

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Verzeichnisdienst FHIR- Directory

Version:	1. 03 .0
Revision:	792635863408
Stand:	01.10 31.07.2021 13
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
1.2.0	12.12.2022	4.2.4 4.2.3 4.3.1	Fachliche Beschreibung Operation wherels ergänzt - C_11233 Aufbau der Föderationsliste aktualisiert - ANFTIM-185 Sicherheits- und Datenschutzanforderungen ergänzt	gematik
1.3.0	31.07.2023		Einarbeitung TI-Messenger Maintenance 23.1 / VZD FHIR Maintenance_23.1	

Inhaltsverzeichnis

1 Einordnung des Dokumentes.....	5
1.1 Zielsetzung.....	5
1.2 Zielgruppe.....	5
1.3 Geltungsbereich.....	5
1.4 Abgrenzungen.....	6
1.5 Methodik.....	6
2 Systemüberblick.....	8
3 Systemkontext.....	10
3.1 Akteure und Rollen.....	10
3.2 User Stories.....	11
3.3 Nachbarsysteme.....	13
4 Zerlegung des Produkttyps.....	14
5 Funktionsmerkmale.....	15
5.1 FHIR-Directory.....	15
5.1.1 Datenmodell.....	15
5.1.2 Mapping von LDAP auf FHIR-Ressourcen.....	16
5.1.3 FHIR RESTful API.....	19
5.2 FHIR-Proxy und PASSporT-Service.....	19
5.2.1 Schnittstellen.....	19
5.2.1.1 TLS-Verbindungsaufbau.....	19
5.2.1.2 FHIR-Schnittstelle für TI-Messenger-Nutzer.....	19
5.2.1.3 FHIR-Schnittstelle für Besitzer.....	21
5.2.1.4 Schnittstelle I_VZD_TIM_Provider_Services.....	22
5.2.2 Aktualisierung der Basiseinträge.....	24
5.2.3 Erzeugung und Verteilung der Föderationsliste.....	24
5.3 Übergreifende Vorgaben.....	25
5.3.1 Sicherheit.....	25
5.3.2 Betrieb.....	25
6 Anwendungsfälle.....	27
6.1 TI-Messenger-Nutzer sucht TI-Organization- und TI-Practitioner-Einträge im VZD-FHIR-Directory.....	27
6.2 TI-Organization-Einträge oder TI-Practitioner-Einträge im VZD-FHIR-Directory ändern.....	30
6.3 Anwendungsfälle der TI-Messenger-Anbieter im VZD-FHIR-Directory.....	32
6.4 Einträge mit dem VZD-LDAP-Directory abgleichen.....	34

7 Verteilungssicht.....	35
8 Anhang A – Verzeichnisse.....	37
8.1 Abkürzungen.....	37
8.2 Glossar.....	37
8.3 Abbildungsverzeichnis.....	38
8.4 Tabellenverzeichnis.....	38
8.5 Referenzierte Dokumente.....	38
8.5.1 Dokumente der gematik.....	38
8.5.2 Weitere Dokumente.....	39
9 Anhang B – Beispiele.....	40
9.1 FHIR Operationen.....	40
9.1.1 Abfrage von TIOrganisation Einträgen.....	40
9.1.1.1 Client Code.....	40
9.1.1.2 Request.....	40
9.1.1.3 Request Headers.....	40
9.1.1.4 Response.....	40
9.1.1.5 Response Headers.....	40
9.1.1.6 Response Body.....	41
1 Einordnung des Dokumentes.....	7
1.1 Zielsetzung.....	7
1.2 Zielgruppe.....	7
1.3 Geltungsbereich.....	7
1.4 Abgrenzungen.....	8
1.5 Methodik.....	8
2 Systemüberblick.....	10
2.1 Nutzer und Rollen.....	11
sich authentisieren und.....	13
Ressourcen zurück geliefert.....	14
2.2 Nachbarsysteme.....	16
3 Zerlegung des Produkttyps.....	18
4 Funktionsmerkmale.....	20
4.1 FHIR-Directory.....	22
4.1.1 Datenmodell.....	22
4.1.2 Mapping von LDAP auf FHIR-Ressourcen.....	24
4.1.3 FHIR RESTful API.....	26
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 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 S.....	27
4.2 FHIR-Proxy.....	27
4.2.1 Schnittstellen.....	27
4.2.1.1 TLS-Verbindungsaufbau.....	27
4.2.1.2 FHIR Schnittstelle für TI-Messenger-Nutzer FHIRDirectorySearchAPI.....	27
4.2.1.3 FHIR-Schnittstelle für Besitzer FHIRDirectoryOwnerAPI.....	29
4.2.1.4 Schnittstelle FHIRDirectoryTIMProviderAPI (I_VZD_TIM_Provider_Services.yaml).....	31
4.2.2 Aktualisierung der Basiseinträge.....	34
4.2.3 Erzeugung und Bereitstellung der Föderationsliste.....	34
4.2.4 Lokalisierung einer MXID (Operation wherels).....	37
4.3 Übergreifende Vorgaben.....	37
Die 100 Sucherg.....	38
4.3.1 Betrieb.....	39
5 Anwendungsfälle.....	41
5.1 TI-Messenger-Nutzer sucht Einträge im FHIR-Directory.....	41
Bei der Registrierung des TI-Messenger Anbieters wird das Signatur-Zertifikat, das für die Signatur des id_tokens verwendet wird, im FHIR-Directory.....	46
5.2 Anwendungsfälle der TI-Messenger-Anbieter im VZD-FHIR-Directory.....	52
5.3 Einträge mit dem VZD-LDAP-Directory abgleichen.....	55
6 Verteilungssicht.....	57
7 Anhang A - Verzeichnisse.....	60
7.1 Abkürzungen.....	60
7.2 Glossar.....	60
7.3 Abbildungsverzeichnis.....	61
7.4 Tabellenverzeichnis.....	61
7.5 Referenzierte Dokumente.....	62
7.5.1 Dokumente der gematik.....	62
7.5.2 Weitere Dokumente.....	62
7.6 odell.....	65

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 [87.5- 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 Anwendungsfalles 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 [EVZD-LDAP-Directory](#) Einträge werden ~~mit den Einträgen im in das~~ [VZD-LDAP-Directory-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 [TIPractitionerDirectory](#)-Ressource und Organisations-Einträge auf die [TIOrganizationDirectory](#)-Ressource abgebildet. Die synchronisierten Einträge bilden die Basis-Einträge, die durch die Besitzer um zusätzliche Daten ergänzt bzw. erweitert werden können. [TIPractitionerDirectory](#) und [TIOrganizationDirectory](#) sind Profilierungen der FHIR-Ressourcen Practitioner und Organization. Die Anbieter von Fachanwendungen werden ebenfalls als [TIOrganizationDirectory](#)-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. [LocationEndpoint](#) 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.

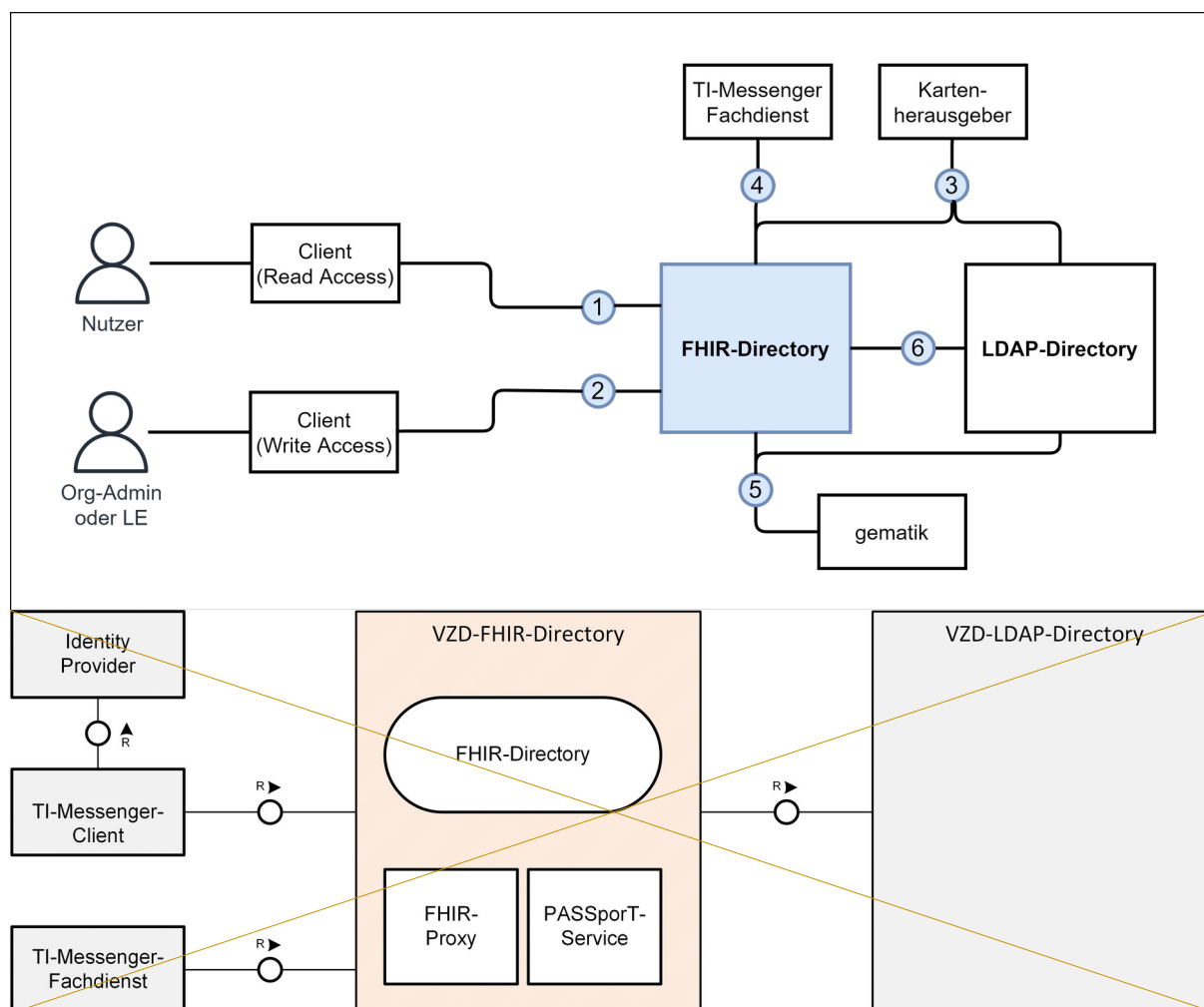


Abbildung 1: Systemüberblick VZD-FHIR-Directory

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>).

2.1 Der FHIR-Proxy terminiert die TLS-Verbindungen, prüft die Zugriffsberechtigung der Nutzer und Rollen

Tabelle 1: Nutzer und verteilt die AnfrRollen

<u>Nutzer und Rolle</u>	<u>Beschreibung</u>
<u>Nutzer</u>	<u>Alle Nutzer können im FHIR-Directory über die Schnittstelle (1) nach Einträgen im Organisationsverzeichnis und im Personenverzeichnis suchen.</u>
<u>Org-Admin oder LE</u>	<u>Administratoren der Organisationen und LE können im FHIR-Directory über die Schnittstelle (2) ihren Eintrag im Organisationsverzeichnis</u>

ändern und um zusätzliche Ressourcen erweitern.

Tagen der Nutzerbelle 2: auf die Instanz Kommunikationsbeziehungen des FHIR-Directory sowie des Pzu IT-Systemen

IT-Systeme	Beschreibung
<u>Kartenherausgeber</u>	<u>Die Kartenherausgeber nutzen die Schnittstelle (3), um die Einträge ihrer Mitglieder im LDAP-Directory und zukünftig im FHIR-Directory zu pflegen.</u>
<u>TI-Messenger-Anbieter</u>	<u>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.</u>
<u>gematik</u>	<u>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.</u>
<u>LDAP-Directory</u>	<u>Die Schnittstelle (6) zwischen FHIR-Directory und LDAP-Directory wird vom Verzeichnisdienst genutzt, um die Einträge zu synchronisieren.</u>

ASSporT-Service. Zusätzlich übernimmt und aktualisiert der FHIR-Proxy die Basiseinträge im VZD-FHIR-Directory mit den geänderten Daten des VZD-LDAP-Directorys.

Der PASSporT-Service ist eine Komponente, die Personal Asserlle Schnittstellen mit Ausnahme (6) sind über das Internet erreichbar. Die Schnittstellen stellen folgende Funktion Token gemäß [RFC8225] ausstellt. Die Token bestätigen, dasbereit:

Für Nutzer gibt es ein Leistungserbringer oder eine Organisation dure Schnittstelle zur Suche nach die EEintragung der TI-Messenger-Adresseägen im VZD-FHIR-Directory damit einOrganisationsverstanden ist, dass eine TI-Messenger-Kommunikation zu diesezeichnis und Personenverzeichnis. Die Schnittstelle kann nur nach erfolgreicher Adresse-aufgebaututhentisierung genutzt werden darf. Für die Signatur des PASSporT wird ein-Zertifikat aus d. Alle TI-Messenger Nutzer Komponentönnen PKI der TI verwendet.

3 Systemkontext

3.1 Akteuresich authentisieren und Rollen

Das VZD bekommen vom FHIR-Directory ist ein Dienst der Telematikinfrastruktur und kann von allen Access tokens ausgestellt, das für die Suchanfragen Nutzern der TI abgefragt werden. Zusätzlich verwendet wird. Die Suche ermöglicht es, es erforderlich, dass die Einträge gepflegt werden nach Volltext oder nach bestimmten werden. Dies erfolgt durch die Kartenherausgaben der einzelnen Attribute über, die Fachanwendungen, falls spezifische Fachdaten den Einträgen zugeordnet sind, und optional über verlinkten Ressourcen zu suchen. Gefundene Ressourcen die Besitzer der Einträge werden in Einträge.

~~Tabelem Bundle 3: von VZD-FHIR-Directory Akteure und Rollen~~

Akteur	Rolle	Beschreibung
TI-Messenger-Nutzer	User	TI-Messenger-Nutzer sind Leistungserbringer, Mitarbeiter in Organisationen des Gesundheitswesens und Versicherte. Sie können im Rahmen der Fachanwendung TI-Messenger Einträge im VZD-FHIR-Directory lesen.
Besitzer	Admin_Owner	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.
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.
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	GTT	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 Us Ressourcen zurück geliefer Stories

1. Als TI-Messenger-Nutzer möchte ich komfortabel nach Leistungserbringern undt. Das Datenformat ist json.
- Für Administratoren der Organisationen suchen können, so dass ich keine Zeitdes Gesundheitswesens und Nerven damit verschwenden muss, für LE gibt es einen geeigneten TI-Messenger-Kommunikationspartner zu finden.
- Als TI-Messenger-Nutzer möchte ich die Ort Schnittstelle zur Änderungsfunktion mein ihres Geräts nutzen können, um nahegelegene Leistungserbringer undEintrags im Organisationen finden zu können, so dass ich spontansverzeichnis. Zur Nutzung den für mich bestgelegene Organisationr Schnittstelle ist eine auswählen kann.
- Als TI-Messenger-Nutzer möchte ich in der Lage sein, Organisthentifizierung mit OIDC Authorizationen herauszufiltern, die gerade geöffnet haben o Code Flow erforder die

bald öffnen werden, so dass ich nicht vor verschlossenen Türen liche. Über diese Schnittstelle, welche kann ich die Organisation aufsuchen will.

- Als TI-Messenger-Nutzer möchte ich, dass die Suchfunktion meiner App bevorzugten Navigations-App eine Route zur ausgewählten Organisation berechnen lässt, so dass eine Verlinkung um zusätzlich nicht-Adressen in meine Navigations-App kopieren muss, um die Einträge erweitert 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, dass die Suchfunktion 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, dass die Suchfunktion meiner App weitere Informationen zu einer Organisation speichern, sodass sie von erhalten, um mich mit ihr in Verbindung setzen oder LE gefunden bzw. über sie informieren zu werden 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.

2. Als Kartenherausgeber erfolgt die Authentifizierung über OIDC. Das FHIR-Datenformat ist json.

- Für Kartenherausgeber brauche ich eine einfache (technische) Möglichkeit, die Daten für die ich verantwortlich bin, in der Directory Administration, um Einträge 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, sie anlegen und zu pflegen. Das Datenformat ist json und ist in der OpenAPI-yaml-Datei DirectoryAdministration.yaml festgelegt. Zukünftig ist vorgesehen, dass ich keine Zeit und Nerven damit verschwenden muss, die Einträge adäquat verwalten zu können.
- Als Kartenherausgeber möchte ich meinen Account auch direkt die Schnittstelle 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 der FHIR in der Störungsphase des VZD-FHIR-Directory JSON, die Nutzer und die Authentifizierung der Kartenherausgeber entsprechendes Feedback und Support erhalten und ggf. Fehlermeldungen korrekt eingestellt und weitergeleitet werden.

3. Als Anbieter einer Fachanwendung.

- TI-Messenger-Fachanwendung brauche ich eine einfache (technische) Möglichkeit, die fachlichen Daten der Fachanwendung im VZD-FHIR-Directory editieren zu können (einstellen, lesen, verändern, löschen).
- Als Anbieter einer Fachanwendung brauche ich eine Möglichkeit, die TI-Messenger-Domänen. Zusätzlich können supportverantwortlichen

Ansprechpartner mit entsprechenden Serviceleveln für die TI-Messenger-Anbieter die Föderationsliste abfragen. Sie technische Schnittstebeinhaltet alle.

- Als Gesamt an der Föderantwortlicher für dietion des TI möchte ich steuern können, wer einen Zugriff auf die Pflegeschnittstell-Messengers beteiligte des VZD-FHIR-Directory erhält und jederzeit eine aktueomains. Um die Kommunikationskontrolle Überszu ermöglicht für alle Umgebunen, fragen (RU/TU/PU) haben.
- Als Gesamtverantwortlicher für TI-Messenger-Fachdie TI möchnste iauch jederzeit wissen,ab, in welche Daten im VZD-FHIR-Directory hinterlegterzeichnis (Personen- oder Organisationsverzeichnis) sind und ob diese korrekt sind bzw. Fehlermeldungen vorliegen.
- 4. Als Gesamtverantwortlicher für diech die TI-Messenger-Adressen befinden. Die Authentifizierung der TI möchte ich, dass nur berechtig-Messenger-Fachdienste Institutionen für die Pflege der Inforerfolgt mit OAuth Client Credential Flow.
- Die gemationen im VZD-FHIR-Directory die entsprechenden Berechtigungen (er)halk hat Schnittstellen, um die Daten-Qualität der Einträge zu prüfen. Dazu wird die Schnittstelle der Karten.
- 5. Als Gesamtverantwortlicher fürherausgeber genutzt. die TI muss ich sicherstellen, dass beigematik hat aber nur Leserechte.
- Die einem Ausfall oder Störungträge im LDAP-Directory werden des VZD-in das FHIR-Directory die NutzerOrganisations- und die Kartenherausgeber entsprechendes Feedback und Support erhalten und ggf. Fehlermeldungen korrekt eingepersonenverzeichnis synchronisiert. Es handelt sich um eine interne Schnittstell und weitergeleitet werdene des Verzeichnisdienstes der TI.

3.3 Nachbarsysteme

Die Nachbarsysteme des VZD-FHIR-Directory sind Client- und Serverkomponenten des TI-Messengers-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.

[<=]

4 Zerlegung des Produkttyps

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

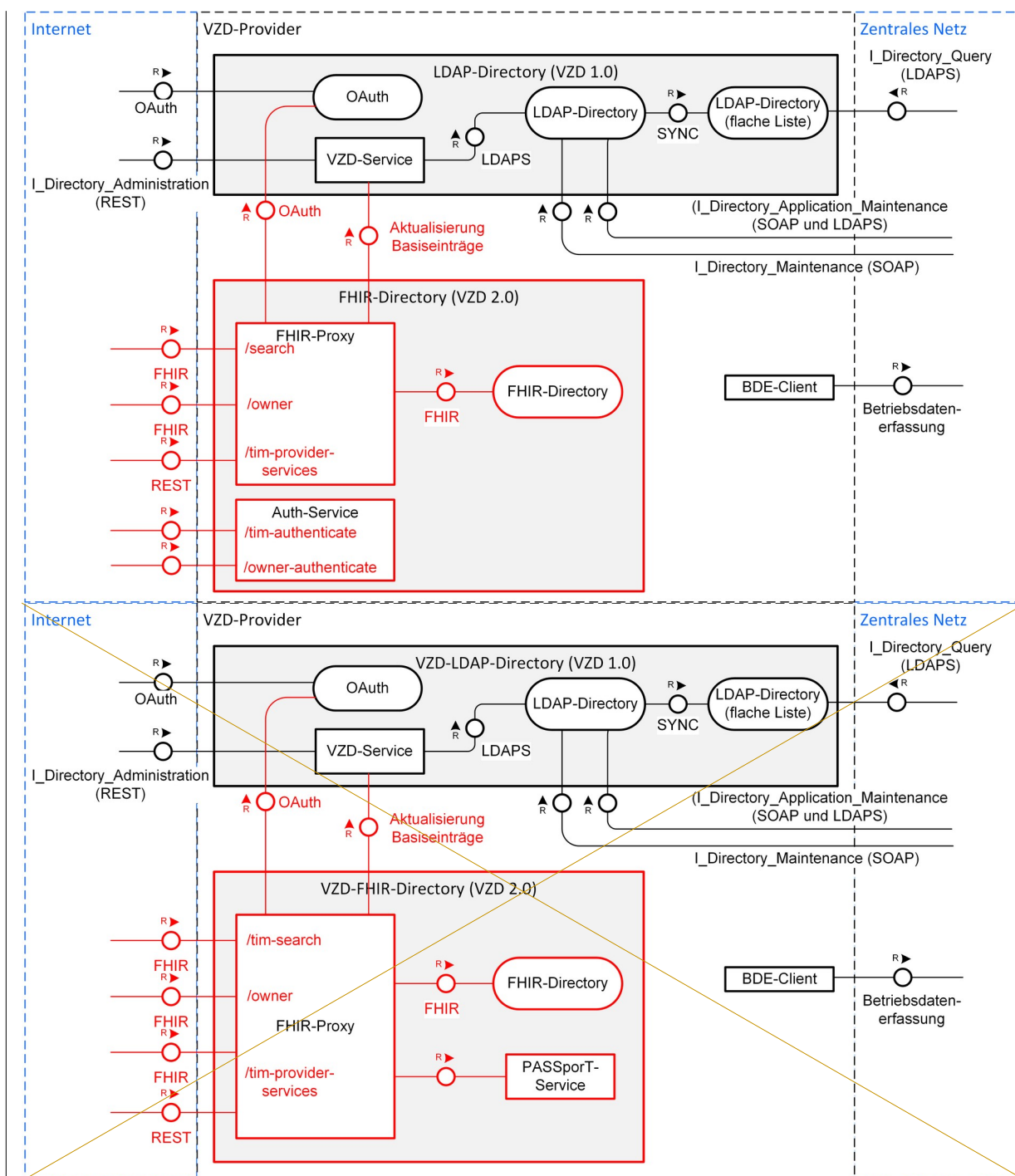


Abbildung 2: Zerlegung des VZD

Das VZD-FHIR-Directory besteht aus den Komponenten FHIR-Proxy und FHIR-Directory sowie ~~PASSPort-Service. Die SAuth-Service.~~

~~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 Verzeichnistelle-zwisdienstes integriert.~~

5 Funktionsmerkmale

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

Das FHIR-Proxy und PASSporDirectory stellt folgende Schnittstellen bereit:

- FHIRDirectoryAuthorizationService

Stellt Accesstokens zum Zugriff auf FHIRDirectory APIs aus. Es wird zukünftig zum anwendungsspezifischen Policy Decision Point (PDP) ausgebaut.

Hierbei werden die zwei folgenden REST-Service wird nicht vorgechnittstellen

- /tim-authenticate und

- /owner-authenticate

verwendet. Die Schnittstelle /tim-authenticate erwartet ein Matrix-OpenID-Token, wohingegen bei der Schnittstelle /owner-authenticate ein ID_TOKEN übergeben-

Die-vo werden muss.

- FHIRDirectorySearchAPI

Die REST-Schnittstelle /search ermöglicht die Suche nach Personen und Institutionen.

Genutzt wird die Standard FHIR Suchoperation <https://build.fhir.org/search.html>

Zur Nutzung der Suchoperation m-VZD-uss ein entsprechendes Accesstoken vom FHIR-Directory zu AuthorizationService vorliefernden Rohdaten-zgen.

- FHIRDirectoryTIMProviderAPI

Die REST-Schnittstelle /tim-provider-services ermöglicht betriebliche Prozesse für TI-Messenger Provider insb. Föderation.

Diese REST Schnittstelle wird hier definiert: <https://github.com/gematik/api-vzd/> und Ermittelter [src/openapi/I_VZD_TIM_Provider_Services.yaml](https://github.com/gematik/api-vzd/blob/main/src/openapi/I_VZD_TIM_Provider_Services.yaml)

- FHIRDirectoryOwnerAPI

Die REST-Schnittstelle /owner ermöglich die Anpassung der Auslastung und Performance wEinträge durch Identitätseigentümer zzgl. Autoritativer Daten der Kartenherausgeber.

Genutzt werden die Standard FHIR Operationen <https://build.fhir.org/http.html> mit ~~derden in den~~ Einschränkung auf eigene Ressourcen und die autoritativer Daten der Kartenherausgeber bereits vorhandenen Betriebsdaten-Erfassungs-Client (BDE-C.

Zur Nutzung dieser Operation muss ein entsprechendes Owner-Accessstokens vom FHIRDirectoryAuthorizationService vorliegen.

- ProviderAuthorizationService

Ermöglicht Authentisierung und Autorisierung der TI-Anbieter zum Zugriff auf FHIR Directory. Am Anfang nur TI-Messenger Anbieter, später auch KIM-Anbieter und zukünftige Anbieter.

Bei Aufruf der REST-Schnittstelle /tim-provider-services wird ein Accesstoken (provider-accesstoken) benötigt. Hierfür muss sich der Client bei des Verzeichnisdienstes integrieren.

6 Funktionsmerkmale

In diesem Km ProviderAuthorizationService des VZD-FHIR-Directory mittels OAuth2 Client Credentials Flow authentisieren. Zuvor MUSS der Client beim VZD-Anbieter Client-Credentials beantragen.

Geplante FHIR-Directory Schnittstellen in zukünftigen Releases:

- FHIRDirectorySearchTI apitel werden die Komponenten des VZD-FHIR-

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

- FHIRDirectories-beschrieben-yAdmin API

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

6.1 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.

6.1.1 Datenmodell

Es werden die FHIR-Ressourcen nachgemäß folgender Tabelle verwendet.

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

Tabelle 4: VZD-FHIR-Directory, FHIR-Ressourcen

FHIR-Ressource	Beschreibung
<u>OrganizaTIOrn in gematik Directory (OrganizationDirectory)</u>	<p>Profil der Organization Ressource. (https://simplifier.net/vzd-fhir-directory/tiorganizationdirectory-)</p> <p>Das Element Identifier wurde so geändert, dass Telematik-IDs als Identifier verwendet werden können (https://gematik.de/fhir/VZD-FHIR-Directory/NamingSystem/TelematikID-).</p> <p>Im Element type wird der Typ der Organisation eingetragen. Dafür werden die CodeSysteme https://gematik.de/fhirsimplifier.net/VZD-FHIR-Directory/CodeSystem/TIOrganizationTypeCSprofessionoid _und- https://gematik.de/fhir/VZD-FHIR-Directory/CodeSyst</p>

	<p>em/TIProfessionOidCS sowie das ValueSet https://gematik.de/fhirsimplifier.net/VZD-FHIR-Directory/ValueSet/TIOrganizapractionTypeVserprofessionoid verwendet.</p> <p>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 <u>d</u> sowie MXID im VZD-FHIR-Directory gesucht wurde).</p> <p>Durch den Besitzer erstellte TIOrganisations-Einträge MÜSSEN mit seinem TIOrganisations-Eintrag über eine partOf-Referenz verlinkt sein.</p> <p>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 das ValueSet https://gematik.de/fhirsimplifier.net/VZD-FHIR-Directory/CodeSystem/TIMessengerCorganizationtypevS 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 eingetragen, für die die TI-Messenger-Domain eingerichtet wurde.</p>
TIPractitioner in gematik Directory (Practitioner Directory)	<p>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/tipractitionerdirectory-)</p>
Endpoint in gematik Directory (Endpoint Directory)	<p>Endpoint Ressource (https://www.hl7.org/simplifier.net/vzd-fhir-directory/e</p>

	ndpoint.html#directory-
Location in gematik Directory (LocationDirectory)	Location (https://www.hl7.org/simplifier.net/vzd-fhir-directory/location.html#directory-)
HealthcareService in gematik Directory (HealthcareServiceDirectory)	HealthcareService (https://www.hl7.org/simplifier.net/vzd-fhir-directory/healthcareservice.html#directory-)
PractitionerRole in gematik Directory (PractitionerRoleDirectory)	PractitionerRole (https://www.hl7.org/simplifier.net/vzd-fhir-directory/practitionerrole.html#directory-)

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. [≤=]

6.1.2 Mapping von LDAP auf FHIR-Ressourcen

Die [TIOrganizationDirectory](#)- und [TIPractitionerDirectory](#)-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:

Tabelle 5: 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, stateOrProvinceN	TIPractitioner TIOrganization	address.use = work address.type = postal address.text = "streetAddress
postalCode 
localityName

	ame		- 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	-	-

https://github.com/gematik/api-vzd/blob/master/docs/LDAP2FHIR_Sync.adoc.

6.1.3 FHIR RESTful API

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

6.2 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-Proxy und PASSport-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 Service

uchergebnis enthält dann in Bundle.total die Gesamtzahl der gefundenen Einträge, aber nicht die die Einträge selbst.

6.3 FHIR-Proxy

6.3.1 Schnittstellen

Alle Verbindungen des FHIR-Proxy sind TLS-Verbindungsschlüsselt. Der Proxy weist sich gegenüber den Clients aus. Für den Zugriff der Clients auf den FHIR-VZD werden signierte Access-Tokens vergeben.

6.3.1.1 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.

6.3.1.2 FHIR Schnittstelle für TI-Messenger-Nutzer_ FHIRDirectorySearchAPI

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>

In der Referenzumgebung ist die URL:- <https://ru-vzd-fhir-directory-testref.vzd.ti-dienste.de/tim-search>

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

Authentisierung

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

Das

Das Search-Accessstoken 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.

Die zeitliche Gültigkeit des Search-Accessstokens beträgt 24 Stunden.

Endpunkte für die Authentisierung

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

In der Referenzumgebung ist die URL: <https://ru-vzd-fhir-directory-testref.vzd.ti-dienste.de/tim-authenticate>

In der Testumgebung ist die URL: <https://tu-vzd-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 zusätzlich zur HL7 FHIR Spezifikation wie im RFC[8225] gefordert erfolgen und wie FHIR VZD 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 Note Suchparameter unterstützen:

- practitioner.qualification

location angegeben. Das folgende Beispiel zeigt eine solche Struktur.

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



endpoint.ad 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-ress (z.B. Suche nach TI-Messenger Adresse)

6.3.1.3 FHIR-Schnittstelle für Besitzerer **FHIRDirectoryOwnerAPI**

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 (**TI**PractitionerDirectory oder **TI**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>

In der Referenzumgebung ist die URL: <https://ru-vzd-fhir-directory-testref.vzd.ti-dienste.de/owner>

In der Testumgebung ist die URL: <https://tu-vzd-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 **TI**OrganizationDirectory-Eintrag KÖNNEN weitere **TI**OrganizationHealthcareService-Einträge erstellt und mit dem eigenen **E**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" ],
  "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.

EndeDie zeitliche Gültigkeit des Owner Accesstokens beträgt 24 Stunden.

Endpunkte für die Authentisierung

In der Produktionsumgebung ist die URL:

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

In der Referenzumgebung ist die URL:

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

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

FHIR VZD Referenzendpunkte für die Authentisierung mit dem SmartcardIDP

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

In der Referenzumgebung ist die URL: <https://ru-vzd-fhir-directory-testref.vzd.ti-dienste.de/owner-authenticatesignin-gematik-idp-dienst>

In der Testumgebung ist die URL: <https://tu-vzd-fhir-directory-test.vzd.ti-dienste.de/owner-authenticatesignin-gematik-idp-dienst>

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.

Schnittstelle Daten

Das VZD-FHIR-Directory Datenmodell wird in Simplifier beschrieben [Simplifier-FHIR-VZD].

Für TI Anwendungen werden die Kommunikationsadressen in den FHIR Endpoint eingetragen:

Tabelle I-X: Tab_VZD_TI-Anwendungen_Endpoint

<u>TI Anwendung</u>	<u>Endpoint.connectionType code</u>	<u>Endpoint.address</u>
<u>TI Messenger</u>	<u>tim</u>	<p>Format (MXID in URL Form) für User entsprechend [matrix-uri-scheme]:</p> <p><u>matrix:u/localpart:domainpart</u></p> <p>Beispiel MatrixID: <u>@1-1tst-auto-ts-ow2:</u> <u>tim.test.gematik.de</u> MatrixID im URL Format in Endpoint.address: <u>matrix:u/1-1tst-auto-ts-ow2:</u> <u>tim.test.gematik.de</u></p>

6.3.1.4 Schnittstelle FHIRDirectoryTIMProviderAPI (I_VZD_TIM_Provider_Services.yaml)

Endpunkte

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

In der Referenzumgebung ist die URL: <https://ru-vzd-fhir-directory-testref.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>

Authentisierung

Um die Schnittstelle nutzen zu können, muss sich der Registrierungsdienst des TI-Messenger-Anbieters zuerst mit einem ti-provider-Accesstoken authentisieren, das vom OTI-Provider OAuth-Server des VZD-Anbieters ausgestellt wurde. Das ti-provider-Accesstoken hat eine Gültigkeitsdauer von 305 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://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,
  "scopeclientid": "tim-provider-services<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.

EndDie zeitliche Gültigkeit des provider-accesstokens beträgt 24 Stunden.

Endpunkte für die Authentisierung

am VZD-FHIR-Directory Auth-Service

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

<https://oauth.vzd.ti-dienste.de/ti-provider-authenticate>

In der Referenzumgebung ist die URL:—

~~<https://ru-oauth-test.vzd.ti-dienste.de/authenticate>~~

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

Registrierung

Für den Zugriff auf den [OTI-Provider OAuth-Server](#) MUSS der TI-Messenger-Anbieter für seinen Registrierungsdienst beim VZD-Anbieter Client-Credentials beantragen. Die Beantragung erfolgt über einen [Segenempfehlungspflichtigen Service-Request](#) an 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](#).

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

- Angaben zur Rolle (hier [Admin TI-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-Sern der clientID](#).
- [Registrierungsserver ID_TOKEN-claim Signatur-Zertifikat \(wird für die vereinfachte Authentisierung an dieser schnchnittstelle bei der Token Prüfung benötigt\)](#)

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/in/src/openapi/I_VZD_TIM_Provider_Services.yaml

Tabelle 6: 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/ <u>federationList.jws</u>	Mit dieser Operation wird die Liste der an der TI-Messenger-Föderation beteiligten Matrix-Domainnamen abgefragt (Föderationsliste).
GET / <u>PASSporTCertificateslocalization</u> <u>"whereIs"</u>	<u>Mit Gibt für dieser Operation werden übergebene MXID den Teil des die PASSporT-Signatur-Zertifikate abgefragt zurück, in dem die MXID enthalten ist.</u>
POST /federation <u>"addTiMessengerDomain"</u>	<u>Eine Domäne zur Föderation hinzufügen.</u>
GET /federation <u>"getTiMessengerDomain"</u>	<u>Lesen einer oder aller eigener Domains.</u>
GET, POST, PUT, DELETE- /FHIRPUT /federation <u>"updateTiMessengerDomain"</u>	Die FHIR-Operationen für das Ändern von eigenen TI-Organization-Einträgen und von Endpoint-Einträgen im VZD-FHIR-Directory sind in der HL7-FHIR-Spezifikation (https://www.hl7.org/fhir/http.html) fAktualisierung einer Domainestgelegt.
DELETE /federation <u>"deleteTiMessengerDomain"</u>	<u>Löschen einer Domäne.</u>
GET /federationCheck <u>"checkTiMessengerDomains"</u>	<u>Prüft, ob alle eigenen Domains (durch Token ermittelbar) zu aktiven Organisationen gehören. Gibt die eigenen Domains zurück, die zu inaktiven Organisationen gehören.</u>

Im Attribut "sub" des Accesstoken_s ist die client_id des TI-Messenger-Registrierungsdienstes enthalten. ~~Wenn der TI-Messenger-Registrierungsdienst~~

Bei Hinzufügen einen TI-Organizr Domain zur Föderation-Eintrag erzeugt, dann (addTiMessengerDomain) MUSS die client_id im er FHIR VZD prüfen, ob für die dazugehörnde tElement-alias-desatikID Einträge enthalten seine aktive Organisation vorliegt.

6.3.2 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.

Z.

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.

6.3.3 Erzeugung und **Verteil**bereitstellung der Föderationsliste

Der FHIR-Proxy Föderationsliste MUSS bei jeder Änderung an den Endpoint-Einträgen derder Domains und/oder telematikIDs durch TIM-Messenger-Anbieter neu erzeugt und zum Download über die Schnittstelle `I_VZD_TIM_Provider_Services` bereitgestellt werden.

Die Föderationsliste hat folgende Struktur:

```
{
  "version": <Version der Föderationsliste (Integer)>,
  "domainList": [
    {
      "domain": "Domain",
      "telematikID": "Telematik-ID der Organisation, welche die Domain nutzt",
      "isInsurance": false,
      "timAnbieter": "Zuweisungsgruppe im TI-ITSM-System vom TI-Messenger
        Anbieter,
        der die Domain angelegt hat"
    }
  ]
}
```

Der Wert für "timAnbieter" MUSS vom AZPD bei der Beantragung der Credentials des TI-Messenger-Anbieters/-Herstellers erfasst und anschließend über ein internes Netz 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-Proxy-InstanzDirectory geändert werden. Mit dieser Automatisierung sollen manuelle Fehler beim Setzen durch die Nutzer verteilt sowie für die Abfrage über die Schnittstelle beseitigt werden.

Die Föderationsliste MUSS mit einer JWS gemäß RFC7797 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 MUSS im Signatur-Header enthalten sein.

Der Signatur-Header hat folgende Struktur:

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

Die `I_VZD_TIM_Provider_Services` signierte Föderationsliste hat gemäß RFC7797 folgende Struktur:

Signatur-Header.Föderationsliste.Signatur

```
{
  "payload": "<Föderationsliste, BASE64URL>",
  "signatures": [
    {

```



```

    "header":<Signatur-Header>,
    "signature":<signature, BASE64URL>
  }
}
}

```

Die bereithalten.

einzelnen Bestandteile der signierten Föderationsliste sind Base64 kodiert.

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

■

■

[eyJ4NWMiOiSiTUZvd0ZBWUhLb1plemowQ0FRWUpLeVFEQXJlSUFRRUhBMElBQkjpMkt6RlEybEs0TFMyajjVNnpYTjkR2w1dG5TSnlGeUNMW3cyM3h1NEExhY2FRROGNHBY0pPdkI4Z3dwajBzQkZvNnpjMUFBaVhjdBVhkbUc1TWFwenlZPSjdLCj0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ2ZXJzaW9uUljo1MDYslmhhc2hBbGdvcmI0aG0iOiJTSEETMjU2liwiZG9tYWluTGldCl6W3siZG9tYWluUljo1MDY3MmQ0M2Q1OWI5MWNjZTMwNjY3MzMzMmQ3MTI1ZGlwY2JiMzA5YW12ODkzM2Y4MGNI MGnmNTU3MDg4MTBIYSIsInRlbGVtYXRpa0EljoiMS0xYXJ2dHNOLWF1dG8tdHMTMDAwMSIsImlzSW5zdXJhbmNlljpmYWxzZX0seyJkb21haW4iOiJlNjRkM2VmYmMyNzk3ZDg0Y2NIOGM0NjAwMTNkYTfmMThiMWE1NTYzNWVhZTBhYTE4ZTljZmQxMGEzYWMyNGQ4liwiZGVsZW1hdGlrSUI0ilxLTfhcnZ0c3QtdGVzdC10cDA3LTAzliwiaXNJbnN1cmFuY2UiOmZhbnHNlfSx7ImRvbWFPbil6ljMzNTJhZjFhZThkY2Y4MjllYjY0YjdITyY2NDk0OTAxMzM4NTg2MGYyZTFINDBjNTUxMmVhYTk2ODg3YjdlNjEiLCJ0ZWxlbWFOaWtJRCl6ljEtMWFydndRzdC10ZXN0LXRwMDgtMDEiLCJpc0luc3VyYW5jZSI6ZmFsc2V9LHsiZG9tYWluUljo1YjRhZTM3OTZhN2Q5YWYzYzdiNmNhNzU5MzYxZTIhZDkyZjK0NmU3ZmFkNzZkZGVkZDEzM2U5ZTBhNjUwMTg1OClSlrNlBgvTYXRpa0EljoiMS0xYXJ2dHNOLXRlc3RvcmtctdHAwOS4wMCIsImlzSW5zdXJhbmNlljpmYWxzZX0seyJkb21haW4iOiJlN2RmNjRmOTQ1NGRkMDA3NjcXZmQ1MjUzYmNjNmMwYzl mZWJkMzBhZTlxZjQ3YjQwZmFINDCzZWQ0NzA2NzM0liwidGVsZW1hdGlrSUI0ilxLTfhcnZ0c3QtdGVzdG9yZy10cDA5LjAxliwiaXNJbnN1cmFuY2UiOmZhbnHNlfSx7ImRvbWFPbil6ljg5NDU3M2U3ZmjhNjYxODE1MGZkMWNkMzUwOTQ5NGE1YT Y2NWM1ZjRiZmQ0YzY4MjlmZmE5NTM0NWZjYTUxYjAiLCJ0ZWxlbWFOaWtJRCl6ljEtMWFydndRzdC10ZXN0b3JnLXRwMDkuMDIlLCJpc0luc3VyYW5jZSI6ZmFsc2V9LHsiZG9tYWluUljo1NWY1YTZhOTA4ODNIMDZjMjEyODAaz mE3OTlwNGUZm2M1MzZkNjgyNTc0MGM5MGVIOGEXMDU3ZDMwZTE4ZTNhZSIsInRlbGVtYXRpa0EljoiMS0xYXJ2dHNOLXRlc3RvcmtctdHAwOS4xliwiaXNJbnN1cmFuY2UiOmZhbnHNlfSx7ImRvbWFPbil6lmY4NzU1YjRiODk0MTViZjNkOGI1YTl4Zm12MzAwYTBhNzE5MDund-den-connectionType.code == "tim-domain" haben.](#)

Für jeden Endpoint-Eintrag wird aus dem Wert des Elements "name" mit dem Hash-Algorithmus "SHA-256" ein

[hash2XNGU0OTQ3YTAzWDEi4MTUyZjJwZDc2YTg4MzQiLCJ0ZWxlbWF0aWtJRCl6lEtMWFydRzdC10ZXN0LXRwMDUeImlCjpc0luc3VyYW5jZSI6ZmFsc2V9LHsiZG9tYWluljoiN2FiNWFKYi](#)
[k1MWZIYmY5ZjUxM2Q4ZDQ3OWYyNjgzMTYzMWU5NGZmNDYwMDkwNTk2Mjk2NWU0NGI](#)
[0MjKxMDAwYiIsInRlbGVtYXRpa0ElEioiMS0xYXJ2dHN0LXRlc3QtdHAwNGEiLCjpc0luc3VyYW5j](#)
[ZSI6ZmFsc2V9LHsiZG9tYWluljoiZGM5Nzg1YjFjNDU5ZjlmZjk3NWFiNGY2NWM3YTUwNzRkY](#)
[TFiYWFiMzc4N2Q5ZDg5OGNkNTE3MWQ5NjdhdTUzNSIsInRlbGVtYXRpa0ElEioiMS0xYXJ2dH](#)
[N0LXRlc3QtdHAwNi1hliliwiaXNJbnN1cmFuY2UiOmZhbmhNfSx7ImRvbWFPbil6ImY2MDQ2OT](#)
[BmNTg2ZTQzYzRiY2FmMmQ5ODM2MTI4NWE3NGY2NDEzY2M4MTBiMzhhyY2FmMTliMdc3Z](#)
[TAzZDIyN2MiLCJ0ZWxlbWF0aWtJRCl6lEtMWFydRzdC10ZXN0LXRwMDYtMDEiLCjpc0luc3](#)
[VyYW5jZSI6ZmFsc2V9LHsiZG9tYWluljoiOWZmNDE0NDNINGUwZDI0YzZkMGNI0GQwYWU2](#)
[YTEzNWRkYzc3ZjUxZGVIMmZmNDI4OWViMjkyZGZkZDY3NjcxcMyIsInRlbGVtYXRpa0ElEioiM](#)
[S0xYXJ2dHN0LXRlc3QtdHAwNi0wMiIsImIzSW5zdXJhbmlNlljpmYWxzZX0seyJkb21haW4iOiJj](#)
[NiYwYTMvN2QwNWZmNjNiZWFIN2ZhN2M0MWRkODY2ZmEzMzlmN2M2OTdiODIIZThiMWU](#)

[illegible]

ML-123677 - Maßnahmen gebildet und **igen die Manipulation** dieer Föderationsliste eingetragen. **(VZD-FHIR-Directory, Sicherheitsgutachten)**
Im Sicherheitsgutachten des VZD-FHIR-Directories sind geeignete Maßnahmen gegen die Manipulation der Föderationsliste **MUSS** das Element **has** beschrieben. **[<=]**

6.3.4 Lokalisierung einer MXID (Operation wherels)

Die Operation prüft, in welchem Teil des Directorys (Organisation, Person) eine MXID enthalten ist. Der Algorithmus den Wert "SHA-256" haben

(siehe `I_VZD_TIM_Provider_Services.yaml`)ten ist, und gibt das Prüfergebnis zurück.

Übergeben wird die MXID an die Operation in URL Form.

Damit diese Operation performant ist, darf bei Aufruf der Operation nicht der gesamte FHIR Datenbestand durchsucht werden. Dies kann z. B. durch eine Performance-optimierte Tabelle mit den MXIDs und dazugehörigem Ergebnis gewährleistet werden.

Die Aktualisierung der Föds Clients erfolgt für Operationsliste `whereIs` entsprechend KANN so implementiert werden, Kapitel 4.2.1.4 Schnittstelle FHIRDirectoryTIMProviderAPI.

Der FHIR-Proxy MUSS die Lokalisierung einer MXID über Operation wherels performant bereitstellen. Dazu MUSS nur die Federationslisten (der MXID darin) die benötigten Daten für die performante Antwort der wherels Operation aktualisiert werden (z. B. überen. Der FHIR-Proxy DARF NICHT die originalen FHIR R4.5.1 Subscrip-Daten für die Ausführung der wherels Operations; siehe <https://build.fhir.org/subscription.html>).

6.4 Übergreifende Vorgaben

Sicherheit und Datenschutz

Der Anbieter/ei folgenden Vorgaben gelten auch für des-n FHIR-VZD-FHIR-Directori.

TIP1-A 5546-01 - VZD, Integritäts- u. Authentizitätsschutz

Der Anbieter des VZD MUSS geeignete Maßnahmen vorsehen, die verhindern, dass die Födie Integrität und Authentizität der im VZD gespeicherten Daten gemäß den Richtlinien des Bundesamtes für Sicherheit in der Informationsliste manipuliert werden kann.

technik für allgemeine Verzeichnisdienste, [BSI APP.2.1], implementieren.【<=】

23677ML-123677TIP1-A_5548 - Maßnahmen geVZD, Protokollierung der Änderungsoperationen

Der VZD MUSS Änderungen ~~die Manipulation der Föderationsler~~ Verzeichnisdiensteinträge protokollieren und muss sie 6 Monate zur Verfügung halten.
[<=]

6 Monate ist die maximale Nachweiste ~~(VZD-FHIR-Directory, Siehe, ohne in den Bereich der Vorratsdatenspeicherheitsgutachten)~~ Im-Sung zu kommen.

TIP1-A_5549 - VZD, Keine Leseprofilbildung

Der VZD DARF Suchanfragen NICHT ~~speicherheitsgutan~~ oder protokollieren.
[<=]

TIP1-A_5550 - VZD, Keine Kopien von gelöschten des Daten

Der VZD-FHIR-Directories sind geeignete Maßnahm ~~DARF~~ von gelöschten Daten KEINE Kopien speichern.
[<=]

TIP1-A_5551 - VZD, Sicher gegen Datenverlust

Der Anbieter des VZD MUSS den ~~Dienst~~ gegen die Manipulationatenverlust absichern.
[<=]

TIP1-A_5552 - VZD, Begrenzung der FöSuchergebnisse

deration VZD MUSS die Ergebnisliste ~~beschriebeiner~~ Suchanfrage auf 100 Suchergebnisse begrenzen.
[<=]

6.5 ÜbDie 100 Suchergreifende Vorgaben

6.5.1 Sicherheit

~~Schutz vor Si~~ebnisse beziehen sich auf die FHIR Ressourcen HealthcareService bzw. PractitionerRole. Alle referenzierten und durch Suchparameter "include" einbezogenen Ressourcen werden bei der Begrenzung der Su**cherheits-Risiken**gebnisse nicht mitgezählt.

Das ~~VZD-Bundle~~ im FHIR-Directory MUSS Maßnahm Suchergebnis MUSS immer zu jeder enthaltenen FHIR Ressource HealthcareService bzw. PractitionerRole alle referenzierten und durch "include" einbezogenen Ressourcen enthalten zum Schutz vound damit ein vollständiges Paket der enthaltenen Ressourcen darstellen.

TIP1-A_5553 - VZD, Private Schlüssel sicher Speicherheits-Risiken gemäß-n

Der VZD MUSS seine privaten Schlüssel sicher speichern und ihr Auslesen ver hinder-aktueh n um Manipulationen zu Version- hinde-OWASP-Top-10-umsetzn.
[<=]

TIP1-A_5554-01 - VZD, Registrierungsdaten (https://owasp.org/www-project-top-ten/-).sicher speichern

Es gelten Die AnfordDer VZD MUSS die Integrität und Authentizität der gespeicherten Registrierungsdaten an-TLS-Verbindungen gemäß [gemgewährleisten].[<=]

TIP1-A_5556 - VZD, Fehler Logging

Der VZD MUSS lokal und remote erkannte Fehler in seinem lokalen Spec_Krypt#3.3.2]-TLS-Verbindungicher protokollieren.

[<=]

23682ML-123682TIP1-A_5558 - MaßnahmVZD, Sicheres Speichern der TSL
Der VZD MUSS die Inhalte der TSL in einem lokalen en zum Schutz vor Trust Store
Sicherheits-Risik speichern und für X.509-Zertifikatsprüfungen lokal zugreifbar halten.

[<=]

Das X.509-Root-CA Zertifikat MUSS für Zertifikatsprüfungen en (im Truststore des FHIR
VZD- gespeichert sein.

Der FHIR-Directory, VZD MUSS wöchentlich prüfen, ob neue X.509-Root-CA-Versionen
existieren und Cross-Zertifikate verfügbar Sicherheitsgutnd. Falls dies der Fall ist, so
MUSS der FHIR VZD diese neuen Root-Versionen in seinen Truststore importieren.

Nachten)

Im Sicherheitsgutachte der Erzeugung einer neuen Root-Version der X.509-Root-CA der TI
wird dessen selbstsigniertes Zertifikat und Cross-Zertifikate auf den Download-Punkt
gemäß [ROOT-CA] abgelegt. Automatisiert kann desr FHIR VZD-FHIR-Directories sind
geeignete Maßnahmen zum Schutz vor Sicherheits-Risiken gemäß von dort die
Verfügbarkeit neuer Versionen überwachen. Zusätzlich kann der folgende Download-
Punkt unter [ROOT-CA-JSON] verwendet werden. Dort werden die aktuellen Root-
Zertifikate inkl. deren Cross-Zertifikate gepflegt. Im Regelfall wird alle zwei Jahre eine
neue Root-Version erzeugt. Die Dateigröße der heruntergeladenen JSON-Datei kann man
als Hashfunktion verwenden. Hiermit kann man beispielsweise mit Hilfe des Tools curl die
HTTP-Methode HEAD verwenden und damit erfahren ob die lokale Kopie der aJSON-Datei
noch aktuellen Version der OWASP Top-10 beschrieben. [<=] ist. Die JSON-Datei ist ein
Array, in dem Associative Arrays als Elemente aufgeführt werden. Diese Elemente
enthalten je ein Root-Zertifikat inkl. Cross-Zertifikate für das chronologisch
vorhergehende und das nachfolgende Root-Zertifikat. D. h., kryptographisch gesehen
stellt dies eine doppelt verkettete Liste dar.

Die Sub-CA Zertifikate werden auf dem Download-Punkt gemäß [Sub-CA] abgelegt.

6.5.2 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 Verfügbarkeidie
Bearbeitungszeit von 99,8 % zur Hauptzeit und 99 % zur Nebenzzeit betreibbar sein.

Der Anbieter des vorgaben unter Last aus Tab_VZD_FHIR-Directories MUSS sein Produkt-
VZD-FHIR-Directory mit einer vollumfänglich-f_Perf unter der für alle Funktionalen
Verfügbarkeit von 99,8 % zur Haupparallel anliegenden Spitzeit und 99 % zur Nebenzzeit-
betrenlast erfüllen.

Tabelle 7: Tab_VZD_FHiben.

R_Perf

<u>Schnittstellenoperation</u>	<u>Lastvorgabe n Spitzenlast [1/sec]</u>	<u>Bearbeitungs- zeitvorgaben Mittelwert [msec]</u>	<u>Bearbeitungs- zeitvorgaben 99%-Quantil [msec]</u>
<u>FHIR Schnittstelle für TI-Messenger-Nutzer (/search)</u>	<u>1000</u>	<u>1000</u>	<u>1250</u>
<u>FHIR-Schnittstelle für Besitzer (/owner)</u>	<u>20</u>	<u>1000</u>	<u>1250</u>
<u>Schnittstelle I_VZD_TIM_Provider_Services (/tim- provider-services)</u>			
<u>- getFederationList</u>	<u>1</u>	<u>1000</u>	<u>1250</u>
<u>- whereIs</u>	<u>50</u>	<u>1000</u>	<u>1250</u>
<u>- addTiMessengerDomain</u>	<u>1</u>	<u>1000</u>	<u>1250</u>
<u>- getTiMessengerDomain</u>	<u>1</u>	<u>1000</u>	<u>1250</u>
<u>- updateTiMessengerDomain</u>	<u>1</u>	<u>1000</u>	<u>1250</u>
<u>- deleteTiMessengerDomain</u>	<u>1</u>	<u>1000</u>	<u>1250</u>
<u>- checkTiMessengerDomains</u>	<u>1</u>	<u>1000</u>	<u>1250</u>

7 Anwendungsfälle

7.1 TI-Messenger-Nutzer sucht ~~TI~~Organization- und ~~TI~~Practitioner-Einträge im ~~VZD~~-FHIR-Directory

AF_10036 - ~~TI~~Messenger-Nutzer sucht ~~TI~~Organization- und ~~TI~~Practitioner-Einträge im ~~VZD~~-FHIR-Directory

Attribute	Bemerkung
Beschreibung	<p>TI-Messenger-ClientsNutzer können im VZD-FHIR-Directory nach TIOrganizationHealthcareServiceDirectory- und TIPractitionerRoleDirectory-Einträgen suchen. <u>Dazu ist eine Authentisierung am Auth-Service erforderlich. Hier ist die Authentisierung mit TI-Messenger-Clients beschrieben.</u></p> <p>Wenn im TI-Messenger-Client kein gültiges <u>tim</u>-Accesstoken vom <u>FHIR-ProxyAuth-Service</u> 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 <u>/tim-search-mit-den-Suchparameternauthenticate-des-Auth-Services</u> aufgerufen. Der <u>FHIR-ProxyAuth-Service</u> 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 <u>FHIR-ProxyAuth-Service</u> ruft am Matrix-Homeserver die Operation GET/openid/userinfo mit dem Matrix-OpenID-Token als Parameter auf und erhält <u>die Bestätigung für in der Response</u> die MXID des TI-Messenger-Nutzers. Damit ist die Authentisierung des Nutzers abgeschlossen. Der <u>FHIR-ProxyAuth-Service</u> erstellt ein <u>Accessearch-accesstoken</u>, <u>dass die MXID des TI-Messenger-Nutzers enthält un und</u> sendet es an den TI-Messenger-Client.</p> <p>Der TI-Messenger-Client sendet ein GET Request gemäß FHIR-Spezifikation an den Endpunkt <u>/tim-search</u> des FHIR-Proxy. Im Authentication Header ist das <u>Accesstoken (inklusive MXID des Nutzers)</u> enthalten. <u>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</u><u>search-accesstoken</u> enthalten.</p> <p>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.</p> <p>Die <u>gefundenen TIOrganization- und TIPractitioner-Einträge können in telecom Elementen MXIDs in url Notation</u> 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, <u>Response</u> 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-</p>

	<p>Datenstruktur der Response an die url notierte MXID des gefundenen Nutzers in folgender Form angehängt: matrix:u/localpart:tim-domain/?PASSporT=[PASSporT-String].</p> <p>Gefundene Einträge ohne MXID und PASSporT werden aus der Response entfernt.</p> <p>Die so geänderte Response wird an den TI-Messenger an den TI-Messenger-Client gesendet.</p> <p>Die Anzahl der gefundenen und zurückgegebenen Einträge wird initial auf 100 begrenzt. 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.</p>
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.

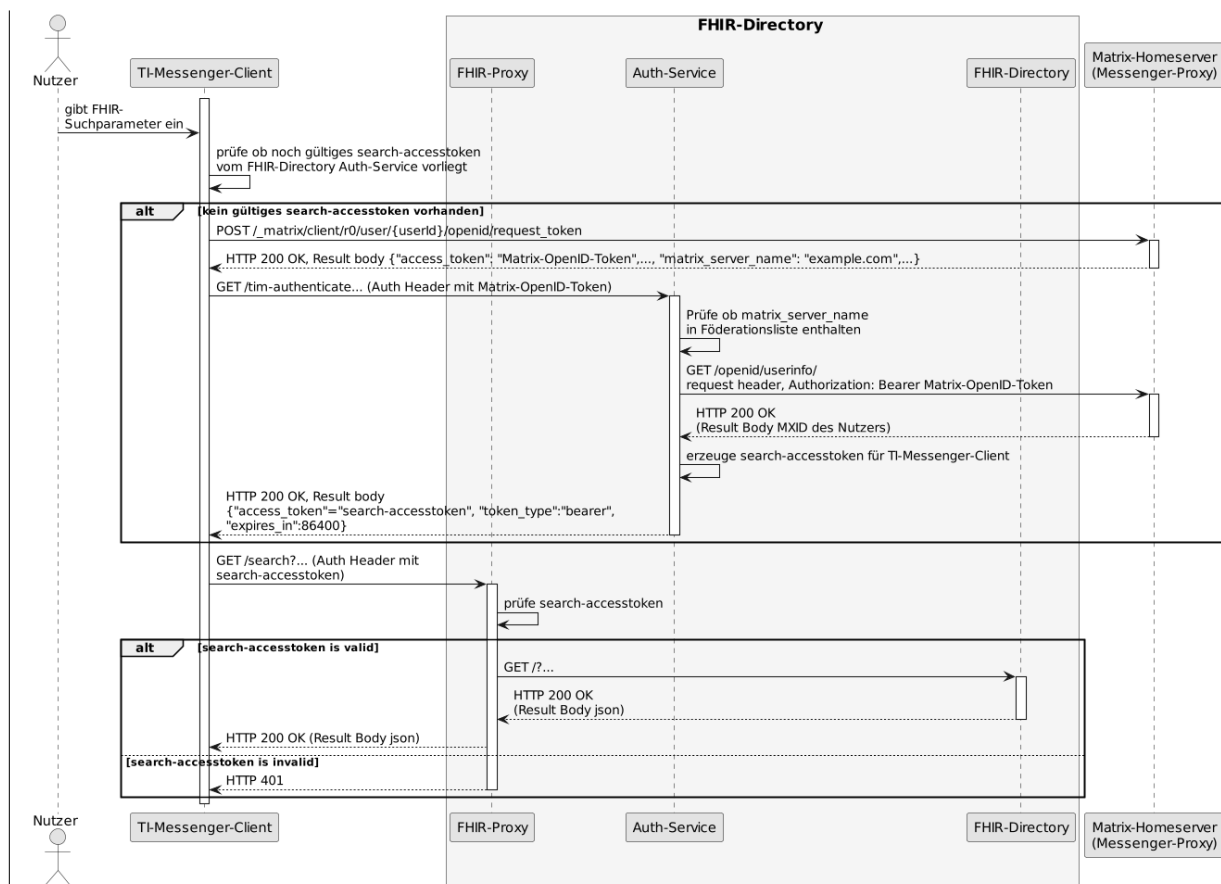


Abbildung 3: Sequence diagram /tim-search

[<=]

Akzeptanzkriterien für den Anwendungsfall AF_10036 Nutzer sucht TI-Organization- und TI-Practitioner-Directory-Einträge im VZD-FHIR-Directory

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

Am Endpunkt /tim-search des FHIR-Proxy darf die Authentifizierung nur für NutzerRequests erfolgreich sein, die an einem Homeein gültiges search-accesstoken im Authentication Header enthalten, das vom Auth-server der TI-Messengice ausgestellt wurde. [<=]

Eigentümer Föderation registriert sind. [<=]t seinen Eintrag im FHIR-Directory

3483ML-123483AF_10037 - PASSporT-Erzeugen Einträge im VZD-FHIR-Directory ändern

Attribute	Bemerkung
Beschreibung	<p>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.</p> <p>Wenn der Org-Admin 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 Auth-Service bekannt. Für den Aufruf der FHIR-Operationen durch den Client stellt der Auth-Service dem Client ein owner-accesstoken aus, dass auch die Telematik-ID des LE oder der Organisation enthält.</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>

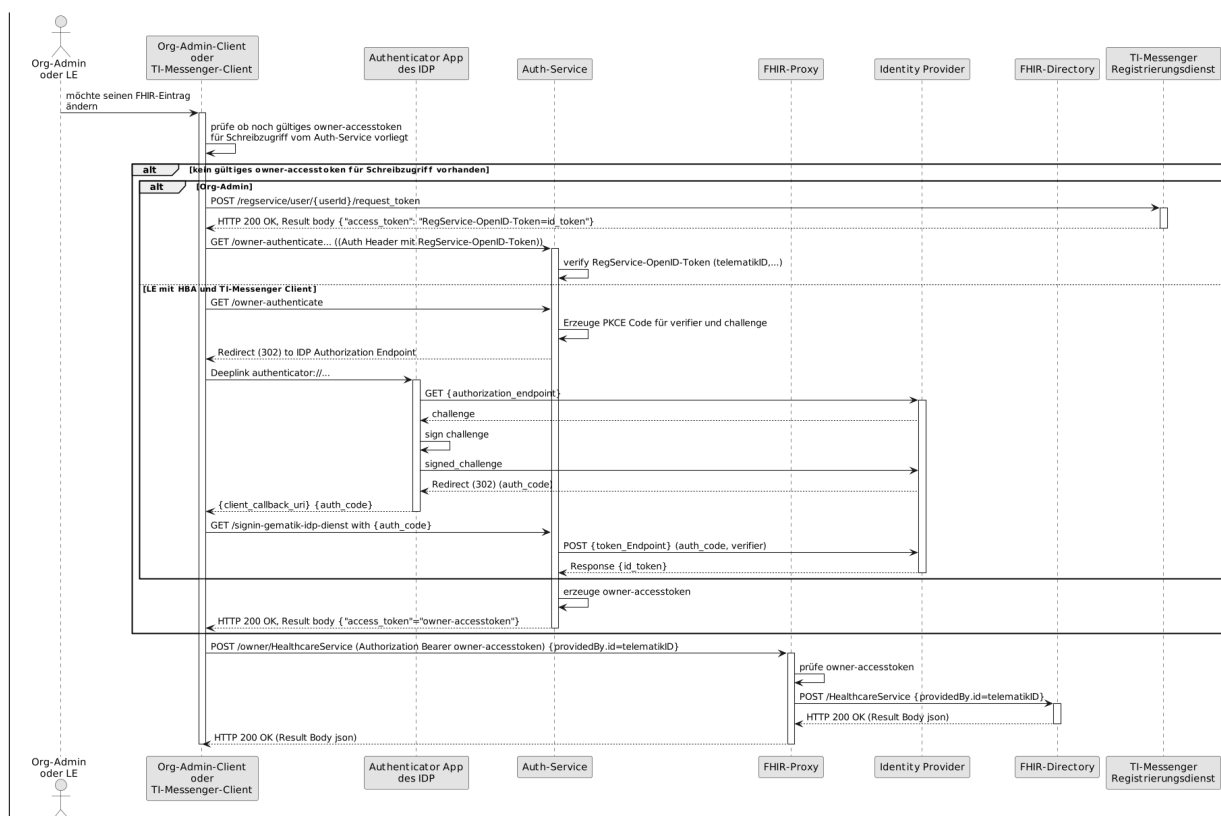


Abbildung 4: Sequenzdiagramm VZD-FHIR-Directory, Sicherheitsgutachten)

Der FHIR-Proxy darf nur PASSport aus Änderung von eigenen OrganizationDirectory- oder PractitionerDirectory-Einträgen

[<=]

Ein Org-Admin-Account kann am Registrierungs-Dienst nur angelegt werden, wenn eine erfolgreiche Authentisierung einer Organisation durchgeführt wurde. Dafür muss das FHIR-Directory den Registrierungs-Diensten allen, wenn im telecom Elementr TI-Messenger-Anbieter vertrauen und die erforderlichen Daten (telematikID, Zertifikatstyp, technische Rolle) im id_token des Eintrags eine MXID in url-Form vorhanden Registrierungs-Dienstes prüfen.

Das Vertrauen zu den Registrierungsdiensden der TI-Messenger Anbieter wird bei der Regist und das period.endDate nicht in der Vergangenheit liegt. **[<=]**

TIOrganization-Einträge oder TIPractitioner-Einträgerierung des TI-Messenger Anbieters beim FHIR-Directory für die Schnittstelle I_VZD_TIM_Provider_Services hergestellt (siehe auch Kap. 4.2.1.4 Schnittstelle FHIRDirectoryTIMProviderAPI).

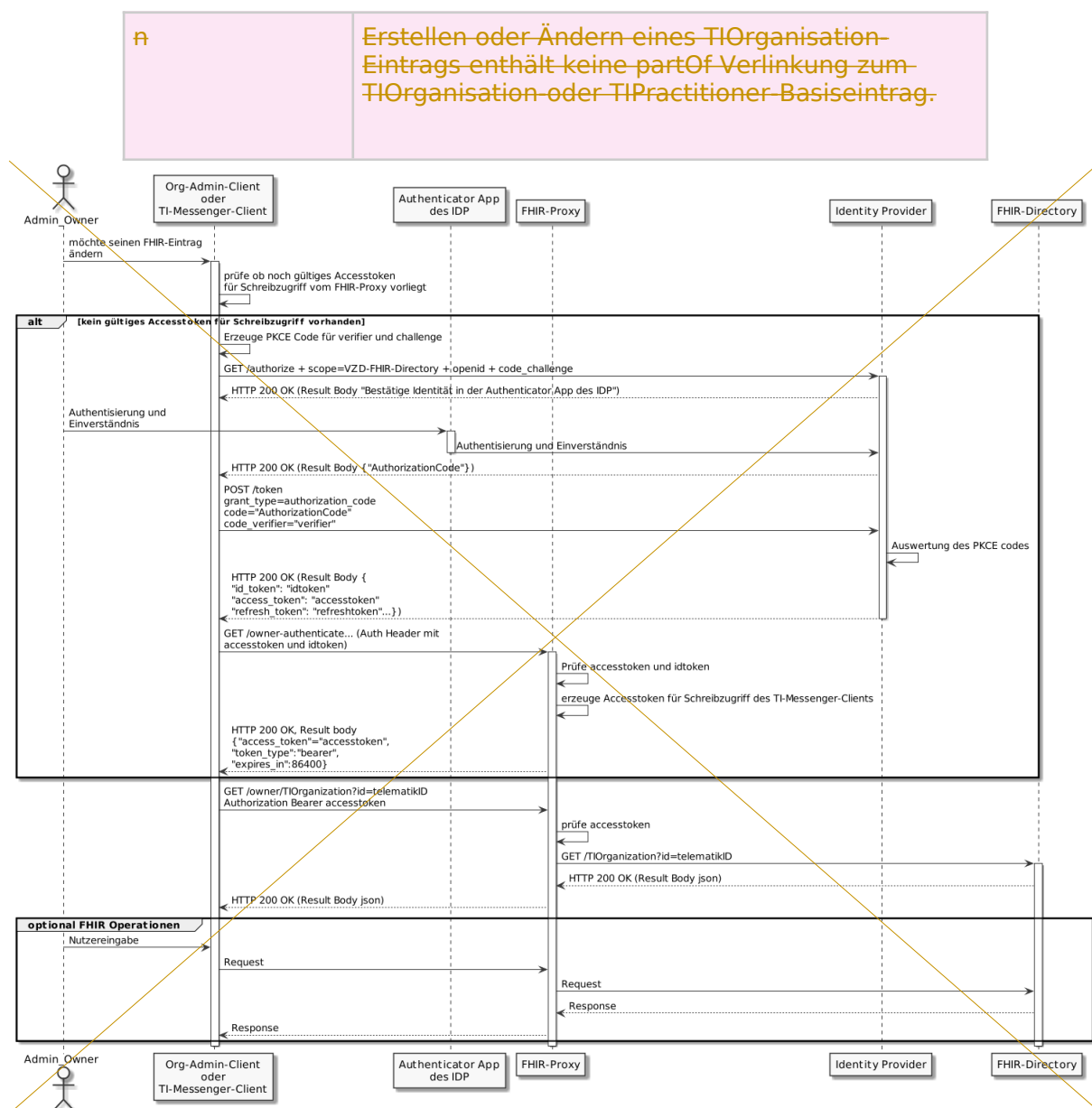
7.2 Bei der Registrierung des TI-Messenger Anbieters wird das Signatur-Zertifikat, das für die Signatur des id_tokens verwendet wird, im VZD-FHIR-Directory ändern

- Mainline_OPB1/hinterlegt.
- Dieses Signatur-Zertifikat wird bei der Token-Prüfung gegen das verwendete Signatur Zertifikat geprüft (siehe Akzeptanzkriterium 22872AF_10037 – TIOrganization-Einträge od36890).

Die Abfrage der owner-accesstoken erfolgt entsprechend dem Kontext / Client / relevanten IDP über **TI Practitioner-Einträge im VZD** die dazu passende URL. Aktuell wird nur den Gematik-IDP unterstützt und damit ist die entsprechende URL [/signin-gematik-idp-dienst](#)

Nach erfolgreicher Prüfung stellt das **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 erstellen, um die Struktur der Organisation abzubilden. Zum Beispiel können Krankenhäuser ihre Fachabteilungen als Organisations-Einträge abbilden, die mit dem Basis-Eintrag verlinkt sind. Der ausführende Akteur hat die Rolle Admin-Owner. Wenn kein gültiges 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 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 ein 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



ein owner-accesstoken Abbildung 5:us und gibt Sequenzdiagramm es zurück.
Wird der Auth-Service des VZD-FHIR-Directory ohne Token aufgerufen, muss er die Authentifizierung von eigenen Tlentsprechend OpenID Connect durchführen.
Der Auth-Service soll die Authentifizierung entsprechend OpenID Connect auch für Zugriffe durch Organ-Admins (SMC-B/Organization oder TI-Practitioner-Einträgen) - zusätzlich zur Authentifizierung mit RegService-OpenID-Token - unterstützen.

Akzeptanzkriterien für den Anwendungsfall AF_10037 TI-Organization Directory-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 τ bei der Authentifizierung verwendeten τ Accesstoken ist die Telematik-ID des Nutzers enthalten. Nur der Eintrag (τ PractitionerDirectory oder τ OrganizationDirectory) mit der eigenen Telematik-ID darf verändert werden. Dabei dürfen nur die Attribute verändert werden, die nicht vom VZD-LDAP-Directory synchronisiert werden.
[<=]

23482 ML-12348238040 - Selbst angelegte τ IOrganisationHealthcareDirectory-Einträge MÜSSEN mit dem eigenen Basiseintrag verlinkt sein (VZD-FHIR-Directory)

Alle selbst durch den Besitzer angelegten FHIR-Einträge MÜSSEN mit dem eigenen Basiseintrag ~~ve~~providedBy verlinkt sein (n. Wenn keine korrekte Verlinkung angegeben ist, dann MUSS der FHIR-Proxy das Erzeugen oder die Änderung des HealthcareDirectory-Eintrags mit der Fehlermeldung (HTTP 422 Unprocessable Entity) ablehnen.[<=]

ML-136899 - AF_10037 IDP-Dienst ID-TOKEN Prüfung (VZD-FHIR-Directory)

Alle Die ID_TOKEN Prüfung basiert auf Informationen aus dem IDP Discovery Dokument des IDP-Dienstes.

Die URL des Downloadpunktes lautet im Internet: " https://idp.app.ti-dienste.de/.well-known/openid-configuration".

Daselbst durch den Besitzer angelegten F Discovery Dokument muss vor Ausführung der Prüfungen für die aktuelle Umgebung (RU/TU/PU) eingelesen worden sein.

Optional und verpflichtend ab FHIR VZD 1.2:

- Prüfung der Signatur des Discovery Dokument: Das VZD-FHIR-Directory muss die Signatur des Discovery Dokument mathematisch prüfen und auf ein zeitlich gültiges C.FD.SIG-Zertifikat mit der Rollen-OID oid_idpd zurückführen können, welches von einer ihm bekannten CA der Komponenten-PKI ausgestellt wurde.
- Prüfung des Signaturzertifikats gegen das X.509-Root-CA Zertifikat der TI.
- OCSP Prüfung des Signaturzertifikats.
- Regelmäßiges Laden des Discovery Dokuments: Das VZD-FHIR-Einträge MÜSSEN mit dem Directory muss das Discovery Dokument regelmäßig alle 24 Stunden von seinem Downloadpunkt laden und nach seiner erfolgreicher Prüfung die enthaltenen Daten zur Prüfung von ID_TOKEN verwenden.

Die vom IDP-Dienst ausgestellten ID_TOKEN müssen vom VZD-FHIR-Directory nach folgenden Kriterien geprüft werden:

- Validierung der gemäß [RFC7519 # section-7.1] vorge~~ig~~eschriebenen Struktur der ID_TOKEN gemäß [RFC7519 # section-7.2].
- ~~Enen~~ Basiseintrag mittels partOf verlinktschlüsselung der verschlüsselten ID_TOKEN entsprechend dem für diese Übertragung vorgesehenen Verfahren mit dem durch das VZD-FHIR-Directory gewählten "token_key". Unverschlüsselte ID_TOKEN sind ungültig und abzulehnen.
- Prüfung der Signatur der ID_TOKEN gegen den öffentlichen Schlüssel des Token-Endpunktes PUK_IDP_SIG. Das VZD-FHIR-Directory muss den öffentlichen Schlüssel PUK_IDP_SIG zuvor dem Discovery Document des IDP-Dienstes entnehmen.
 - Algorithmus: "alg": Muss einem zulässigen Wert aus dem Discovery Dokument des IDP-Dienstes, Attribut "id_token_signing_alg_values_supported" entsprechen. Z.B. "BP256R1"

- Reaktion bei ungültiger oder fehlender Signatur des "ID_TOKEN": Das VZD-FHIR-Directory muss alle mit dem ID_TOKEN verbundenen Vorgänge abbrechen, wenn das ID_TOKEN nicht ~~sein-~~igniert oder dessen Signatur fehlerhaft ist.
- Das VZD-FHIR-Directory muss sicherstellen, dass der Zeitraum der VerWenn keine-korrekte Verlinkung angegeben ist, dann MUSS der-dung des Tokens zwischen den im Token mitgelieferten Werten der Attribute iat und exp liegt.
- Telematik-ID Prüfung: Das ID-Token muss im Attribut idNummer eine Telematik-ID enthalten. ID-Token mit leerem Attribut idNummer müssen abgelehnt werden.
- Das VZD-FHIR-Directory muss ID_TOKEN ablehnen, wenn die in einem Attribut vorgetragenen Werte nicht dem schematisch erwarteten Datentyp des Attributes entsprechen.

Optional und verpflichtend ab FHIR VZD 1.2:

- Das VZD-FHIR-Directory muss den Claim "aud" des ID_TOKEN gegen seine beim IDP-Dienst registrierte client-id prüfen. Nur wenn diese übereinstimmen, gilt die Prüfung als positiv validiert.
- Das VZD-FHIR-Directory muss die im ID_TOKEN übertragenen Attribute mit denen vergleichen, die mit dem IDP-Dienst bei der Registrierung 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
- Optional: Wenn das VZD-FHIR-Proxy das Erzeugen oder die ÄDirectory im Authorization Request an den IDP-Dienst einen nonce-Parameter gesetzt hat, dann enthält das vom IDP-Dienst ausgestellten ID-Token genau dieser Wert als claim. Das VZD-FHIR-Directory muss dann prüfen, ob der von im im Authorization-Request übergebene nonce-Wert mit dem im ID-Token übereinstimmt.

[<=]

ML-136890 - 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 TI~~Organisation-Ein~~id token gemäß RFC7515 (das verwendete Zertifikat muss aus der Komponenten-PKI der TI stammen)
 - Zertifikatstyp: C.FD.SIG
 - technische Rolle: oid_tim
- Die telematikID muss im Token Attribut idNummer enthalten sein.

Optional und verpflichtend ab FHIR VZD 1.2:

- Prüfung des id_token Signatur-Zertifikats (oder sein Hash) gegen das bei der Beantrags-mit der Fehlermeldung (HTTP 422 Unprocessabung der Credentials für die Schnittstelle I_VZD_TIM_Provider_Services übergebene Signatur-Zertifikat.
- OCSP Prüfung des id_token Signatur-Zertifikats

- Prüfung Algorithmus: "alg": "ES256"
- Prüfung des Signaturzertifikats gegen das X.509-Root-CA Zertifikat der TI.
- Prüfung der zeitlichen Gültigkeit des id_token für den Zugriff auf den VZD-FHIR-Directory: Das VZD-FHIR-Directory muss sicherstellen, dass der Zeitraum der Verwendung des Tokens zwischen den im Token mitgelieferten Werten der Attribute iat und exp liegt.
- Das VZD-FHIR-Directory muss die im id_token übertragenen Attribute mit denen vergleichen, die mit dem Registrierungsdienst vereinbart wurden und alle mit dem id_token in Verbindung stehenden Vorgänge 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.

[<=]

ML-136887 - AF_10037 TI-Provider-Access-Token Prüfung (VZD-FHIR-Directory)

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

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

Optional und verpflichtend ab FHIR VZD 1.2:

- Das VZD-FHIR-Directory muss die im ACCESS_TOKEN übertragenen Attribute mit denen vergleichen, die vereinbart wurden und alle mit dem ACCESS_TOKEN in Verbindung stehenden Vorgänge abbrechen, wenn dem ID_TOKEN für die Verarbeitung notwendige Claims fehlen oder aber andere als die vereinbarten personenbezogenen Attribute vorhanden sind.
- Prüfung Audience "aud" aus dem Token (muss der /tim-provider-services Schnittstelle entsprechen, z.B. <https://fhir-directory.vzd.ti-dienste.de/tim-provider-services>)
- Hinweis: Als unerwartete personenbezogenes Attribute gelten gemäß Tabelle: [gemSpec_IDP_FD#TAB_IDP_DIENST_0005] die Claims given_name, family_name, und organizationName
- Sicherstellung der korrekten Signatur des Tokens gemäß RFC7515:

- Prüfung Algorithmus: "alg": "ES256"

[<=]

7.3 Anwendungsfälle der TI-Messenger-Anbieter im VZD-FHIR-Directory

23334AF_10048-01 - 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 Endpoint-Einträgen gespeichert. Die Endpoint-Einträge eines TI-Messenger-Anbieters sind verlinkt mit seinem TI-Organization-Directory-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 <code>I_VZD_TIM_Provider_Services</code>. Mit den Credentials erhält der Registrierungsdienst vom VZD TI-Provider-OAuth-Server ein ti-provider-Access-Token. Dieses tauscht er bei dem VZD-FHIR-Directory Auth-Service gegen ein provider-access-token, das zur Authentifizierung an der Schnittstelle genutzt wird. Nach erfolgreicher Authentisierung kann der Registrierungsdienst die FHIR-Operationen zur Verwaltung des eigenen TI-Organization-Directory-Eintrags und der eigenen Endpoint-Einträge nutzen.</p> <p>Um die Gesamtheit der an der Föderation beteiligten Matrix-Domainnamen zu erhalten, wird die Operation <code>GET /FederationList</code> 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> <p>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</p>
Vorbedingung	<p>Der Registrierungsdienst des TI-Messenger-Anbieters ist bereits als Nutzer des VZD-FHIR-Directories registriert und hat TI-Provider OAuth Client Credentials (<code>client_id</code> und <code>client_secret</code>) für die Umgebungen RU, TU und PU erhalten.</p>

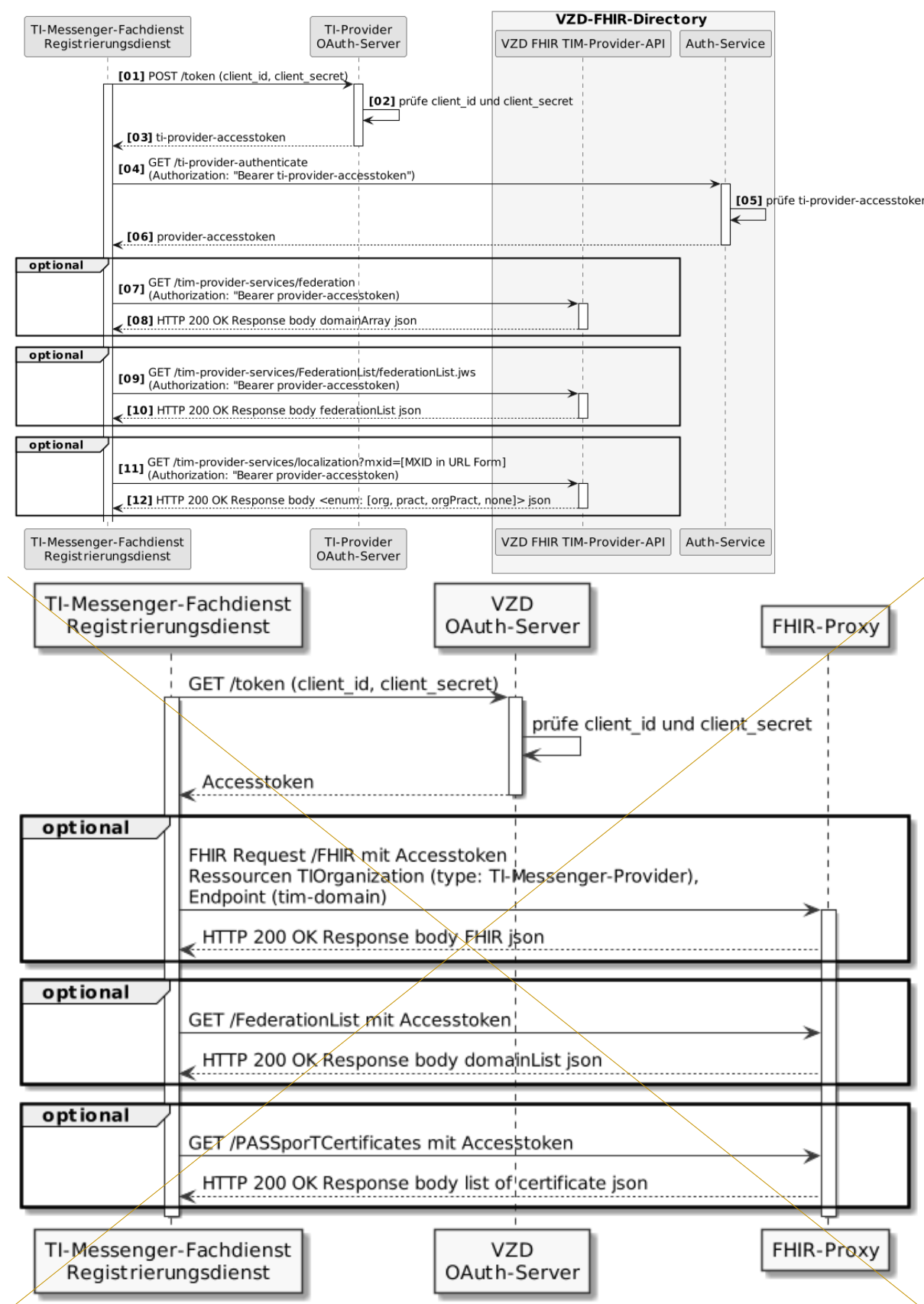


Abbildung 6: VZD-FHIR-Directory_Sequenzdiagramm_TI-Messenger-Provider-Services

[<=]

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.

[<=]

7.4 Einträge mit dem VZD-LDAP-Directory abgleichen

22988AF_10047-01 - Einträge mit dem VZD-LDAP-Directory abgleichen

Attribute	Bemerkung
Beschreibung	<p>Der FHIR-Proxy aktualisiert regelmäßig in einem konfigurierbaren Intervall die im VZD-LDAP-Directory seit der letzten Aktualisierung geänderten Einträge.</p> <p>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 <u>Tabelle [VZD-FHIR-Directory Mapping LDAP to FHIR]</u> aktualisiert. Dabei MÜSSEN auch im VZD-LDAP-Directory gelöschte Einträge erkannt und ebenfalls im VZD-FHIR-Directory gelöscht werden. <u>Einträge ohne Zertifikat erhalten</u>.</p> <p><u>Im VZD-FHIR-Directory</u> <u>den</u><u>wird der</u> Wert <u>TI</u><u> von</u> <u>Organization.active</u> <u>= false</u> bzw. <u>TI</u><u>Practitioner</u><u>Directory.active</u> <u>= false</u></p> <p><u>Wird zu einem Eintrag</u> <u>ibei der Synchronisation aus dem</u> VZD-LDAP-Directory <u>wieder ein Enc-Zertifikat ergänzt, dann erhält der</u> <u>entsprechend LDAP Basis</u> <u>Eintrag im VZD-FHIR-Directory den Wert</u> <u>TI</u><u>Organization.s-Attributs</u> <u>"active = true</u> bzw. <u>TI</u><u>Practitioner.active = true"</u> <u>gesetzt.</u></p>

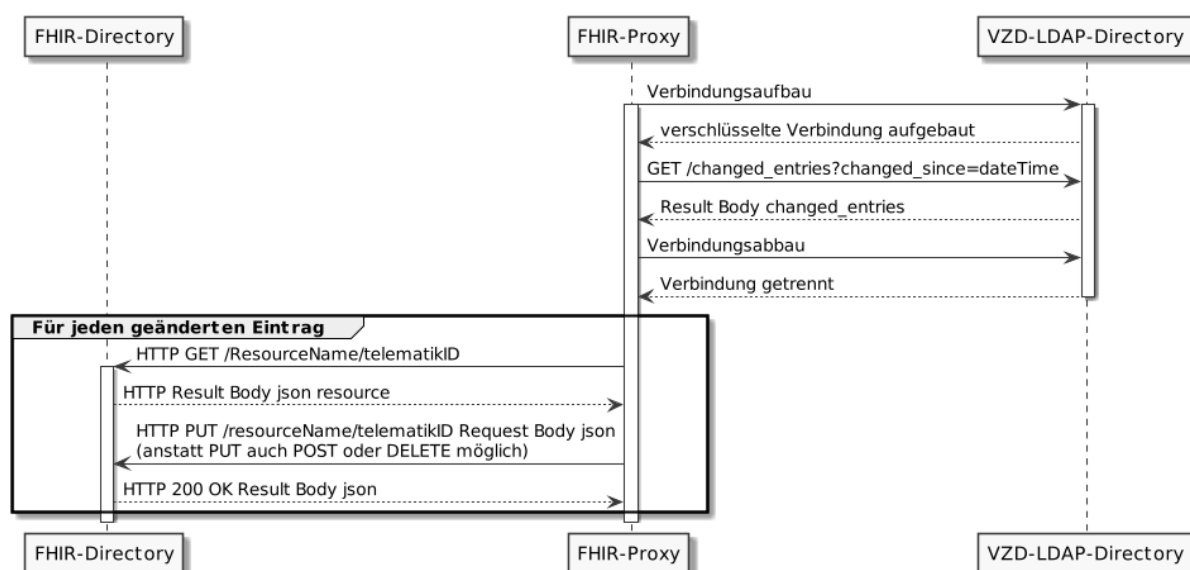


Abbildung 7: VZD-FHIR-Directory, Aktualisierung der Basiseinträge

[<=]

ML-134278 - Synchronisierung VZD-LDAP-Directory mit FHIR-Directory (VZD-FHIR-Directory)

Der VZD FHIR-Proxy muss gewährleisten, dass nach einem konfigurierbaren Intervall die im VZD-LDAP-Directory seit der letzten Aktualisierung geänderten Einträge in das VZD-FHIR-Directory synchronisiert wurden.

[<=]

8 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 unter 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.

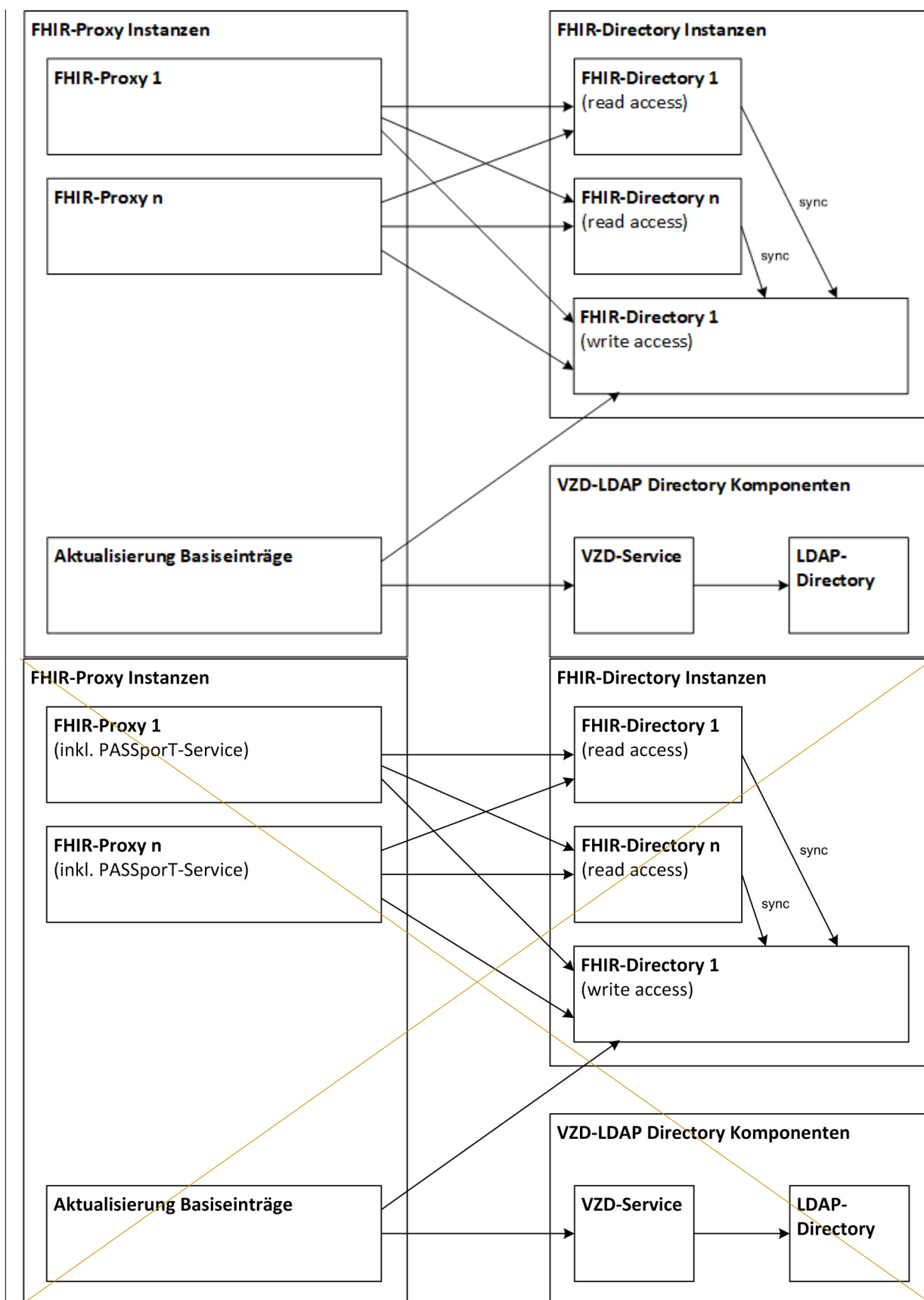


Abbildung 8: VZD-FHIR-Directory, Verteilungssicht

| —

9 Anhang A - Verzeichnisse

9.1 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

9.2 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.

9.3 Abbildungsverzeichnis

Abbildung 1: Systemüberblick VZD-FHIR-Directory.....	8
Abbildung 2: Zerlegung des VZD.....	14
Abbildung 3: Sequence diagram /tim-search.....	29
Abbildung 4: Sequenzdiagramm VZD-FHIR-Directory Änderung von eigenen TI-Organization oder TI-Practitioner Einträgen.....	31
Abbildung 5: VZD-FHIR-Directory Sequenzdiagramm TI-Messenger-Provider-Services....	33
Abbildung 6: VZD-FHIR-Directory, Aktualisierung der Basiseinträge.....	34
Abbildung 7: VZD-FHIR-Directory, Verteilungssicht.....	36

Abbildung 1: Systemüberblick VZD-FHIR-Directory.....	11
Abbildung 2: Zerlegung des VZD.....	19
Abbildung 3: Sequence diagram /search.....	44
Abbildung 4: Sequenzdiagramm VZD-FHIR-Directory.....	46
Abbildung 5: VZD-FHIR-Directory Sequenzdiagramm TI-Messenger-Provider-Services....	54
Abbildung 6: VZD-FHIR-Directory, Aktualisierung der Basiseinträge.....	56
Abbildung 7: VZD-FHIR-Directory, Verteilungssicht.....	58

9.4 Tabellenverzeichnis

Tabelle 1: VZD_FHIR_Directory_Akteure_und_Rollen.....	10
Tabelle 2: VZD_FHIR_Directory, FHIR-Ressourcen.....	15
Tabelle 3: VZD_FHIR_Directory_Mapping_LDAP_to_FHIR.....	17
Tabelle 4: Tab_VZD_TIM-Provider-Services_Operations.....	24

Tabelle 1: Nutzer und Rollen.....	11
Tabelle 2: Kommunikationsbeziehungen zu IT-Systemen.....	12
Tabelle 3: VZD-FHIR-Directory, FHIR-Ressourcen.....	22
Tabelle 4: Tab_VZD_TIM-Provider-Services_Operations.....	33
Tabelle 5: Tab_VZD_FHi.....	39

9.5 Referenzierte Dokumente

9.5.1 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
[VZD-FHIR-Directory_Mapping_LDAP_to_FHIR]	gematik: VZD Mapping LDAP zu FHIR Resourcen https://github.com/gematik/api-vzd/blob/23456d9ef61263185edfbcaabf09086ba7b26a20/docs/LDAP2FHIR_Sync.adoc
[Simplifier-FHIR-VZD]	gematik: FHIR VZD Datenmodell https://simplifier.net/vzd-fhir-directory

9.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[CAB-Forum]	Liste vertrauenswürdiger Zertifikatsherausgeber (Root-CAs) für Anwendungen im Internet https://cabforum.org/members/
[ROOT-CA]	ROOT-CA Download Punkt PU-Root https://download.tsl.ti-dienste.de/ECC/ROOT-CA/ TU-Root https://download-test.tsl.ti-dienste.de/ECC/ROOT-CA/ RU-Root https://download-ref.tsl.ti-dienste.de/ECC/ROOT-CA/
[ROOT-CA-JSON]	ROOT-CA Download Punkt als JSON-Datei PU-Root https://download.tsl.ti-dienste.de/ECC/ROOT-CA/roots.json

	TU-Root https://download-test.tsl.ti-dienste.de/ECC/ROOT-CA/roots.json RU-Root https://download-ref.tsl.ti-dienste.de/ECC/ROOT-CA/roots.json
<u>[Sub-CA]</u>	Sub-CA Download Punkt PU-Sub https://download.tsl.ti-dienste.de/ECC/SUB-CA/ TU-Sub https://download-test.tsl.ti-dienste.de/ECC/SUB-CA/ RU-Sub https://download-ref.tsl.ti-dienste.de/ECC/SUB-CA/

10 Anhang B – Beispiele

10.1 FHIR Operationen

10.1.1 Abfrage von TIOrganisation Einträgen

10.1.1.1 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.class).where(new
StringClientParam("address").matches().value("10117"))
.include(new Include("TIOrganization:endpoint"))
.prettyPrint()
.execute();
```

10.1.1.2 Request

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

10.1.1.3 Request Headers

```
Accept-Charset: utf-8
Accept: application/fhir+xVersionierung Datenml;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
```

10.1.1.4 Response

```
HTTP 200 OK
```

10.1.1.5 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

```

10.1.1.6 Response Body

10.2 {

```

  "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/IIOrganization?
    _include=IIOrganization%3Aendpoint
    &_pretty=true&address=10117"
  } ],
  "entry": [ {
    "fullUrl":
    "http://hapi.fhir.org/baseR4/IIOrganization/2500949",
    "resource": {
      "resourceType": "IIOrganization",
      "id": "2500949",
      "meta": {
        "odell

```

```

Folgende versionId": "1",
  "lastUpdated": "2021-08-04T15:51:20.261+00:00",
  "source": "#0j3wXiC80VNH7wON"
},
  "name": "Test Organisation en der II",
  "telecom": [ {
    "system": "url",
    "value": "matrix:u/testorg:gematik.de"
  } ],
  "address": [ {
    "line": [ "Friedrichstr. 136" ],
    "city": "Berlin",
    "state": "Berlin",
    "postalCode": "10117",
    "country": "Germany"
  } ]
},
  "search": {
    "m_Datenmode": "match"

```

```

    }
  }, {
    "fullUrl": "http://hapi.fhir.org/baseR4/TIOrganization/2500973",
    "resource": {
      "resourceType": "TIOrganization",
      "url": "https://simplifier.net/vzd-fhir-directory/ "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"
    }
  }
]

```

) sind für die vorliegende Spezifikation relevant:

```

de.gematik.fhir.directory 0.10.1 "mode": "include"
}
}
}

```

|

|

