
Inhaltsverzeichnis

1 Änderung in gemSpec_VZD_FHIR_Directory.....	3
2 Änderung in gemSpec_VZD.....	31
3 Änderungen in Steckbriefen.....	52
3.1 Änderungen in gemProdT_VZD_FHIR.....	52
3.2 Änderungen in gemProdT_VZD.....	53

1 Änderung in gemSpec_VZD_FHIR_Directory

Es wird Kapitel "4 Funktionsmerkmale" wie folgt angepasst

...

Geplante FHIR-Directory-Schnittstellen in zukünftigen Releases:

- **FHIRDirectorySearchTI API**

Geplante Schnittstelle für die Suche der Einträge ohne Authentisierung im geschlossenen Netz der TI (TI-Anbindung erforderlich).

- **FHIRDirectoryAdmin API**

Geplante Schnittstelle für die Administration der Daten im FHIR-Verzeichnisdienst als Nachfolger für REST-Pflegeschnittstelle (DirectoryAdministration).

Es wird am Ende von Kapitel "4.1.2 Mapping von LDAP auf FHIR-Ressourcen" wie folgt aufgenommen

Zu jedem LDAP-VZD-SMC-B-Eintrag werden im FHIR VZD je eine Instanz der Ressourcen "Organization", "HealthcareService" und "Location" erzeugt bzw. aktualisiert.

Zu jedem LDAP-VZD-HBA-Eintrag werden im FHIR VZD je eine Instanz der Ressourcen "Practitioner", "PractitionerRole" und "Location" erzeugt bzw. aktualisiert.

Berücksichtigung der Zertifikate im LDAP VZD

Der Status von LDAP- und FHIR-VZD-Einträgen wird über das "active" Attribut des LDAP-Basiseintrags, der FHIR Organization Ressource und der FHIR Practitioner Ressource abgebildet. Das "active" Attribut des LDAP-Basiseintrags wird auf die "active" Attribute der FHIR Ressourcen gemappt.

Im LDAP VZD werden VZD-Einträge nicht gefunden, wenn keine gültigen Zertifikate für sie im LDAP VZD vorhanden sind. Diesem Mechanismus wird oft vertraut und der VZD-Eintrag am Ende seiner Laufzeit (bzw. am Ende der Laufzeit seiner Zertifikate) nicht über das "active" Attribut des LDAP-Basiseintrags gesperrt. Im FHIR VZD sind diese VZD-Einträge aktuell aktiv ("active" Attribut der FHIR Ressourcen) und können genutzt werden. Da dies zu Problemen führt (z.B. Zuweisung von eRezepten, die dann nicht abgerufen werden können), wird das Mapping vom LDAP VZD in den FHIR VZD erweitert.

Das Mapping der LDAP-Einträge in die FHIR-Einträge berücksichtigt die Zertifikate im LDAP VZD wie folgt:

- Ist für einen VZD-Eintrag kein aktives Zertifikat im LDAP VZD verknüpft, wird der Datensatz im VZD FHIR deaktiviert (active = false). Dies erfolgt unabhängig vom "active" Attribut des LDAP-VZD-Basiseintrags.
- Wird dem LDAP-VZD-Eintrag nachträglich ein aktives Zertifikat hinzugefügt, wird der Datensatz erneut synchronisiert. Der Status ("active") wird von dem Attribut "active" des LDAP-VZD-Basiseintrags übernommen.
- Die Deaktivierung von VZD-Einträgen über das "active" Attribut des LDAP-VZD-Basiseintrags wird unabhängig von der Datenkonsistenz des LDAP-VZD-Eintrags in

den VZD FHIR synchronisiert. Damit werden auch VZD-Einträge mit inkonsistenten Daten im LDAP VZD im FHIR VZD deaktiviert.

Es wird Kapitel "4.1.3 FHIR RESTful API" wie folgt angepasst

Die Operationen der FHIR-Schnittstelle sind durch die FHIR-Spezifikation festgelegt (<https://www.hl7.org/fhir/http.html>).

Die Anzahl der mittels /search und /fdv/search Operation gefundenen und zurückgegebenen Einträge wird initial auf 100 begrenzt. Dieser Wert MUSS durch den FHIR-VZD-Anbieter konfigurierbar sein. Die zurückgegebenen Einträge werden in einem FHIR-Ressource-Bundle zusammengefasst. Im Attribut Bundle.total MUSS die Gesamtanzahl der Einträge im Bundle zurückgegeben werden. Für die Ermittlung der Gesamtzahl der gefundenen Einträge kann die Suchoperation _summary=count (<https://hl7.org/fhir/search.html#summary>) genutzt werden. Das Suchergebnis enthält dann in Bundle.total die Gesamtzahl der gefundenen Einträge, aber nicht die Einträge selbst.

Mit Angabe des Parameters _total=accurate (https://www.hl7.org/fhir/search.html#_total) in der Suchoperation enthält das Suchergebnis die gefundenen Einträge (maximal 100) und in Attribut Bundle.total die gesamte Anzahl der Suchergebnisse im FHIR VZD (ohne Einschränkung auf 100 Ergebnisse).

Bei Verwendung von Parameter _total=accurate bitte beachten, dass die Suche mit diesem Suchparameter für den FHIR VZD performance-intensiver ist, da er die akkurate Gesamtanzahl ermitteln muss. Dieser Parameter darf deshalb durch den Client nur benutzt werden, wenn er diese Anzahl benötigt.

Es wird Kapitel "4.2.1.2 FHIR Schnittstelle für TI-Messenger-Nutzer FHIRDirectorySearchAPI" wie folgt angepasst

Endpunkte für die Suche von Einträgen im VZD-FHIR-Directory durch TI-Messenger-Clients

In der Produktionsumgebung (PU) ist die URL:
<https://fhir-directory.vzd.ti-dienste.de/search>

In der Referenzumgebung (RU) ist die URL:
<https://fhir-directory-ref.vzd.ti-dienste.de/search>

In der Testumgebung (TU) ist die URL: <https://fhir-directory-tu.vzd.ti-dienste.de/search>

Authentisierung

Um die Schnittstelle nutzen zu können, MÜSSEN sich die Clients mit einem gültigen Token authentisieren, das von einem Matrix-Homeserver aus der TI-Messenger-Föderation ausgestellt wurde. Im Folgenden werden diese Accesstoken Matrix-OpenID-Token genannt. Nach erfolgreicher Prüfung des Matrix-OpenID-Token stellt der FHIR-Proxy dem TI-Messenger-Client ein neues OAuth Accesstoken aus (search-access_token), das für Suchanfragen des TI-Messenger-Clients verwendet wird.

Das search-access_token enthält folgende Attribute:

```
{
  "iss": "https://fhir-directory.vzd.ti-dienste.de/tim-
authenticate",
  "aud": "https://fhir-directory.vzd.ti-dienste.de/search",
  "exp": 1726648516,
```

```
"scope": [ "search:read certificate:read" ],  
"iat": 1726562116  
}
```

Das Attribut "iss" enthält die URL des Endpunktes für die Authentisierung in der jeweiligen Umgebung RU, TU oder PU.

Das Attribut "aud" enthält die URL des Endpunktes in der jeweiligen Umgebung RU, TU oder PU.

Die zeitliche Gültigkeit des search-access_tokens beträgt 24 Stunden.

Endpunkte für die Authentisierung

In der Produktionsumgebung (PU) ist die URL: <https://fhir-directory.vzd.ti-dienste.de/tim-authenticate>

In der Referenzumgebung (RU) ist die URL: <https://fhir-directory-ref.vzd.ti-dienste.de/tim-authenticate>

In der Testumgebung (TU) ist die URL: <https://fhir-directory-tu.vzd.ti-dienste.de/tim-authenticate>

Operationen

Die FHIR-Operationen für die Suche nach Einträgen im VZD-FHIR-Directory sind in der HL7-FHIR-Spezifikation (<https://www.hl7.org/fhir/http.html>) festgelegt.

Zusätzlich zur HL7-FHIR-Spezifikation muss der FHIR VZD folgende Suchparameter unterstützen:

- practitioner.qualification
- **location** endpoint.address (z.B. Suche nach TI-Messenger Adresse)

Es wird Kapitel "4.2.1.3 FHIR-Schnittstelle für Besitzer FHIRDirectoryOwnerAPI" wie folgt angepasst

Die Schnittstelle ermöglicht es den Besitzern einer Telematik-ID, ihren Eintrag im VZD-FHIR-Directory zu ändern. Im bei der Authentifizierung verwendeten Accesstoken ist die Telematik-ID des Nutzers enthalten. Nur der Eintrag (PractitionerDirectory oder OrganizationDirectory) mit der eigenen Telematik-ID darf verändert werden. Dabei dürfen nur die Attribute verändert werden, die nicht vom VZD-LDAP-Directory synchronisiert werden.

Endpunkte für das Ändern von eigenen Einträgen im VZD-FHIR-Directory durch TI-Messenger Clients und Org-Admin-Clients

In der Produktionsumgebung (PU) ist die URL: <https://fhir-directory.vzd.ti-dienste.de/owner>

In der Referenzumgebung (RU) ist die URL: <https://fhir-directory-ref.vzd.ti-dienste.de/owner>

In der Testumgebung (TU) ist die URL: <https://fhir-directory-tu.vzd.ti-dienste.de/owner>

Authentisierung

Um die Schnittstelle nutzen zu können, MÜSSEN sich die Clients mit einem gültigen Accesstoken authentisieren, das vom FHIR-Proxy ausgestellt wurde. Wenn kein gültiges

Accesstoken im Client vorhanden ist, dann muss sich der Client an einem IDP der TI-IDP-Föderation authentisieren.

Nur der eigene Eintrag mit einem Identifier passend zur Telematik-ID aus dem Accesstoken KANN bearbeitet werden. Für einen eigenen OrganizationDirectory-Eintrag KÖNNEN weitere HealthcareService-Einträge erstellt und mit dem eigenen OrganizationDirectory-Eintrag verlinkt werden.

Das Accesstoken enthält folgende Attribute:

```
{
  "iss": "https://vzd-fhir-directory.vzd.ti-dienste.de/owner-
authenticate",
  "sub": "<telematikID>",
  "aud": [ "https://vzd-fhir-directory.vzd.ti-dienste.de/owner", "https://fhir-
directory.vzd.ti-dienste.de/search" ],
  "iat": 1630306800,
  "exp": 1630393200
  "Scope": "search:read owner:writecertificate:read"
}
```

Das Attribut "iss" enthält die URL des Endpunktes für die Authentisierung in der jeweiligen Umgebung RU, TU oder PU.

Das Attribut "aud" enthält die URL des Endpunktes in der jeweiligen Umgebung RU, TU oder PU.

Die zeitliche Gültigkeit des Owner Accesstokens beträgt 24 Stunden.

Das Holder-Access-Token enthält folgende Attribute:

```
{
  "iss": " https://fhir-directory.vzd.ti-dienste.de/holder-
authenticate",
  "clientId": "<ClientID die im KeyCloak für den Holder vergeben wurde>",
  "aud": [ "https://vzd-fhir-directory.vzd.ti-dienste.de/owner", "https://fhir-
directory.vzd.ti-dienste.de/search" ],
  "iat": 1630306800,
  "exp": 1630393200
  "Scope": "search:read, owner:read, certificate:read"
}
```

Das Attribut "iss" enthält die URL des Endpunktes für die Authentisierung in der jeweiligen Umgebung RU, TU oder PU.

Das Attribut "aud" enthält die URL des Endpunktes in der jeweiligen Umgebung RU, TU oder PU.

Die zeitliche Gültigkeit des Holder-Access-Tokens beträgt 24 Stunden.

Das Attribut "Scope" enthält die Rechte, zukünftig auch owner:write.

Endpunkte für die Authentisierung

In der Produktionsumgebung (PU) ist die URL:

<https://fhir-directory.vzd.ti-dienste.de/owner-authenticate>

In der Referenzumgebung (RU) ist die URL: <https://vzd-fhir-directory-ref.vzd.ti-dienste.de/owner-authenticate>

In der Testumgebung (TU) ist die URL: <https://fhir-directory-tu.vzd.ti-dienste.de/owner-authenticate>

FHIR VZD Endpunkte für die Authentisierung mit dem SmartcardIDP

In der Produktionsumgebung (PU) ist die URL: <https://fhir-directory.vzd.ti-dienste.de/signin-gematik-idp-dienst>

In der Referenzumgebung (RU) ist die URL: <https://vzd-fhir-directory-ref.vzd.ti-dienste.de/signin-gematik-idp-dienst>

In der Testumgebung (TU) ist die URL: <https://fhir-directory-tu.vzd.ti-dienste.de/signin-gematik-idp-dienst>

FHIR-VZD-Endpunkte für die Authentisierung mit dem gematik Authenticator und Polling Endpunkt

In der Produktionsumgebung (PU) sind die URLs:

- <https://fhir-directory.vzd.ti-dienste.de/owner-authenticate-decoupled>
- <https://fhir-directory.vzd.ti-dienste.de/owner-authenticate-poll>
- <https://fhir-directory.vzd.ti-dienste.de/signin-gematik-idp-dienst-decoupled>

In der Referenzumgebung (RU) sind die URLs:

- <https://vzd-fhir-directory-ref.vzd.ti-dienste.de/owner-authenticate-decoupled>
- <https://vzd-fhir-directory-ref.vzd.ti-dienste.de/owner-authenticate-poll>
- <https://vzd-fhir-directory-ref.vzd.ti-dienste.de/signin-gematik-idp-dienst-decoupled>

In der Testumgebung (TU) sind die URLs:

- <https://fhir-directory-tu.vzd.ti-dienste.de/owner-authenticate-decoupled>
- <https://fhir-directory-tu.vzd.ti-dienste.de/owner-authenticate-poll>
- <https://fhir-directory-tu.vzd.ti-dienste.de/signin-gematik-idp-dienst-decoupled>

FHIR-VZD-Endpunkte für die Holder Authentisierung

- In der Produktionsumgebung (PU) ist die URL: <https://fhir-directory.vzd.ti-dienste.de/holder-authenticate>
- In der Referenzumgebung (RU) ist die URL: <https://vzd-fhir-directory-ref.vzd.ti-dienste.de/holder-authenticate>
- In der Testumgebung (TU) ist die URL: <https://fhir-directory-tu.vzd.ti-dienste.de/holder-authenticate>

...

Es wird Kapitel "4.2.1.4 Schnittstelle FHIRDirectoryTIMProviderAPI (I_VZD_TIM_Provider_Services.yaml)" wie folgt angepasst

Endpunkte

In der Produktionsumgebung (PU) ist die URL: <https://fhir-directory.vzd.ti-dienste.de/ti-provider-services>

In der Referenzumgebung (RU) ist die URL: <https://fhir-directory-ref.vzd.ti-dienste.de/ti-provider-services>

In der Testumgebung (TU) ist die URL: <https://fhir-directory-tu.vzd.ti-dienste.de/ti-provider-services>

Authentisierung

Um die Schnittstelle nutzen zu können, muss sich der Registrierungsdienst des TI-Messenger-Anbieters zuerst mit einem ti-provider-accesstoken authentisieren, das vom TI-Provider OAuth-Server des VZD-Anbieters ausgestellt wurde. Das ti-provider-accesstoken hat eine Gültigkeitsdauer von 5 Minuten. Dieses tauscht er bei dem VZD-FHIR-Directory Auth-Service gegen ein provider-accesstoken, das zur Authentifizierung an der Schnittstelle genutzt wird.

Das provider-accesstoken enthält folgende Attribute:

```
{
  "iss": "https://fhir-directory.vzd.ti-dienste.de/ti-provider-
authenticate",
  "sub": "<client_id>",
  "aud": [ "https://fhir-directory.vzd.ti-dienste.de/ti-provider-
services"],
  "iat": 1630306800,
  "exp": 1630308600,
  "clientId": "<client_id>"
}
```

Das Attribut "iss" enthält die URL des Endpunktes für die Authentisierung in der jeweiligen Umgebung RU, TU oder PU.

Das Attribut "aud" enthält die URL des Endpunktes in der jeweiligen Umgebung RU, TU oder PU.

Die zeitliche Gültigkeit des provider-accesstokens beträgt 24 Stunden.

Endpunkte für die Authentisierung am VZD-FHIR-Directory Auth-Service

In der Produktionsumgebung (PU) ist die URL: <https://fhir-directory.vzd.ti-dienste.de/ti-provider-authenticate>

In der Referenzumgebung (RU) ist die URL: <https://fhir-directory-ref.vzd.ti-dienste.de/ti-provider-authenticate>

In der Testumgebung (TU) ist die URL: <https://fhir-directory-tu.vzd.ti-dienste.de/ti-provider-authenticate>

Endpunkte um mit Client Credentials ein Token zu erhalten, das am Endpunkt ti-provider-authenticate eingetauscht werden kann

In der Referenzumgebung (RU) ist die URL: <https://auth-ref.vzd.ti-dienste.de:9443/auth/realms/TI-Provider/protocol/openid-connect/token>

In der Testumgebung (TU) ist die URL: <https://auth-test.vzd.ti-dienste.de:9443/auth/realms/TI-Provider/protocol/openid-connect/token>

In der Produktionsumgebung (PU) ist die URL: <https://auth.vzd.ti-dienste.de:9443/auth/realms/TI-Provider/protocol/openid-connect/token>

Es wird Kapitel "4.2.1.5 FHIR Schnittstelle für Versicherte FHIRDirectoryFdvSearchAPI" wie folgt angepasst

Endpunkte für die Suche von Einträgen im VZD-FHIR-Directory durch Versicherte

In der Produktionsumgebung (PU) ist die URL:

<https://fhir-directory.vzd.ti-dienste.de/fdv/search>

In der Referenzumgebung (RU) ist die URL:

<https://fhir-directory-ref.vzd.ti-dienste.de/fdv/search>

In der Testumgebung (TU) ist die

URL: <https://fhir-directory-tu.vzd.ti-dienste.de/fdv/search>

Authentisierung

Um die Schnittstelle nutzen zu können, MÜSSEN sich die Clients mit einem gültigen search-access_token authentisieren, das vom FHIR-Directory Auth-Service ausgestellt wurde. Das search-access_token erhalten Fachdienste nach Authentisierung am FHIR-OAuth-Server /token Endpunkt im Austausch gegen das service-authz-token und TIM-Clients von Versicherten nach Authentisierung am Matrix-Homeserver im Austausch gegen das Matrix-OpenID-Token.

Das search-access_token (Fachdienste) enthält folgende Attribute:

```
{
  "scope": "fdv_search:read certificate:read",
  "iss": "https://fhir-directory.vzd.ti-dienste.de/service-authenticate",
  "aud": "https://fhir-directory.vzd.ti-dienste.de/fdv/search",
  "iat": 1726556719,
  "exp": 1726643119
}
```

Das search-access_token (TIM-Clients von Versicherten) enthält folgende Attribute:

```
{
  "iss": "https://fhir-directory.vzd.ti-dienste.de/tim-authenticate",
  "aud": [ "https://fhir-directory.vzd.ti-dienste.de/fdv/search" ],
  "iat": 1630306800,
  "exp": 1630393200,
  "scope": "fdv_search:read certificate:read"
}
```

Das Attribut "iss" enthält die URL des Endpunktes für die Authentisierung in der jeweiligen Umgebung RU, TU oder PU.

Das Attribut "aud" enthält die URL des Endpunktes in der jeweiligen Umgebung RU, TU oder PU.

Die zeitliche Gültigkeit des search-access_tokens beträgt 24 Stunden.

Endpunkte um mit Client Credentials ein Token zu erhalten, das am Endpunkt service-authenticate eingetauscht werden kann

In der Referenzumgebung (RU) ist die URL: <https://auth-ref.vzd.ti-dienste.de:9443/auth/realms/Service-Authenticate/protocol/openid-connect/token>

In der Testumgebung (TU) ist die URL: <https://auth-test.vzd.ti-dienste.de:9443/auth/realms/Service-Authenticate/protocol/openid-connect/token>

In der Produktionsumgebung (PU) ist die URL:
<https://auth.vzd.ti-dienste.de:9443/auth/realms/Service-Authenticate/protocol/openid-connect/token>

Endpunkte für die Authentisierung (Fachdienste)

In der Produktionsumgebung (PU) ist die URL:
<https://fhir-directory.vzd.ti-dienste.de/service-authenticate>

In der Referenzumgebung (RU) ist die URL:
<https://fhir-directory-ref.vzd.ti-dienste.de/service-authenticate>

In der Testumgebung (TU) ist die URL: <https://fhir-directory-tu.vzd.ti-dienste.de/service-authenticate>

Endpunkte für die Authentisierung (TIM-Clients von Versicherten)

In der Produktionsumgebung (PU) ist die URL: <https://fhir-directory.vzd.ti-dienste.de/tim-authenticate>

In der Referenzumgebung (RU) ist die URL: <https://fhir-directory-ref.vzd.ti-dienste.de/tim-authenticate>

In der Testumgebung (TU) ist die URL: <https://fhir-directory-tu.vzd.ti-dienste.de/tim-authenticate>

Operationen

Die FHIR-Operationen für die Suche nach Einträgen im VZD-FHIR-Directory sind in der HL7-FHIR-Spezifikation (<https://www.hl7.org/fhir/http.html>) festgelegt.

Zusätzlich zur HL7-FHIR-Spezifikation muss der FHIR VZD folgende Suchparameter unterstützen:

- practitioner.qualification
- location.endpoint.address (z.B. Suche nach TI-Messenger Adresse)

Falls der Versicherte im Rahmen einer Anwendung nur eine Teilmenge aus dem VZD-FHIR-Directory sehen soll (z.B. nur Apotheken oder nur bestimmte Organisationen), muss das durch den Client durch eine geeignete Suche sichergestellt werden.

Sichtbarkeit von FHIR-Ressourcen

Die Sichtbarkeit von definierten FHIR-Ressourcen kann vom Eigentümer (Owner) des FHIR-VZD-Eintrags eingeschränkt werden. Folgende Einschränkungen der Sichtbarkeit sind möglich:

- Die gesamte Organisation (FHIR Ressource "Organization" über Organization.extension:organizationVisibility == hide-erezeptApp)
- Kommunikations-Endpunkte (FHIR Ressource "Endpoint" über Endpoint.extension:endpointVisibility == hide-versicherte)

FHIR-Ressourcen mit eingeschränkter Sichtbarkeit werden an Schnittstelle FHIRDirectoryFdvSearchAPI (/fdv/search) durch den FHIR VZD aus dem Suchergebnis entfernt. Bei der FHIR-Ressource "Organization" werden auch alle verlinkten FHIR-Ressourcen aus dem Suchergebnis entfernt.

Die Sichtbarkeit seiner FHIR-Ressourcen kann der Eigentümer (Owner) über die Schnittstelle für Besitzer FHIRDirectoryOwnerAPI (/owner) verwalten.

Es wird Kapitel 4.2.1 neu aufgenommen

4.2.1.6 Schnittstelle zum Lesen von Zertifikaten von Verzeichniseinträgen I_FHIR_VZD_Certificates

Endpunkte zum Lesen von Zertifikaten von Verzeichniseinträgen (read_FhirVZD_Certificates)

In der Produktionsumgebung (PU) ist die URL:

<https://fhir-directory.vzd.ti-dienste.de/certificates/Certificates>

In der Referenzumgebung (RU) ist die URL:

<https://fhir-directory-ref.vzd.ti-dienste.de/certificates/Certificates>

In der Testumgebung (TU) ist die URL:

<https://fhir-directory-tu.vzd.ti-dienste.de/certificates/Certificates>

Abfrageschnittstelle Zertifikat-Version (getInfo)

In der Produktionsumgebung (PU) ist die URL:

<https://fhir-directory.vzd.ti-dienste.de/certificates/>

In der Referenzumgebung (RU) ist die URL:

<https://fhir-directory-ref.vzd.ti-dienste.de/certificates/>

In der Testumgebung (TU) ist die URL:

<https://fhir-directory-tu.vzd.ti-dienste.de/certificates/>

Authentisierung

Um die Schnittstelle nutzen zu können, MÜSSEN sich die Clients mit einem gültigen Token authentisieren, das vom FHIR-Directory Auth-Service ausgestellt wurde. Akzeptiert werden die folgenden Token:

- search-access_token von der FHIRDirectorySearchAPI Schnittstelle (/search)
- search-access_token von der FHIRDirectoryFdvSearchAPI Schnittstelle (/fdv/search)
- Accesstoken von der FHIRDirectoryOwnerAPI Schnittstelle (/owner)

Operationen

Die Schnittstelle ist in I_FHIR_VZD_Certificates.yaml als OpenAPI RESTful Service spezifiziert.

https://github.com/gematik/api-vzd/blob/main/src/openapi/I_FHIR_VZD_Certificates.yaml

Tabelle 1: Tab_I_FHIR_VZD_Certificates_Operations

Operation	Beschreibung
GET / "getInfo"	Mit dieser Operation können Metadaten (insbesondere auch die Version und das verwendete yaml-File) dieser Schnittstelle abgefragt werden.
GET /Certificates	Mit dieser Operation werden die Zertifikate vom FHIR VZD

"read_FhirVZD_Certificates"	abgefragt.
"	

Akzeptanzkriterien

ML-161973 - VZD-FHIR-Directory - I_FHIR_VZD_Certificates Authentisierung

Der FHIR VZD muss bei der Authentisierung für Schnittstelle I_FHIR_VZD_Certificates das übergebene Token auf Gültigkeit und den enthaltenen Scope "certificate:read" prüfen. [≤]

ML-161974 - VZD-FHIR-Directory - I_FHIR_VZD_Certificates leeres

Abfrageergebnis

Wenn für die Abfrage von Zertifikaten über Schnittstelle I_FHIR_VZD_Certificates keine Treffer gefunden werden, muss der FHIR VZD ein leeres Ergebnis liefern. [≤]

ML-161981 - VZD-FHIR-Directory - I_FHIR_VZD_Certificates Performance

Der FHIR VZD muss die Abfrage von Zertifikaten über Schnittstelle I_FHIR_VZD_Certificates performant bereitstellen (z.B. über eine performance-optimierte Datenbank). [≤]

Es wird Kapitel 4.2.3 angepasst

...

Die Föderationsliste hat folgende Struktur:

```
{
  "version": <Version der Föderationsliste (Integer)>,
  "domainList": [
    {
      "domain": "Domain",
      "telematikID": "Telematik-ID der Organisation, welche die Domain nutzt",
      "isInsurance": true,
      "ik": [108433248, 104127692],
      "timProvider" "timAnbieter": "Zuweisungsgruppe im TI-ITSM-System vom
      TI-Messenger Anbieter,
      der die Domain angelegt hat",
      "redirectDomains": [ domain1.fr, domain7.de ] "Zu berücksichtigende
      redirect-Domains,
      proxy-Server"
    }
  ]
}
```

Zu Domänen, die Accounts von Versicherten bereitstellen (isInsurance: true) MUSS mindestens ein Institutionskennzeichen (IK) eingetragen werden. Bei Einträgen mit dem Wert (isInsurance:false) DARF kein IK hinterlegt werden. Ein IK DARF in der gesamten Föderationsliste nur einmal enthalten sein.

Das VZD-FHIR-Directory MUSS für das Format des IK sicherstellen:

Das Institutionskennzeichen MUSS aus einer neunstelligen Ziffernfolge bestehen, deren erste 2 Stellen (Klassifikation für Krankenversicherungsträger) einem Wert aus einer konfigurierbaren Liste entsprechen muss. Initial enthält diese konfigurierbare Liste die Werte

- "10" (Krankenversicherungsträger),
- "16" (Private Krankenversicherungen) und
- "95" (Krankenversicherungsträger außerhalb der gesetzlichen Krankenversicherung).

Beim Hinterlegen von Institutionskennzeichen MÜSSEN diese - entsprechend [GR-IK-2023-11] Kapitel 1.2.5 - gegen die enthaltene Prüfziffer validiert werden und nur bei erfolgreicher Prüfung der Eintrag erstellt werden.

Der Wert für "timAnbieter" MUSS vom AZPD bei der Beantragung der Credentials des TI-Messenger Anbieters/-Herstellers erfasst und bei jeder Änderung der anderen Felder vom VZD-FHIR-Directory aktualisiert werden. Der Wert für "timAnbieter" DARF AUSSCHLIEßLICH durch den AZPD bzw. durch das VZD-FHIR-Directory geändert werden. Mit dieser Automatisierung sollen manuelle Fehler beim Setzen durch die Nutzer vermieden werden.

Die redirectDomains werden mit dem Förderungseintrag persistiert und vom Proxy freigeschaltet.

Ohne entsprechende Pflege von RedirectDomains ist der Aufruf entsprechender URLs bei der Matrix-Server-Discovery (z.B. bei einem Redirect) nicht möglich.

...

Es wird Kapitel 4.3 neu aufgenommen

4.3.3 FHIR Suchoptionen

Die Suche im FHIR VZD basiert auf den Standard-FHIR-Suchmöglichkeiten <https://build.fhir.org/search.html>.

In diesem Kapitel werden Suchoptionen mit besonderer Bedeutung für TI-Anwendungen beschrieben.

4.3.3.1 FHIR Umkreissuche

Der FHIR VZD muss die Umkreissuche um eine bestimmte Geoposition unterstützen. Dafür muss die FHIR-Suche über den "near" Parameter für Location Ressourcen erlaubt werden <https://www.hl7.org/fhir/location.html#8.7.6.1.1>, <https://build.fhir.org/location.html#search>

Der Client muss bei der Umkreissuche alle "near" Suchparameter obligatorisch angeben ([latitude][longitude][distance][units]).

Es wird Kapitel 5.1 wie folgt angepasst

AF_10036-02 - Nutzer sucht Einträge im FHIR-Directory

Attribute	Bemerkung
Akteure	<ul style="list-style-type: none"> • Mitarbeiter im Gesundheitswesen • Versicherte

Beschreibung	<p>Nutzer können im FHIR-Directory nach über die Einstiegspunkte HealthcareServiceDirectory-, und PractitionerRoleDirectory- und EndpointDirectory-Einträgen nach allen FHIR VZD Ressourcen suchen.</p> <p>Für die Suche von TI-Messenger Nutzern im FHIR-Directory ist eine Authentisierung am FHIR-Directory Auth-Service erforderlich. Hier ist die Authentisierung mit TI-Messenger-Clients beschrieben.</p> <ol style="list-style-type: none"> 1. Der TIM-Client des Nutzers prüft, ob er ein gültiges search-access_token vom FHIR VZD Auth-Service vorliegen hat. [1] 2. Wenn dem TIM-Client kein gültiges search-access_token vorliegt, fragt er bei seinem Matrix-Homeserver ein Matrix-OpenID-Token ab. [2-4] 3. Abruf search-access_token [5-13] <ul style="list-style-type: none"> Der TIM-Client tauscht das Matrix-OpenID-Token gegen ein search-access_token ein. Der FHIR-Directory Auth-Service a. prüft ob das Matrix-OpenID-Token von einem Matrix-Homeserver aus der TI-Föderation stammt [6] b. ermittelt den Port unter dem der Userinfo Endpunkt des Matrix-Homeservers zu erreichen ist [7] c. validiert die Gültigkeit des Matrix-OpenID-Token mit Hilfe des Matrix-Homeserver [8-9] d. ermittelt den handelnden Akteuer anhand des Status von isInsurance in der Föderationsliste für den Matrix-Homeserver[10] <ol style="list-style-type: none"> i. bei isInsurance=false(Mitarbeiter im Gesundheitswesen) wird ein search-access_token mit aud:https://fhir-directory.vzd.ti-dienste.de/search erzeugt [11] ii. bei isInsurance=true(Versicherter) wird ein search-access_token mit aud:https://fhir-directory.vzd.ti-dienste.de/fdv/search erzeugt [12] e. übermittelt das search-access_token an den Client [13]
Vorbedingung	Der Nutzer ist an seinem Homeserver registriert.
Nachbedingung	Der TI-Messenger-Client hat alle gefundenen Einträge empfangen.

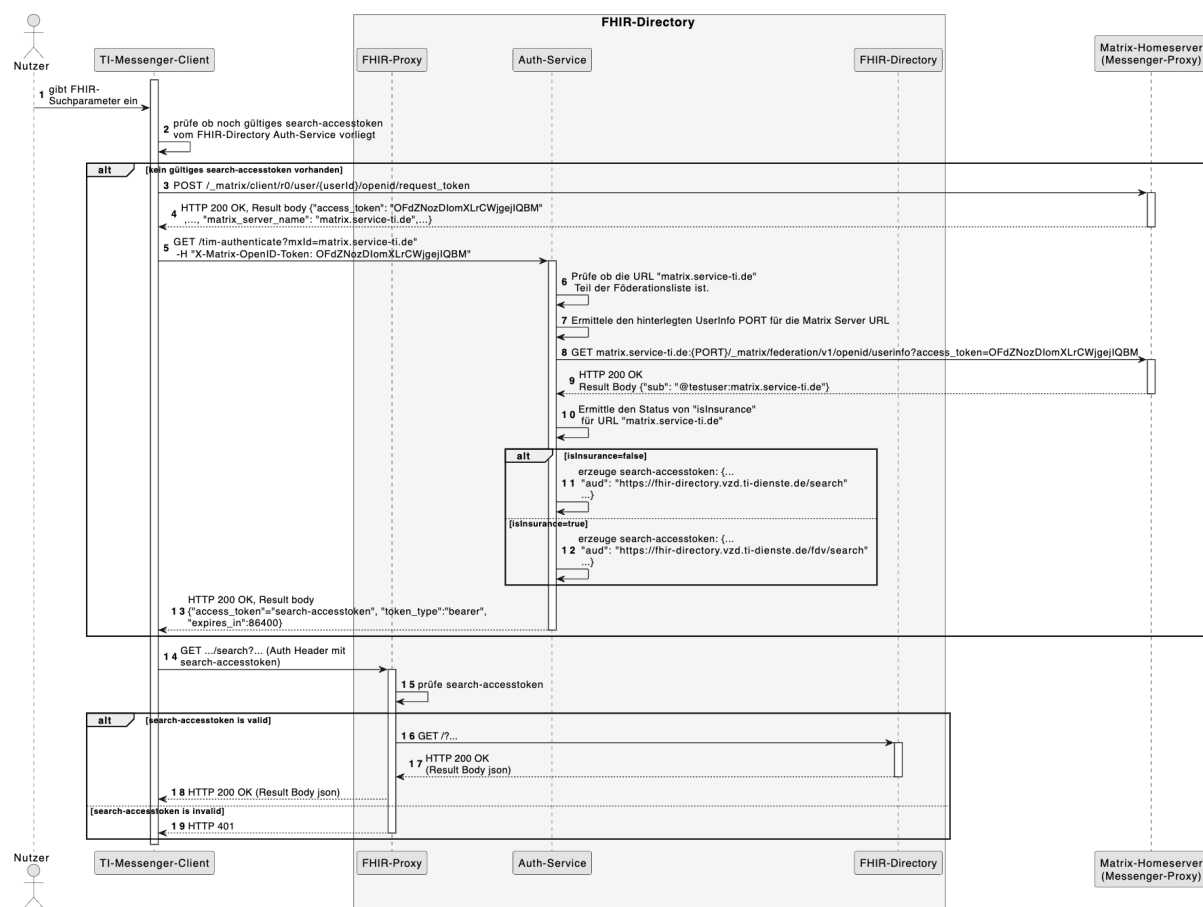


Abbildung 1: Sequence diagram /search

[<=, TI-M_Client_Basis, VZD_FHIR, TIM_FD, TI-M_FD_Basis, TIM_Client, funkt. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA]

Akzeptanzkriterien für den Anwendungsfall AF_10036 Nutzer sucht OrganizationDirectory- und PractitionerDirectory-Einträge im VZD-FHIR-Directory

ML-123485 - Authentifizierung am Endpunkt /search (VZD-FHIR-Directory, Sicherheitsgutachten)

Am Endpunkt /search des FHIR-Proxy darf die Authentifizierung nur für Requests erfolgreich sein, die ein gültiges search-access_token im Authentication Header enthalten, das vom Auth-Service ausgestellt wurde. Das search-access_token MUSS im aud Feld den Servernamen des VZD-FHIR-Directory und den Endpunkt /search enthalten. [<=]

ML-148295 - Authentifizierung am Endpunkt /fdv/search (VZD-FHIR-Directory, Sicherheitsgutachten)

Am Endpunkt /fdv/search des FHIR-Proxy darf die Authentifizierung nur für Requests erfolgreich sein, die ein gültiges search-access_token im Authentication Header enthalten, das vom Auth-Service ausgestellt wurde. Das search-access_token MUSS im aud Feld den Servernamen des VZD-FHIR-Directory und den Endpunkt /fdv/search enthalten. [<=]

Es wird Kapitel 5.2 wie folgt angepasst

AF_10037-03 - Einträge im VZD-FHIR-Directory ändern und suchen

Attribute	Bemerkung
Beschreibung	<p>Über die Authentisierung mit HBA/SMC-B erfolgt ist die Authentisierung für die VZD-FHIR-Directory Schnittstellen /owner und /search möglich.</p> <p>Ob man sich für die /owner, /search oder beide Schnittstellen authentisieren will, gibt man im Scope des GET /owner-authenticate an:</p> <ul style="list-style-type: none"> GET /owner-authenticate... ((Auth Header mit RegService OpenID-Token)) Authentisierung für die Änderung eigener Daten im VZD-FHIR-Directory GET /owner-authenticate?Scope=search:read%20owner:write Authentisierung für die die Suche über die /search Schnittstelle und für die Änderung eigener Daten im VZD-FHIR-Directory über die /owner Schnittstelle. GET /owner-authenticate?Scope=search:read Authentisierung für die die Suche über die /search Schnittstelle im VZD-FHIR-Directory. GET /owner-authenticate?Scope=owner:write Authentisierung für die die Änderung eigener Daten im VZD-FHIR-Directory. GET /owner-authenticate Kompatibel für TIM 1.0 ohne Scope Parameter: Authentisierung für die die Änderung eigener Daten im VZD-FHIR-Directory. <p>Änderung von eigenen Daten im VZD-FHIR-Directory Organisationen können ihren Eintrag im VZD-FHIR-Directory an die eigenen Strukturen anpassen. Leistungserbringer können z. B. die TI-Messenger-Adresse in ihrem Eintrag hinzufügen. Der Basiseintrag einer Organisation oder eines Leistungserbringers wird wie bisher durch die Kartenherausgeber erstellt. Die Organisation KANN eigene mit dem Basiseintrag verlinkte FHIR-Ressourcen erstellen, um die Struktur der Organisation abzubilden. Zum Beispiel können Krankenhäuser ihre Fachabteilungen als HealthcareService-Einträge abbilden, die mit dem Organization-Eintrag verlinkt sind. Wenn der Org-Admin oder LE kein gültiges owner-access_token vom VZD-FHIR-Directory im Client vorliegt, muss die Authentisierung mittels OIDC an einem IDP der TI-IDP-Föderation erfolgen. Nach erfolgreicher Authentisierung ist die durch den IDP bestätigte Telematik-ID des Leistungserbringers oder der Organisation am Auth-Service bekannt. Für den Aufruf der FHIR-Operationen durch den Client stellt der Auth-Service dem Client ein owner-access_token aus, dass auch die Telematik-ID des LE oder der Organisation enthält.</p> <p>Suche von Daten im VZD-FHIR-Directory Mit gleicher Authentisierung kann auch ein Token für die Suche im</p>

	<p>VZD-FHIR-Directory über die /search Schnittstelle erzeugt werden. Das erzeugte Token kann auch für die Suche im VZD-FHIR-Directory über die /search Schnittstelle genutzt werden.</p> <ul style="list-style-type: none"> Für die Suche im Zusammenhang von Datenänderungen im VZD-FHIR-Directory kann die Suche in der /owner Schnittstelle genutzt werden. Für die normale Suche MUSS der Client die VZD-FHIR-Directory Suche über die /search Schnittstelle nutzen (die /search Schnittstelle kann entsprechend der Last skaliert werden). <p>Der Auth-Service vom VZD-FHIR-Directory erzeugt das Token entsprechend den angefragten Scopes [20].</p>
Vorbedingung	<p>Die Organisation oder der Leistungserbringer hat bereits einen Basiseintrag im VZD-FHIR-Directory.</p> <p>Eine Authenticator-App des IDP steht zur Verfügung, mit der die Organisations-Identität oder die Leistungserbringer-Identität bei einem IDP der TI-IDP-Föderation bestätigt werden kann.</p>

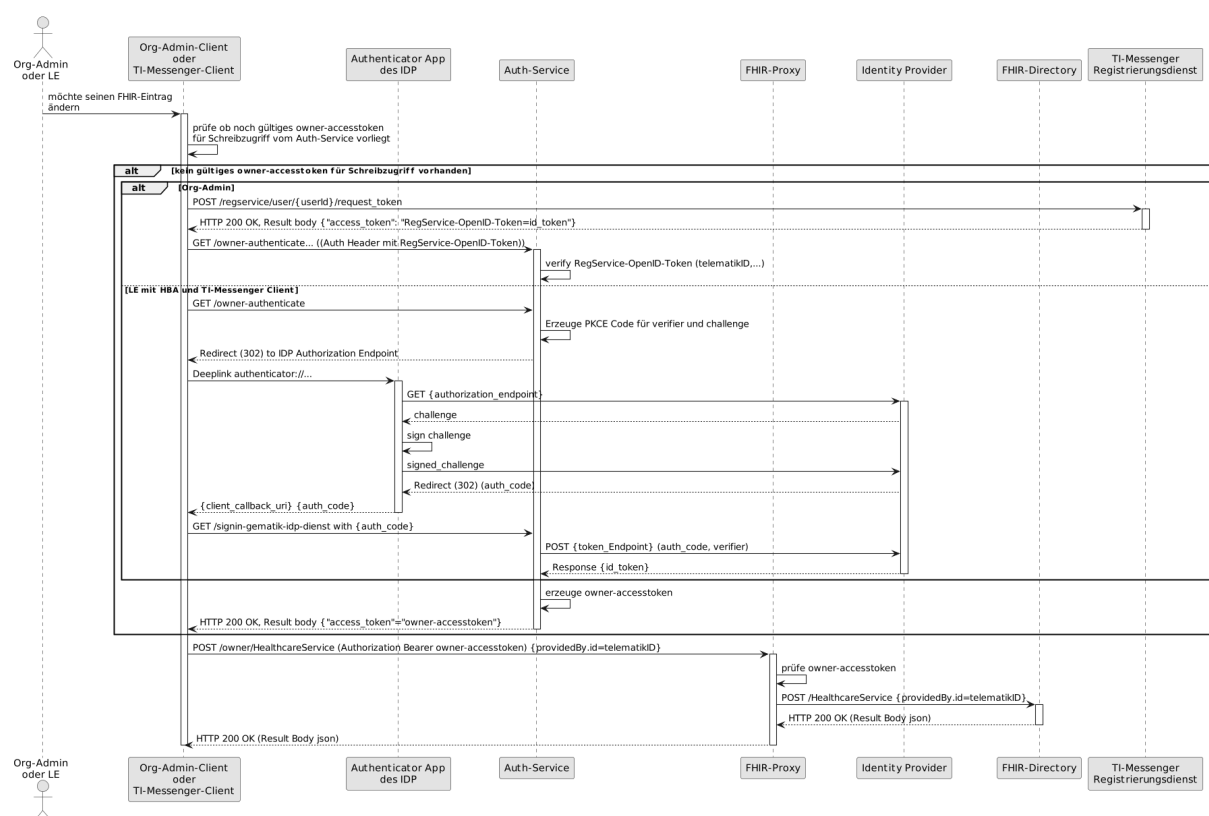


Abbildung 2: Sequenzdiagramm VZD-FHIR-Directory Änderung von eigenen OrganizationDirectory- oder PractitionerDirectory-Einträgen

[<=, VZD_FHIR, TIM_Client, funkt. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA]

...

ML-156761 - Selbst angelegte FHIR Ressourcen MÜSSEN mit dem eigenen Basiseintrag verlinkt sein (VZD-FHIR-Directory)

Alle selbst durch den Besitzer angelegten FHIR-Einträge Ressourcen MÜSSEN mit dem eigenen Basiseintrag (Practitioner, Organization) **providedBy** direkt oder indirekt - über **HealthcareService** bzw. **PractitionerRole** - verlinkt sein. Wenn keine korrekte Verlinkung angegeben ist, dann MUSS der FHIR-Proxy das Erzeugen oder die Änderung **des HealthcareDirectory-Eintrags der FHIR Ressource** mit der Fehlermeldung (HTTP 422 Unprocessable Entity) ablehnen.

[<=]

...

ML-165946 - 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
 - **Prüfung des Gültigkeitszeitraums des Signaturzertifikats**
- Die telematikID muss im Token Attribut idNummer enthalten sein.
- Prüfung des id_token Signatur-Zertifikats (oder sein Hash) gegen das bei der Beantragung der Credentials für die Schnittstelle I_VZD_TIM_Provider_Services übergebenen Signatur-Zertifikates.
- OCSP Prüfung des id_token Signatur-Zertifikats
- Prüfung Algorithmus: "alg": "ES256" oder "BP256R1"
- Prüfung des Signaturzertifikats gegen **das X.509-Root-CA Zertifikat der TI, die Zertifikate der TSL, die als Truststore konfiguriert sind.**
- 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 abbrechen, 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 personenbezogenes 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.

[<=]

Es wird Kapitel 5.3 wie folgt angepasst

AF_10048-02 - Anwendungsfälle der TI-Messenger-Anbieter im VZD-FHIR-Directory

Attribute	Bemerkung
Beschreibung	<p>Für den Betrieb eines TI-Messenger-Fachdienstes ist es erforderlich, alle an der Föderation beteiligten Matrix-Domänen zu kennen, um nicht an der Föderation beteiligte Matrix-Domänen ausschließen zu können. Die Domänen werden im VZD-FHIR-Directory in der Föderationsliste gespeichert. Endpoint-Einträgen gespeichert. Die Endpoint-Einträge eines TI-Messenger-Anbieters sind verlinkt mit seinem OrganizationDirectory-Eintrag. Der TI-Messenger-Anbieter verwaltet seine Einträge im VZD-FHIR-Directory selbst. Dazu beantragt der TI-Messenger-Anbieter für seinen Registrierungsdienst Client Credentials für die Nutzung der Schnittstelle I_VZD_TIM_Provider_Services. Mit den Credentials erhält der Registrierungsdienst vom VZD TI-Provider-OAuth-Server ein ti-provider-accesstoken. Dieses tauscht er bei dem VZD-FHIR-Directory Auth-Service gegen ein provider-accesstoken, das zur Authentifizierung an der Schnittstelle genutzt wird. Nach erfolgreicher Authentisierung kann der Registrierungsdienst die Operationen zur Verwaltung der Föderationsliste, FHIR-Operationen zur Verwaltung des eigenen OrganizationDirectory-Eintrags und der eigenen Endpoint-Einträge nutzen.</p> <p>Um die Gesamtheit der an der Föderation beteiligten Matrix-Domainnamen zu erhalten, wird die Operation GET /FederationList aufgerufen. Optional KANN die bereits bekannte Version im Request angegeben werden. Als Ergebnis erhält der Registrierungsdienst eine Liste der Hashes der an der Föderation beteiligten Domainnamen oder keine Liste, falls keine neuere Version existiert. Die Hashes der Domainnamen werden verwendet, um zu verhindern, dass jeder TI-Messenger-Anbieter alle Domainnamen im Klartext kennt.</p>
Vorbedingung	Der Registrierungsdienst des TI-Messenger-Anbieters ist bereits als Nutzer des VZD-FHIR-Directories registriert und hat TI-Provider OAuth Client Credentials (client_id und client_secret) für die Umgebungen RU, TU und PU erhalten.

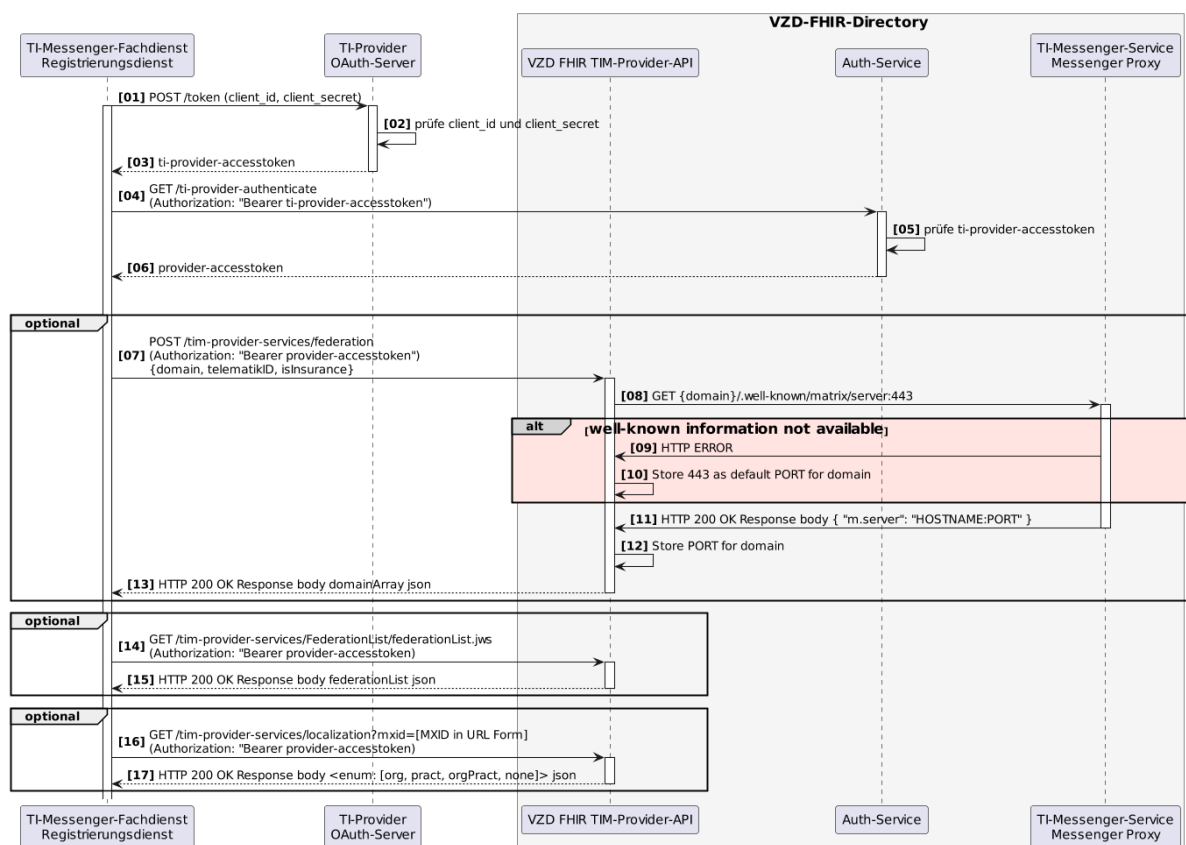


Abbildung 3: VZD-FHIR-Directory_Sequenzdiagramm_TI-Messenger-Provider-Services

[<=, VZD_FHIR, TIM_FD, TI-M_FD_Basis, funkt. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA]

5.3.1 Eintragen einer Matrix Domain - Matrix-Server Discovery

Über die Matrix-Server Discovery muss

- beim Eintragen einer Domain (POST /tim-provider-services/federation) und
- periodisch für alle vorhandenen Domains in der Föderationsliste

über die Matrix Funktion "Server Discovery" die konkrete Matrix-Chat-Server-URL inkl. verwendeten Port ermitteln und in die Föderationsliste übernehmen.

Dies ist notwendig, da der Standardport 443 nicht von allen Matrix-Servern verwendet wird, die Matrix-Chat-Server-URL von der gewünschten Domain abweichen kann und sich Konfigurationen nachträglich ändern können.

Server-URL-Syntax

<Matrix-Homeserver-URL>:443/.well-known/matrix/server

Beispiel-URL

Beispiel Ergebnis

Bei dem Aufruf des WellKnown-Dokuments (Server Discovery) muss es möglich sein, Redirect-URLs zu folgen. Damit diese Redirect-URLs nicht durch die Firewall blockiert werden, können in Schnittstelle I_VZD_TIM_Provider_Services über die "domainAdministration" Operationen (addTiMessengerDomain, updateTiMessengerDomain) mit dem optionalen Attribut "redirectDomains" Redirect-URLs übergeben werden. Diese werden persistiert und in der Firewall freigeschaltet.

Die persistierten redirectDomains müssen im Ergebnis der Operation getTiMessengerDomain enthalten sein, dürfen aber nicht in der Föderationsliste enthalten sein (Operation getFederationList).

Bei redirectDomains ist zu beachten

- Die Pflege einer Wildcard-Domäne (Beispiele *.domain.de) ist nicht zulässig und führt zu einem Fehler. "Wildcard domains are not allowed."
- Domän-Namen länger als 255 Zeichen werden mit einem Fehler abgelehnt.
- Domänen-Namen mit Präfix "http / https" werden mit einem Fehler abgelehnt.

Initiale Ermittlung des Server-Ports inkl. ServerUrl-Anpassung

1. Bei dem Hinzufügen von Einträgen (Matrix-Servern) in der Federations-Liste wird die Matrix-Chat-Server-URL mit dem Standardport 443 gesetzt.
2. Zudem muss der konkrete Port asynchron durch das von Matrix bereitgestellte Discovery-Dokument ermittelt werden.
(Für die Beschreibung Server Discovery siehe Matrix-Spezifikation [Server-Server API](#)).
 - a. Der Server Discovery Lookup erfolgt asynchron. Die Häufigkeit wird durch Konfigurationsparameter gesteuert.
 - b. Es kommt vor, dass das Discovery-Dokument zum Zeitpunkt der Ermittlung aufgrund von einer ausstehender Firewall/Squid-Freigabe nicht erreichbar ist. Eine entsprechende Warning muss im TI-Service-Provider-Log protokolliert werden.
Mit dem nächsten Lauf (je nach konfigurierter Häufigkeit) muss der nächste Versuch erfolgen.
 - c. Das Server-Discovery-Dokument muss zwingend auf dem Port **443** erreichbar sein.

Aktualisierung des Server-Ports inkl. ServerUrl-Anpassung

Regelmäßig muss für alle in der Federations-Liste enthaltenen Einträge der Server-Port ermittelt und aktualisiert werden.

Das Vorgehen muss dabei wie folgt umgesetzt werden.

1. Der Server Discovery Lookup erfolgt asynchron. Die Häufigkeit wird durch Konfigurationsparameter gesteuert.
2. Es kommt vor, dass das Discovery-Dokument zum Zeitpunkt der Ermittlung aufgrund von einer ausstehender Firewall/Squid-Freigabe nicht erreichbar ist.

Eine entsprechende Warning muss im TI-Service-Provider-Log protokolliert werden. Mit dem nächsten Lauf (je nach konfigurierter Häufigkeit) muss der nächste Versuch erfolgen.

3. Das Server Discovery Dokument muss zwingend auf dem Port **443** erreichbar sein.

Es wird Kapitel 5.5 wie folgt angepasst

AF_10219-01 - Versicherter sucht Einträge im FHIR-Directory

Attribute	Bemerkung
Beschreibung	<p>Für die Suche von Versicherten im FHIR-Directory nach Organisationen (HealthcareServiceDirectory-Einträgen), Practitioner'n (PractitionerRoleDirectory-Einträgen) und Endpoints (EndpointDirectory-Einträgen) eine Authentisierung der Fachanwendung am Auth-Service patient-authenticate Endpunkt erforderlich. Der Ablauf entsprechend Abbildung "Sequence diagram /fdv/search":</p> <ol style="list-style-type: none"> 1. Der Client prüft, ob er ein gültiges search-access_token vom FHIR VZD Auth-Service vorliegen hat. [1] 2. Client Anfrage von search-access_token [2] Wenn im Client kein gültiges search-access_token vom FHIR VZD Auth-Service vorhanden ist, stellt der Client eine Anfrage an den Fachdienst (siehe I_FHIR_VZD_token_FD.yaml). Vor dieser Anfrage muss sich der Client des Versicherten gegenüber dem Fachdienst authentisiert haben. 3. Der Fachdienst benötigt zur Authentisierung gegenüber dem OAuth-Server Client Credentials. Diese erhält er in einem Registrierungsprozess vom Betreiber FHIR-Directory und kann sie z.B. in einem Konfigurationsfile auf dem Fachdienst ablegen. [3] 4. Authentisierung des Fachdiensts mit Client Credentials [4-6] Der Fachdienst authentisiert sich mit seinen Client Credentials und erhält nach erfolgreicher Prüfung ein service-authz-token. 5. Abruf search-access_token [7-10] Der Fachdienst tauscht das service-authz-token gegen ein search-access_token ein. 6. Cachen vom search-access_token [11] Optional kann der Fachdienst das search-access_token cachen und für Anfragen mehrerer Clients nutzen, solange die zeitliche Gültigkeit von dem search-access_token ausreicht. 7. Rückgabe von dem search-access_token an den Client [12] 8. Suche im FHIR-Directory [13-17] Mit dem search-access_token kann der Client im FHIR-Directory suchen und erhält eine Antwort mit dem Suchergebnis. Wenn das search-access_token ungültig ist (z.B. zeitlich abgelaufen), erhält er als Antwort den HTTP Status Code 401. <p>Bei der Suche über Endpunkt HealthcareServices werden Ressourcen (HealthcareService, referenzierte Organization, referenzierte Location, ggf. referenzierte Endpoints) vom FHIR VZD aus dem Ergebnis entfernt sobald die referenzierte Organization das Flag (Extension)</p>

	<p>Organization.organizationVisibility = "hide-erezeptApp" gesetzt hat.</p> <p>Bei allen Suchen über /fdv/search werden vom FHIR VZD aus dem Ergebnis die Endpoints entfernt, deren Attribut (Extension) Endpoint.extension:endpointVisibility = "hide-versicherte" gesetzt hat.</p>
Vorbedingung	<p>Der Versicherte ist bei seiner Kasse registriert.</p> <p>Der Client des Versicherten hat sich gegenüber dem Fachdienst authentisiert.</p> <p>Der Fachdienst des Versicherten hat sich bei FHIR VZD Anbieter für Schnittstelle /fdv/search registriert und Client Credentials vorliegen.</p>
Nachbedingung	Der Client hat alle gefundenen Einträge empfangen.

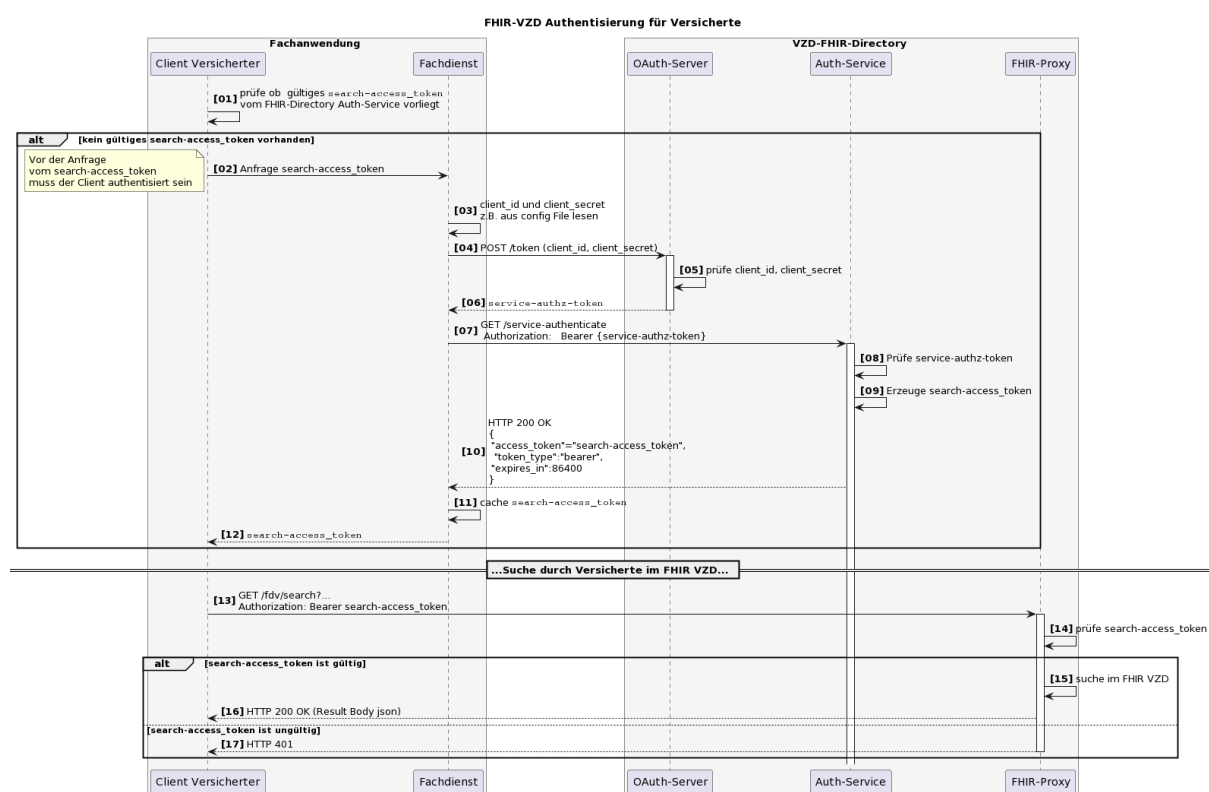


Abbildung 4: Sequence diagram /fdv/search

[<=, Aktensystem_ePA, VZD_FHIR, Frontend_Vers_ePA, funkt. Eignung: Herstellererklärung]

Hinweis für Hersteller und Anbieter von Clients für Versicherte: Die Client Secrets zur Authentifizierung am OAuth-Server dürfen nur auf einem zentralen Fachdienst/Server verwendet und sicher abgelegt werden, nicht im Client des Versicherten.

Es wird Kapitel 5.9 wie folgt eingefügt

5.9 Leistungserbringer/Organisation sucht im FHIR-Directory

AF_10374 - Leistungserbringer/Organisation sucht im FHIR-Directory

Attribute	Bemerkung
Beschreibung	<p>Über die Authentisierung mit HBA/SMC-B ist die Authentisierung für die VZD-FHIR-Directory Schnittstelle /search möglich. Diese Authentisierung entspricht Anwendungsfall AF_10037.</p> <p>Suche von Daten im VZD-FHIR-Directory Mit erfolgter Authentisierung kann das Token für die Suche im VZD-FHIR-Directory über die /search Schnittstelle genutzt werden. Für die Suche MUSS der Client die VZD-FHIR-Directory Suche über die /search Schnittstelle nutzen (die /search Schnittstelle kann entsprechend der Last skaliert werden).</p>
Vorbedingung	<p>Die Organisation oder der Leistungserbringer hat bereits einen Basiseintrag im VZD-FHIR-Directory. Eine Authenticator-App des IDP steht zur Verfügung, mit der die Organisations-Identität oder die Leistungserbringer-Identität bei einem IDP der TI-IDP-Föderation bestätigt werden kann.</p>
Ablauf	Siehe Anwendungsfall AF_10037. Die Suche MUSS über die VZD-FHIR-Directory /search Schnittstelle erfolgen.

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

Es wird Kapitel 5.10 wie folgt eingefügt

5.10 Holder sucht im FHIR-Directory

AF_10375 - Holder sucht im FHIR VZD

Attribute	Bemerkung
Beschreibung	<p>Die Kartenherausgeber der TI benötigen Zugriff auf die FHIR VZD Daten. Dafür wird ein zweischrittiges Auth-Verfahren vom FHIR VZD angeboten. Im ersten Schritt erfolgt der Token-Austausch via Client-Secret. Anschließend wird dieser Token an der TI-Provider-Authenticate-Schnittstelle gegen den Access-Token ausgetauscht.</p>
Vorbedingung	<p>Der FHIR VZD-Anbieter stellt einen Registrierungsprozess für Kartenherausgeber bereit. Ist ein Kartenherausgeber bereits für die LDAP VZD Schnittstelle Directory_Administration registriert, ist keine erneute Registrierung nötig. Während der Registrierung muss die Berechtigung des Antragstellers (Clients) durch den FHIR VZD-Anbieter geprüft und durch die gematik bestätigt werden. Nach erfolgreicher Registrierung MÜSSEN dem Antragsteller alle nötigen Daten - inklusive OAuth Client Credentials, CA-Zertifikat (welches zur Prüfung des Serverzertifikats durch den Client benötigt wird) zur Nutzung der Schnittstelle bereitgestellt werden.</p>

Nachbedingung	Der Kartenherausgeber/Holder kann sich authentisieren und hat Lesezugriff über die FHIR VZD /search Schnittstelle.
Ablauf	Die Authentisierung für Kartenherausgeber/Holder entspricht der Authentisierung von TI-Messenger-Anbietern im Anwendungsfall AF_10048.

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

Es wird Kapitel 5.11 wie folgt eingefügt

5.11 Fachdienst sucht Einträge im FHIR-Directory

AF_10403 - Fachdienst sucht Einträge im FHIR-Directory

Attribute	Bemerkung
Beschreibung	<p>Für die Suche von Fachdiensten am FHIR-Directory nach Organisationen (HealthcareServiceDirectory-Einträgen) ist eine Authentisierung des Fachdienstes am Auth-Service Endpunkt erforderlich. Der Ablauf entsprechend Abbildung "Sequence diagram /search":</p> <ol style="list-style-type: none"> 1. Der Fachdienst prüft, ob er ein gültiges search-access_token vom FHIR VZD Auth-Service vorliegen hat. [1] 2. Der Fachdienst benötigt zur Authentisierung gegenüber dem OAuth-Server Client Credentials. Diese erhält er in einem Registrierungsprozess vom Betreiber FHIR-Directory und kann sie z.B. in einem Konfigurationsfile auf dem Fachdienst ablegen. [2] 3. Authentisierung des Fachdienstes mit Client Credentials [3-5] Der Fachdienst authentisiert sich mit seinen Client Credentials und erhält nach erfolgreicher Prüfung ein service-authz-token. 4. Abruf search-access_token [6-9] Der Fachdienst tauscht das service-authz-token gegen ein search-access_token ein. 5. Cachen vom search-access_token [10] Optional kann der Fachdienst das search-access_token cachen solange die zeitliche Gültigkeit von dem search-access_token ausreicht. 6. Suche im FHIR-Directory [11-13] Mit dem search-access_token kann der Fachdienst im FHIR-Directory suchen und erhält eine Antwort mit dem Suchergebnis. Wenn das search-access_token ungültig ist (z.B. zeitlich abgelaufen), erhält er als Antwort den HTTP Status Code 401.
Vorbedingung	Der Fachdienst hat sich bei FHIR VZD Anbieter für Schnittstelle /fdv/search registriert und Client Credentials vorliegen.
Nachbedingung	Der Fachdienst hat alle gefundenen Einträge empfangen.

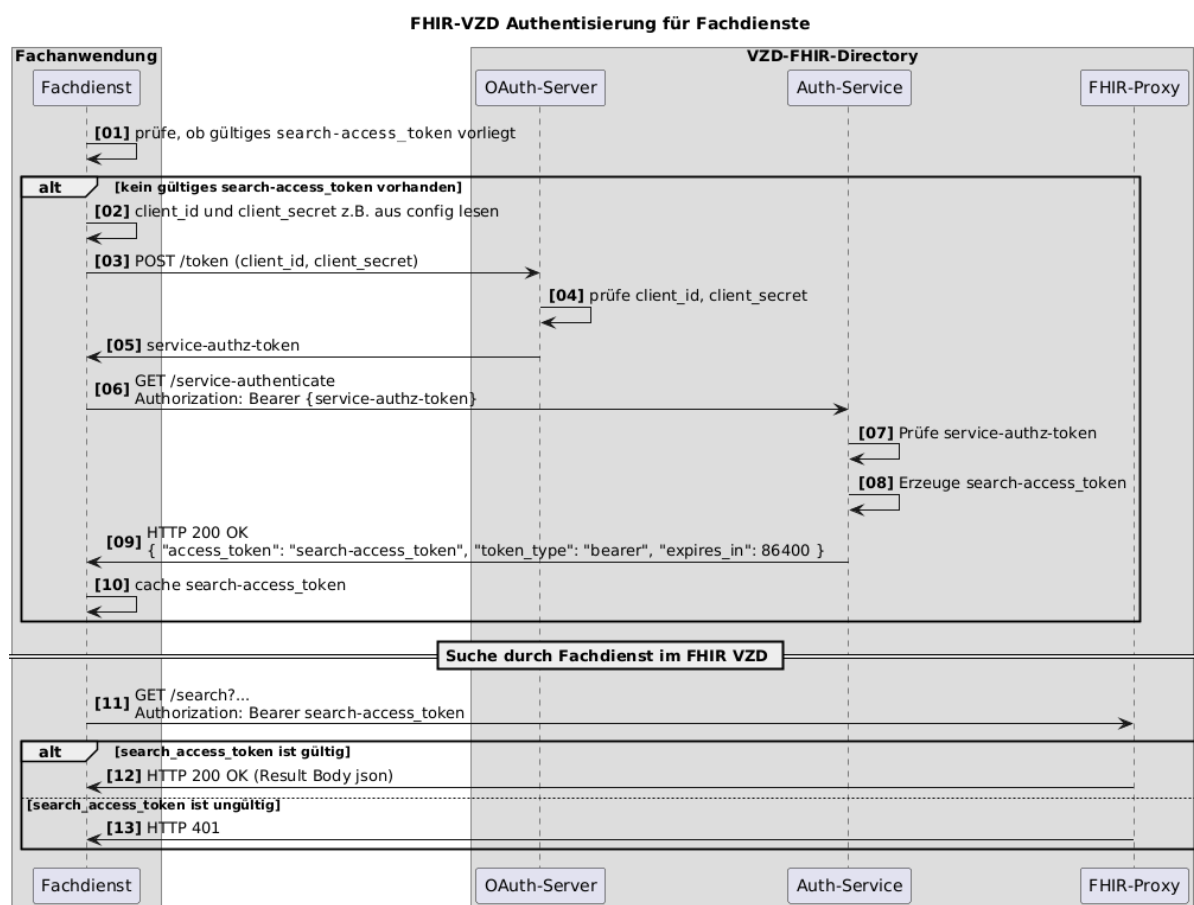


Abbildung 5 Sequence diagram - Fachdienst Authentisierung und Suche

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

Es wird Kapitel 5.12 wie folgt eingefügt

5.12 Holder Authentifizierung

AF_10404 - FHIR VZD - Holder Authentifizierung

Attribute	Bemerkung
Beschreibung	<p>Für die Suche am FHIR-Directory durch einen Holder ist eine Authentisierung am Auth-Service Endpunkt erforderlich. Der Ablauf entsprechend Abbildung "Sequence diagram /search":</p> <ol style="list-style-type: none"> Der Holder/Client prüft, ob er ein gültiges Holder-Access-Token vorliegen hat. [1] Der Holder benötigt zur Authentisierung gegenüber dem FHIR VZD Client Credentials. Diese erhält er in einem Registrierungsprozess vom Betreiber FHIR-Directory. Authentisierung des Holders mit Client Credentials [2-4] Der Holder authentisiert sich mit seinen Client Credentials und

	<p>erhält nach erfolgreicher Prüfung ein Key Cloak Holder-Access-Token.</p> <p>3. Abruf Holder-Access-Token [5-8] Der Holder/Client tauscht das Key Cloak Holder-Access-Token gegen ein Holder-Access-Token ein. Optional kann der Holder/Client das Holder-Access-Token cachen solange die zeitliche Gültigkeit ausreicht.</p>
Vorbedingung	Der Holder hat sich bei FHIR VZD Anbieter registriert und Client Credentials vorliegen.
Nachbedingung	Der Holder hat das Holder-Access-Token vorliegen.

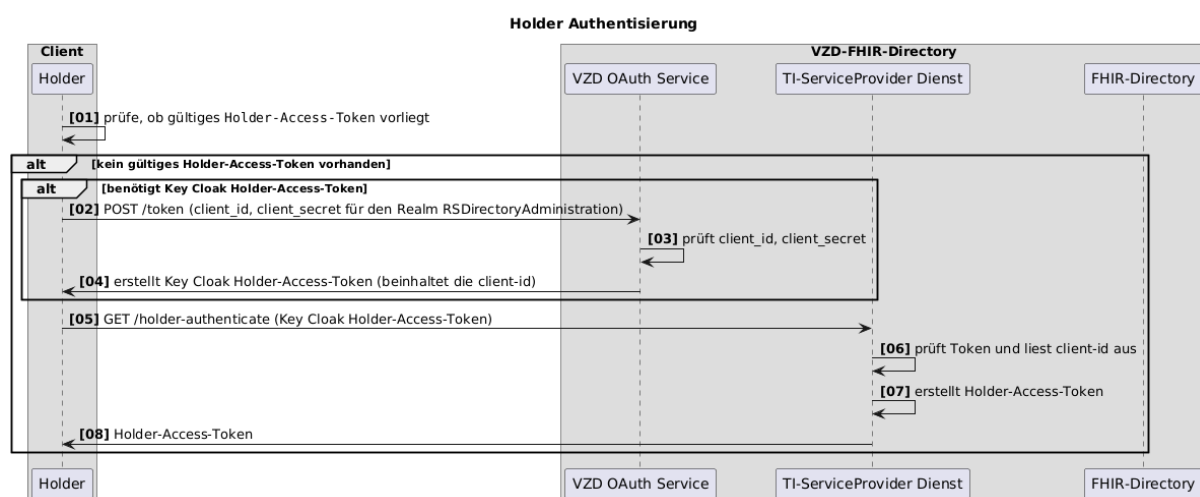


Abbildung 6 Sequence diagram - Holder Authentisierung

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

Es wird Kapitel 5.13 wie folgt eingefügt

5.13 Nutzer setzt Sichtbarkeit für Versicherte

AF_10377-01 - FHIR-VZD Sichtbarkeit für Versicherte setzen

Mit diesem Anwendungsfall kann ein berechtigter Nutzer die Sichtbarkeit der Endpoints, die seinem Practitioner- bzw. Organization-Eintrag zugeordnet sind, für Versicherte verwalten. Möchte der Nutzer verhindern, dass Versicherte z. B. eine hinterlegte MXID über die Suche finden können, dann kann er dies am Endpunkt konfigurieren oder im umgekehrten Fall wieder zurücknehmen.

Tabelle 2: TI-Messenger-Nutzer setzt Sichtbarkeit für Versicherte

Attribute	Bemerkung
Akteur	Mitarbeiter im Gesundheitswesen

Auslöser	Der Nutzer möchte einen Endpunkt im VZD-FHIR Directory für Versicherte nicht sichtbar (a) bzw. sichtbar (b) schalten.
Komponenten	<ul style="list-style-type: none"> Client FHIR-Proxy FHIR-Directory
Vorbedingungen	<ol style="list-style-type: none"> Der Nutzer ist bei einem zugelassenen Client angemeldet. Der Nutzer hat nach dem in AF_10037 beschriebenen Verfahren ein owneraccess-token erzeugt. Die seinem Practitioner- bzw. Organization-Eintrag zugehörigen Endpoints aus dem VZD-FHIR-Directory liegen dem Client vor.
Eingangsdaten	FHIR-Endpoint mit neuer endpointVisibility
Ergebnis	Der Eintrag ist in der Suche für Versicherte nicht sichtbar (a) bzw. sichtbar (b).
Ausgangsdaten	FHIR-Endpoint mit aktualisierter endpointVisibility

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es sich um eine **vereinfachte Laufzeitansicht**, in der zum Beispiel die TLS-Terminierung am FHIR-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde.

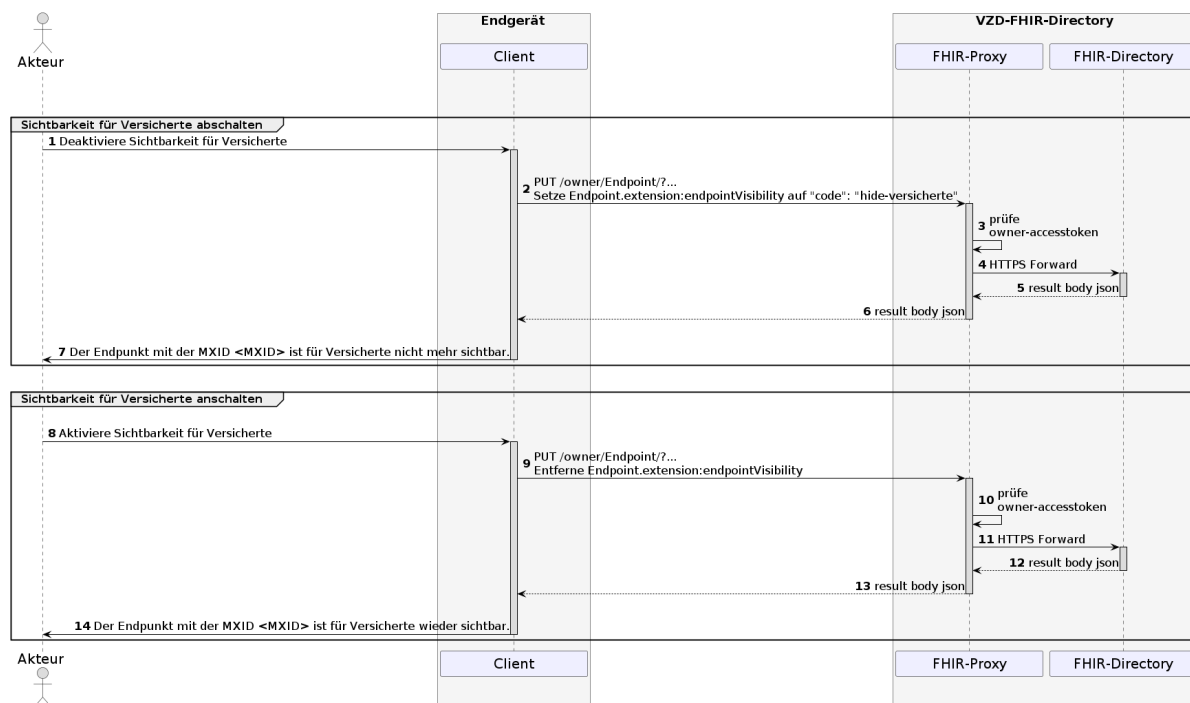


Abbildung 7: Laufzeitsicht - Organization - FHIR-VZD Sichtbarkeit für Versicherte setzen

[<=, Verzeichnisdienst, TI-M_FD_Pro, TI-M_Client_Pro, funkt. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA]

Es wird Kapitel 7.6 wie folgt angepasst

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

- de.gematik.fhir.directory/0.10.211.22

2 Änderung in gemSpec_VZD

Es wird in Kapitel 3.1 wie folgt eingefügt

...

TIP1-A_5548-01 - VZD, Protokollierung der Änderungsoperationen

Der VZD MUSS Änderungen der Verzeichnisdiensteinträge protokollieren und muss sie **6 24** Monate zur Verfügung halten.

[<=, VZD_FHIR, Verzeichnisdienst, Sich.techn. Eignung: Gutachten, funkt. Eignung: Test Produkt/FA]

6 Monate ist die maximale Nachweistiefe ohne in den Bereich der Vorratsdatenspeicherung zu kommen.

...

A_27215 - VZD, Zertifikatsprüfung über HTTP Forwarder

Der VZD MUSS Status-Prüfung von Zertifikaten - deren OCSP nicht in der TI erreichbar ist - über den HTTP Forwarder [gemSpec_VPN_ZugD#"3.8 http-Forwarder"] durchführen.

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

Es wird Kapitel 3.2 wie folgt angepasst

...

A_20262-01 - VZD, Maximale Anzahl von KOM-LE Adressen in den Fachdaten

Der VZD MUSS bei dem Hinzufügen von KOM-LE Adressen in den Fachdaten folgende Regeln beachten:

- Wenn maxKOMLEadr im Verzeichniseintrag keinen Wert enthält, MUSS der VZD das Eintragen **beliebig-vieler von** KOM-LE Adressen **entsprechend dem - im Datenmodell definierten - Maximalwert** in den Fachdaten erlauben.
- Wenn maxKOMLEadr im Verzeichniseintrag einen Wert enthält, MUSS der VZD das Eintragen von maximal so vielen KOM-LE Adressen in den Fachdaten erlauben.
- Wenn der Wert von maxKOMLEadr im Verzeichniseintrag gleich oder kleiner ist als die Anzahl der KOM-LE Adressen in den Fachdaten (z.B. falls der Wert herabgesetzt wurde), MUSS der VZD das Eintragen von weiteren KOM-LE Adressen in den Fachdaten ablehnen.

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

...

Es wird Kapitel 4.3 wie folgt angepasst

TIP1-A_5583-03 - VZD, Schnittstelle I_Directory_Application_Maintenance

Der VZD MUSS die Schnittstelle I_Directory_Application_Maintenance gemäß Tabelle Tab_VZD_Schnittstelle_I_Directory_Application_Maintenance anbieten.

Tabelle 3: Tab_VZD_Schnittstelle_I_Directory_Application_Maintenance

Name	I_Directory_Application_Maintenance	
Version	wird im Produkttypsteckbrief des VZD definiert	
Operationen	Operation	Kurzbeschreibung
	getInfo	Lesen der Metadaten dieser Schnittstelle (nur für die REST-Ausprägung verfügbar)
	add_Directory_FA-Attributes	Erzeugung eines Fachdaten-Eintrags
	delete_Directory_FA-Attributes	Löschen von einzelnen oder allen zu einem FAD gehörenden Fachdaten eines Eintrags.
	modify_Directory_FA-Attributes	Ändern fachspezifischer Attribute
	get_Directory_FA_Attributes	Lesen fachspezifischer Attribute
	search_Directory_FA-Attributes	Suche mit Hilfe des Attributs FAD1.mail
	getAppTags	Lesen Anwendungskennzeichen
	read_Directory_Entry	Suche Verzeichniseintrag
	readLog	Lesen Log Daten

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

Es wird Kapitel 4.3.4.1 wie folgt angepasst

TIP1-A_5599-01 - VZD, Umsetzung modify_Directory_FA-Attributes

Der VZD MUSS nach folgenden Vorgaben die Operation modify_Directory_FA-Attributes implementieren:

1. Wenn kein zur Telematik-ID gehörender Basisdatensatz gefunden wurde, wird der Request mit einem gematik SOAP-Fault beendet:
faultcode: 4312,
faultstring: Basisdaten konnten nicht gefunden werden.
2. Ein bereits zur Telematik-ID gehörender Fachdatensatz wird überschrieben.

3. Die Daten aus dem SOAP Request werden gemäß VZD_TAB_I_Directory_Application_Maintenance_Modify_Mapping zum Basisdatensatz hinzugefügt.
4. Für die Koexistenz dieser Operation mit den Erweiterungen für das Anwendungskennzeichen MÜSSEN folgende Vorgaben umgesetzt werden:
 - a. Beim Aufruf von modify_Directory_FA-Attributes wird das Attribut "Mail" übergeben. KimData MUSS basierend auf der übergebenen Mail-Adresse gefüllt werden, wobei die Subattribute "Version" und "AppTags" (falls vorhanden) erhalten bleiben.
 - b. Wenn das KimData-Attribut für eine Mail-Adresse vor dem Aufruf von modify_Directory_FA-Attributes gepflegt ist, das KomLeData-Attribut jedoch leer ist, DÜRFEN keine Änderungen an den Attributen KomLeData und KimData für diese Mail-Adresse vorgenommen werden.
 - c. Bestehende KimData-Einträge DÜRFEN durch modifyDirectoryFAAttributes NICHT entfernt werden.

Tabelle 4: VZD_TAB_I_Directory_Application_Maintenance_Modify_Mapping

SOAP-Request Element	LDAP-Directory Basisdatensatz Attribut
VZD:timestamp	wird nicht in das LDAP-Directory eingetragen
VZD:Telematik-ID	
<FA-Attributes>	fachdienstspezifische Attribute. Die SOAP-Request-Elemente werden namensgleich als LDAP-Attribute übernommen.

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0010 verwendet werden.
 [<=, Verzeichnisdienst, funkt. Eignung: Test Produkt/FA]

Es wird Kapitel 4.3.7 wie folgt eingefügt

4.3.7 Operation search_Directory_FA-Attributes

Die Anwendungsdaten können mit der im Folgenden beschriebenen Operation eingesehen werden.

A_27223 - VZD, I_Directory_Application_Maintenance, search_Directory_FA-Attributes

Der VZD MUSS die Operation „search_Directory_FA-Attributes“ gemäß Tabelle Tab_VZD „search_Directory_FA-Attributes“ umsetzen.

Tabelle 5: Tab_VZD „search_Directory_FA-Attributes“

Name	search_Directory_FA-Attributes
Beschreibung	Diese Operation ermöglicht die Suche und das Lesen von Anwendungsdaten.
Eingangsdaten	REST-Request GET /DirectoryEntries/KOM-LE_Fachdaten

	operationId: search_Directory_FA-Attributes (siehe DirectoryApplicationMaintenance.yaml)	
	Parameter	Beschreibung
	Parameter zur Selektion der Anwendungsdaten	Siehe DirectoryApplicationMaintenance.yaml
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit allen zu den Filter-Parametern passenden Anwendungsdaten.	
Ablauf	Der VZD sucht im LDAP-Verzeichnis die zu den Such-Parametern passenden Anwendungsdaten. Bei mehr als 100 gefundenen Einträgen werden nur 100 gefundene Einträge zurückgegeben.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryApplicationMaintenance.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

【<=, Verzeichnisdienst, funkt. Eignung: Herstellererklärung】

Es wird Kapitel 4.3.8 wie folgt eingefügt

4.3.8 Operation readLog

Die Logdaten können mit der im Folgenden beschriebenen Operation eingesehen werden.

A_27224 - VZD, I_Directory_Application_Maintenance, readLog

Der VZD MUSS Operation „readLog“ gemäß Tabelle Tab_VZD „readLog“ umsetzen.

Tabelle 6: Tab_VZD „readLog“

Name	readLog	
Beschreibung	Diese Operation ermöglicht das Lesen von Logdaten.	
Eingangsdaten	REST-Request GET /Log operationId:readLog (siehe DirectoryApplicationMaintenance.yaml)	
	Parameter	Beschreibung
	Parameter zur Selektion der Logdaten	Siehe DirectoryApplicationMaintenance.yaml
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit allen zu den Filter-Parametern passenden Anwendungsdaten.	
Ablauf	Der VZD sucht im LDAP-Verzeichnis die zu den Such-Parametern passenden Logdaten und gibt sie als Ergebnis der Operation.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryApplicationMaintenance.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

【<=, Verzeichnisdienst, funkt. Eignung: Herstellererklärung】

Es wird Kapitel 4.6.1 wie folgt angepasst

A_18371-05 - VZD, Schnittstelle I_Directory_Administration

Der VZD MUSS die Schnittstelle I_Directory_Administration gemäß Tabelle Tab_VZD_Schnittstelle_I_Directory_Administration im Internet anbieten.

Tabelle 7: Tab_VZD_Schnittstelle_I_Directory_Administration

Name	I_Directory_Administration	
Version	wird im Produkttypsteckbrief des VZD definiert	
Operationen	Resource: / (übergreifend für gesamte Schnittstelle)	
	Name	Kurzbeschreibung
	GET	Lesen der Metadaten dieser Schnittstelle
	Resource: DirectoryEntries	
	Name	Kurzbeschreibung
	POST	Hinzufügen eines Verzeichniseintrages inklusive dazugehörendem Zertifikat.
	GET	Abfrage aller Daten von Verzeichniseinträgen.
	PUT	Änderung eines Basisdaten-Verzeichniseintrages.
	PUT	Änderung Status des Verzeichniseintrages
	DELETE	Löschung eines Verzeichniseintrages (kompletter Datensatz inklusive aller Zertifikate und Fachdaten).
	Resource: /DirectoryEntriesSync	
	Name	Kurzbeschreibung
	GET	Abfrage aller Daten von Verzeichniseinträgen zu Synchronisationszwecken.
	Resource: /v2/DirectoryEntriesSync	

Name	Kurzbeschreibung
GET	Abfrage aller Daten von Verzeichniseinträgen zu Synchronisationszwecken mit Paging.
Resource: /v2/DirectoryEntriesSync/KOM-LE_Fachdaten	
Name	Kurzbeschreibung
GET	Abfrage aller Fachdaten von Verzeichniseinträgen zu Synchronisationszwecken mit Paging.
Resource: Certificate	
Name	Kurzbeschreibung
POST	Hinzufügen eines Zertifikatseintrags zu einem Verzeichniseintrag.
GET	Abfrage von Zertifikatseinträgen.
DELETE	Löschen von Zertifikatseinträgen.
Resource: /DirectoryEntries/KOM-LE_Fachdaten	
Name	Kurzbeschreibung
GET	Abfrage der Fachdaten von Verzeichniseinträgen.
Resource: /DirectoryEntries/Log	
Name	Kurzbeschreibung
GET	Abfrage der Logdaten

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

Es wird Kapitel 4.6.1.4.1 wie folgt angepasst

A_21230-04 - VZD, I_Directory_Administration, read_Directory_Entry_for_Sync

Der VZD MUSS Operation „read_Directory_Entry_for_Sync“ gemäß Tabelle Tab_VZD „read_Directory_Entry_for_Sync“ umsetzen.

Tabelle 8: Tab_VZD „read_Directory_Entry_for_Sync“

Name	read_Directory_Entry_for_Sync
Beschreibung	Diese Operation ermöglicht die Suche und Lesen von

	Verzeichniseinträgen im LDAP-Verzeichnis. Diese Operation liefert auch Einträge, die ohne gültige Zertifikate sind.	
Eingangsdaten	REST-Request GET /DirectoryEntries operationId: read_Directory_Entry (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung
	Parameter zur Selektion der Verzeichniseinträge	Alle im Datenmodell aufgeführten Felder des Basiseintrags - insbesondere auch dataFromAuthority - können zur Suche genutzt werden. Die angegebenen Parameter werden zur Suche mit einem logischen UND verknüpft.
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit allen zu den Filterparametern passenden Verzeichniseinträgen. Die Verzeichniseinträge werden optional inklusive Zertifikatseinträgen und Fachdaten geliefert.	
Ablauf	Der VZD sucht im LDAP-Verzeichnis die zu den Suchparametern passenden Verzeichniseinträge. Bei mehr als 100 gefundenen Einträgen werden nur 100 gefundene Einträge zurückgegeben. Wenn über den "holder" Suchparameter nach eigenen Verzeichniseinträgen oder Verzeichniseinträgen ohne gesetztes "holder" Attribut gesucht wird, MÜSSEN Vom VZD MÜSSEN über den Paging Mechanismus (entsprechend RFC2696 und Definition in DirectoryAdministration.yaml) alle Suchergebnisse - ohne Beschränkung auf 100 Einträge - zurückgegeben werden.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

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

A_20402-03 - VZD, I_Directory_Administration, read_Directory_Entry_for_Sync, Paging, Berechtigung

Der VZD MUSS für den Paging Mechanismus von Operation „read_Directory_Entry_for_Sync“ sicherstellen:

- Der "holder" Suchparameter muss den gleichen Wert enthalten wie der ACCESS_TOKEN claim scope.
- Die pagingSize darf die Maximalgröße entsprechend TIP1-A_5552 nicht überschreiten.
- Die Suchparameter dürfen sich während eines Pagings (mit mehreren Request/Response Sequenzen) nicht ändern (nur das "cookie" ändert sich).

Bei Abweichungen von diesen Festlegungen MUSS der VZD mit einem Fehler (HTTP-Status-Code 403) antworten.

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

Es wird Kapitel 4.6.1.5 wie folgt eingefügt

4.6.1.5 Application Data Administration

Die Anwendungsdaten können mit den im Folgenden beschriebenen Operationen eingesehen werden.

A_27218 - VZD, I_Directory_Administration, search_Directory_FA-Attributes

Der VZD MUSS Operation „search_Directory_FA-Attributes“ gemäß Tabelle Tab_VZD „search_Directory_FA-Attributes“ umsetzen.

Tabelle 9: Tab_VZD „search_Directory_FA-Attributes“

Name	search_Directory_FA-Attributes	
Beschreibung	Diese Operation ermöglicht die Suche und Lesen von Anwendungsdaten.	
Eingangsdaten	REST-Request GET /DirectoryEntries/KOM-LE_Fachdaten operationId: search_Directory_FA-Attributes (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung
	Parameter zur Selektion der Anwendungsdaten	Siehe DirectoryAdministration
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit allen zu den Filter-Parametern passenden Anwendungsdaten.	
Ablauf	Der VZD sucht im LDAP-Verzeichnis die zu den Such-Parametern passenden Anwendung Bei mehr als 100 gefundenen Einträgen werden nur 100 gefundenen Einträge zurückge	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und i DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

【<=, Verzeichnisdienst, funkt. Eignung: Herstellererklärung】

4.6.1.6 Log Daten- Operation readLog

Die Logdaten können mit der im Folgenden beschriebenen Operation eingesehen werden.

A_27225 - VZD, I_Directory_Administration, readLog

Der VZD MUSS Operation „readLog“ gemäß Tabelle Tab_VZD „readLog“ umsetzen.

Tabelle 10: Tab_VZD „readLog“

Name	readLog
Beschreibung	Diese Operation ermöglicht das Lesen von Logdaten.
Eingangsdaten	REST-Request GET /Log operationId:readLog (siehe DirectoryAdministration.yaml)

	Parameter	Beschreibung
	Parameter zur Selektion der Logdaten	Siehe DirectoryAdministration.yaml
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit allen zu den Filter-Parametern passenden Anwendungsdaten.	
Ablauf	Der VZD sucht im LDAP-Verzeichnis die zu den Such-Parametern passenden Logdaten und gibt sie als Ergebnis der Operation.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

【<=, Verzeichnisdienst, funkt. Eignung: Herstellererklärung】

Es wird Kapitel 4.6.1.4 wie folgt angepasst

4.6.1.4 DirectoryEntry Synchronization

Zur Unterstützung der Pflege der Basiseinträge (Verzeichnisdienst_Eintrag) wird werden die hier beschriebenen Operationen zur Verfügung gestellt. Sie dienen der Synchronisation mit dem Datenbestand des Verzeichnisdienstes und erlauben – im Gegensatz zur Operation „read_Directory_Entry“ – das Lesen beliebig vieler eigener Verzeichniseinträge.

Es wird Kapitel 4.6.1.4.2 wie folgt eingefügt

4.6.1.4.2 GET search_Directory_FA-Attributes_for_Sync_paging

Die Anwendungsdaten können mit den im Folgenden beschriebenen Operationen eingesehen werden.

A_27222 - VZD, I_Directory_Administration, search_Directory_FA-Attributes_for_Sync_paging

Der VZD MUSS Operation „search_Directory_FA-Attributes_for_Sync_paging“ gemäß Tabelle Tab_VZD „search_Directory_FA-Attributes_for_Sync_paging“ umsetzen.

Tabelle 11: Tab_VZD „search_Directory_FA-Attributes“

Name	search_Directory_FA-Attributes_for_Sync_paging	
Beschreibung	Diese Operation ermöglicht die Suche und Lesen von Anwendungsdaten mit Pagingfunktionalität.	
Eingangsdaten	REST-Request GET /v2/DirectoryEntriesSync/KOM-LE_Fachdaten operationId: search_Directory_FA-Attributes_for_Sync_paging (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung

	Parameter zur Selektion der Anwendungsdaten	Siehe DirectoryAdministration
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit allen zu den Filter-Parametern passenden Anwendungsdaten.	
Ablauf	Der VZD sucht im LDAP-Verzeichnis die zu den Such-Parametern passenden Anwendungsdaten. Diese Operation entspricht der Operation search_Directory_FA-Attributes mit Erweiterung des Paging. Über die Paging Funktionalität können mehr als 100 gefundenen Einträge gelistet werden.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

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

Es wird Kapitel 4.6.3 wie folgt angepasst

A_24059-01 - 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 12: Tab_VZD_Datenmapping_linked

LDAP Attribut	FHIR HealthcareService 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.
specialization	speciality	Mapping auf HealthcareServices.specialty, HealthcareServices.type und Organization.type.
domainID	identifier	Wird normalerweise auf Organization.identifier gemappt. Mapping erfolgt hier auf HealthcareService.identifier.
streetAddress, postalCode, countryCode,	Location	Normales Mapping auf Location Attribute und Verlinkung der Location mit dem

localityName, stateOrProvinceName		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. 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 normalerweise in Organization.type abgelegt. Mapping erfolgt hier auf HealthcareService.type. Wird nicht in den FHIR VZD übernommen. Die ProfessionOID der Organisation ist in FHIR bereits in Organization.type enthalten.
active	-	Wird nicht in den HealthcareService gemappt. Der Status für den generierten HealthcareService ergibt sich aus dem "active" Status der Organisation (wie für alle HealthcareServices). Wenn der untergeordnete LDAP Datensatz über das "active" Attribut deaktiviert wird, hat das keine Auswirkungen auf den FHIR HealthcareService. Wenn der übergeordnete LDAP Datensatz über das "active" Attribut deaktiviert wird, hat dies im FHIR VZD Auswirkungen auf alle verlinkten HealthcareService.

【<=, VZD_FHIR, funkt. Eignung: Herstellererklärung】

Es wird Kapitel 4.6.4 neu aufgenommen

4.6.4 Synchronisation Zertifikatsstatus in den FHIR VZD

Im VZD sind Verzeichniseinträge nur auffindbar, wenn für ihn ein gültiges Zertifikat vorliegt. Dies muss auch für den FHIR VZD umgesetzt werden.

A_25997 - VZD - Synchronisation Zertifikatsstatus LDAP VZD - FHIR VZD

Der VZD MUSS bei der Synchronisation der LDAP VZD Einträge in den FHIR VZD das "active" Attribut von der FHIR Organization bzw. Practitioner nach folgenden Regeln setzen:

- Wenn das LDAP "active" Attribut den Wert TRUE hat und mindestens ein gültiges Zertifikat für den LDAP VZD Eintrag vorliegt: FHIR VZD "active" Attribut auf TRUE setzen.
- In allen anderen Fällen (LDAP "active" == FALSE ODER/UND kein gültiges Zertifikat vorhanden): FHIR VZD "active" Attribut auf FALSE setzen.

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

A_25998 - VZD - Synchronisation Zertifikatsstatus - Logging

Der VZD MUSS bei der Synchronisation die Änderungen der "active" Attribute von den FHIR Organisationen bzw. Practitionern in einem Logfile dokumentieren.

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

Es wird Kapitel 5 wie folgt angepasst

TIP1-A_5607-12 - 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.

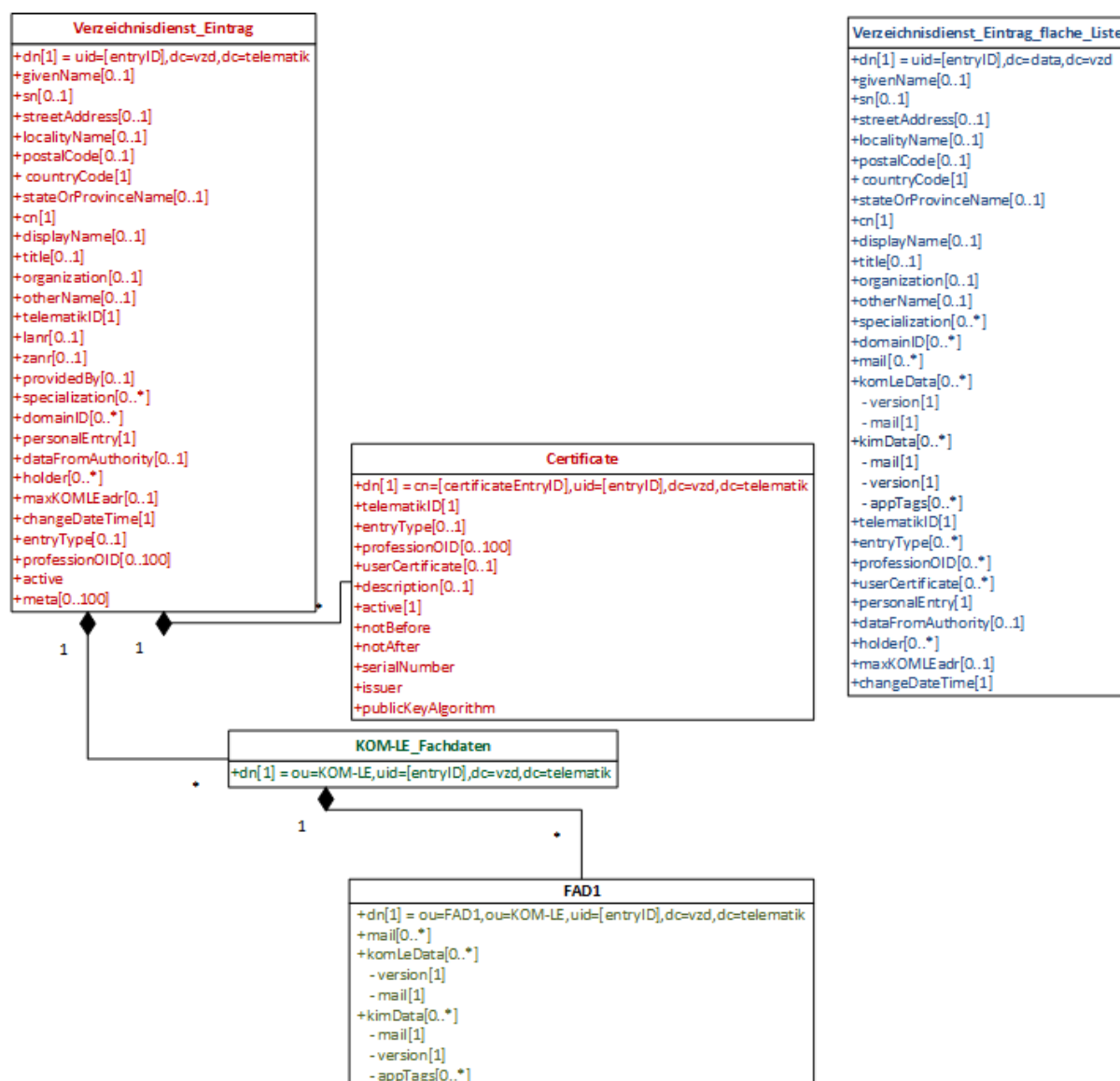


Abbildung 8: Abb_VZD_logisches_Datenmodell

Tabelle 13: Tab_VZD_Datenbeschreibung

LDAP-Directory Attribut	Pflichtfeld?	Erläuterung
givenName	optional	<p>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.</p> <p>Wird dem Verzeichniseintrag ein neues Zertifikat hinzu gefügt, wird der aktuelle Wert des Attributs durch der Wert aus Zertifikatsattribut givenName überschrieben.</p> <p>SMC-B-Eintrag: wird nicht verwendet</p>

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

		Wird cn als Parameter übergeben, wird der angegebene Wert übernommen.
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	Bezeichner: Postleitzahl
countryCode	obligatorisch	Kann beim Anlegen des Datensatzes und beim Ändern gesetzt werden (falls nicht gesetzt, ergänzt der VZD den Defaultwert für Deutschland).
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	<p>HBA: Bezeichner: Titel</p> <p>SMC-B: nicht verwendet</p>
organization	optional	<p>HBA: Bezeichner: Name der Organisation oder Name der Betriebsstätte</p> <p>SMC-B: Alternativer Name, nach dem der Eintrag von Nutzern gesucht wird, und unter dem gefundene Einträge angezeigt werden</p>
otherName	optional	<p>Bezeichner: Anderer Name</p> <p>Veraltet: Wird für die Suche nach Einträgen und die Anzeige von gefundenen Einträgen nicht benötigt (siehe displayName und</p>

		organization)
specialization	optional	<p>Bezeichner: Fachgebiet Kann mehrfach vorkommen (1..100).</p> <p>Für Einträge der Leistungserbringerorganisationen außer Apotheken (SMC-B Eintrag) Der Wertebereich entspricht den in hl7 definierten und für ePA festgelegten Werten (https://wiki.hl7.de/index.php?title=IG:Value_Sets_f%C3%BCr_XDS#DocumentEntry.practiceSettingCode). 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 Krankenhaus: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.4:GESU</p> <p>Für Einträge der Apotheken (SMC-B Eintrag) Im Attribut specialization werden die ApothekenTypen (OffizinApo, Versand etc) erfasst. Hierfür wird das dafür definierten CodeSysteme PharmacyTypeCS (https://simplifier.net/vzd-fhir-directory/pharmacytypecs) genutzt. Default für das Attribut ist LEER. LEER wird in der eRezept Anwendung gleich behandelt wie "Sonstige_offen".</p> <p>Für Einträge der Leistungserbringer (HBA-Eintrag) Der Wertebereich entspricht den in hl7 definierten Werten (https://wiki.hl7.de/index.php?title=IG:Value_Sets_f%C3%BCr_XDS#DocumentEntry.authorSpecialty). 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</p>
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.

dataFromAuthority	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 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. 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. 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). 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 Wird vom VZD anhand der im jeweiligen Zertifikat enthaltenen Telematik-ID (Feld registrationNumber der Extension Admission) übernommen. Ist in den Basisdaten und in den Zertifikatsdaten enthalten.</p>
lanr	obligatorisch für alle Ärzte mit LANR	<p>Bezeichner: LANR Die lebenslange Arztnummer, kurz LANR, dient der Suche nach Ärzten. Insbesondere für die Suche durch Clients, welche die TelematikID nicht vorliegen haben.</p>
zanr	obligatorisch für alle Zahnärzte mit ZANR	<p>Bezeichner: ZANR Die lebenslangen Zahnarzt Nummer, kurz ZANR, dient der Suche nach Zahnärzten. Insbesondere für die Suche durch Clients, welche die TelematikID nicht vorliegen haben.</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 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</p> <p>Dieses Attribut ermöglicht das Zertifikat zu beschreiben, um die Administration des VZD-Eintrags zu vereinfachen.</p> <p>Hinweis: wird aktuell nicht verwendet.</p>
mail	optional	<p>Bezeichner: KOM-LE-Mail-Adresse</p> <p>kann mehrfach vorkommen (0..1000)</p> <p>Wird vom KOM-LE-Fachdienst-Anbieter eingetragen.</p>
komLeData	optional	<p>Bezeichner: komLeData</p> <p>kann mehrfach vorkommen (0..1000)</p> <p>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.</p> <p>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.</p> <p>Jeder Datensatz - bestehend aus Version und KOM-LE-Mail-Adresse - muss vollständig sein (beide Attribute sind obligatorisch).</p> <p>Zu beachten ist bei der Auswertung bzw. Pflege dieser Daten:</p> <ul style="list-style-type: none"> • Ein komLeData Eintrag setzt sich zusammen aus der Mail Adresse (Attribut "mail") und der zugehörigen KOM-LE Version (Attribut "version"). • 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. • 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. • Beispiel für den Wert eines komLeData Eintrags in der flachen Liste (Ausgabe einer LDAP Suche): <ul style="list-style-type: none"> 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
kimData	optional	<p>Bezeichner: kimData</p> <p>kann mehrfach vorkommen (0..1000)</p> <p>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 zusätzliches "+" angegeben ist, dann können mit dieser "mail" Adresse Nachrichten größer 15MiB verarbeitet werden.</p>

		<p>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"> • 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"). • Bei Angabe von mehreren Anwendungskennzeichen werden sie im LDAP Attribut durch das ' ' Zeichen getrennt (siehe Beispiel unten). • Für jede Mail Adresse darf es nur einen Eintrag in der Datenstruktur kimData geben. • 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. • Beispiel für den Wert eines kimData Eintrags in der flachen Liste (Ausgabe einer LDAP Suche): 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 kimData: mb_secu_sm@dom4.kim.telematik-test,1.0 kimData: ak_secu_102@dom5.kim.telematik-test,1.5
changeDateTi	obligato	Der VZD setzt dieses Attribut bei jeder Schreiboperation für den Datensatz (Basisdaten und Zertifikate) auf die aktuelle Zeit. Format

me	risch	entsprechend RFC 3339, section 5.6.
----	-------	-------------------------------------

【<=, Verzeichnisdienst, funkt. Eignung: Herstellererklärung】

3 Änderungen in Steckbriefen

3.1 Änderungen in gemProdT_VZD_FHIR

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_VZD_FHIR]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 14: Festlegungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
AF_10036-01	Nutzer sucht Einträge im FHIR-Directory	gemSpec_VZD_FHIR_Directory
AF_10036-02	Nutzer sucht Einträge im FHIR-Directory	gemSpec_VZD_FHIR_Directory
AF_10037-02	Einträge im VZD-FHIR-Directory ändern und suchen	gemSpec_VZD_FHIR_Directory
AF_10037-03	Einträge im VZD-FHIR-Directory ändern und suchen	gemSpec_VZD_FHIR_Directory
AF_10048-01	Anwendungsfälle der TI-Messenger-Anbieter im VZD-FHIR-Directory	gemSpec_VZD_FHIR_Directory
AF_10048-02	Anwendungsfälle der TI-Messenger-Anbieter im VZD-FHIR-Directory	gemSpec_VZD_FHIR_Directory
AF_10219	Versicherter sucht Einträge im FHIR-Directory	gemSpec_VZD_FHIR_Directory
AF_10219-01	Versicherter sucht Einträge im FHIR-Directory	gemSpec_VZD_FHIR_Directory
AF_10374	Leistungserbringer/Organisation sucht im FHIR-Directory	gemSpec_VZD_FHIR_Directory
AF_10375	Holder sucht im FHIR VZD	gemSpec_VZD_FHIR_Directory
AF_10403	Fachdienst sucht Einträge im FHIR-Directory	gemSpec_VZD_FHIR_Directory
AF_10404	FHIR VZD - Holder Authentifizierung	gemSpec_VZD_FHIR_Directory

AF_10377-01	FHIR-VZD Sichtbarkeit für Versicherte setzen	gemSpec_VZD_FHIR_Directory
A_24059-01	VZD, I_Directory_Administration, Synchronisationsregeln für verlinkte LDAP Datensätze	gemSpec_VZD

3.2 Änderungen in gemProdT_VZD

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_VZD]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

**Tabelle 15: Anforderungen zur funktionalen Eignung
"Produkttest/Produktübergreifender Test"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_20262	VZD, Maximale Anzahl von KOM-LE Adressen in den Fachdaten	gemSpec_VZD
A_20262-01	VZD, Maximale Anzahl von KOM-LE Adressen in den Fachdaten	gemSpec_VZD
TIP1-A_5599	VZD, Umsetzung modify_Directory_FA-Attributes	gemSpec_VZD
TIP1-A_5599-01	VZD, Umsetzung modify_Directory_FA-Attributes	gemSpec_VZD
A_18371-01	VZD, Schnittstelle I_Directory_Administration	gemSpec_VZD
A_18371-05	VZD, Schnittstelle I_Directory_Administration	gemSpec_VZD
A_21230-01	VZD, I_Directory_Administration, read_Directory_Entry_for_SyncVZD, I_Directory_Administration, read_Directory_Entry_for_Sync	gemSpec_VZD
A_21230-04	VZD, I_Directory_Administration, read_Directory_Entry_for_Sync	gemSpec_VZD
A_20402-02	VZD, I_Directory_Administration, read_Directory_Entry_for_Sync, Paging, Berechtigung	gemSpec_VZD
A_20402-03	VZD, I_Directory_Administration, read_Directory_Entry_for_Sync, Paging,	gemSpec_VZD

	Berechtigung	
--	--------------	--

Tabelle 16: Festlegungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_27215	VZD, Zertifikatsprüfung über HTTP Forwarder	gemSpec_VZD
TIP1-A_5583-02	VZD, Schnittstelle I_Directory_Application_Maintenance	gemSpec_VZD
TIP1-A_5583-03	VZD, Schnittstelle I_Directory_Application_Maintenance	gemSpec_VZD
A_27223	VZD, I_Directory_Application_Maintenance, search_Directory_FA-Attributes	gemSpec_VZD
A_27224	VZD, I_Directory_Application_Maintenance, readLog	gemSpec_VZD
A_27218	VZD, I_Directory_Administration, search_Directory_FA-Attributes	gemSpec_VZD
A_27225	VZD, I_Directory_Administration, readLog	gemSpec_VZD
A_27222	VZD, I_Directory_Administration, search_Directory_FA-Attributes_for_Sync_paging	gemSpec_VZD
A_25997	VZD - Synchronisation Zertifikatsstatus LDAP VZD - FHIR VZD	gemSpec_VZD
A_25998	VZD - Synchronisation Zertifikatsstatus - Logging	gemSpec_VZD
TIP1-A_5607-11	VZD, logisches Datenmodell	gemSpec_VZD
TIP1-A_5607-12	VZD, logisches Datenmodell	gemSpec_VZD