Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Verzeichnisdienst FHIR-Directory

Version:	1.1.0~~.0~~
Revision:	~~408158~~482259
Stand:	~~01.10.2021~~29.07.2022
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_VZD_FHIR_Directory

Dokumentinformationen

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	01.10.2021		Erstversion des Dokumentes	gematik
1.1.0	29.07.2022		Fortschreibung und insbesondere Anpassungen gemäß TI-Messenger-Spezifikation Version 1.1.0	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes

Dieses Dokument beschreibt das FHIR-Directory des Verzeichnisdienstes der TI. Die Spezifikation umfasst Schnittstellen zum Abruf von Informationen der im FHIR-Directory eingetragenen Organization-FHIR-Ressourcen und der Practitioner-FHIR-Ressourcen durch Clientsysteme sowie Schnittstellen und Prozesse zur Pflege der Informationen innerhalb des VZD-FHIR-Directories.

1.1 Zielsetzung

Die Spezifikation soll die Entwicklung und den Betrieb eines VZD-FHIR-Directories für die Telematikinfrastruktur unterstützen, indem die funktionalen und nicht-funktionalen Anforderungen sowie die Sicherheits-Anforderungen an den Dienst festgelegt werden.

1.2 Zielgruppe

Das Dokument richtet sich zwecks der Realisierung an den Hersteller des VZD-FHIR-Directories sowie an den Anbieter, welcher dieses Produkt betreibt [gemKPT_Betr]. Alle Hersteller und Anbieter von TI-Anwendungen, die das VZD-FHIR-Directory nutzen, müssen dieses Dokument ebenso berücksichtigen. Gleichfalls ist das Dokument auch für die Nutzer relevant welche die Daten im VZD-FHIR-Directory eintragen, abfragen, ändern und löschen wollen.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. gemPTV_ATV_Festlegungen, Produkttypsteckbrief, Anbietertypsteckbrief, u.a.) oder Webplattformen (z.B. gitHub, u.a.) festgelegt und bekanntgegeben.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzungen

Spezifiziert werden in dem Dokument nur die mit dem VZD-FHIR-Directory neu eingeführten Komponenten und Schnittstellen des Verzeichnisdienstes der TI. Das VZD-LDAP-Directory ist in [gemSpec_VZD] spezifiziert.

Benutzte Schnittstellen werden in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang, Kapitel ~~8~~7.5- Referenzierte Dokumente).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief des Produkttyps VZD-FHIR-Directory verzeichnet.

1.5 Methodik

Die Spezifikation ist im Stil einer RFC-Spezifikation verfasst. Dies bedeutet:

- **Der gesamte Text in der Spezifikation ist sowohl für den Hersteller des Produktes VZD-FHIR-Directory als auch für den betreibenden Anbieter entsprechend [gemKPT_Betr] verbindlich zu betrachten und gilt sowohl als Zulassungskriterium beim Produkt und Anbieter.**
- Auch für technisch mit dem Produkt und Dienst verbundene Anwendungen ist dieses Dokument verbindlich. Gleichfalls für die Nutzer, welche zur Datenpflege im VZD-FHIR-Directory beitragen oder Daten abfragen.
- Die Verbindlichkeit SOLL durch die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet werden.
- Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen.“ die Phrase „DARF NICHT“ semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen „Eine leere Liste DARF KEIN Element besitzen.“ verwendet.
- Die Schlüsselworte KÖNNEN außerdem um Pronomen in Großbuchstaben ergänzt werden, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

Anwendungsfälle und Akzeptanzkriterien als Ausdruck normativer Festlegungen werden als Grundlage für Erlangung der Zulassung durch Tests geprüft und nachgewiesen. Sie besitzen eine eindeutige, permanente ID, welche als Referenz verwendet werden SOLL. Die Tests werden gegen eine von der gematik gestellte Referenz-Implementierung durchgeführt.

Anwendungsfälle und Akzeptanzkriterien werden im Dokument wie folgt dargestellt:
<ID> - <Titel des Anwendungsfalles / Akzeptanzkriteriums>
Text / Beschreibung
[<=]

Die einzelnen Elemente beschreiben:

- **ID**: einen eindeutigen Identifier.
  - Bei einem Anwendungsfall besteht der Identifier aus der Zeichenfolge 'AF_' gefolgt von einer Zahl,
  - Der Identifier eines Akzeptanzkriteriums wird von System vergeben, z.B. die Zeichenfolge 'ML_' gefolgt von einer Zahl

- **Titel des Anwendungsfalles / Akzeptanzkriteriums**: Ein Titel, welcher zusammenfassend den Inhalt beschreibt
- **Text / Beschreibung**: Ausführliche Beschreibung des Inhalts. Kann neben Text Tabellen, Abbildungen und Modelle enthalten

Dabei umfasst der Anwendungsfall bzw. das Akzeptanzkriterium sämtliche zwischen ID und Textmarke [<=] angeführten Inhalte.

Der für die Erlangung einer Zulassung notwendige Nachweis der Erfüllung des Anwendungsfalls wird in den jeweiligen Steckbriefen festgelegt, in denen jeweils der Anwendungsfall gelistet ist. Akzeptanzkriterien werden in der Regel nicht im Steckbrief gelistet.

Hinweis auf offene Punkte

Offener Punkt: Das Kapitel wird in einer späteren Version des Dokumentes ergänzt.

2 Systemüberblick

Das VZD-FHIR-Directory ist eine Erweiterung des bisherigen Verzeichnisdienstes der TI. Im VZD-FHIR-Directory werden Einträge von Organisationen und Leistungserbringern gespeichert. Die ~~Einträge werden mit den Einträgen im~~ VZD-LDAP-Directory Einträge werden in das VZD-FHIR-Verzeichnis synchronisiert. Bei diesem Vorgang erfolgt eine Umsetzung von der LDAP-Datenstruktur auf die Datenstruktur der FHIR-Ressourcen. Personeneinträge der Leistungserbringer werden auf die ~~TIPractitioner~~PractitionerDirectory-Ressource und Organisations-Einträge auf die ~~TIOrganization~~OrganizationDirectory-Ressource abgebildet. Die synchronisierten Einträge bilden die Basis-Einträge, die durch die Besitzer um zusätzliche Daten ergänzt bzw. erweitert werden können. ~~TIPractitioner~~PractitionerDirectory und TIOrganization sind Profilierungen der FHIR-Ressourcen Practitioner und Organization. Die Anbieter von Fachanwendungen werden ebenfalls als TIOrganization-Einträge im FHIR-Directory eingetragen um Daten der Fachanwendung zu dieser Organisation zuordnen zu können.

Der Besitzer einer Telematik-ID erhält das Recht seinen Eintrag zu erweitern (um z. B. Unterstrukturen für eine Organisation einzutragen) und Fachdaten zu ergänzen (z. B. TI-Messenger-Adressen). Die von den Kartenherausgebern eingetragenen Daten dürfen durch die Besitzer nicht verändert werden. Zusätzliche FHIR-Ressourcen (wie z. B. Location und HealthcareService) können durch die Besitzer ergänzt werden, um den Komfort bei der Suche nach Einträgen zu erhöhen.

Alle vom VZD-FHIR-Directory bereitgestellten Schnittstellen sind über das Internet erreichbar und TLS-gesichert. Die Authentisierung erfolgt mit:

- OpenID Connect Authorization Code Flow für Schreibzugriffe der Besitzer von Einträgen
- OAuth2 Client Credential Flow für Schreibzugriffe der Fachdienste
- Matrix-OpenID-Token für Lesezugriffe von TI-Messenger-Nutzern

Eine Nutzung der Schnittstellen des VZD-FHIR-Directory ohne Authentisierung der Nutzer ~~ist nicht zulässig~~MUSS durch das VZD-FHIR-Directory verhindert werden.

Als erste Anwendung wird der TI-Messenger-Dienst das VZD-FHIR-Directory nutzen.

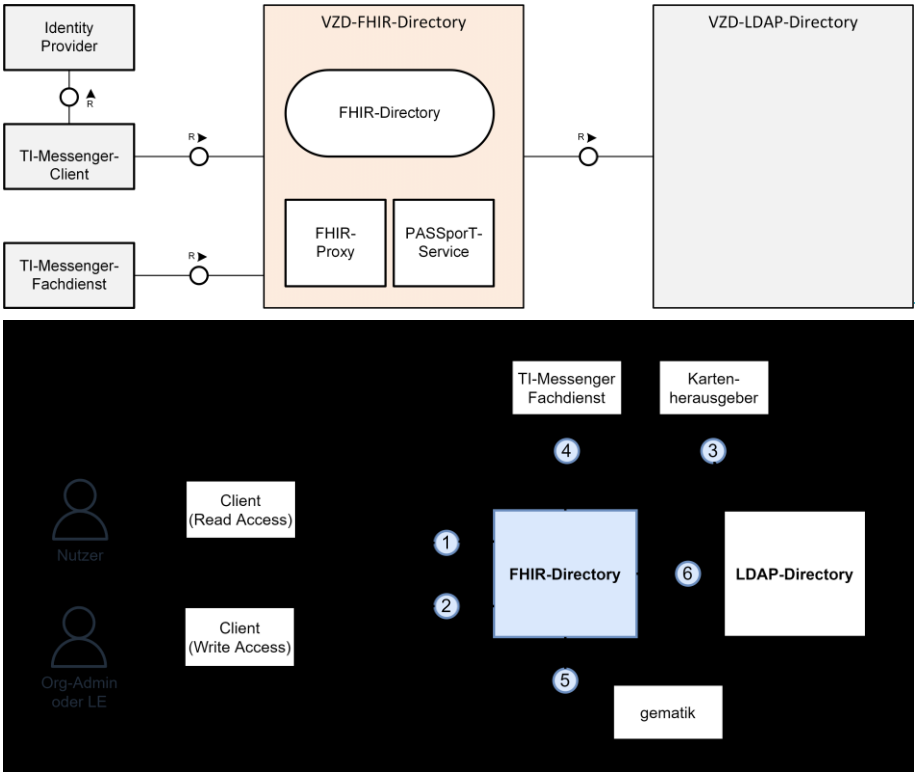


Abbildung 1: Systemüberblick VZD-FHIR-Directory

~~Das VZD-FHIR-Directory besteht aus den logischen Komponenten FHIR-Directory, FHIR-Proxy und PASSporT-Service.~~

Das FHIR-Directory ist eine Implementierung der FHIR-Spezifikation (http://hl7.org/fhir/summary.html).

~~Der FHIR-Proxy terminiert die TLS-Verbindungen, prüft die Zugriffsberechtigung der Nutzer und verteilt die Anfragen der Nutzer auf die Instanzen des FHIR-Directory sowie des PASSporT-Service. Zusätzlich übernimmt und aktualisiert der FHIR-Proxy die Basiseinträge im VZD-FHIR-Directory mit den geänderten Daten des VZD-LDAP-Directories.~~

~~Der PASSporT-Service ist eine Komponente, die Personal-Assertion-Token gemäß [RFC8225] ausstellt. Die Token bestätigen, dass ein Leistungserbringer oder eine Organisation durch die Eintragung der TI-Messenger-Adresse im VZD-FHIR-Directory damit einverstanden ist, dass eine TI-Messenger-Kommunikation zu dieser Adresse aufgebaut werden darf. Für die Signatur des PASSporT wird ein Zertifikat aus der Komponenten-PKI der TI verwendet.~~

~~3 Systemkontext~~

~~3.1 Akteure und Rollen~~

~~Das VZD-FHIR-Directory ist ein Dienst der Telematikinfrastruktur und kann von allen Nutzern der TI abgefragt werden. Zusätzlich ist es erforderlich, dass die Einträge gepflegt werden. Dies erfolgt durch die Kartenherausgeber, die Fachanwendungen, falls spezifische Fachdaten den Einträgen zugeordnet sind, und optional durch die Besitzer der Einträge.~~

2.1 Nutzer und Rollen

Tabelle 1: ~~VZD_FHIR_Directory_Akteure_und_~~Nutzer und Rollen

~~Akteur~~	Nutzer und Rolle	Beschreibung
~~TI-Messenger-~~ Nutzer	~~User~~	~~TI-Messenger-~~ Alle Nutzer ~~sind Leistungserbringer, Mitarbeiter in Organisationen des Gesundheitswesens und Versicherte. Sie~~ können im ~~Rahmen der Fachanwendung TI-Messenger Einträge im VZD~~ FHIR-Directory ~~lesen.~~über die Schnittstelle (1) nach Einträgen im Organisationsverzeichnis und im Personenverzeichnis suchen.
~~Besitzer~~	Org-Admin~~, Owner~~ oder LE	~~Ein Besitzer ist der Leistungserbringer oder die Organisation des Gesundheitswesens dessen bzw. deren Daten im Eintrag gespeichert sind.~~ ~~Ein Besitzer eines Eintrags im VZD-FHIR-Directory ist berechtigt, ihm zugeordnete Attribute in eigenen Eintrag anzulegen, zu ändern, zu löschen und zu lesen.~~Administratoren der Organisationen und LE können im FHIR-Directory über die Schnittstelle (2) ihren Eintrag im Organisationsverzeichnis ändern und um zusätzliche Ressourcen erweitern.
~~Kartenherausgeber~~	~~Admin_Base_Entry~~	~~Kartenherausgeber sind berechtigt, Basiseinträge für von ihnen mit Telematik-IDs ausgestattete Leistungserbringer und Organisationen des Gesundheitswesens anzulegen, zu bearbeiten, zu lesen und zu löschen.~~

Gelöschte Zellen

Gelöschte Zellen

Gelöschte Zellen

Fachanwendung	Admin_Application_Data	Die Fachanwendung ist ein generischer Akteur. Fachanwendungen sind berechtigt, ihnen zugeordnete Attribute von Einträgen im Directory anzulegen, zu ändern und zu löschen. Sie sind im Rahmen ihrer Aufgabe berechtigt, die Einträge zu lesen.
TI-Messenger-Registrierungsdienst	Admin_TI_Messenger_Data	Der TI-Messenger-Registrierungsdienst ist berechtigt, einen TIOrganization-Eintrag anzulegen. Der Admin_TI_Messenger_Data KANN Endpoint-Einträge anlegen, in denen die von ihm verwalteten TI-Messenger-Domains eingetragen sind. Die Endpoint-Einträge MÜSSEN mit dem eigenen TIOrganization-Eintrag verlinkt sein.
Gesamtverantwortlicher TI	GTI	Die gematik als Gesamtverantwortlicher TI und damit für den sicheren, funktionalen und interoperablen Betrieb der Anwendungen und Komponenten erhält im Rahmen des Monitorings und Reporting sowohl Informationen über die technischen Vorgänge als auch über die Datenbestände innerhalb des Dienstes.

3.2 User Stories

- Als TI-Messenger-Nutzer möchte ich komfortabel nach Leistungserbringern und Organisationen suchen können, so dass ich keine Zeit und Nerven damit verschwenden muss, einen geeigneten TI-Messenger-Kommunikationspartner zu finden.
- Als TI-Messenger-Nutzer möchte ich die Ortungsfunktion meines Geräts nutzen können, um nahegelegene Leistungserbringer und Organisationen finden zu können, so dass ich spontan den für mich bestgelegene Organisation auswählen kann.
- Als TI-Messenger-Nutzer möchte ich in der Lage sein, Organisationen herauszufiltern, die gerade geöffnet haben oder die bald öffnen werden, so dass ich nicht vor verschlossenen Türen stehe, wenn ich die Organisation aufsuchen will.

- ~~Als TI-Messenger-Nutzer möchte ich in der Lage sein, mir von meiner bevorzugten Navigations-App eine Route zur ausgewählten Organisation berechnen zu lassen, so dass ich nicht Adressen in meine Navigations-App kopieren muss, um den Weg zu finden.~~
- ~~Als TI-Messenger-Nutzer möchte ich, dass die Suchfunktion meiner App fehlertolerant ist, wenn ich mich beim Eingeben des Organisationsnamens vertippe oder es mehrere Organisationen mit ähnlichem Namen gibt.~~
- ~~Als TI-Messenger-Nutzer möchte ich in meiner App verschiedene Such- und Filterfunktionen kombinieren können wie z.B. die Ortungsfunktion und die Filterung nach Öffnungszeiten, um eine Organisation zu finden.~~
- ~~Als TI-Messenger-Nutzer möchte ich weitere Informationen zu einer Organisation erhalten, um mich mit ihr in Verbindung setzen bzw. über sie informieren zu können (z.B. TI-Messenger-Adresse, Webseite, E-Mail-Adresse, Telefonnummer, Fax).~~
- ~~Als Besitzer eines Eintrags im VZD-FHIR-Directory, brauche ich einen supportverantwortlichen Ansprechpartner mit entsprechenden Serviceleveln für die technische Schnittstelle.~~
- ~~Als Kartenherausgeber brauche ich eine einfache (technische) Möglichkeit, die Daten für die ich verantwortlich bin, im VZD-FHIR-Directory editieren zu können (einstellen, lesen, verändern, löschen).~~
- ~~Als Kartenherausgeber brauche ich einen supportverantwortlichen Ansprechpartner mit entsprechenden Serviceleveln für die technische Schnittstelle.~~
- ~~Als Kartenherausgeber möchte ich komfortabel und in angemessener Antwortzeit nach Leistungserbringern bzw. Organisationen in meinem Verantwortungsbereich suchen können, so dass ich keine Zeit und Nerven damit verschwenden muss, die Einträge adäquat verwalten zu können.~~
- ~~Als Kartenherausgeber möchte ich meinen Account zum VZD-FHIR-Directory komfortabel erhalten und verwalten können, so dass ich keine Zeit und Nerven damit verschwenden muss.~~
- ~~Als Kartenherausgeber möchte ich, dass bei einem Ausfall oder Störungen des VZD-FHIR-Directory die Nutzer und die Kartenherausgeber entsprechendes Feedback und Support erhalten und ggf. Fehlermeldungen korrekt eingestellt und weitergeleitet werden.~~
- ~~Als Anbieter einer Fachanwendung brauche ich eine einfache (technische) Möglichkeit, die fachlichen Daten meiner Fachanwendung im VZD-FHIR-Directory editieren zu können (einstellen, lesen, verändern, löschen).~~
- ~~Als Anbieter einer Fachanwendung brauche ich einen supportverantwortlichen Ansprechpartner mit entsprechenden Serviceleveln für die technische Schnittstelle.~~
- ~~Als Gesamtverantwortlicher für die TI möchte ich steuern können, wer einen Zugriff auf die Pflegeschnittstelle des VZD-FHIR-Directory erhält und jederzeit eine aktuelle Übersicht für alle Umgebungen (RU/TU/PU) haben.~~
- ~~Als Gesamtverantwortlicher für die TI möchte ich jederzeit wissen, welche Daten im VZD-FHIR-Directory hinterlegt sind und ob diese korrekt sind bzw. Fehlermeldungen vorliegen.~~

- ~~Als Gesamtverantwortlicher für die TI möchte ich, dass nur berechtigte Institutionen für die Pflege der Informationen im VZD-FHIR-Directory die entsprechenden Berechtigungen (er)halten.~~
- ~~Als Gesamtverantwortlicher für die TI muss ich sicherstellen, dass bei einem Ausfall oder Störungen des VZD-FHIR-Directory die Nutzer und die Kartenherausgeber entsprechendes Feedback und Support erhalten und ggf. Fehlermeldungen korrekt eingestellt und weitergeleitet werden.~~

Tabelle 2: Kommunikationsbeziehungen zu IT-Systemen

IT-Systeme	Beschreibung
Kartenherausgeber	Die Kartenherausgeber nutzen die Schnittstelle (3) um die Einträge ihrer Mitglieder im LDAP-Directory und zukünftig im FHIR-Directory zu pflegen.
TI-Messenger-Anbieter	Die TI-Messenger-Anbieter nutzen die Schnittstelle (4) um die Föderationsliste des TI-Messengers abzufragen und um die Domains der von ihnen betriebenen Messenger-Services als Teil der TI-Messenger Föderation zu verwalten.
gematik	Die gematik kann über die Schnittstelle (5) lesend auf die Einträge im FHIR-Directory und im LDAP-Directory zugreifen um die Daten-Qualität der Einträge zu prüfen und um Fehler zu analysieren.
LDAP-Directory	Die Schnittstelle (6) zwischen FHIR-Directory und LDAP-Directory wird vom Verzeichnisdienst genutzt, um die Einträge zu synchronisieren.

Alle Schnittstellen mit Ausnahme (6) sind über das Internet erreichbar. Die Schnittstellen stellen folgende Funktionen bereit:

1. Für Nutzer gibt es eine Schnittstelle zur Suche nach Einträgen im FHIR-Directory Organisationsverzeichnis und Personenverzeichnis. Die Schnittstelle kann nur nach erfolgreicher Authentisierung genutzt werden. Alle TI-Messenger Nutzer können sich authentisieren und bekommen vom FHIR-Directory ein Accesstoken ausgestellt, dass für die Suchanfragen verwendet wird. Die Suche ermöglicht es komfortabel nach Volltext oder nach bestimmten Werten der einzelnen Attribute über die verlinkten Ressourcen zu suchen. Gefundene Ressourcen werden in einem Bundle von FHIR Ressourcen zurück geliefert. Das Datenformat ist json.
2. Für Administratoren der Organisationen des Gesundheitswesens und für LE gibt es eine Schnittstelle zur Änderung Ihres Eintrags im Organisationsverzeichnis. Zur Nutzung der Schnittstelle ist eine Authentifizierung mit OIDC Authorization Code Flow erforderlich. Über diese Schnittstelle kann im Organisationsverzeichnis der eigene Eintrag der Organisation über eine Verlinkung um zusätzliche Einträge erweitert werden. TI-Messenger Nutzer die auch LE sind, können diese Schnittstelle nutzen, um ihre TI-Messenger-Adresse in ihrem Eintrag im Personenverzeichnis zu speichern, sodass sie von anderen LE gefunden werden können. Auch hier erfolgt die Authentifizierung über OIDC. Das FHIR-Datenformat ist json.

3. Für Kartenherausgeber gibt es eine die Schnittstelle I_Directory_Administration um Einträge im LDAP-Directory anzulegen und zu pflegen. Das Datenformat ist json und ist in der OpenAPI-yaml-Datei DirectoryAdministration.yaml festgelegt. Zukünftig ist vorgesehen, dass die Kartenherausgeber auch direkt die Schnittstelle zum FHIR-Directory nutzen können. Dann ist das Datenformat FHIR in der Ausprägung JSON. Die Authentifizierung der Kartenherausgeber erfolgt mit OAuth Client Credential Flow.
4. TI-Messenger-Fachdienste pflegen im FHIR-Directory für die von ihnen angebotenen Messenger-Services die TI-Messenger-Domänen. Zusätzlich können die TI-Messenger-Anbieter die Föderationsliste abfragen. Sie beinhaltet alle an der Föderation des TI-Messengers beteiligte Domains. Um die Kommunikationskontrolle zu ermöglichen, fragen TI-Messenger-Fachdienste auch ab, in welchem Verzeichnis (Personen- oder Organisationsverzeichnis) sich die Hashes von TI-Messenger-Adressen befinden. Die Authentifizierung der TI-Messenger-Fachdienste erfolgt mit OAuth Client Credential Flow.
5. Die gematik hat Schnittstellen, um die Daten-Qualität der Einträge zu prüfen. Dazu wird die Schnittstelle der Kartenherausgeber genutzt. Die gematik hat aber nur Leserechte.
6. Die Einträge im LDAP-Directory werden in das FHIR-Directory Organisations- und Personenverzeichnis synchronisiert. Es handelt sich um eine interne Schnittstelle des Verzeichnisdienstes der TI.

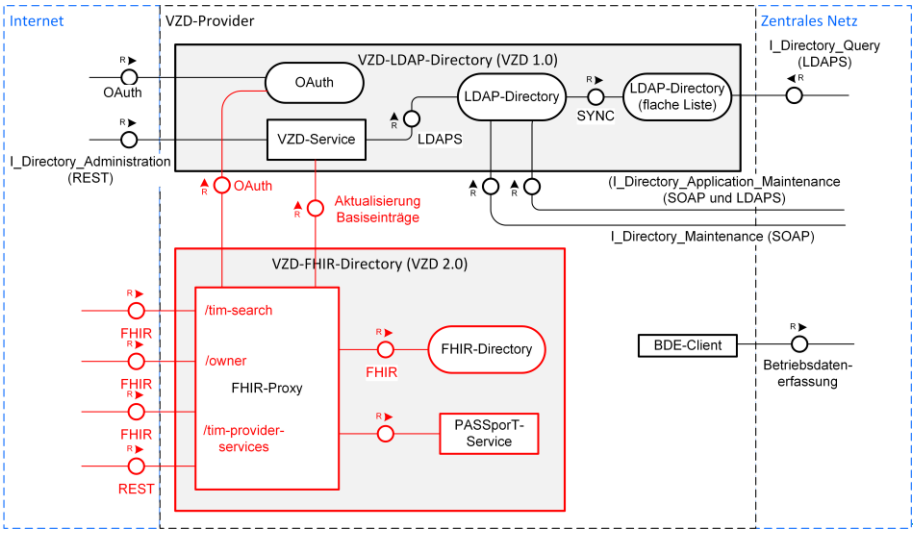
~~3.3~~2.2 Nachbarsysteme

Die Nachbarsysteme des VZD-FHIR-Directory sind Client- und Serverkomponenten des TI-~~Messengers~~Messenger-Dienstes, das VZD-LDAP-Directory, die IDPs aus der TI-IDP-Föderation und die Betriebsdatenerfassung der gematik.

ML-123876 **- Test gegen die Referenzimplementierung der Nachbarsysteme (VZD-FHIR-Directory)**
Es MÜSSEN alle Anwendungsfälle des VZD-FHIR-Directories erfolgreich gegen die Referenzimplementierung der Nachbarsysteme getestet sein.
[<=]

43 Zerlegung des Produkttyps

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



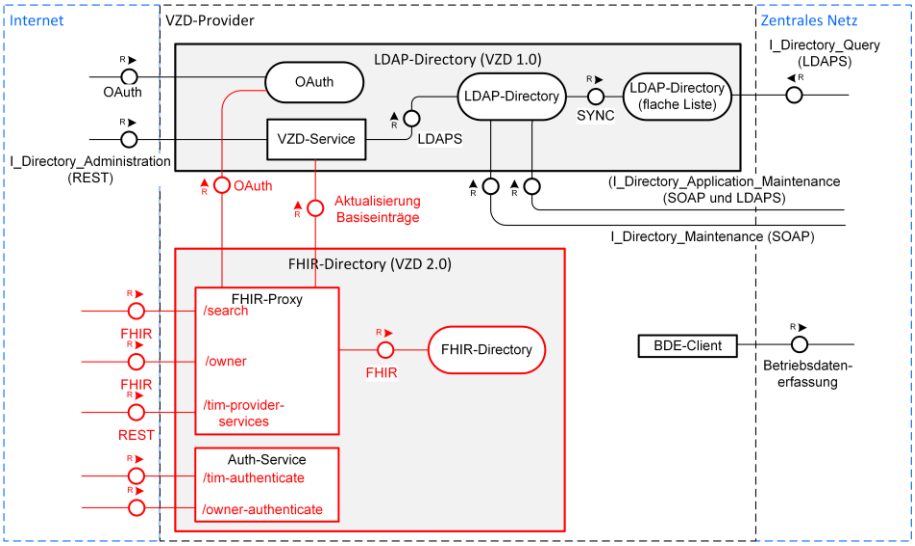


Abbildung 2: Zerlegung des VZD

Das VZD-FHIR-Directory besteht aus den Komponenten FHIR-Proxy und FHIR-Directory sowie ~~PASSPorT~~Auth-Service. ~~Die Schnittstelle zwischen FHIR-Proxy und PASSporT-Service wird nicht vorgegeben.~~

Die vom VZD-FHIR-Directory zu liefernden Rohdaten zur Ermittlung der Auslastung und Performance werden in den bereits vorhandenen Betriebsdaten-Erfassungs-Client (BDE-Client) des Verzeichnisdienstes integriert.

~~5~~4 Funktionsmerkmale

In diesem Kapitel werden die Komponenten des VZD-FHIR-Directories beschrieben.

~~5.1~~4.1 FHIR-Directory

Das FHIR-Directory ist eine Implementierung der HL7-FHIR-Spezifikation Release 4.0.1 (https://www.hl7.org/fhir/http.html).

Das FHIR-Directory ist nur über den FHIR-Proxy erreichbar.

~~5.1.1~~4.1.1 Datenmodell

Es werden die FHIR-Ressourcen nach folgender Tabelle verwendet.

Alle Änderungen und Erweiterungen der FHIR Ressourcen sind in https://simplifier.net/vzd-fhir-directory veröffentlicht.

Tabelle 3: VZD-FHIR-Directory, FHIR-Ressourcen

FHIR-Ressource	Beschreibung
~~TIOrganization~~Organization in gematik Directory (OrganizationDirectory)	Profil der Organization Ressource. (~~https://simplifier.net/vzd-fhir-directory/tiorganization~~)https://simplifier.net/vzd-fhir-directory/organizationdirectory) Das Element Identifier wurde so geändert, dass Telematik-IDs als Identifier verwendet werden können ~~(https://gematik.de/fhir/VZD-FHIR-Directory/NamingSystem/TelematikID).~~. Im Element type wird der Typ der Organisation eingetragen. Dafür werden die CodeSysteme ~~https://gematik.de/fhir/VZD-FHIR-Directory/CodeSystem/TIOrganizationTypeCS und https://gematik.de/fhir/VZD-FHIR-Directory/CodeSystem/TIProfessionOidCS sowie das ValueSet https://gematik.de/fhir/VZD-FHIR-Directory/ValueSet/TIOrganizationTypeVS verwendet.~~ ~~Im Element telecom KANN der Besitzer eines TIOrganisation Eintrags oder eines TIPractitioner Eintrags TI-Messenger-Adressen (MXID) in url-Notation speichern (telecom.system = url; telecom.value = MXID in url Notation matrix:u/localpart:tim-domain).~~ ~~Mit telecom.period.end lässt sich steuern, ob der Besitzer einverstanden ist, dass andere TI-Messenger-Nutzer mit der in telecom.value gespeicherten MXID Kontakt aufnehmen dürfen.~~ ~~telecom.period.end = leer oder Datum in der Zukunft bedeutet: Kontaktaufnahme ist erlaubt~~

	~~telecom.period.end = Datum in der Vergangenheit bedeutet: Kontaktaufnahme ist nicht erlaubt (gilt nur, wenn die MXID im VZD-FHIR-Directory gesucht wurde).~~ ~~Durch den Besitzer erstellte TIOrganisations-Einträge MÜSSEN mit seinem TIOrganisations-Eintrag über eine partOf-Referenz verlinkt sein~~https://simplifier.net/vzd-fhir-directory/organizationprofessionoid und https://simplifier.net/vzd-fhir-directory/practitionerprofessionoid sowie das ValueSet https://simplifier.net/vzd-fhir-directory/organizationtypevs verwendet. Wenn das Element type den Wert "TI-Messenger-Provider" hat, dann handelt es sich um eine Organisation, die einen TI-Messenger-Dienst innerhalb der Telematikinfrastruktur bereitstellt. In endpoint-Referenzen der Organisation werden die Domainnamen der TI-Messenger-Service-Instanzen eingetragen. Dazu wird im Element connectionType das Codesystem ~~https://gematik.de/fhir/VZD-FHIR-Directory/CodeSystem/TIMessengerCS mit~~https://simplifier.net/vzd-fhir-directory/endpointconnectiontype mit code value="tim-domain" display value="TI-Messenger domain name" verwendet. Im Element "name" wird der TI-Messenger Domainname eingetragen. In "managingOrganization" wird die ~~TIOrganization~~OrganizationDirectory eingetragen, für die die TI-Messenger-Domain eingerichtet wurde.
~~TIPractitioner~~Practitioner in gematik Directory (PractitionerDirectory)	Profil der Practitioner Ressource. Lediglich das Element Identifier wurde so geändert, dass Telematik-IDs als Identifier verwendet werden können. ~~(~~ ~~https://simplifier.net/vzd-fhir-directory/tipractitioner)~~(https://simplifier.net/vzd-fhir-directory/practitionerdirectory)
Endpoint in gematik Directory (EndpointDirectory)	~~Endpoint Ressource (~~ ~~https://www.hl7.org/fhir/endpoint.html)~~Endpoint Ressource (https://simplifier.net/vzd-fhir-directory/endpointdirectory)
Location in gematik Directory (LocationDirectory)	~~Location (~~ ~~https://www.hl7.org/fhir/location.html)~~Location (https://simplifier.net/vzd-fhir-directory/locationdirectory)

HealthcareService in gematik Directory (HealthcareServiceDirectory)	~~HealthcareService (~~ ~~https://www.hl7.org/fhir/healthcareservice.html)~~Healthcare Service (https://simplifier.net/vzd-fhir-directory/healthcareservicedirectory)
PractitionerRole in gematik Directory (PractitionerRoleDirectory)	~~PractitionerRole (~~ ~~https://www.hl7.org/fhir/practitionerrole.html)~~PractitionerRole (https://simplifier.net/vzd-fhir-directory/practitionerroledirectory)

ML-123880 **- Einschränkung der nutzbaren FHIR-Ressourcen (VZD-FHIR-Directory)**
Nur die in Tabelle "VZD-FHIR-Directory, FHIR-Ressourcen" angegebenen Ressourcen dürfen im VZD-FHIR-Directory erzeugt werden.**[<=]**

~~5.1.2~~4.1.2 Mapping von LDAP auf FHIR-Ressourcen

Die ~~TIOrganization~~OrganizationDirectory- und ~~TIPractitioner~~PractitionerDirectory-Basiseinträge werden durch den FHIR Proxy mit den Daten aus dem VZD-LDAP-Directory initial erzeugt und anschließend fortlaufend aktualisiert. Die synchronisierten Daten können nicht durch die Besitzer (Leistungserbringer und Organisationen) geändert werden.

Die Daten aus dem VZD-LDAP-Directory werden wie folgt den FHIR-Ressourcen zugeordnet~~:~~: https://github.com/gematik/api-vzd/blob/master/docs/LDAP2FHIR_Sync.adoc

~~**Tabelle 3: VZD-FHIR-Directory_Mapping_LDAP_to_FHIR**~~

~~**LDAP-Eintragstyp**~~	~~**LDAP-Attribut**~~	~~**FHIR-Ressource**~~	~~**FHIR-Element**~~
~~HBA und SMC-B~~	~~givenName~~	~~–~~	~~–~~
~~HBA und SMC-B~~	~~sn~~	~~–~~	~~–~~
~~HBA und SMC-B~~	~~cn~~	~~–~~	~~–~~
~~HBA und SMC-B~~	~~displayName~~	~~TIPractitioner TIOrganization~~	~~name = displayName~~
~~HBA und SMC-B~~	~~streetAddress, postalCode, countryCode, localityName,~~	~~TIPractitioner TIOrganization~~	~~address. use = work address.type = postal address.text = "streetAddress
postalCode
localityName
~~

	~~stateOrProvinceName~~		~~stateOrProvinceName
countryCode"~~ ~~address.line="streetAddress"~~ ~~address.city = localityName~~ ~~address.state = stateOrProvinceName~~ ~~address.postalCode = postalCode~~ ~~address.country = countryCode~~
	~~title~~		
~~SMC-B~~	~~organization~~	~~TIOrganization~~	~~alias = organization~~
~~HBA~~	~~organization~~	~~–~~	~~–~~
~~HBA und SMC-B~~	~~otherName~~	~~–~~	~~–~~
~~SMC-B~~	~~specialization Format urn:psc:<OID Codesystem:Code>~~	~~HealthcareService~~	~~specialty.coding.system = Codesystem~~ ~~specialty.coding.code = Code~~ ~~specialty.coding.display = <added by FHIR-Proxy>~~
~~HBA~~	~~specialization Format urn:as:<OID Codesystem:Code>~~	~~TIPractitioner~~	~~qualification.code.coding.system = Codesystem~~ ~~qualification.code.coding.code = Code~~ ~~qualification.code.coding.display = <added by FHIR-Proxy>~~
~~HBA und SMC-B~~	~~domainID~~	~~–~~	~~–~~
~~HBA und SMC-B~~	~~holder~~	~~–~~	~~–~~
~~HBA und SMC-B~~	~~maxKOMLEadr~~	~~—~~	~~–~~
~~HBA und SMC-B~~	~~personalEntry~~	~~–~~	~~–~~
~~HBA und SMC-B~~	~~dataFromAuthority~~	~~–~~	~~–~~
~~HBA und SMC-B~~	~~userCertificate~~	~~TIPractitioner~~ ~~TIOrganization~~	~~telecom.system = other~~ ~~telecom.value = userCertificate (im PEM-Format)~~

~~HBA und SMC-B~~	~~entryType~~	~~–~~	~~–~~
~~HBA und SMC-B~~	~~telematikID~~	~~TIPractitioner TIOrganization~~	~~identifier.value = telematikID~~
~~SMC-B~~	~~professionOID~~	~~TIOrganization~~	~~type.coding.system = https://gematik.de/fhir/VZD-FHIR-Directory/CodeSystem/TIProfessionOidCS type.coding.code = professionOID type.coding.display = display aus https://gematik.de/fhir/VZD-FHIR-Directory/ValueSet/TIOrganizationTypeVS~~
~~HBA und SMC-B~~	~~usage~~	~~–~~	~~–~~
~~HBA und SMC-B~~	~~description~~	~~–~~	~~–~~
~~HBA und SMC-B~~	~~mail~~	~~–~~	~~––~~
~~HBA und SMC-B~~	~~KOM-LE-Version~~	~~––~~	~~–~~
~~HBA und SMC-B~~	~~changeDateTime~~	~~–~~	~~–~~

~~5.1.3~~4.1.3 FHIR RESTful API

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

Die Anzahl der mittels /search Operation gefundenen und zurückgegebenen Einträge wird initial auf 100 begrenzt. Dieser Wert MUSS konfigurierbar sein. Die zurückgegebenen Einträge werden in einem FHIR-Ressource-Bundle zusammengefasst. Im Attribut Bundle.total MUSS die Gesamtanzahl der gefundenen Einträge (total number of matches) zurück gegeben werden.

Zusätzlich MUSS konfigurierbar sein, ob Paging eingesetzt wird und wie groß die page_size ist. Paging ist initial eingeschaltet mit page_size = 10. Wenn eine Suche mehr Treffer enthält, als in page_size angegeben, dann enthält die Response ein bundle mit den gefundenen Einträgen gemäß page_size und einen Link auf die nächste page.

~~5.2~~4.2 FHIR-Proxy ~~und PASSporT Service~~

~~5.2.1~~4.2.1 Schnittstellen

~~5.2.1.1~~4.2.1.1 TLS-Verbindungsaufbau

Der FHIR-Proxy MUSS sich beim TLS-Verbindungsaufbau an den Endpunkten gegenüber Clients mit einem Extended Validation TLS-Zertifikat eines Herausgebers gemäß [CAB-Forum] authentisieren. Das Zertifikat MUSS an die Schnittstelle des Eingangspunkts für Clientsysteme gebunden werden, damit Clientsysteme beim TLS-Verbindungsaufbau eine vereinfachte Zertifikatsprüfung mit TLS-Standardbibliotheken durchführen können.

~~5.2.1.2~~4.2.1.2 FHIR Schnittstelle für TI-Messenger-Nutzer

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

In der Produktionsumgebung ist die URL: ~~https://vzd-fhir-directory.vzd.ti-dienste.de/tim-search~~https://fhir-directory.vzd.ti-dienste.de/search

In der Referenzumgebung ist die URL: ~~https://ru-vzd-fhir-directory-test.vzd.ti-dienste.de/tim-search~~https://fhir-directory-ref.vzd.ti-dienste.de/search

In der Testumgebung ist die URL: ~~https://tu-vzd-fhir-directory-test.vzd.ti-dienste.de/tim-search~~https://fhir-directory-test.vzd.ti-dienste.de/search

Authentisierung

Um die Schnittstelle nutzen zu können MÜSSEN sich die Clients mit einem gültigen ~~Accesstoken~~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~~,~~ (tim-accesstoken), dass für Suchanfragen des TI-Messenger-Clients verwendet wird. Die Gültigkeitsdauer ist 24 Stunden.

Das Accesstoken enthält folgende Attribute:

```
{
  "iss": "https://vzd-fhir-directory.vzd.ti-dienste.de/tim-
authenticate",
  "sub": "<MXID des TI-Messenger-Nutzers in url Notation>",
  "aud": [ "https://vzd-fhir-directory.vzd.ti-dienste.de/tim-
search"],
  "iat": 1630306800,
  "exp": 1630393200,
  "scope": "tim-search"
}
```

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.

Endpunkte für die Authentisierung

In der Produktionsumgebung ist die URL: ~~https://vzd-fhir-directory.vzd.ti-dienste.de/tim-authenticate~~https://fhir-directory.vzd.ti-dienste.de/tim-authenticate

In der Referenzumgebung ist die URL: ~~https://ru-vzd-fhir-directory-test.vzd.ti-dienste.de/tim-authenticate~~https://fhir-directory-ref.vzd.ti-dienste.de/tim-authenticate

In der Testumgebung ist die URL: ~~https://tu-vzd-fhir-directory-test.vzd.ti-dienste.de/tim-authenticate~~https://fhir-directory-test.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.

~~**PASSporT-Service**~~

~~Das VZD-FHIR-Directory MUSS für alle gefundenen MXIDs PASSporT erzeugen und in die Response einfügen (siehe AF_10036).~~

~~Der Aufbau des PASSporT MUSS wie im RFC[8225] beschrieben erfolgen. Die Befüllung der gezeigten Header-Elemente MUSS wie im RFC[8225] gefordert erfolgen und wie folgt aufgebaut sein:~~

```
Header:
  {
    "typ":"passport",
    "alg":"ES256",
    "x5u":"https://cert.example.org/passport.cer"
  }
```

~~Die TI-Messenger-spezifischen PASSporT-Claims sind durch den PASSporT-Service wie folgt zu befüllen. Der Claim mit dem Bezeichner "orig" ist die MXID des Nutzers der den GET /tim_search Request ausgeführt hat. Der Claim "dest" wird mit der MXID des gefundenen Eintrags befüllt. Die MXIDs werden in url-Notation angegeben. Das folgende Beispiel zeigt eine solche Struktur.~~

```
Claims:
  {
    "orig": {
        "uri": "matrix:u/me:example.org"
    },
    "dest": {
        "uri": [
            "matrix:u/you:example.org"
        ]
    }
  }
```

~~Dieses erzeugte PASSporT wird dann durch den PASSporT-Service signiert und anschließend an die gefundene MXID angefügt (matrix:u/you:example.org~~**~~/?PASSporT=[PASSporT-String])~~**~~.~~

~~Die ausgestellten PASSporT werden mit einem Zertifikat aus der Komponenten-PKI der TI signiert. Die Zertifikate haben die keyUsage = digitalSignature.~~

~~5.2.1.3~~4.2.1.3 FHIR-Schnittstelle für Besitzer

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 (~~TIPractitioner~~PractitionerDirectory oder ~~TIOrganization~~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 ist die URL: ~~https://vzd-fhir-directory.vzd.ti-dienste.de/owner~~https://fhir-directory.vzd.ti-dienste.de/owner

In der Referenzumgebung ist die URL: ~~https://ru-vzd-fhir-directory-test.vzd.ti-dienste.de/owner~~https://fhir-directory-ref.vzd.ti-dienste.de/owner

In der Testumgebung ist die URL: ~~https://tu-vzd-fhir-directory-test.vzd.ti-dienste.de/owner~~https://fhir-directory-test.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 ~~TIOrganization~~OrganizationDirectory-Eintrag KÖNNEN weitere ~~TIOrganization~~OrganizationDirectory-Einträge erstellt und mit dem eigenen Eintrag verlinkt werden.

Das Accesstoken enthält folgende Attribute:

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"],
  "iat": 1630306800,
  "exp": 1630393200~~,~~
~~  "scope": "owner"~~
~~}~~
}
```

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.

Endpunkte für die Authentisierung

In der Produktionsumgebung ist die URL: ~~https://vzd-fhir-directory.vzd.ti-dienste.de/owner-authenticate~~ https://fhir-directory.vzd.ti-dienste.de/owner-authenticate

In der Referenzumgebung ist die URL: ~~https://ru-vzd-fhir-directory-test.vzd.ti-dienste.de/owner-authenticate~~https://vzd-fhir-directory-ref.vzd.ti-dienste.de/owner-authenticate

In der Testumgebung ist die URL: ~~https://tu-vzd-fhir-directory-test.vzd.ti-dienste.de/owner-authenticate~~https://vzd-fhir-directory-test.vzd.ti-dienste.de/owner-authenticate

Operationen

Die FHIR-Operationen für das Ändern von eigenen Einträgen im VZD-FHIR-Directory sind in der HL7-FHIR-Spezifikation (https://www.hl7.org/fhir/http.html) festgelegt.

~~5.2.1.~~4.2.1.4 Schnittstelle I_VZD_TIM_Provider_Services

Endpunkte

In der Produktionsumgebung ist die URL: ~~https://vzd-fhir-directory.vzd.ti-dienste.de/tim-provider-services~~ https://fhir-directory.vzd.ti-dienste.de/tim-provider-services

In der Referenzumgebung ist die URL: ~~https://ru-vzd-fhir-directory-test.vzd.ti-dienste.de/tim-provider-services~~https://fhir-directory-ref.vzd.ti-dienste.de/tim-provider-services

In der Testumgebung ist die URL: ~~https://tu-vzd-fhir-directory-test.vzd.ti-dienste.de/tim-provider-services~~https://fhir-directory-test.vzd.ti-dienste.de/tim-provider-services

Authentisierung

Um die Schnittstelle nutzen zu können muss sich der Registrierungsdienst des TI-Messenger-Anbieters mit einem Accesstoken authentisieren, das vom OAuth-Server des VZD-Anbieters ausgestellt wurde. Das Accesstoken hat eine Gültigkeitsdauer von 30 Minuten.

Das Accesstoken enthält folgende Attribute:

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

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.

Endpunkte für die Authentisierung

In der Produktionsumgebung ist die URL: https://oauth.vzd.ti-dienste.de/authenticate

In der Referenzumgebung ist die URL: https://ru-oauth-test.vzd.ti-dienste.de/authenticate

In der Testumgebung ist die URL: https://tu-oauth-test.vzd.ti-dienste.de/authenticate

Registrierung

Für ~~die~~den Zugriff auf den OAuth-Server MUSS der TI-Messenger-Anbieter für seinen Registrierungsdienst beim VZD-Anbieter Client-Credentials beantragen. Die Beantragung erfolgt über einen genehmigungspflichtigen Service-Request ~~an betrieb@gematik.de mit dem Betreff "VZD FHIR Directory (De)/Registrierung" notwendig~~im TI-ITSM-System.

Die Registrierung und Vergabe der Credentials erfolgt dabei auf ~~Organisationsebene~~Anbieterebene.

Der Antrag MUSS folgende Informationen enthalten um weiter bearbeitet werden zu können:

- Angaben zur Rolle (hier ~~Admin~~ TI ~~-~~ Messenger ~~Data)~~ -Anbieter) und Organisation des Antragstellers, Erläuterung der Berechtigung und des Bedarfs (zur Verifikation notwendig)
- Kontaktdaten zu Ansprechpartnern beim Antragsteller (2 Personen) inkl. Telefonnummer, E-Mail-Adresse, Anschrift
- Angabe der Betriebsumgebung (RU/PU)
- E-Mail-Adresse und dazugehöriges S/MIME-Zertifikat (in einer ZIP-Datei als Anhang) an welche die Zugangsdaten verschlüsselt übermittelt werden können (kostenlose Zertifikate sind z.B. beim DGN erhältlich)
- falls bereits vorhanden, eine entsprechende Ticketnummer
- nur bei Deregistrierung durch den Antragsteller: vorab vergebene Client-ID
- gewünschte Bezeichnung im OAuth2-Server ID_TOKEN claim scope

Nach Prüfung der Angaben, werden die Zugangsdaten direkt vom Anbieter Zentrale Plattformdienste (vgl. gemKPT_Betr) an die gewünschte E-Mail-Adresse übermittelt.

Es ist zu beachten, dass dieser Prozess ausschließlich für Neuanlagen und Löschungen vorgesehen ist. Änderungen oder der Neuversand von Zugangsdaten können nicht bearbeitet werden.

Operationen

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

~~https://github.com/gematik/api-vzd/blob/master/src/I_VZD_TIM_Provider_Services.yaml~~

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

Tabelle 4: Tab_VZD_TIM-Provider-Services_Operations

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

GET /FederationList/federationList.json	Mit dieser Operation wird die Liste der an der TI-Messenger-Föderation beteiligten Matrix-Domainnamen abgefragt (Föderationsliste).
GET /~~PASSporTCertificates~~localization "whereIs"	~~Mit dieser Operation werden die PASSporT-Signatur-Zertifikate abgefragt.~~ Gibt für den übergebenen Hash einer MXID den Teil des Directories zurück, in dem die MXID enthalten ist.
POST /federation "addTiMessengerDomain"	Eine Domaine zur Föderation hinzufügen.
GET /federation "getTiMessengerDomain"	Lesen einer oder aller eigener Domains.
PUT /federation "updateTiMessengerDomain"	Aktualisierung einer Domaine.
DELETE /federation "deleteTiMessengerDomain"	Löschen einer Domaine.
~~GET, POST, PUT, DELETE /FHIR~~GET /federationCheck "checkTiMessengerDomains"	~~Die FHIR-Operationen für das Ändern von eigenen TIOrganization-Einträgen und von Endpoint-Einträgen im VZD-FHIR-Directory sind in der HL7-FHIR-Spezifikation (https://www.hl7.org/fhir/http.html) festgelegt.~~ Prüft, ob alle eigenen Domains (durch Token ermittelbar) zu aktiven Organisationen gehören. Gibt die eigenen Domains zurück, die zu inaktiven Organisationen gehören.

Im Attribut "sub" des Accesstoken ist die client_id des TI-Messenger-Registrierungsdienstes enthalten. Wenn der TI-Messenger-Registrierungsdienst einen ~~TIOrganization~~OrganizationDirectory-Eintrag erzeugt, dann MUSS die client_id im Element alias des ~~Eintrage~~Eintrags enthalten sein

~~5.2.2~~4.2.2 Aktualisierung der Basiseinträge

Der FHIR-Proxy aktualisiert regelmäßig die Basiseinträge im VZD-FHIR-Directory mit den geänderten Daten des VZD-LDAP-Directories (siehe AF_10047 Einträge mit dem VZD-LDAP-Directory abgleichen). Das Intervall für die regelmäßige Aktualisierung MUSS konfigurierbar sein und wird initial auf 2 Stunden festgelegt.

Es MUSS (analog dem Background-Sync-Verfahren in die LDAP flache Liste) eine weitere Synchronisation mittels PUSH in den FHIR VZD möglich sein.

Zukünftig ist vorgesehen, dass Kartenherausgeber direkt die Basiseinträge ihrer Mitglieder im VZD-FHIR-Directory über eine FHIR-Schnittstelle verwalten können.

~~5.2.3~~4.2.3 Erzeugung und ~~Verteilung~~Bereitstellung der Föderationsliste

~~Der FHIR-Proxy~~ Die Föderationsliste MUSS bei ~~jeder~~ Änderung ~~an den Endpoint-Einträgen~~ der ~~TIM~~Domains durch TI-Messenger-Anbieter oder regelmäßig (7 Tage vor Ablauf der Gültigkeit) neu erzeugt und zum Download über die Schnittstelle I_VZD_TIM_Provider_Services~~ die Föderationsliste aktualisieren und dabei die Versionsnummer erhöhen und anschließend über ein internes Netzwerk des Anbieters auf alle FHIR-Proxy-Instanzen verteilen sowie für die Abfrage über die Schnittstelle I_VZD_TIM_Provider_Services bereithalten.~~

~~Die Föderationsliste wird vollständig erzeugt, indem alle Endpoint-Einträge abgefragt~~ bereitgestellt werden~~, die das CodeSystem connectionType.System = https://gematik.de/fhir/VZD-FHIR-Directory/CodeSystem/TIMessengerCS~~.

~~und den connectionType.code == "tim-domain" haben.~~

~~Für jeden Endpoint-Eintrag wird aus dem Wert des Elements "name" mit dem Hash-Algorithmus "SHA-256" ein hash gebildet und in~~

Die Föderationsliste ~~eingetragen. In der~~hat folgende Struktur:

```
{
  "iat": <Unix Timestamp, Zeitpunkt der Erzeugung == Beginn der
Gültigkeit>,
  "exp": <Unix Timestamp, Beginn der Gültigkeit + 30 Tage>,
  "hashAlgorithm": "sha256",
  "domainList": [
    {
      "domain": "hash der Domain",
      "isInsurance": false
    }
  ]
}
```

Die Föderationsliste MUSS mit einer JWS gemäß RFC7515 signiert werden. Der zu verwendende Signatur-Algorithmus MUSS "ES256" sein. Dazu MUSS ein Signatur-Zertifikat der Komponenten-PKI der TI (C.FD.SIG) verwendet werden. Das Signatur-Zertifikat und das ~~Element hashAlgorithm den Wert "SHA-256" haben~~ausstellende CA-Zertifikat MÜSSEN im Signatur-Header enthalten sein.

~~(siehe I_VZD_TIM_Provider_Services.yaml).~~

~~Die Aktualisierung der Föderationsliste KANN so implementiert werden, dass nur die geänderten Endpoint-Einträge in der Föderationsliste aktualisiert werden (z. B. über FHIR R4.5.1 Subscriptions; siehe https://build.fhir.org/subscription.html).~~

~~Der Anbieter des VZD-FHIR-Directories MUSS geeignete Maßnahmen vorsehen, die verhindern, dass die Föderationsliste manipuliert werden kann.~~

Der Signatur-Header hat folgende Struktur:

```
{
  "alg": "ES256",
  "x5c": [
    "<X.509 Sig-Cert, base64-encoded DER>",
```

```
    "<X.509 CA-Cert, base64-encoded DER>"
  ]
}
```

Die signierte Föderationsliste hat gemäß RFC7515 folgende Struktur:

```
{
  "payload": "<Föderationsliste, BASE64URL>",
  "signatures": [
    {
      "header":<Signatur-Header>,
      "signature":"<signature, BASE64URL>"
    }
  ]
}
```

ML-123677 **- Maßnahmen gegen die Manipulation der Föderationsliste (VZD-FHIR-Directory, Sicherheitsgutachten)**
Im Sicherheitsgutachten des VZD-FHIR-Directories sind geeignete Maßnahmen gegen die Manipulation der Föderationsliste beschrieben.**[<=]**

4.2.4 Lokalisierung einer MXID (Operation whereIs)

Der FHIR-Proxy MUSS die Lokalisierung einer MXID über Operation whereIs performant bereitstellen. Dazu MUSS der FHIR-Proxy bei jeder Änderung an den Endpoint-Einträgen (der MXID darin) die benötigten Daten für die performante Antwort der whereIs Operation aktualisieren. Der FHIR-Proxy DARF NICHT die originalen FHIR-Daten für die Ausführung der whereIs Operation durchsuchen.

~~5.3~~4.3 Übergreifende Vorgaben

~~5.3.1~~4.3.1 Sicherheit

Schutz vor Sicherheits-Risiken

Das VZD-FHIR-Directory MUSS Maßnahmen zum Schutz vor Sicherheits-Risiken gemäß der aktuellen Version der OWASP-Top-10 umsetzen (https://owasp.org/www-project-top-ten/).

Es gelten die Anforderungen an TLS-Verbindungen gemäß [gemSpec_Krypt#3.3.2] TLS-Verbindungen.

ML-123682 **- Maßnahmen zum Schutz vor Sicherheits-Risiken (VZD-FHIR-Directory, Sicherheitsgutachten)**
Im Sicherheitsgutachten des VZD-FHIR-Directories sind geeignete Maßnahmen zum Schutz vor Sicherheits-Risiken gemäß der aktuellen Version der OWASP-Top-10 beschrieben.**[<=]**

~~5.3.2~~4.3.2 Betrieb

Das VZD-FHIR-Directory wird betrieblich als eine weitere Servicekomponente im Sinne der Weiterentwicklung des Verzeichnisdienstes betrachtet. Diese Servicekomponente kann, bis auf die Schnittstellen, unabhängig vom VZD-LDAP-Directory entwickelt und deployt werden. Aus Nutzersicht ist weniger die interne, logische Struktur der Verzeichnisdienste relevant, sondern die Verfügbarkeit der Schnittstellen und die im Verzeichnis enthaltenen Daten.

Das VZD-FHIR-Directory MUSS ~~mit einer vollumfänglich funktionalen Verfügbarkeit von 99,8 % zur Hauptzeit und 99 % zur Nebenzeit betreibbar sein.~~

~~Der Anbieter des~~ die Bearbeitungszeitvorgaben unter Last aus Tab_VZD~~_~~FHIR~~_~~Directorys MUSS sein Produkt VZD-FHIR-Directory mit einer vollumfänglich funktionalen Verfügbarkeit von 99,8 % zur Hauptzeit und 99 % zur Nebenzeit betreiben~~_~~Perf unter der für alle Funktionen parallel anliegenden Spitzenlast erfüllen.

Tabelle 5: Tab_VZD_FHIR_Perf

Schnittstellenoperation	Lastvorgaben Spitzenlast [1/sec]	Bearbeitungszeitvorgaben Mittelwert [msec]	Bearbeitungszeitvorgaben 99%-Quantil [msec]
FHIR Schnittstelle für TI-Messenger-Nutzer (/search)	1000	1000	1250
FHIR-Schnittstelle für Besitzer (/owner)	20	1000	1250
Schnittstelle I_VZD_TIM_Provider_Services (/tim-provider-services)			
- getFederationList	1	1000	1250
- whereIs	50	1000	1250
- addTiMessengerDomain	1	1000	1250
- getTiMessengerDomain	1	1000	1250

- updateTiMessengerDomain	1	1000	1250
- deleteTiMessengerDomain	1	1000	1250
- checkTiMessengerDomains	1	1000	1250

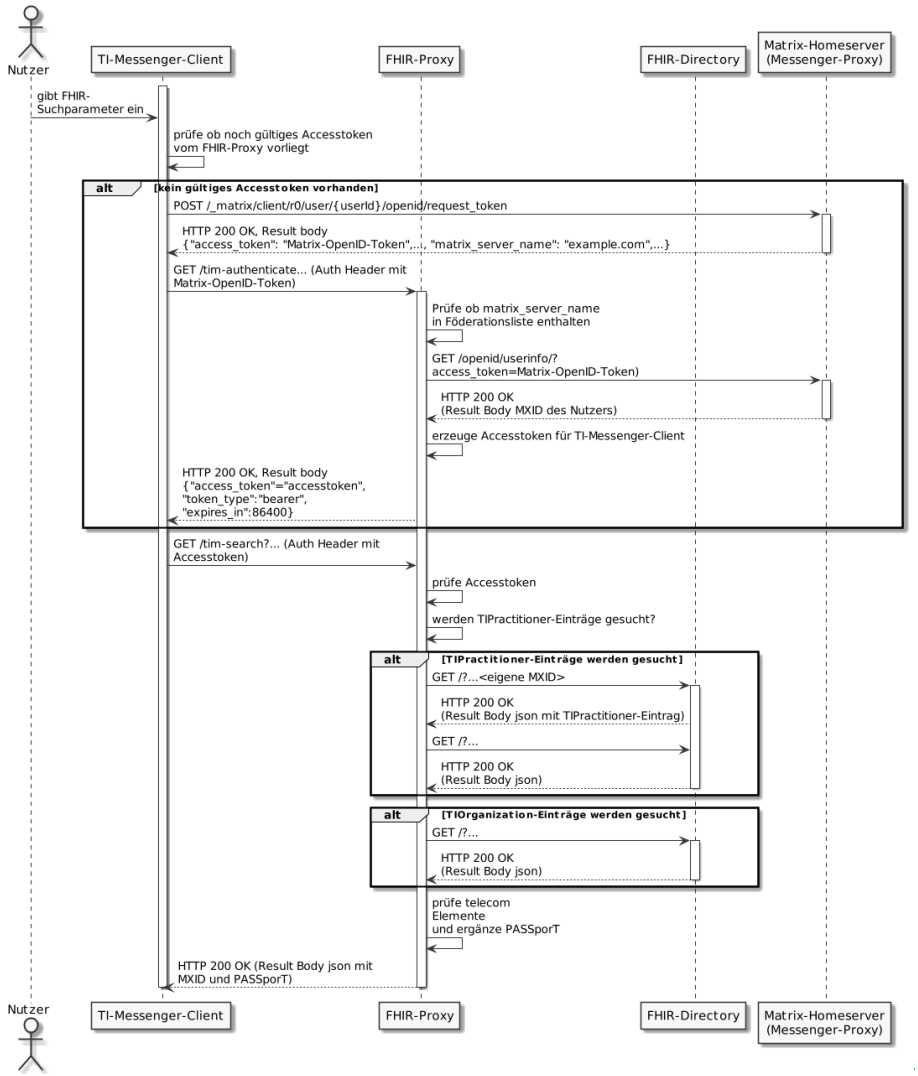
6 Anwendungsfälle

6.1.1 TI-Messenger-Nutzer sucht TIOrganization- und TIPractitioner-Einträge im VZD-FHIR-Directory

AF_10036 - TI-Messenger-Nutzer sucht TIOrganization- und TIPractitioner-Einträge im VZD-FHIR-DirectoryNutzer sucht Einträge im FHIR-Directory

Attribute	Bemerkung
Beschreibung	TI-Messenger-Clients-Nutzer können im VZD-FHIR-Directory nach TIOrganizationHealthcareServiceDirectory- und TIPractitionerPractitionerRoleDirectory-Einträgen suchen. Dazu ist eine Authentisierung am Auth-Service erforderlich. Hier ist die Authentisierung mit TI-Messenger-Clients beschrieben. Wenn im TI-Messenger-Client kein gültiges tim-accesstoken vom FHIR-ProxyAuth-Service vorhanden ist, wird vom TI-Messenger-Client am Matrix-Homeserver ein Matrix-OpenID-Token abgefragt und mit dem Matrix-OpenID-Token im Auth-Header der Endpunkt /tim-search mit den Suchparameternauthenticate des Auth-Services aufgerufen. Der FHIR-ProxyAuth-Service prüft das vom TI-Messenger-Client übergebene Matrix-OpenID-Token. Dabei MUSS der im Matrix-OpenID-Token angegebene matrix_server_name in der TI-Messenger Föderationsliste enthalten sein. Der FHIR-ProxyAuth-Service ruft am Matrix-Homeserver die Operation GET/openid/userinfo mit dem Matrix-OpenID-Token als Parameter auf und erhält die Bestätigung fürin der Response die MXID des TI-Messenger-Nutzers. Damit ist die Authentisierung des Nutzers abgeschlossen. Der FHIR-ProxyAuth-Service erstellt ein Accesstoken, dass die MXID des TI-Messenger-Nutzers enthält undsearch-accesstokenund sendet es an den TI-Messenger-Client. Der TI-Messenger-Client sendet ein GET Request gemäß FHIR-Spezifikation an den Endpunkt /tim-search des FHIR-Proxy. Im Authentication Header ist das Accesstoken (inklusive MXID des Nutzers)search-accesstoken enthalten. Wenn nach TIPractitioner-Einträgen gesucht wird, dann prüft der FHIR-Proxy, ob die MXID des anfragenden Nutzers in einem TIPractitioner-Eintrag im FHIR-Directory gespeichert ist. Falls nicht, dann werden keine TIPractitioner-Einträge gesucht. Der GET Request gemäß FHIR-Spezifikation wird vom FHIR-Proxy an das FHIR-Directory per http-Forward weitergeleitet. Der FHIR-Proxy erhält vom FHIR-Directory eine Response mit den gefundenen Einträgen als json Daten. Die gefundenen TIOrganization- und TIPractitioner-Einträge können in telecom-Elementen MXIDs in url-Notation enthalten sein. Der FHIR-Proxy prüft jedes telecom-Element. Wenn eine MXID url enthalten ist und kein period.end-Element angegeben ist, dass in der Vergangenheit liegt, wird über die logische Komponente PASSporT-Service ein PASSporT erzeugt, dass die MXID des anfragenden Nutzers (im Attribut orig) und die MXID des gefundenen Nutzers (im

	~~Attribut dest) enthält. Das PASSporT wird in die json-Datenstruktur der Response an die url notierte MXID des gefundenen Nutzers in folgender Form angehängt: matrix:u/localpart:tim-domain~~**~~/?PASSporT=[PASSporT String]~~**~~.~~ ~~Gefundene Einträge ohne MXID und PASSporT werden aus der Response entfernt.~~ ~~Die so geänderte Response wird an den TI-Messenger-Client gesendet.~~ ~~Die Anzahl der gefundenen und zurückgegebenen Einträge wird initial auf 100 begrenzt.~~ Die Response wird an den TI-Messenger-Client gesendet. ~~Dieser Wert MUSS konfigurierbar sein.Zusätzlich MUSS konfigurierbar sein, ob Paging eingesetzt wird und wie groß die page_size ist. Paging ist initial eingeschaltet mit page_size = 10.~~
Vorbedingung	Der Nutzer ist an seinem Homeserver registriert.
Nachbedingung	Der TI-Messenger-Client hat alle gefundenen Einträge empfangen. ~~Für MXIDs, mit denen eine Kommunikation begonnen werden darf liegt ein PASSporT vor.~~


Nutzer
TI-Messenger-Client
FHIR-Proxy
FHIR-Directory
Matrix-Homeserver (Messenger-Proxy)
gibt FHIR-Suchparameter ein
prüfe ob noch gültiges Accesstoken vom FHIR-Proxy vorliegt
alt
[kein gültiges Accesstoken vorhanden]
POST /_matrix/client/r0/user/{userId}/openid/request_token
HTTP 200 OK, Result body {"access_token": "Matrix-OpenID-Token",..., "matrix_server_name": "example.com",...}
GET /tim-authenticate... (Auth Header mit Matrix-OpenID-Token)
Prüfe ob matrix_server_name in Föderationsliste enthalten
GET /openid/userinfo/?access_token=Matrix-OpenID-Token)
HTTP 200 OK (Result Body MXID des Nutzers)
erzeuge Accesstoken für TI-Messenger-Client
HTTP 200 OK, Result body {"access_token"="accesstoken", "token_type":"bearer", "expires_in":86400}
GET /tim-search?... (Auth Header mit Accesstoken)
prüfe Accesstoken
werden TIPractitioner-Einträge gesucht?
alt
[TIPractitioner-Einträge werden gesucht]
GET /?...<eigene MXID>
HTTP 200 OK (Result Body json mit TIPractitioner-Eintrag)
GET /?...
HTTP 200 OK (Result Body json)
alt
[TIOrganization-Einträge werden gesucht]
GET /?...
HTTP 200 OK (Result Body json)
prüfe telecom Elemente und ergänze PASSporT
HTTP 200 OK (Result Body json mit MXID und PASSporT)
Nutzer
TI-Messenger-Client
FHIR-Proxy
FHIR-Directory
Matrix-Homeserver (Messenger-Proxy)

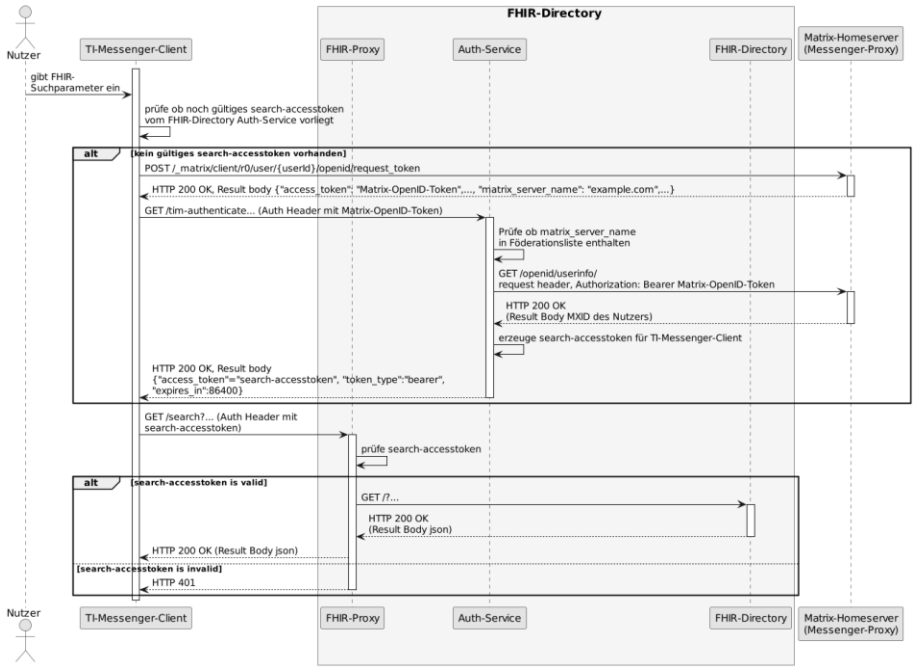


Abbildung 3: Sequence diagram /~~tim~~ search

[<=]

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

ML-123485 - ~~**Authentifizierung am Endpunkt /tim-search (VZD-FHIR-Directory, Sicherheitsgutachten)**~~**Authentifizierung am Endpunkt /search (VZD-FHIR-Directory, Sicherheitsgutachten)**
Am Endpunkt /~~tim~~ search des FHIR-Proxy darf die Authentifizierung nur für ~~Nutzer~~Requests erfolgreich sein, die ein gültiges search-accesstoken im Authentication Header enthalten, dass vom Auth-Service ausgestellt wurde.**[**<=~~an einem Homeserver der TI-Messenger-Föderation registriert sind.~~**[<=]**

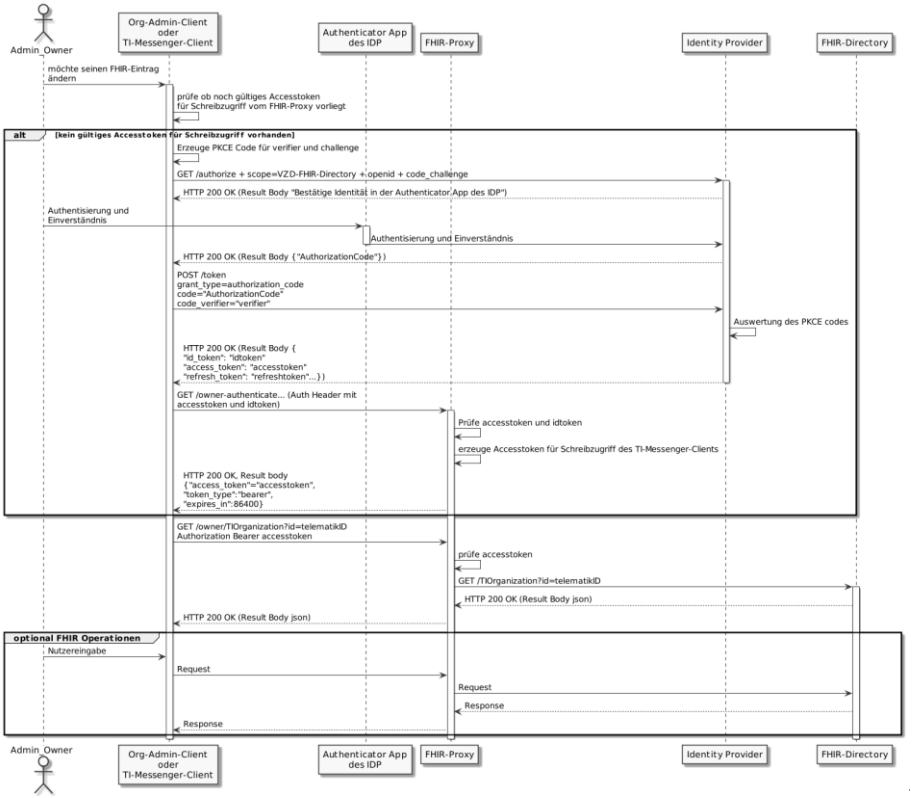
~~**ML-123483 - PASSporT-Erzeugung (VZD-FHIR-Directory, Sicherheitsgutachten)**~~Eigentümer ändert seinen Eintrag im FHIR-Directory

~~6.25.2 Der FHIR-Proxy darf nur PASSporT ausstellen, wenn im telecom-Element des Eintrags eine MXID in url-Form vorhanden ist und das period.endDate nicht in der Vergangenheit liegt.[<=]~~

~~6.3 TIOrganization-Einträge oder TIPractitioner-Einträge im VZD-FHIR-Directory ändern~~

AF_10037 - ~~TIOrganization-Einträge oder TIPractitioner-Einträge im VZD-FHIR-Directory ändern~~Einträge im VZD-FHIR-Directory ändern

Attribute	Bemerkung
Beschreibung	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 ~~Organisationseinträge mit eigenen Daten~~FHIR-Ressourcen erstellen, um die Struktur der Organisation abzubilden. Zum Beispiel können Krankenhäuser ihre Fachabteilungen als ~~Organisations~~HealthcareService-Einträge abbilden, die mit dem ~~Basis~~Organization-Eintrag verlinkt sind. ~~Der ausführende Akteur hat die Rolle~~ Wenn der Org-Admin ~~Owner. Wenn~~ oder LE kein gültiges owner-accesstoken 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 ~~FHIR-Proxy~~Auth-Service bekannt. ~~Dadurch erhält der Client das Recht den Eintrag im FHIR-Directory mit dieser Telematik-ID zu ändern.~~ Für den Aufruf der FHIR-Operationen durch den Client stellt der ~~FHIR-Proxy~~ Auth-Service dem Client ein owner-accesstoken aus, dass auch die Telematik-ID des LE oder der Organisation enthält. ~~Voraussetzung für das Erzeugen oder Ändern von TIOrganization-Einträgen unterhalb des Basiseintrags ist, dass immer eine partOf Referenz zum Basiseintrag der eigenen Organisation angegeben ist. Wenn eine Kette von TIOrganization-Einträgen mit partOf Referenzen erzeugt werden soll, dann MUSS am Ende der Kette immer die eigene TIOrganization verlinkt sein.~~
Vorbedingung	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.
Fehlermeldungen	~~HTTP 422 Unprocessable Entity: Request zum Erstellen oder Ändern eines TIOrganisation-Eintrags enthält keine partOf-Verlinkung zum TIOrganisation- oder TIPractitioner-Basiseintrag.~~


Admin_Owner
Org-Admin-Client oder TI-Messenger-Client
Authenticator App des IDP
FHIR-Proxy
Identity Provider
FHIR-Directory
möchte seinen FHIR-Eintrag ändern
prüfe ob noch gültiges Accesstoken für Schreibzugriff vom FHIR-Proxy vorliegt
alt
[kein gültiges Accesstoken für Schreibzugriff vorhanden]
Erzeuge PKCE Code für verifier und challenge
GET /authorize + scope=VZD-FHIR-Directory +openid + code_challenge
HTTP 200 OK (Result Body "Bestätige Identität in der Authenticator App des IDP")
Authentisierung und Einverständnis
Authentisierung und Einverständnis
HTTP 200 OK (Result Body {"AuthorizationCode"})
POST /token
grant_type=authorization_code
code="AuthorizationCode"
code_verifier="verifier"
Auswertung des PKCE codes
HTTP 200 OK (Result Body {
"id_token": "idtoken"
"access_token": "accesstoken"
"refresh_token": "refreshtoken"...})
GET /owner-authenticate... (Auth Header mit accesstoken und idtoken)
Prüfe accesstoken und idtoken
erzeuge Accesstoken für Schreibzugriff des TI-Messenger-Clients
HTTP 200 OK, Result body
{"access_token"="accesstoken",
"token_type":"bearer",
"expires_in":86400}
GET /owner/TIOrganization?id=telematikID
Authorization Bearer accesstoken
prüfe accesstoken
GET /TIOrganization?id=telematikID
HTTP 200 OK (Result Body json)
HTTP 200 OK (Result Body json)
optional FHIR Operationen
Nutzereingabe
Request
Request
Response
Response
Admin_Owner
Org-Admin-Client oder TI-Messenger-Client
Authenticator App des IDP
FHIR-Proxy
Identity Provider
FHIR-Directory

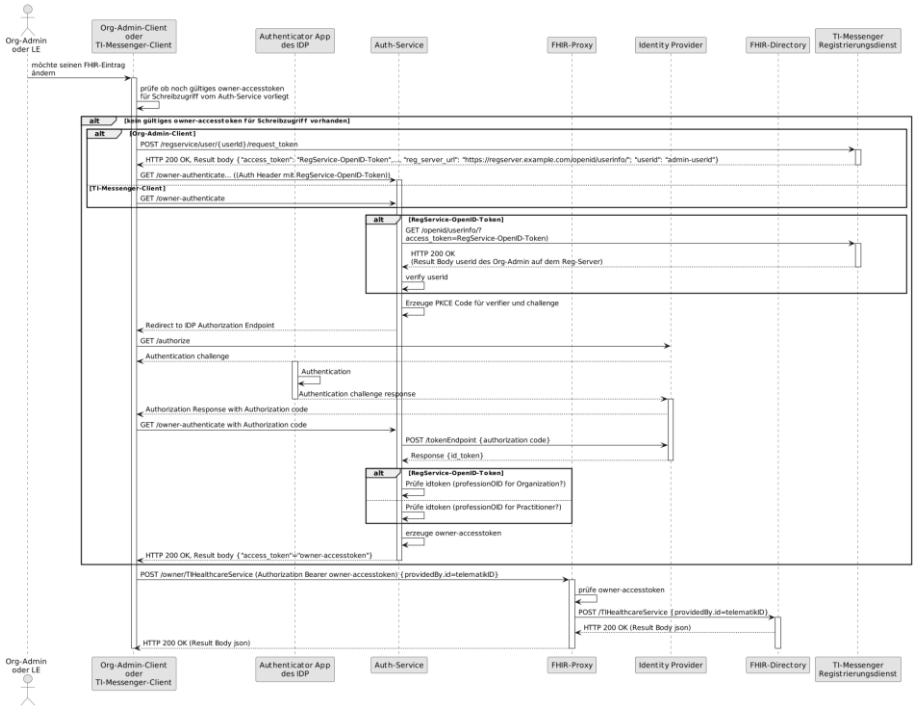


Abbildung 4: Sequenzdiagramm VZD-FHIR-Directory Änderung von eigenen ~~TIOrganization~~OrganizationDirectory- oder ~~TIPractitioner~~PractitionerDirectory-Einträgen

[<=]

Akzeptanzkriterien für den Anwendungsfall AF_10037 ~~TIOrganization~~OrganizationDirectory-Einträge im VZD-FHIR-Directory ändern

ML-123873 **- Authentifizierung am Endpunkt /owner (VZD-FHIR-Directory, Sicherheitsgutachten)**
Am Endpunkt /owner des FHIR-Proxy darf die Authentifizierung nur für Nutzer erfolgreich sein, die ein gültiges Accesstoken vom VZD-FHIR-Directory vorweisen.
[<=]

ML-123874 **- Nur Einträge mit eigener Telematik-ID verändern (VZD-FHIR-Directory)**
Im, bei der Authentifizierung verwendeten, Accesstoken ist die Telematik-ID des Nutzers enthalten. Nur der Eintrag (~~TIPractitioner oder TIOrganization~~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.
[<=]

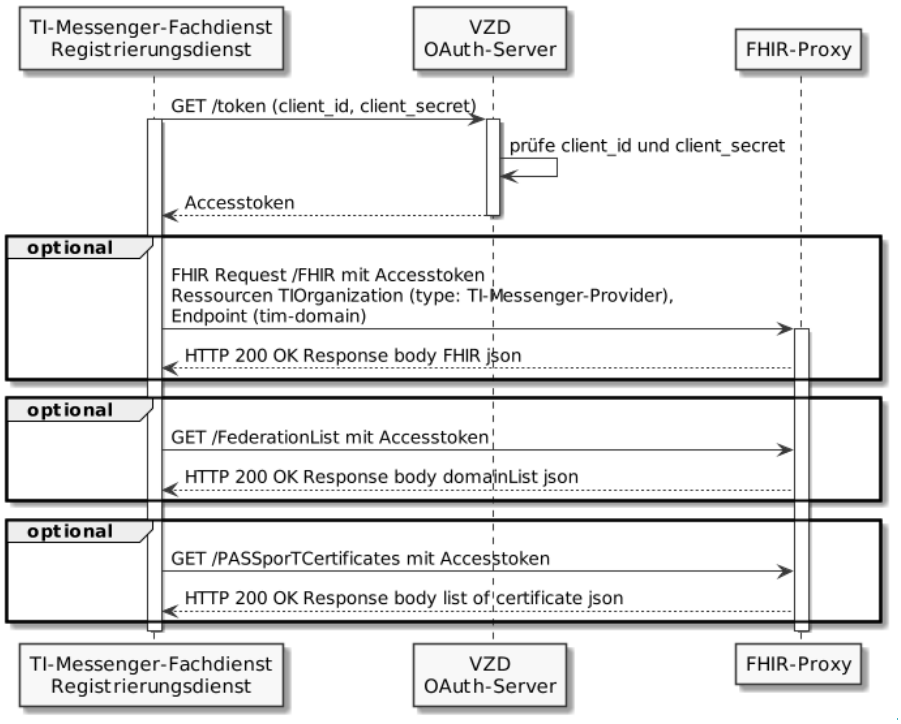
ML-123482 - ~~Selbst angelegte TIOrganisation-Einträge MÜSSEN mit dem eigenen Basiseintrag verlinkt sein (VZD-FHIR-Directory)~~**Selbst angelegte OrganizationDirectory-Einträge MÜSSEN mit dem eigenen Basiseintrag verlinkt sein (VZD-FHIR-Directory)**
Alle selbst durch den Besitzer angelegten FHIR-Einträge MÜSSEN mit dem eigenen Basiseintrag mittels partOf verlinkt sein. Wenn keine korrekte Verlinkung angegeben ist, dann MUSS der FHIR-Proxy das Erzeugen oder die Änderung des ~~TIOrganisation~~OrganizationDirectory-Eintrags mit der Fehlermeldung (HTTP 422 Unprocessable Entity) ablehnen.**[**<=**]**

~~6.~~45.3 Anwendungsfälle der TI-Messenger-Anbieter im VZD-FHIR-Directory

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

Attribute	Bemerkung
Beschreibung	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 Endpoint-Einträgen gespeichert. Die Endpoint-Einträge eines TI-Messenger-Anbieters sind verlinkt mit seinem ~~TIOrganization~~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 OAuth-Server ein Accesstoken, das zur Authentifizierung an der Schnittstelle genutzt wird. Nach erfolgreicher Authentisierung kann der Registrierungsdienst die FHIR-Operationen zur Verwaltung des eigenen ~~TIOrganisation~~OrganizationDirectory-Eintrags und der eigenen Endpoint-Einträge nutzen. 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. ~~Das VZD-FHIR-Directory stellt für gefundene MXIDs (Matrix-Adressen) Personal Assertion Token (PASSporT) aus. Die PASSporT werden vom TI-Messenger-Service geprüft. Um die PASSporT-Signatur prüfen zu können wird das zugehörige Zertifikat benötigt. Mit der Operation GET /PASSporTCertificates können die Zertifikate abgefragt werden.~~ ~~Siehe auch: https://github.com/gematik/api-vzd/blob/master/src/I_VZD_TIM_Provider_Services.yaml~~

Vorbedingung	Der Registrierungsdienst des TI-Messenger-Anbieters ist bereits als Nutzer des VZD-FHIR-Directories registriert und hat OAuth Client Credentials (client_id und client_secret) für die Umgebungen RU, TU und PU erhalten.


TI-Messenger-Fachdienst
Registrierungsdienst
VZD
OAuth-Server
FHIR-Proxy
GET /token (client_id, client_secret)
prüfe client_id und client_secret
Accesstoken
optional
FHIR Request /FHIR mit Accesstoken
Ressourcen TIOrganization (type: TI-Messenger-Provider),
Endpoint (tim-domain)
HTTP 200 OK Response body FHIR json
optional
GET /FederationList mit Accesstoken
HTTP 200 OK Response body domainList json
optional
GET /PASSporTCertificates mit Accesstoken
HTTP 200 OK Response body list of certificate json
TI-Messenger-Fachdienst
Registrierungsdienst
VZD
OAuth-Server
FHIR-Proxy

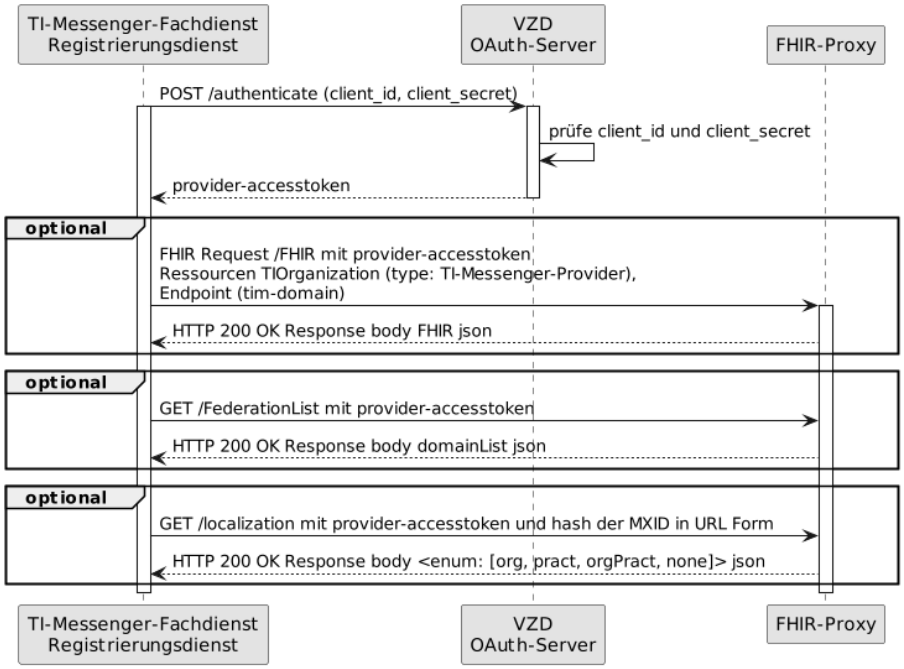


Abbildung 5: VZD-FHIR-Directory_Sequenzdiagramm_TI-Messenger-Provider-Services

[<=]

ML-123881 **- Authentifizierung an der Schnittstelle I_VZD_TIM_Provider_Services (VZD-FHIR-Directory, Sicherheitsgutachten)**
An der Schnittstelle I_VZD_TIM_Provider_Services darf die Authentifizierung nur für Clients erfolgreich sein, die ein gültiges provider-accesstoken vom OAuth-Server des VZD-Anbieters vorweisen.
[<=]

~~6.~~55.4 Einträge mit dem VZD-LDAP-Directory abgleichen

AF_10047 **- Einträge mit dem VZD-LDAP-Directory abgleichen**

Attribute	Bemerkung
Beschreibung	Der FHIR-Proxy aktualisiert regelmäßig in einem konfigurierbaren Intervall die im VZD-LDAP-Directory seit der letzten Aktualisierung geänderten Einträge. Da es sich um eine interne Schnittstelle des Verzeichnisdienstes handelt, wird nicht vorgegeben, wie die Schnittstelle zu implementieren ist. Die Übertragung der Daten MUSS TLS-verschlüsselt in einem internen Netzwerk des Verzeichnisdienstes erfolgen. Es werden alle

	geänderten Einträge seit der letzten Aktualisierung durch den FHIR-Proxy vom VZD-LDAP-Directory abgefragt und gemäß Tabelle VZD-FHIR-Directory_Mapping_LDAP_to_FHIR aktualisiert. Dabei MÜSSEN auch im VZD-LDAP-Directory gelöschte Einträge erkannt und ebenfalls im VZD-FHIR-Directory gelöscht werden. Einträge ohne Zertifikat erhalten im VZD-FHIR-Directory den Wert ~~TIOrganization~~OrganizationDirectory.active = false bzw. ~~TIPractitioner~~PractitionerDirectory.active = false Wird zu einem Eintrag im VZD-LDAP-Directory wieder ein Enc-Zertifikat ergänzt, dann erhält der Eintrag im VZD-FHIR-Directory den Wert TIOrganization.active = true bzw. ~~TIPractitioner~~PractitionerDirectory.active = true.

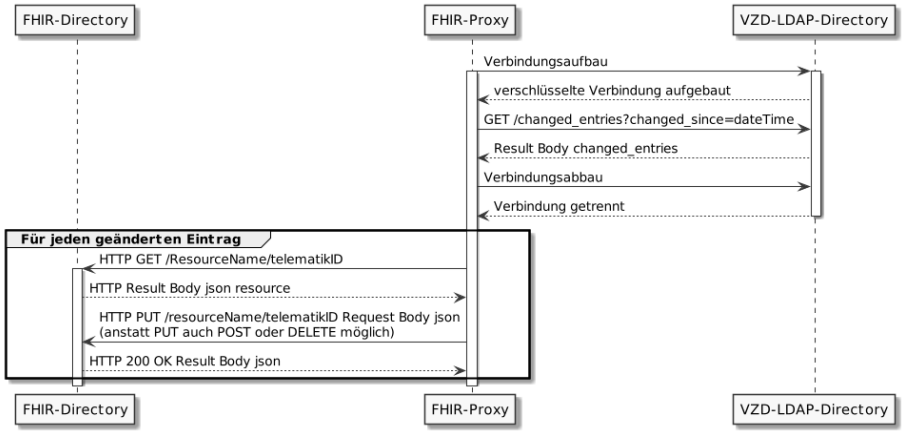


Abbildung 6: VZD-FHIR-Directory, Aktualisierung der Basiseinträge

[<=]

~~7~~6 Verteilungssicht

Das VZD-FHIR-Directory unterstützt initial die Anwendung TI-Messenger; wird zukünftig aber auch die anderen Anwendungen wie ePA und KIM in deren Folgeversionen sowie bisher unbekannte Fachanwendungen und neue Nutzergruppen unterstützen. Es ist daher erforderlich, dass das VZD-FHIR-Directory mit der Anzahl der Nutzerzugriffe skalieren und anwendungsspezifische Ressourcen speichern kann.

Der FHIR-Proxy MUSS in mehreren Instanzen betrieben werden können, die die Schnittstellen Richtung Internet für Abfragen der TI-Messenger-Nutzer und Änderungen durch die Besitzer implementieren. Das Load-Balancing der Client-Requests erfolgt per DNS, indem für jede Instanz des FHIR-Proxy ein A und ein AAAA Resource Record für die RU, TU und PU FQDNs der Schnittstellen im DNS eingetragen wird. Instanzen des FHIR-Proxies werden je nach Last hinzugefügt oder entfernt.

Die FHIR-Proxy sind auch die HTTP-Load-Balancer für die Lesezugriffe auf FHIR-Directory-Instanzen. Für den Schreibzugriff wird eine Instanz implementiert. Die Datenbanken der Instanzen für den Lesezugriff werden mit der Datenbank für den Schreibzugriff synchronisiert.

Eine weitere Komponente setzt die Aktualisierung der Basiseinträge im FHIR-Directory mit den geänderten Daten aus dem VZD-LDAP-Directory um. Zusätzlich implementiert diese Komponente die Schnittstelle I_VZD_TIM_Provider_Services.

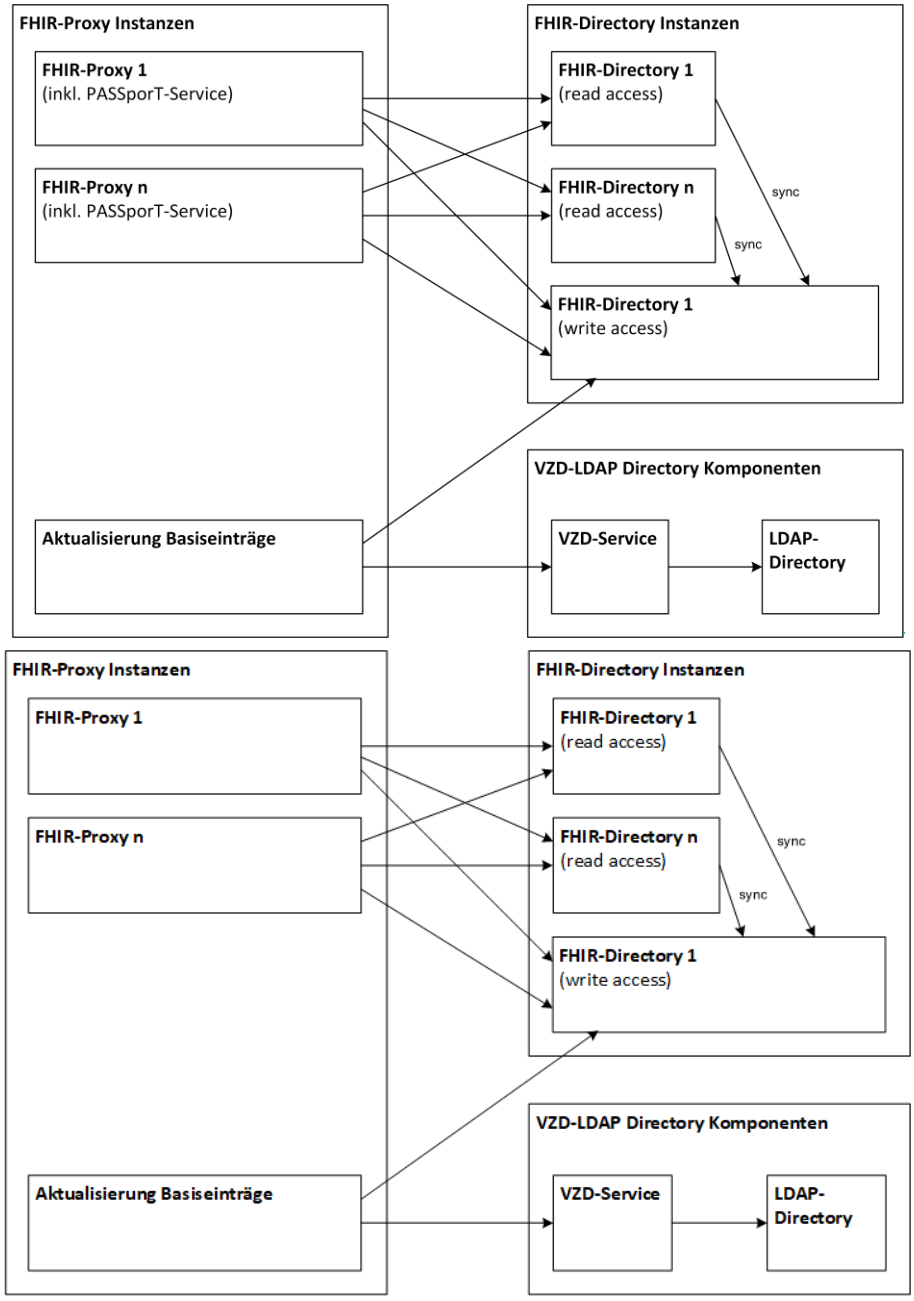


Abbildung 7: VZD-FHIR-Directory, Verteilungssicht

~~8~~ 7 Anhang A – Verzeichnisse

~~8.1~~ 7.1 Abkürzungen

Kürzel	Erläuterung
AF	Anwendungsfall
DNS	Domain Name System
FHIR	Fast Healthcare Interoperable Resources
FQDN	Fully Qualified Domain Name
LDAP	Lightweight Directory Access Protocol
OWASP	Open Web Application Security Project
~~PASSporT~~	~~Personal Assertion Token~~
PU	Produktivumgebung
RU	Referenzumgebung
SHA	Secure Hash Algorithm
TLS	Transport Layer Security
TI	Telematikinfrastruktur
TIM	TI-Messenger (ausschließliche Verwendung der Abkürzung in Attributen, Parametern oder URLs)
TU	Testumgebung
VZD	Verzeichnisdienst

~~8.2~~ 7.2 Glossar

Begriff	Erläuterung

Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.

Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung gestellt.

~~8.3~~7.3 Abbildungsverzeichnis

~~8.4~~7.4 Tabellenverzeichnis

~~8.5~~7.5 Referenzierte Dokumente

~~8.5.1~~7.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar
[gemSpec_VZD]	g ematik: Spezifikation Verzeichnisdienst
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktivbetrieb

~~8.5.2~~7.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[CAB-Forum]	Liste vertrauenswürdiger Zertifikatsherausgeber (Root-CAs) für Anwendungen im Internet https://cabforum.org/members/

7.6 Versionierung Datenmodell

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

- de.gematik.fhir.directory 0.6.1

~~9~~8 Anhang B - Beispiele

~~9.1~~8.1 FHIR Operationen

~~9.1.1~~8.1.1 Abfrage von ~~TIOrganisation~~OrganizationDirectory Einträgen

~~9.1.1.1~~8.1.1.1 Client Code

```
// Create a client (only needed once)
FhirContext ctx = new FhirContext();
IGenericClient client =
ctx.newRestfulGenericClient("http://hapi.fhir.org/baseR4");

// Invoke the client
Bundle bundle =
client.search().forResource(~~TIOrganization~~HealthcareService.class).where(ne
w StringClientParam("location.address").matches().value("10117"))
.include(new Include("~~TIOrganization:endpoint~~Organization"))
.prettyPrint()
.execute();
```

~~9.1.1.2~~8.1.1.2 Request

~~GET http://hapi.fhir.org/baseR4/TIOrganization?address=10117&_include=TIOrganizatio n:endpoint&_pretty=true~~

GET http://hapi.fhir.org/baseR4/HealthcareService?location.address=10117&_include=O rganization&_pretty=true

~~9.1.1.3~~8.1.1.3 Request Headers

```
Accept-Charset: utf-8
Accept: application/fhir+xml;q=1.0, application/fhir+json;q=1.0,
application/xml+fhir;q=0.9, application/json+fhir;q=0.9
User-Agent: HAPI-FHIR/5.5.0-PRE1-SNAPSHOT (FHIR Client; FHIR 4.0.1/R4;
apache)
Accept-Encoding: gzip
```

~~9.1.1.4~~8.1.1.4 Response

HTTP 200 OK

~~9.1.1.5~~8.1.1.5 Response Headers

```
x-request-id: hr3p6Pi0jorUblN7
date: Fri, 06 Aug 2021 10:22:24 GMT
```

```
last-modified: Fri, 06 Aug 2021 10:22:23 GMT
server: nginx/1.18.0 (Ubuntu)
transfer-encoding: chunked
x-powered-by: HAPI FHIR 5.5.0-PRE1-SNAPSHOT/1703568840/2021-05-28 REST
Server (FHIR Server; FHIR 4.0.1/R4)
connection: keep-alive
content-type: application/fhir+json;charset=utf-8
```

~~9.1.1.6~~8.1.1.6 Response Body


```
{
  "resourceType": "Bundle",
  "id": "ec8a4846-5719-4760-833f-606f01ea6055",
  "meta": {
    "lastUpdated": "2021-08-06T06:56:44.620+00:00"
  },
  "type": "searchset",
  "total": 2,
  "link": [ {
    "relation": "self",
    "url":
"http://hapi.fhir.org/baseR4/TIOrganization?_include=TIOrganization%3Aendpo
int
&_pretty=true&address=10117"
  } ],
  "entry": [ {
    "fullUrl": "http://hapi.fhir.org/baseR4/TIOrganization/2500949",
    "resource": {
      "resourceType": "TIOrganization",
      "id": "2500949",
      "meta": {
        "versionId": "1",
        "lastUpdated": "2021-08-04T15:51:20.261+00:00",
        "source": "#0j3wXiC80VNH7wON"
      },
      "name": "Test Organisation der TI",
      "telecom": [ {
        "system": "url",
        "value": "matrix:u/testorg:gematik.de"
      } ],
      "address": [ {
        "line": [ "Friedrichstr. 136" ],
        "city": "Berlin",
        "state": "Berlin",
        "postalCode": "10117",
        "country": "Germany"
      } ]
    },
    "search": {
      "mode": "match"
    }
  }, {
    "fullUrl": "http://hapi.fhir.org/baseR4/TIOrganization/2500973",
    "resource": {
      "resourceType": "TIOrganization",
      "id": "2500973",
      "meta": {
```

```
        "versionId": "1",
        "lastUpdated": "2021-08-04T16:55:16.931+00:00",
        "source": "#q5G1swl1SHzfbbjj"
      },
      "name": "Test Organisation 2 der TI",
      "telecom": [ {
        "system": "url",
        "value": "matrix:u/testorg2:gematik.de"
      } ],
      "address": [ {
        "line": [ "Friedrichstr. 136" ],
        "city": "Berlin",
        "state": "Berlin",
        "postalCode": "10117",
        "country": "Germany"
      } ],
      "endpoint": [ {
        "reference": "Endpoint/2500968"
      } ]
    },
    "search": {
      "mode": "match"
    }
  }, {
    "fullUrl": "http://hapi.fhir.org/baseR4/Endpoint/2500968",
    "resource": {
      "resourceType": "Endpoint",
      "id": "2500968",
      "meta": {
        "versionId": "1",
        "lastUpdated": "2021-08-04T16:27:54.228+00:00",
        "source": "#bsfK2WXBApjsoYj8"
      },
      "connectionType": {
        "system": "https://gematik.de/fhir/VZD-FHIR-
Directory/CodeSystem/TIMessengerCS",
        "code": "tim-domain"
      },
      "name": "gematik.de",
      "managingOrganization": {
        "reference": "TIOrganization/2500949"
      }
    },
    "search": {
      "mode": "include"
    }
  } ]
}
```