischen Organisation und Leistungserbringern.

Die Verlinkungsanfragen und Bestätigungen werden nicht in FHIR Daten abgelegt, sondern separat abgelegt. Erst mit Erteilung des beidseitigen Einverständnisses wird die Verlinkung in die FHIR Daten eingetragen.

Für das Eintragen der Verlinkungsdaten muss sich der Nutzer authentisieren. Die Authentisierung erfolgt je Rolle über folgende Authentisierungstoken.

#### 1. Leistungserbringer

- a. Ein Leistungserbringer authentisiert sich über das Owner-Authenticate-Verfahren (mit Gematik-IDP).
- b. Dabei erhält dieser einen Owner-Authenticate-Token, welcher an der administrativen Schnittstelle genutzt werden kann.

#### 2. Verantwortlicher einer Institution (Organisation)

- a. Der Verantwortliche authentisiert sich über das Owner-Authenticate-Verfahren (vereinfachtes Verfahren SMC-B oder Gematik IDP-Verfahren).
- b. Dabei erhält dieser einen Owner-Authenticate-Token, welcher an der administrativen Schnittstelle genutzt werden kann.

#### 3. Kartenherausgeber (Holder)

- a. Ein Kartenherausgeber authentisiert sich über die neue Schnittstelle Holder-Authenticate.
- b. Hierzu verwendet er den bereits bekannten Keycloak, um sich ein entsprechenden Keycloak-IdToken per Client-Secret-Verfahren zu holen.
- c. Im Anschluss tauscht er diesen Token gegen einen Holder-AccessToken aus, welcher an der administrativen Schnittstelle genutzt werden kann.

### Akzeptanzkriterien

#### ML-143700 - VZD-FHIR-Directory - Sichtbare Verbindung zwischen Personen und Organisationen

Für FHIR VZD Nutzer muss die Zugehörigkeit von Personen (Practitioner) zu Organisationen (Organization) sichtbar sein. Die Zugehörigkeit darf erst nach beidseitiger Bestätigung (von Person und Organisation) sichtbar sein. [<=]

#### ML-143701 - VZD-FHIR-Directory - Genehmigungspflichtige Verbindung zwischen Personen und Organisationen

Die Verbindung zwischen Personen und Organisationen muss beidseitig von den verlinkten Personen und Organisationen bestätigt werden. [<=]

### **ML-143703 - VZD-FHIR-Directory - Dokumentation der Verlinkungs-Genehmigungen zwischen Personen und Organisationen**

Die Genehmigungen, Ablehnungen und Löschungen der Verbindung zwischen Personen und Organisationen müssen dokumentiert werden und einsehbar sein. [ $\leq$ ]

### **ML-143702 - VZD-FHIR-Directory - Widerruf der Verbindung zwischen Personen und Organisationen**

Die Widerrufung der Verbindung zwischen Personen und Organisationen muss einseitig möglich sein

- durch den verlinkten Leistungserbringer,
- als Verantwortlicher einer verlinkten Institution und
- als Kartenherausgeber (der Organisation oder des Practitioners).

[ $\leq$ ]

### **ML-143800 - VZD-FHIR-Directory - Authentisierung für Verlinkung zwischen Personen und Organisationen**

Der FHIR VZD muss die Nutzer vor dem Eintragen von Verlinkungsdaten entsprechend ihrer Nutzergruppe authentisieren. Folgende Nutzergruppen müssen berücksichtigt werden

- Leistungserbringer
- Verantwortlicher eine Institution (Organisation)
- Kartenherausgeber (Holder)

[ $\leq$ ]

### **ML-143878 - VZD-FHIR-Directory - Verbot von Ressourcen-Verlinkungen ohne Verknüpfungsauftrag**

Der FHIR VZD muss das direkte Eintragen der Verbindung zwischen Personen und Organisationen über die FHIR VZD Owner Schnittstelle verhindern. Das Eintragen dieser Verbindung ist nur im beidseitiges Einverständnis zwischen Organisation und Leistungserbringern erlaubt. [ $\leq$ ]

**Es wird in gemSpec\_VZD\_FHIR\_Directory Kapitel 5 wie folgt ergänzt:**

## **5.5 Erstellen einer Verlinkungsanfrage**

### **AF\_10208 - FHIR-Directory - Erstellen einer Verlinkungsanfrage**

Attribute	Bemerkung
Beschreibung	Der authentifizierte Institutionsverantwortliche oder Leistungserbringer erstellt eine Verbindungsanfrage für seine Organisation bzw. Practitioner. In der Anfrage vermerkt er mit welchen HealthcareService bzw. PractitionerRole sein FHIR VZD Datensatz verbunden werden sollen. Die Bestätigung der Verlinkung erfolgt beidseitig. Die Antragsteller stimmt bereits mit dem Verlinkungsantrag zu.
Vorbedingung	Die Institution und der Leistungserbringer sind bereits im FHIR VZD eingetragen.

	Der Nutzer ist authentisiert.
Nachbedingung	Die Verlinkungsanfrage wurde erfasst. Die Verlinkung ist noch nicht im FHIR VZD sichtbar.

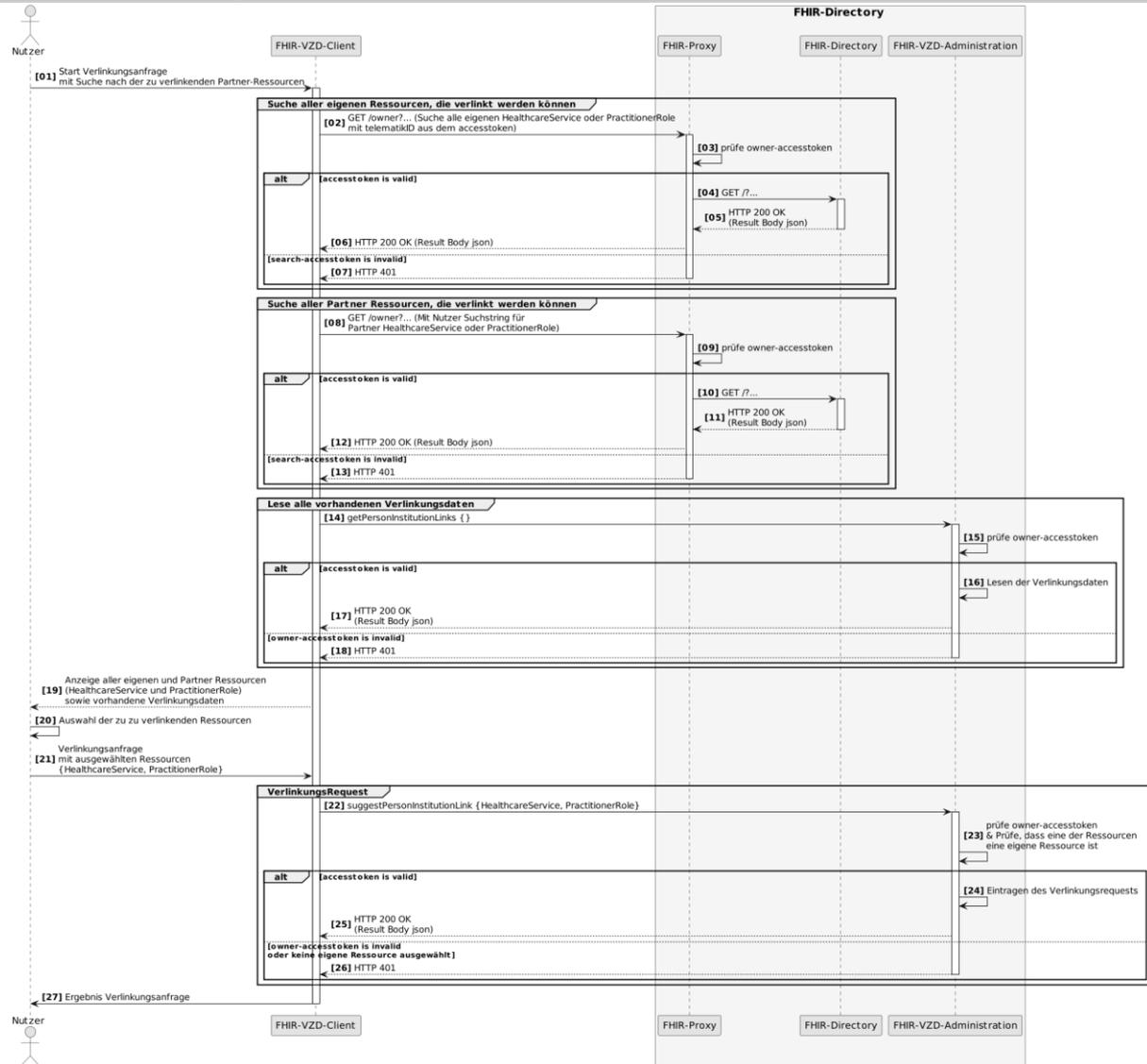


Abbildung 3: Sequence diagram - Erstellen einer Verlinkungsanfrage

[<=]

### Akzeptanzkriterien für den Anwendungsfall AF\_10208 FHIR-Directory - Erstellen einer Verlinkungsanfrage

#### ML-143802 - Erstellen einer Verlinkungsanfrage

Der FHIR VZD muss für Verlinkungsanfragen sicherstellen:

- Nur authentifizierte Nutzer dürfen Verlinkungsanfragen für ihre FHIR VZD Einträge stellen.
- Die Verlinkungsanfragen werden gespeichert und sind noch nicht in den normalen FHIR VZD Daten sichtbar.

[<=]

### 5.6 Bestätigen einer Verlinkungsanfrage

#### AF\_10207 - FHIR-Directory - Bestätigen einer Verlinkungsanfrage

Attribute	Bemerkung
Beschreibung	Der authentifizierte Institutionsverantwortliche oder Leistungserbringer bestätigt eine Verbindungsanfrage für seine Organisation bzw. Practitioner. Die Bestätigung der Verlinkung erfolgt beidseitig. Die Antragsteller stimmt bereits mit dem Verlinkungsantrag zu.
Vorbedingung	Die Institution und der Leistungserbringer sind im FHIR VZD eingetragen. Der Nutzer ist authentifziert.
Nachbedingung	Die Verlinkungsanfrage wurde bestätigt. Die Verlinkungsdaten wurden aktualisiert. Die Verlinkung ist im FHIR VZD sichtbar.

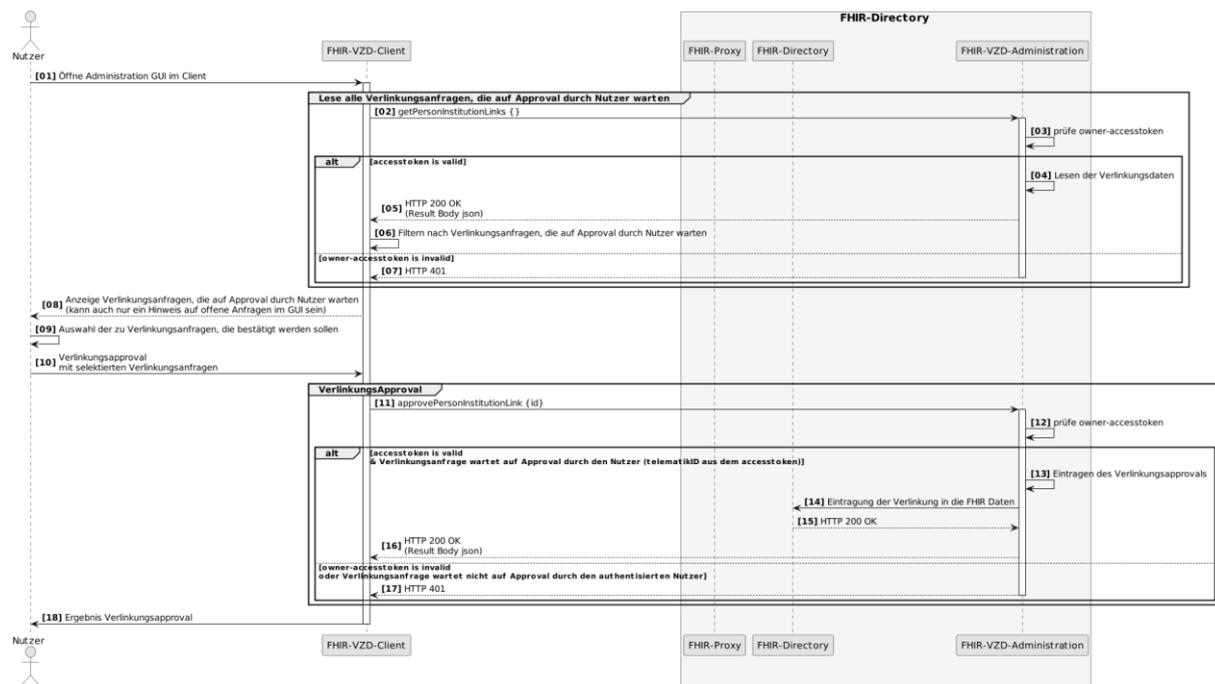


Abbildung 4: Sequence diagram - Bestätigen einer Verlinkungsanfrage

[<=]

### Akzeptanzkriterien für den Anwendungsfall AF\_10207 FHIR-Directory - Bestätigung einer Verlinkungsanfrage

#### ML-143808 - Bestätigung einer Verlinkungsanfrage

Der FHIR VZD muss für die Bestätigung von Verlinkungsanfragen sicherstellen:

- Nur authentifizierte Nutzer dürfen offene Verlinkungsanfragen für ihre FHIR VZD Einträge bestätigen.
- Die Verlinkungsbestätigungen werden in den Verlinkungsdaten gespeichert.

- In den FHIR VZD Daten wurde die Verlinkung ergänzt.

[<=]

**ML-143872 - Ablehnung einer Verlinkungsanfrage**

Der FHIR VZD muss die Ablehnung von Verlinkungsanfragen erlauben:

- Nur authentifizierte Nutzer dürfen offene Verlinkungsanfragen für ihre FHIR VZD Einträge ablehnen/zurückziehen (beide beteiligten Seiten).
- Die Verlinkungsablehnungen werden in den Verlinkungsdaten gespeichert.
- In den FHIR VZD Daten wurde die Verlinkung nicht eingetragen.

[<=]

**5.7 Löschen einer Verlinkung**

**AF\_10209 - FHIR-Directory - Löschen einer Verlinkung**

Attribute	Bemerkung
Beschreibung	Der authentifizierte Institutionsverantwortliche, Leistungserbringer oder Kartenherausgeber löscht eine Verlinkung für seine Organisation bzw. Practitioner bzw. seinen Zuständigkeitsbereich (Kartenherausgeber). Die Löschung der Verlinkung erfolgt einseitig und kann von jeder verlinkten Partei oder dem zuständigen Kartenherausgeber erfolgen.
Vorbedingung	Die Institution und der Leistungserbringer sind im FHIR VZD verlinkt. Der Nutzer ist authentifziert.
Nachbedingung	Die Verlinkung wurde gelöscht. Die Verlinkungsdaten wurden aktualisiert. Die Verlinkung ist im FHIR VZD nicht mehr sichtbar.

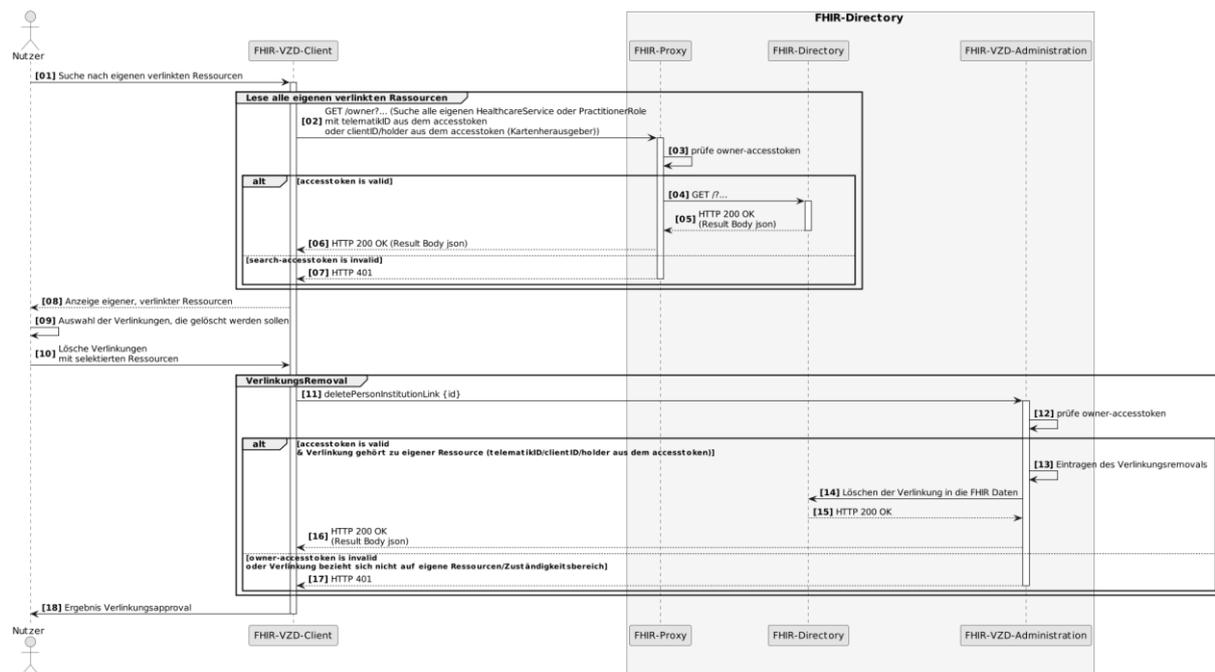


Abbildung 5: Sequence diagram - Löschen einer Verlinkung

[<=]

**Akzeptanzkriterien für den Anwendungsfall AF\_10209 FHIR-Directory - Löschen einer Verlinkung**

**ML-143811 - Löschen einer Verlinkung**

Der FHIR VZD muss für die Löschung von Verlinkungen sicherstellen:

- Nur authentifizierte Nutzer dürfen Verlinkung für ihre FHIR VZD Einträge bzw. für ihren Zuständigkeitsbereich löschen.
- Die Löschung der Verlinkung wird in den Verlinkungsdaten gespeichert.
- In den FHIR VZD Daten wurde die Verlinkung gelöscht.

[<=]

## 5 Support und Unterstützungsleistungen Produktivbetrieb TI-Messenger

Es wird in gemSpec\_VZD Kapitel 5. wie folgt ergänzt

Es wird in gemSpec\_VZD Kapitel 5. wie folgt ergänzt

Tabelle 4: Tab\_VZD\_Mapping\_Eintragstyp\_und\_ProfessionOID

Eintragstyp	Eintragstyp Bedeutung	ProfessionOID (ProfessionItem)
<b>1</b>	<b>Berufsgruppe</b>	1.2.276.0.76.4.30 (Ärztin/Arzt) 1.3.6.1.4.1.24796.4.11.1 (Ärztin/Arzt)* 1.2.276.0.76.4.31 (Zahnärztin/Zahnarzt) 1.2.276.0.76.4.32 (Apotheker/-in) 1.2.276.0.76.4.33 (Apothekerassistent/-in) 1.2.276.0.76.4.34 (Pharmazieingenieur/-in) 1.2.276.0.76.4.35 (pharmazeutisch-technische/-r Assistent/-in) 1.2.276.0.76.4.36 (pharmazeutisch-kaufmännische/-r Angestellte) 1.2.276.0.76.4.37 (Apothekenhelfer/-in) 1.2.276.0.76.4.38 (Apothekenassistent/-in) 1.2.276.0.76.4.39 (Pharmazeutische/-r Assistent/-in) 1.2.276.0.76.4.40 (Apothekenfacharbeiter/-in) 1.2.276.0.76.4.41 (Pharmaziepraktikant/-in) 1.2.276.0.76.4.42 (Stud.pharm. oder Famulant/-in) 1.2.276.0.76.4.43 (PTA-Praktikant/-in) 1.2.276.0.76.4.44 (PKA Auszubildende/-r) 1.2.276.0.76.4.45 (Psychotherapeut/-in) 1.2.276.0.76.4.46 (Psychologische/-r Psychotherapeut/-in) 1.2.276.0.76.4.47 (Kinder- und Jugendlichenpsychotherapeut/-in) 1.2.276.0.76.4.48 (Rettungsassistent/-in) 1.2.276.0.76.4.178 (Notfallsanitäter/-in) 1.2.276.0.76.4.232 (Gesundheits- und Krankenpfleger/-in, Gesundheits- und Kinderkrankenpfleger/-in) 1.2.276.0.76.4.233 (Altenpfleger/-in) 1.2.276.0.76.4.234 (Pflegefachfrauen und Pflegefachmänner) 1.2.276.0.76.4.235 (Hebamme) 1.2.276.0.76.4.236 (Physiotherapeut/-in) 1.2.276.0.76.4.237 (Augenoptiker/-in und

		<p>Optometrist/-in)  1.2.276.0.76.4.238 (Hörakustiker/-in)  1.2.276.0.76.4.239  (Orthopädieschuhmacher/-in)  1.2.276.0.76.4.240 (Orthopädietechniker/-in)  1.2.276.0.76.4.241 (Zahntechniker/-in)  1.2.276.0.76.4.274 (Ergotherapeut/-in)  1.2.276.0.76.4.275 (Logopäde/Logopädin)  1.2.276.0.76.4.276 (Podologe/Podologin)  1.2.276.0.76.4.277 (Ernährungstherapeut/-in)</p>
<b>2</b>	<b>Versicherte/-r</b>	1.2.276.0.76.4.49 (Versicherte/-r)
<b>3</b>	<b>Leistungserbringerinstitution</b>	<p>1.2.276.0.76.4.50 (Betriebsstätte Arzt)  1.2.276.0.76.4.51 (Zahnarztpraxis)  1.2.276.0.76.4.52 (Betriebsstätte Psychotherapeut)  1.2.276.0.76.4.53 (Krankenhaus)  1.2.276.0.76.4.54 (Öffentliche Apotheke)  1.2.276.0.76.4.55 (Krankenhausapotheke)  1.2.276.0.76.4.56 (Bundeswehraphotheke)  1.2.276.0.76.4.57 (Betriebsstätte Mobile Einrichtung Rettungsdienst)  1.2.276.0.76.4.245 (Betriebsstätte Gesundheits-, Kranken- und Altenpflege)  1.2.276.0.76.4.246 (Betriebsstätte Geburtshilfe)  1.2.276.0.76.4.247 (Betriebsstätte Physiotherapie)  1.2.276.0.76.4.248 (Betriebsstätte Augenoptiker)  1.2.276.0.76.4.249 (Betriebsstätte Hörakustiker)  1.2.276.0.76.4.250 (Betriebsstätte Orthopädieschuhmacher)  1.2.276.0.76.4.251 (Betriebsstätte Orthopädietechniker)  1.2.276.0.76.4.252 (Betriebsstätte Zahntechniker)  1.2.276.0.76.4.253 (Rettungsleitstelle)  1.2.276.0.76.4.254 (Betriebsstätte Sanitätsdienst Bundeswehr)  1.2.276.0.76.4.255 (Betriebsstätte Öffentlicher Gesundheitsdienst)  1.2.276.0.76.4.256 (Betriebsstätte Arbeitsmedizin)  1.2.276.0.76.4.257 (Betriebsstätte Vorsorge- und Rehabilitation)  1.2.276.0.76.4.278 (Ergotherapiepraxis)  1.2.276.0.76.4.279 (Logopaedische Praxis)  1.2.276.0.76.4.280 (Podologiepraxis)</p>

		1.2.276.0.76.4.281 (Ernährungstherapeutische Praxis)
<b>4</b>	<b>Organisation</b>	1.2.276.0.76.4.187 (Betriebsstätte Leistungserbringerorganisation Vertragszahnärzte) 1.2.276.0.76.4.58 (Betriebsstätte gematik) 1.2.276.0.76.4.190 (AdV-Umgebung bei Kostenträger) 1.2.276.0.76.4.210 (Betriebsstätte Leistungserbringerorganisation Kassenärztliche Vereinigung) 1.2.276.0.76.4.223 (Betriebsstätte GKV-Spitzenverband) 1.2.276.0.76.4.226 (Betriebsstätte Mitgliedsverband der Krankenhäuser) 1.2.276.0.76.4.227 (Betriebsstätte der Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH) 1.2.276.0.76.4.228 (Betriebsstätte der Deutschen Krankenhausgesellschaft) 1.2.276.0.76.4.224 (Betriebsstätte Apothekerverband) 1.2.276.0.76.4.225 (Betriebsstätte Deutscher Apothekerverband) 1.2.276.0.76.4.229 (Betriebsstätte der Bundesärztekammer) 1.2.276.0.76.4.230 (Betriebsstätte einer Ärztekammer) 1.2.276.0.76.4.231 (Betriebsstätte einer Zahnärztekammer) 1.2.276.0.76.4.242 (Betriebsstätte der Kassenärztlichen Bundesvereinigung) 1.2.276.0.76.4.243 (Betriebsstätte der Bundeszahnärztekammer) 1.2.276.0.76.4.244 (Betriebsstätte der Kassenzahnärztlichen Bundesvereinigung) 1.2.276.0.76.4.262 (Betriebsstätte Pflegeberatung nach § 7a SGB XI) 1.2.276.0.76.4.263 (Betriebsstätte Psychotherapeutenkammer) 1.2.276.0.76.4.264 (Betriebsstätte Bundespsychotherapeutenkammer) 1.2.276.0.76.4.265 (Betriebsstätte Landesapothekerkammer) 1.2.276.0.76.4.266 (Betriebsstätte Bundesapothekerkammer) 1.2.276.0.76.4.267 (Betriebsstätte elektronisches Gesundheitsberuferegister) 1.2.276.0.76.4.268 (Betriebsstätte Handwerkskammer) 1.2.276.0.76.4.269 (Betriebsstätte Register für Gesundheitsdaten)

		1.2.276.0.76.4.270 (Betriebsstätte Abrechnungsdienstleister) 1.2.276.0.76.4.271 (Betriebsstätte PKV-Verband) 1.2.276.0.76.4.284 (Betriebsstätte Weitere Kostenträger im Gesundheitswesen) 1.2.276.0.76.4.285 (Weitere Organisationen der Gesundheitsversorgung)
<b>5</b>	<b>Krankenkasse</b>	1.2.276.0.76.4.59 (Betriebsstätte Kostenträger)
<b>6</b>	<b>Krankenkasse ePA</b>	1.2.276.0.76.4.273 (ePA KTR-Zugriffsautorisierung)
<b>7</b>	<b>KIM</b>	1.2.276.0.76.4.286 (KIM-Hersteller und -Anbieter)
<b>8</b>	<b>TIM</b>	1.2.276.0.76.4.295 (TIM-Hersteller und -Anbieter)
<b>9</b>	<b>DiGA</b>	1.2.276.0.76.4.282 (DiGA-Hersteller und Anbieter)

\* Definition für G0-HBA bis 23.09.2018 durch die Bundesärztekammer, siehe <https://www.bundesaerztekammer.de/aerzte/telematiktelemedizin/earztausweis/technische-spezifikationen/>

### Es wird in gemSpec\_VZD\_FHIR\_Directory Kapitel "7.6 Versionierung Datenmodell" wie folgt aktualisiert

Folgende Versionen der Datenmodell Ressourcen ( <https://simplifier.net/vzd-fhir-directory/> ) sind für die vorliegende Spezifikation relevant:

- de.gematik.fhir.directory/0.10.2

## 6 Korrekturen

### Es wird in gemSpec\_VZD\_FHIR\_Directory Kapitel 3 wie folgt angepasst

Die folgende Abbildung zeigt die Teilkomponenten des bisherigen VZD-LDAP-Directory und die rot dargestellten neuen Komponenten des VZD-FHIR-Directory.

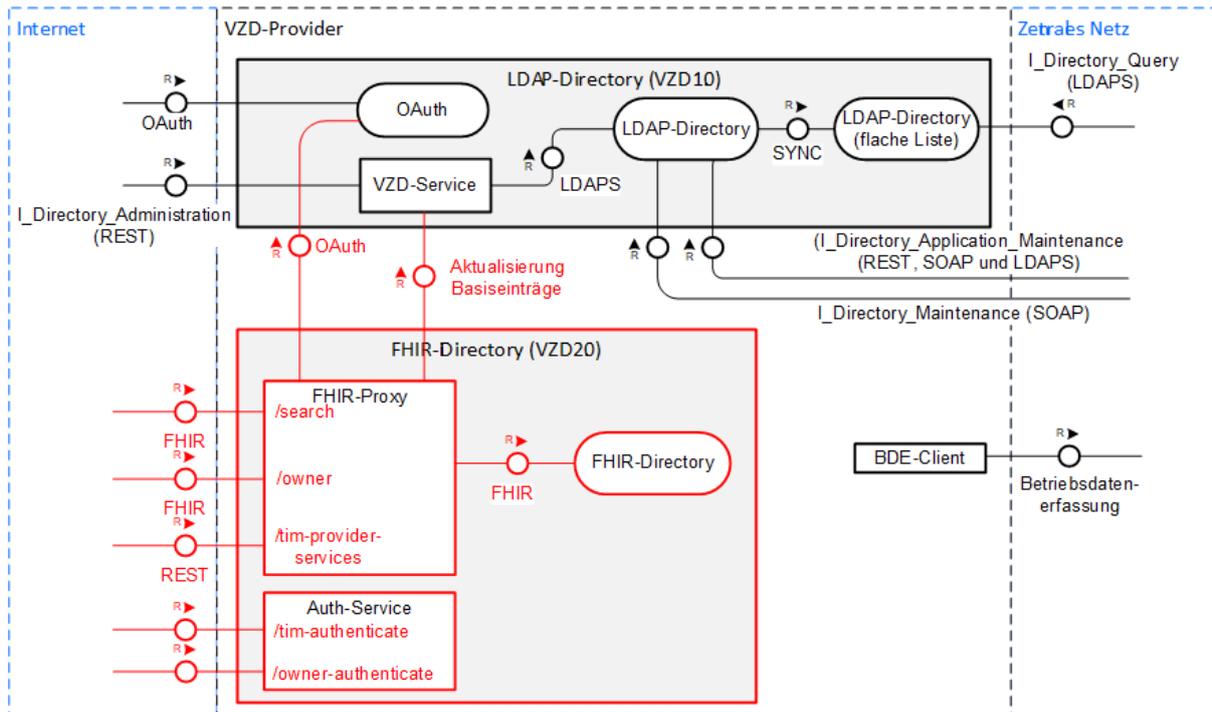


Abbildung 6: Zerlegung des VZD

### Es wird in gemSpec\_VZD\_FHIR\_Directory Kapitel "4.2.3 Erzeugung und Bereitstellung der Föderationsliste

" wie folgt angepasst

#### ~~ML-123677 – Maßnahmen gegen die Manipulation der Föderationsliste (VZD-FHIR-Directory, Sicherheitsgutachten)~~

~~Im Sicherheitsgutachten des VZD-FHIR-Directories sind geeignete Maßnahmen gegen die Manipulation der Föderationsliste beschrieben. <= [HU1]~~

Tabelle 5: Mitgeltende Dokumente und Web-Inhalte

Quelle	Herausgeber: Bezeichnung / URL	Version Branch / Tag

[VZD-FHIR-PACKAGE-DIRECTORY]	<a href="https://simplifier.net/packages/de.gematik.fhir.directory/0.10.2">https://simplifier.net/packages/de.gematik.fhir.directory/0.10.2</a>	0.10.2
------------------------------	---	--------