Electronic health card and telematics infrastructure

Specification
FHIR Directory Service

Note: This document is non-binding.

Version:	1.1.1
Revision:	682411
Last updated:	31/07/2023
Status:	released
Classification:	public
Referencing:	gemSpec_VZD_FHIR_Directory

Document information

Changes to previous version

Adjustments to this document compared to the previous version can be found in the table below.

Document history

Version	Last updated	Section/Page	Reason for change, special notes	Editing
1.0.0	01/10/2021		Initial version of document	gematik
1.1.0	29/07/2022		Update and, in particular, adaptations in accordance with TI-Messenger specification version 1.1.0	gematik
1.2.0	12/12/2022	4.2.4 4.2.3 4.3.1	Technical description Operation whereIs added – C_11233 Structure of the federation list updated – ANFTIM-185 Security and data protection requirements added	gematik
1.3.0	31/07/2023		Integration of TI-Messenger Maintenance 23.1 / VZD FHIR Maintenance_23.1	gematik

Contents

1 Classification of document

This document describes the FHIR directory of the TI directory service. The specification includes interfaces to retrieve information from organisation FHIR resources registered in the FHIR directory and practitioner FHIR resources from client systems, as well as interfaces and processes to maintain information within the VZD-FHIR directory.

1.1 Objective

The specification is to support the development and operation of a VZD-FHIR directory for the telematics infrastructure by defining the functional and non-functional requirements as well as the security requirements for the service.

1.2 Target group

The document is intended for implementation by the manufacturer of the VZD-FHIR directory as well as by the supplier who operates this product [gemKPT_Betr]. All manufacturers and providers of TI applications that use the VZD-FHIR directory must also take this document into account. The document is also relevant for users who want to enter, query, modify and delete data in the VZD-FHIR directory.

1.3 Coverage

This document contains normative provisions on the telematics infrastructure of the German healthcare system. The validity period of the present version and its application in approval or acceptance procedures is defined and disclosed by gematik GmbH in separate documents (e.g. gemPTV_ATV_definitions, product type profile, supplier type profile, etc.) or web platforms (e.g. gitHub, etc.).

Intellectual property / Patent legal notice

The following specification has been created by gematik solely from a technical point of view. In individual cases, it cannot be excluded that the implementation of the specification interferes with the technical property rights of third parties. It is solely the responsibility of the supplier or manufacturer to take appropriate measures to ensure that the products and/or services offered by it on the basis of the specification do not violate the property rights of third parties and to obtain the necessary permissions/licences from the affected property right holders. Gematik GmbH therefore assumes no warranty whatsoever.

1.4 Demarcation

Only the newly introduced components and interfaces of the TI directory service are specified in the document. The VZD-LDAP directory is specified in [gemSpec_VZD].

Used interfaces are described in the specification of the product type that provides this interface. Reference is made to the corresponding documents (also see annex, Section 7.5 – Referenced documents).

The complete requirements for the product type result from further concept and specification documents, which are recorded in the product type profile of the product type VZD-FHIR directory.

1.5 Methodology

The specification is written in the style of an RFC specification. This means:

- **The entire text in the specification is to be considered binding for the manufacturer of the VZD-FHIR directory product as well as for the operating provider according to [gemKPT_Betr] and is to be considered as approval criteria for both the product and the supplier.**
- This document is also binding for applications connected to the product and service. Also for users who contribute to data maintenance in the VZD-FHIR directory or query data.
- The binding nature SHOULD be indicated by the keywords MUST, MUST NOT, SHOULD, SHOULD NOT, MAY, written in capital letters and corresponding to [RFC2119].
- As in the example sentence "An empty list MUST NOT contain an item." the phrase "MUST NOT" would be semantically misleading (if not one, maybe two?), "An empty list MUST NOT contain any items." is used in this document instead.
- The keywords MAY also be completed with pronouns in capital letters if this improves the language flow or clarifies semantics.

Use cases and acceptance criteria as expressions of normative requirements are examined and verified through tests as a basis for obtaining approval. They have a unique, permanent ID, which SHOULD be used as a reference. The tests are carried out against a reference implementation performed by gematik.

Use cases and acceptance criteria are presented in the document as follows:
<ID> – <Title of use case / acceptance criteria>
Text / Description
[<=]

The individual elements describe:

- **ID**: a unique identifier.
    - In a use case, the identifier consists of the string 'AF_' followed by a number,
    - The identifier of an acceptance criterion is assigned by the system, e.g., the string 'ML_' followed by a number
- **Title of use case / acceptance criteria:** A title that summarises the content
- **Text/description**: Detailed description of the content; can contain tables, illustrations and models in addition to text

The use case or acceptance criteria include all contents listed between the ID and the text mark [<=].

The proof of fulfilment of the use case necessary for obtaining an approval is specified in the respective profiles, in which each use case is listed. Acceptance criteria are usually not listed in the profile.

Reference to open points

Open point: The section will be supplemented in a later version of the document.

2 System overview

The VZD-FHIR directory is an extension of the previous TI directory service. Entries from organisations and service providers are stored in the VZD-FHIR directory. The VZD-LDAP directory entries are synchronised into the VZD-FHIR directory. This process involves a conversion from the LDAP data structure to the FHIR resource data structure. Personal entries of the service providers are mapped to the PractitionerDirectory resource and organisational entries to the OrganizationDirectory resource. The synchronised entries form the base entries, which can be supplemented or extended by the owners. PractitionerDirectory and OrganizationDirectory are profilings of the FHIR resources Practitioner and Organization. Providers of specialist applications are also entered as OrganizationDirectory entries in the FHIR directory in order to be able to assign data of the specialist application to this organisation.

The owner of a telematics ID receives the right to expand their entry (e.g. to enter substructures for an organisation) and to supplement technical data (e.g. TI-Messenger addresses). The data entered by the card issuers must not be changed by the holders. Additional FHIR resources (such as Endpoint and HealthcareService) can be added by owners to increase the convenience of searching for entries.

All interfaces provided by the VZD-FHIR directory are accessible via the internet and TLS-secured. Authentication is performed using:

- OpenID Connect Authorisation Code Flow for write access of entry owners
- OAuth2 Client Credentials Flow for write access of specialist services
- Matrix OpenID token for read access by TI-Messenger users

The VZD-FHIR directory MUST prevent the use of the interfaces without authenticating the users.

As a first application, the TI-Messenger service will use the VZD-FHIR directory.

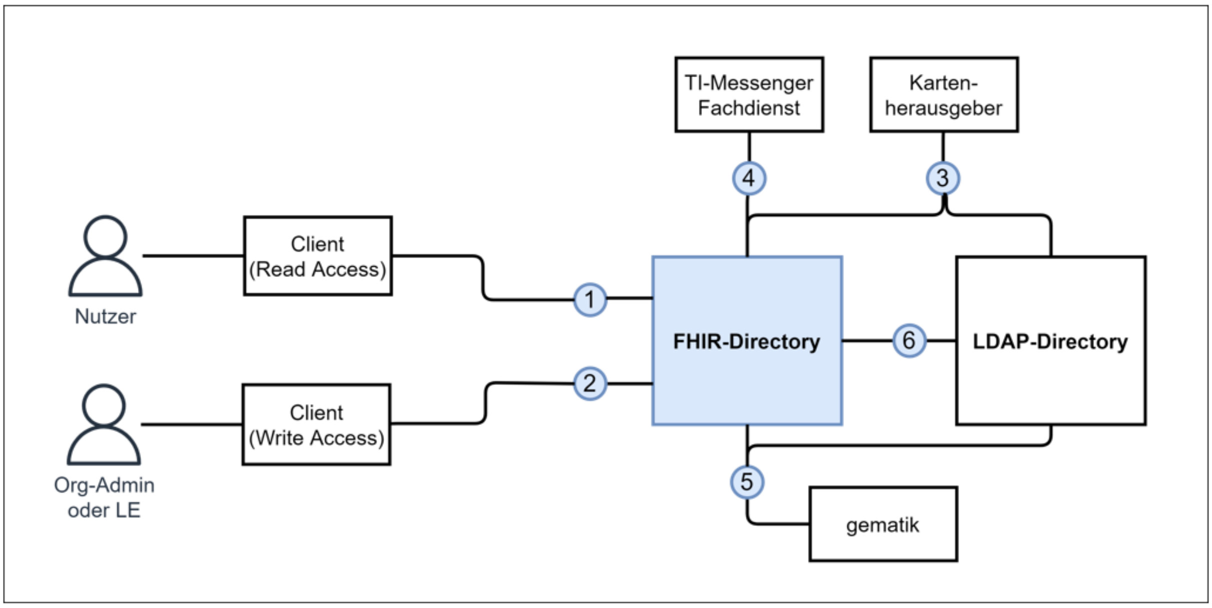

Figure 1: VZD-FHIR directory system overview

The FHIR directory is an implementation of the FHIR specification (http://hl7.org/fhir/summary.html).

2.1 Users and roles

Table 1: Users and roles

User and role	Description
Users	All users can search for entries in the organisation directory and the person directory in the FHIR directory using the interface (1).
Org Admin or SP	Administrators of the organisations and SP can change their entry in the FHIR directory using the interface (2) and add additional resources.

Table 2: Communication relations with IT systems

IT systems	Description
Card issuers	Card issuers use the interface (3) to maintain the entries of their members in the LDAP directory and in the future in the FHIR directory.
TI-Messenger providers	TI-Messenger providers use the interface (4) to query the federation list of the TI-Messenger and to manage the domains of the messenger services they operate as part of the TI-Messenger federation.
gematik	gematik can read the entries in the FHIR directory and in the LDAP directory via the interface (5) to check the data quality of the entries and to analyse errors.
LDAP directory	The interface (6) between the FHIR directory and the LDAP directory is used by the directory service to synchronise entries.

All interfaces with the exception of (6) are accessible via the internet. The interfaces provide the following functions:

1. For users there is an interface for searching for entries in the FHIR directory organisation directory and person directory. The interface can only be used after successful authentication. All TI-Messenger users can authenticate themselves and receive an access token from the FHIR directory that is used for search queries. The search makes it easy to search for full text or specific values of each attribute via the linked resources. Found resources are returned in a bundle of FHIR resources. The data format is json.
2. For administrators of the healthcare organisations and for SPs, there is an interface to change their entry in the organisation directory. Authentication using an OIDC Authorisation Code Flow is required to use the interface. Using this interface, additional entries can be added to the organisation's own entry in the organisational directory via a link. TI-Messenger users who are also SPs can use this interface to store their TI-Messenger address in their entry in the person

directory so that they can be found by other SPs. Here, too, authentication is performed via OIDC. The FHIR data format is json.

3. The I_Directory_Administration interface is available for card issuers to create and maintain entries in the LDAP directory. The data format is json and is specified in the OpenAPI yaml file DirectoryAdministration.yaml. In the future, it is planned that the card issuers can also directly use the interface to the FHIR directory. The data format is then FHIR in the form JSON. The card issuer is authenticated using OAuth Client Credentials Flow.
4. TI-Messenger specialist services maintain the TI-Messenger domains in the FHIR directory for the messenger services they offer. In addition, TI-Messenger providers can query the federation list. It includes all domains involved in the federation of the TI-Messenger. To enable communication control, TI-Messenger specialist services also query in which directory (person or organisation directory) the TI-Messenger addresses are located. Authentication of the TI-Messenger specialist services is done using OAuth Client Credentials Flow.
5. gematik has interfaces to check the data quality of the entries. The interface of the card issuers is used for this purpose. However, the system only has read rights.
6. The entries in the LDAP directory are synchronised into the FHIR directory organisation and person directory. It is an internal interface of the TI directory service.

2.2 Neighbouring systems

The neighbouring systems of the VZD-FHIR directory are client and server components of the TI-Messenger service, the VZD-LDAP directory, the IDPs from the TI-IDP federation and the operational data recording of gematik.

ML-123876 – Test against the reference implementation of neighbouring systems (VZD-FHIR directory)
All use cases of the VZD-FHIR directory MUST be successfully tested against the reference implementation of neighbouring systems.
[<=]

3 Breakdown of the product type

The following figure shows the subcomponents of the previous VZD-LDAP directory and the new components of the VZD-FHIR directory shown in red.

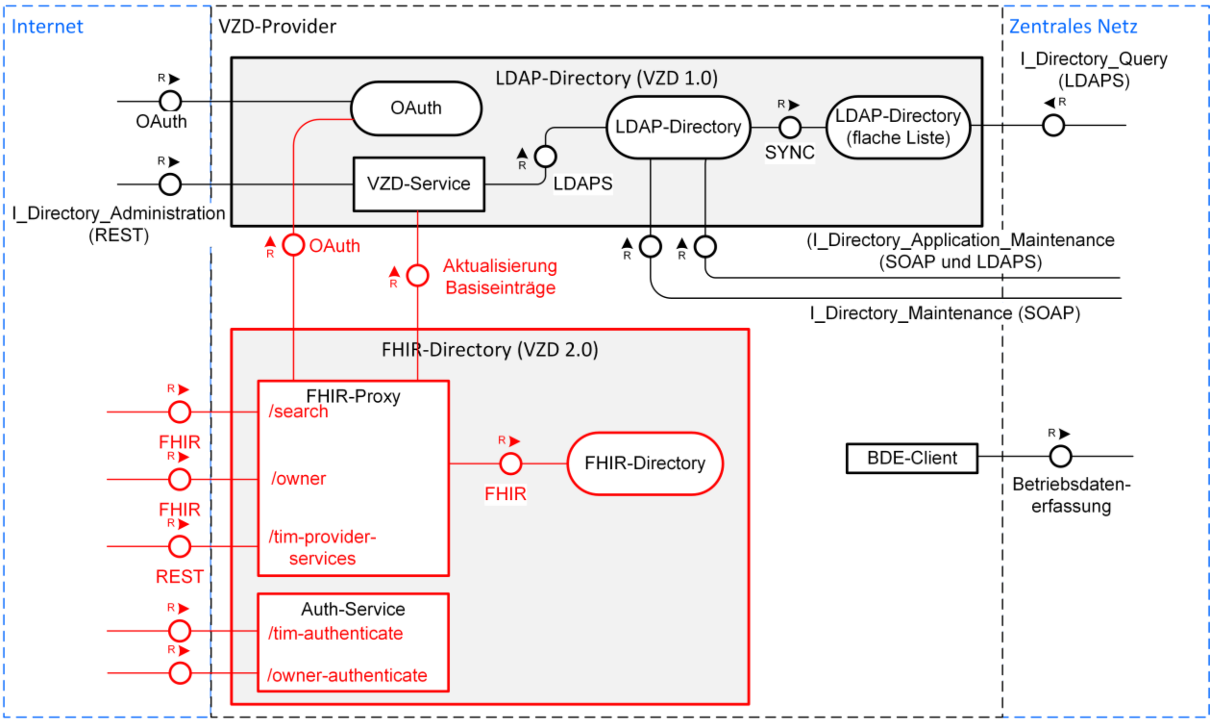

Figure 2: Breakdown of the VZD

The VZD-FHIR directory consists of the FHIR proxy and FHIR directory as well as Auth service components.

The raw data to be delivered by the VZD-FHIR directory to determine utilisation and performance is integrated into the already existing operating data acquisition client (BDE client) of the directory service.

4 Functional features

This section describes the components of the VZD FHIR directory.

The FHIR directory provides the following interfaces:

- FHIRDirectoryAuthorizationService

  Issues access tokens for access to FHIRDirectory APIs. In the future it will be expanded into an application-specific Policy Decision Point (PDP).

  The two following REST interfaces

  - `/tim-authenticate` and
  - `/owner-authenticate`

  are used here. The `/tim-authenticate` interface expects a matrix OpenID token, whereas the `/owner-authenticate` interface requires an ID_TOKEN.

- FHIRDirectorySearchAPI

  The REST interface /search allows persons and institutions to be searched for.

  The standard FHIR search operation https://build.fhir.org/search.html is used.

  To use the search operation, a corresponding access token must be available from the FHIRDirectoryAuthorizationService.

- FHIRDirectoryTIMProviderAPI

  The REST interface /tim-provider-services enables operational processes for TI-Messenger providers, esp. Federation.

  This REST interface is defined here: https://github.com/gematik/api-vzd/ under src/openapi/I_VZD_TIM_Provider_Services.yaml

- FHIRDirectoryOwnerAPI

  The REST interface `/owner` enables the adjustment of entries by identity owners plus authoritative data of card issuers.

  The standard FHIR operations https://build.fhir.org/http.html are used with the restriction to the card issuers' own resources and authoritative data.

  To use this operation, a corresponding owner access token must be available from the FHIRDirectoryAuthorizationService.

- ProviderAuthorizationService

  Enables authentication and authorisation of TI providers to access the FHIR directory. Initially only TI-Messenger providers, later also KIM providers and future providers.

  When calling the REST interface `/tim-provider-services`, an access token (provider-accesstoken) is required. For this, the client must authenticate itself with the ProviderAuthorizationService of the VZD-FHIR directory by means of the OAuth2 Client Credentials Flow. Prior to this, the client MUST apply for client credentials from the VZD provider.

Planned FHIR directory interfaces in future releases:

- FHIRDirectorySearchTI API

  Planned interface for searching the entries without authentication in the closed network of the TI (TI connection required).

- FHIRDirectoryAdmin API

  Planned interface for the administration of data in the FHIR directory service as successor to REST maintenance interface (DirectoryAdministration).

4.1 FHIR directory

The FHIR directory is an implementation of the HL7-FHIR specification Release 4.0.1 (https://www.hl7.org/fhir/http.html).

The FHIR directory can only be reached via the FHIR proxy.

4.1.1 Data model

The FHIR resources are used according to the following table.

All changes to and extensions of FHIR resources are published in https://simplifier.net/vzd-fhir-directory.

Table 3: VZD-FIR directory, FHIR resources

FHIR resource	Description
Organisation in gematik directory (OrganizationDirectory)	Profile of the Organization resource. (https://simplifier.net/vzd-fhir-directory/organizationdirectory) The Identifier element has been changed so that telematics IDs can be used as identifiers. In the element type, the type of organisation is entered. For this purpose the CodeSystems https://simplifier.net/vzd-fhir-directory/organizationprofessionoid and https://simplifier.net/vzd-fhir-directory/practitionerprofessionoid and the ValueSet https://simplifier.net/vzd-fhir-directory/organizationtypevs are used.
Practitioner in gematik directory (PractitionerDirectory)	Profile of the practitioner resource. Only the Identifier element has been changed so that telematics IDs can be used as identifiers. (https://simplifier.net/vzd-fhir-directory/practitionerdirectory)
Endpoint in gematik directory (EndpointDirectory)	Endpoint resource (https://simplifier.net/vzd-fhir-directory/endpointdirectory)

FHIR resource	Description
Location in gematik directory (LocationDirectory)	Location (https://simplifier.net/vzd-fhir-directory/locationdirectory)
HealthcareService in gematik directory (HealthcareServiceDirectory)	HealthcareService (https://simplifier.net/vzd-fhir-directory/healthcareservicedirectory)
PractitionerRole in gematik directory (PractitionerRoleDirectory)	PractitionerRole (https://simplifier.net/vzd-fhir-directory/practitionerroledirectory)

ML-123880 – Restriction of usable FHIR resources (VZD-FHIR directory)
Only the resources specified in the "VZD-FHIR directory, FHIR resources" table may be generated in the VZD-FHIR directory. **[<=]**

4.1.2 Mapping of LDAP to FHIR resources

The OrganizationDirectory and PractitionerDirectory basic entries are initially generated by the FHIR proxy with the data from the VZD-LDAP directory and then continuously updated. The synchronised data cannot be changed by the owners (service providers and organisations).

The data from the VZD-LDAP directory is mapped to FHIR resources as follows: https://github.com/gematik/api-vzd/blob/master/docs/LDAP2FHIR_Sync.adoc.

4.1.3 FHIR RESTful API

FHIR interface operations are defined by the FHIR specification (https://www.hl7.org/fhir/http.html).

The number of entries found and returned by search operation is initially limited to 100. This value MUST be configurable. The returned entries are merged into an FHIR resource bundle. The total number of entries in the bundle MUST be returned in the Bundle.total attribute. To determine the total number of entries found, the search operation _summary=count (https://hl7.org/fhir/search.html#summary) can be used. The search result then contains the total number of entries found in Bundle.total, but not the entries themselves.

4.2 FHIR proxy

4.2.1 Interfaces

All connections of the FHIR proxy are TLS-encrypted. The proxy identifies itself to the clients. Signed access tokens are issued for client access to the FHIR-VZD.

4.2.1.1 TLS connection setup

The FHIR proxy MUST authenticate itself to clients with an Extended Validation TLS certificate from an issuer according to [CAB Forum] when establishing TLS connections at the endpoints. The certificate MUST be bound to the interface of the entry point for client systems so that client systems can perform a simplified certificate check with TLS standard libraries during the TLS connection setup.

4.2.1.2 FHIR interface for TI-Messenger users FHIRDirectorySearchAPI

Endpoints for searching VZD-FHIR directory entries through TI-Messenger clients

In the production environment, the URL is: https://fhir-directory.vzd.ti-dienste.de/search

In the reference environment, the URL is: https://fhir-directory-ref.vzd.ti-dienste.de/search

In the test environment, the URL is: https://fhir-directory-test.vzd.ti-dienste.de/search

Authentication

To use the interface, clients MUST authenticate themselves with a valid token issued by a Matrix home server from the TI-Messenger federation. In the following, these access tokens are called Matrix OpenID tokens. After successfully checking the Matrix OpenID token, the FHIR proxy displays a new OAuth Accesstoken (search-accesstoken) to the TI-Messenger client.

The search-access token contains the following attributes:

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

The "iss" attribute contains the URL of the endpoint for authentication in the respective environment RU, TU or PU.

The "aud" attribute contains the URL of the endpoint in the respective environment RU, TU or PU.

The validity period of the search-accesstoken is 24 hours.

Endpoints for authentication

In the production environment, the URL is: https://fhir-directory.vzd.ti-dienste.de/tim-authenticate

In the reference environment, the URL is: https://fhir-directory-ref.vzd.ti-dienste.de/tim-authenticate

In the test environment, the URL is: https://fhir-directory-test.vzd.ti-dienste.de/tim-authenticate

Operations

The FHIR operations used to search for entries in the VZD-FHIR directory are defined in the HL7 FHIR specification (https://www.hl7.org/fhir/http.html).

In addition to the HL7 FHIR specification, the FHIR VZD must support the following search parameters:

- practitioner.qualification
- location endpoint.address (e.g. search for TI-Messenger address)

4.2.1.3 FHIR interface for owners FHIRDirectoryOwnerAPI

The interface allows owners of a telematics ID to change their entry in the VZD-FHIR directory. The access token used for authentication contains the telematics ID of the user. Only the (PractitionerDirectory or OrganizationDirectory) entry with its own telematics ID may be changed. Only those attributes that are not synchronised by the VZD-LDAP directory may be changed.

Endpoints for changing your own entries in the VZD FHIR directory through TI-Messenger clients and Org-Admin clients

In the production environment, the URL is: https://fhir-directory.vzd.ti-dienste.de/owner

In the reference environment, the URL is: https://fhir-directory-ref.vzd.ti-dienste.de/owner

In the test environment, the URL is: https://fhir-directory-test.vzd.ti-dienste.de/owner

Authentication

To use the interface, clients MUST authenticate themselves with a valid access token issued by the FHIR proxy. If there is no valid access token in the client, the client must authenticate itself at an IDP of the TI-IDP federation.

Only your own entry with an identifier that matches the telematics ID from the access token MAY be processed. For your own OrganizationDirectory entry, additional HealthcareService entries MAY be created and linked to your own OrganizationDirectory entry.

The access token contains the following attributes:

```
{
  "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
}
```

The "iss" attribute contains the URL of the endpoint for authentication in the respective environment RU, TU or PU.

The "aud" attribute contains the URL of the endpoint in the respective environment RU, TU or PU.

The validity period of the owner access token is 24 hours.

Endpoints for authentication

In the production environment, the URL is: https://fhir-directory.vzd.ti-dienste.de/owner-authenticate

In the reference environment, the URL is: https://vzd-fhir-directory-ref.vzd.ti-dienste.de/owner-authenticate

In the test environment, the URL is: https://vzd-fhir-directory-test.vzd.ti-dienste.de/owner-authenticate

FHIR VZD endpoints for authentication with the SmartcardIDP

In the production environment, the URL is: https://fhir-directory.vzd.ti-dienste.de/signin-gematik-idp-dienst

In the reference environment, the URL is: https://vzd-fhir-directory-ref.vzd.ti-dienste.de/signin-gematik-idp-dienst

In the test environment, the URL is: https://vzd-fhir-directory-test.vzd.ti-dienste.de/signin-gematik-idp-dienst

Operations

The FHIR operations for changing your own entries in the VZD-FHIR directory are specified in the HL7-FHIR specification (https://www.hl7.org/fhir/http.html).

Data

The VZD-FHIR directory data model is described in Simplifier [Simplifier-FHIR-VZD].

For TI applications, the communication addresses are entered in the FHIR endpoint:

Table 4: Tab_VZD_TI Applications_Endpoint

TI application	Endpoint.connectionType code	Endpoint.address
TI Messenger	tim	Format (MXID in URL form) for users according to [matrix-uri-scheme]: matrix:u/localpart:domainpart Example MatrixID: @1-1tst-auto-ts-ow2: tim.test.gematik.de MatrixID in URL format in Endpoint.address: matrix:u/1-1tst-auto-ts-ow2: tim.test.gematik.de

4.2.1.4 Interface FHIRDirectoryTIMProviderAPI (I_VZD_TIM_Provider_Services.yaml)

Endpoints

In the production environment, the URL is:

https://fhir-directory.vzd.ti-dienste.de/tim-provider-services

In the reference environment, the URL is: https://fhir-directory-ref.vzd.ti-dienste.de/tim-provider-services

In the test environment, the URL is: https://fhir-directory-test.vzd.ti-dienste.de/tim-provider-services

Authentication

To use the interface, the registration service of the TI-Messenger provider must first authenticate itself with a ti-provider-accesstoken issued by the TI provider OAuth server of the VZD provider. The ti-provider-accesstoken has a validity period of 5 minutes. It exchanges this for a provider-accesstoken from the VZD-FHIR directory Auth service, which is used for authentication at the interface.

The provider-accesstoken contains the following attributes:

```
{
  "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,
  "clientId": "<client_id>"
}
```

The "iss" attribute contains the URL of the endpoint for authentication in the respective environment RU, TU or PU.

The "aud" attribute contains the URL of the endpoint in the respective environment RU, TU or PU.

The validity period of the provider-accesstoken is 24 hours.

Endpoints for authentication at the VZD-FHIR directory Auth service

In the production environment, the URL is: https://oauth.vzd.ti-dienste.de/ti-provider-authenticate
In the reference environment, the URL is: https://ru-oauth-test.vzd.ti-dienste.de/ti-provider-authenticate
In the test environment, the URL is: https://tu-oauth-test.vzd.ti-dienste.de/ti-provider-authenticate

Registration

To access the TI provider OAuth server, the TI-Messenger provider MUST request client credentials for its registration service from the VZD provider. The application is made via a service request requiring approval in the TI-ITSM system.

Registration and assignment of credentials takes place at the provider level.

The application MUST contain the following information for further processing:

- Information on the role (here TI-Messenger provider) and applicant organisation, explanation of entitlement and needs (required for verification)
- Contact details for contact persons with the applicant (2 persons) incl. telephone number, email address, address
- Specification of the operating environment (RU/PU)

- Email address and associated S/MIME certificate (in a ZIP file as annex) to which the access data can be encrypted (free certificates are available, e.g., from DGN)
- If existing, a corresponding ticket number
- Only in case of deregistration by the applicant: pre-assigned client ID
- Desired designation in the clientID
- Registration server id_token signature certificate (required for simplified authentication at this interface during token verification)

After checking the information, the access data is transmitted directly from the provider central platform services (cf. gemKPT_Betr) to the desired email address.

It should be noted that this process is only intended for new installations and deletions. Changes or reshipment of access data cannot be processed.

Operations

The interface is specified in I_VZD_TIM_Provider_Services.yaml as OpenAPI RESTful Service.

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

Table 5: Tab_VZD_TIM-Provider-Services_Operations

Operation	Description
GET / "getInfo"	This operation can query metadata (especially the version and the used yaml file) of this interface.
GET /FederationList/federationList.jws	This operation queries the list of Matrix domain names involved in the TI-Messenger federation (federation list).
GET /localization "whereIs"	Returns the part of the directory containing the MXID for the passed MXID.
POST /federation "addTiMessengerDomain"	Add a domain to the federation.
GET /federation "getTiMessengerDomain"	Read one or all of your own domains.
PUT /federation "updateTiMessengerDomain"	Update a domain.
DELETE /federation "deleteTiMessengerDomain"	Delete a domain.
GET /federationCheck "checkTiMessengerDomains"	Tests whether all its own domains (identified by token) belong to active organisations. Returns own domains belonging to inactive organisations.

The "sub" attribute of the access token contains the client_id of the TI-Messenger registration service.

When adding a domain to the federation (addTiMessengerDomain), the FHIR VZD MUST check whether there is an active organisation for the associated telematicsID.

4.2.2 Updating the basic entries

The FHIR proxy regularly updates the basic entries in the VZD-FHIR directory with the changed data of the VZD-LDAP directory (see Compare AF_10047 entries with the VZD-LDAP directory). The periodic update interval MUST be configurable and is initially set to 2 hours.

Another synchronisation using PUSH in the FHIR VZD must be possible (similar to the background sync procedure in the LDAP flat list).

In the future, card issuers will be able to directly manage the basic entries of their members in the VZD-FHIR directory via an FHIR interface.

4.2.3 Creation and provision of the federation list

The federation list MUST be newly created when the domains and/or telematicsIDs are changed by TI-Messenger providers and provided for download via the I_VZD_TIM_Provider_Services interface.

The federation list has the following structure:

```
{
  "version": <Version of the federation list (integer)>,
   "domainList": [
   {
     "domain": "Domain",
     "telematikID": "Telematics ID of the organisation using the domain",
     "isInsurance": false,
     "timAnbieter": "Assignment group in the TI-ITSM system from the TI-Messenger
provider who created the domain"
   }
  ]
}
```

The value for "timProvider" MUST be recorded by the AZPD when applying for the TI-Messenger provider/manufacturer credentials and updated by the VZD-FHIR directory whenever the other fields are changed. The value for "timProvider" MAY ONLY be changed by the AZPD or by the VZD-FHIR directory. This automation is intended to avoid manual errors when setting by users.

The federation list MUST be signed with a JWS in accordance with RFC7797. The signature algorithm to be used MUST be "ES256". For this purpose, a signature certificate of the TI PKI component (C.FD.SIG) must be used. The signature certificate MUST be included in the signature header.

The signature header has the following structure:

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

The signed federation list has the following structure according to RFC7797:

Signature header.Federation list.Signature

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

The individual components of the signed federation list are Base64 encoded.

An example for the federation list:

eyJ4NWMiOlsiTUZvd0ZBWUhLb1pJemowQ0FRWUpLeVFEQXdJSUFRRUhBMElBQkpMkt6Rl
E4bEs0TFMyajJVNnpYTjJkR2w1dG5TSnlGeUNMV3cyM3h1NExhY2RNOGNHY0pPdkI4Z3dw
ajBzQkZvNnpjMUFBaVhjdEhkbUc1TWFwenlZPSJdLCJ0eXAiOiJKV1QiLCJhbGciOiJFUzI1NiJ9
.eyJ2ZXJzaW9uIjo1MDYsImhhc2hBbGdvcml0aG0iOiJTSEEtMjU2IiwiZG9tYWluTGlzdCI6W3
siZG9tYWluIjoiZWY3MmQ0M2Q1OWI5MWNjZTMwNjY3MzMzNmQ3MTI1ZGIwY2JiMzA5YW
I2ODkzM2Y4MGNlMGNmNTU3MDg4MTBlYSIsInRlbGVtYXRpa0lEIjoiMS0xYXJ2dHN0LWF1d
G8tdHMtMDAwMSIsImlzSW5zdXJhbmNlIjpmYWxzZX0seyJkb21haW4iOiJjNjRkM2VmYmMy
Nzk3ZDg0Y2NlOGM0NjAwMTNkYTFmMThiMWE1NTYzNWVhZTBhYTE4ZTljZmQxMGEzYWM
yNGQ4IiwidGVsZW1hdGlrSUQiOiIxLTFhcnZ0c3QtdGVzdC10cDA3LTAzIiwiaXNJbnN1cmFuY
2UiOmZhbHNlfSx7ImRvbWFpbiI6IjMzNTJhZjFhZThkY2Y4MjljYjM0YjdlYTY2NDk0OTAxMzM
4NTg2MGYyZTFlNDBjNTUxMmVhYTk2ODg3YjdlNjEiLCJ0ZWxlbWF0aWtJRCI6IjEtMWFydnR
zdC10ZXN0LXRwMDgtMDEiLCJpc0luc3VyYW5jZSI6ZmFsc2V9LHsiZG9tYWluIjoiYjRhZTM3
OTZhN2Q5YWYzYzdiNmNhNzU5MzYxZTlhZDkyZjk0NmU3ZmFkNzZkZGVkZDEzM2U5ZTBh
NjUwMTg1OCIsInRlbGVtYXRpa0lEIjoiMS0xYXJ2dHN0LXRlc3RvcmctdHAwOS4wMCIsImlzS
W5zdXJhbmNlIjpmYWxzZX0seyJkb21haW4iOiJlN2RmNjRmOTQ1NGRkMDA3NjcxZmQ1Mj
UzYmNjNmMwYzlmZWJkMzBhZTIxZjQ3YjQwZmFlNDczZWQ0NzA2NzM0IiwidGVsZW1hdGl
rSUQiOiIxLTFhcnZ0c3QtdGVzdG9yZy10cDA5LjAxIiwiaXNJbnN1cmFuY2UiOmZhbHNlfSx7I
mRvbWFpbiI6Ijg5NDU3M2U3ZmJhNjYxODE1MGZkMWNkMzUwOTQ5NGE1YTY2NWM1ZjRi
ZmQ0YzY4MjlmZmE5NTM0NWZjYTUxYjAiLCJ0ZWxlbWF0aWtJRCI6IjEtMWFydnRzdC10ZX
N0b3JnLXRwMDkuMDIiLCJpc0luc3VyYW5jZSI6ZmFsc2V9LHsiZG9tYWluIjoiNWY1YTZhOTA
4ODNlMDZjMjEyODAzZmE3OTIwNGUzM2M1MzZkNjgyNTc0MGM5MGVlOGExMDU3ZDMwZ
TE4ZTNhZSIsInRlbGVtYXRpa0lEIjoiMS0xYXJ2dHN0LXRlc3RvcmctdHAwOS4xIiwiaXNJbnN1
cmFuY2UiOmZhbHNlfSx7ImRvbWFpbiI6ImY4NzU1YjRiODk0MTViZjNkOGI1YTI4ZmI2MzA
wYTBhNzE5MDU2NGU0OTQ3YTAzYWE4MTUyZjIwZDc2YTg4MzQiLCJ0ZWxlbWF0aWtJRCI6

```
IjEtMWFydnRzdC10ZXN0LXRwMDUtMDEiLCJpc0luc3VyYW5jZSI6ZmFsc2V9LHsiZG9tYWluI
joiN2FiNWFkYjk1MWZlYmY5ZjUxM2Q4ZDQ3OWYyNjgzMTYzMWU5NGZmNDYwMDkwNTk2
Mjk2NWU0NGI0MjkxMDAwYiIsInRlbGVtYXRpa0lEIjoiMS0xYXJ2dHN0LXRlc3QtdHAwNGEiLC
Jpc0luc3VyYW5jZSI6ZmFsc2V9LHsiZG9tYWluIjoiZGM5Nzg1YjFjNDU5ZjJmZjk3NWFjNGY2
NWM3YTUwNzRkYTFiYWFiMzc4N2Q5ZDg5OGNkNTE3MWQ5NjdhMTUzNSIsInRlbGVtYXRpa
0lEIjoiMS0xYXJ2dHN0LXRlc3QtdHAwNi1hIiwiaXNJbnN1cmFuY2UiOmZhbHNlfSx7ImRvbWF
pbiI6ImY2MDQ2OTBmNTg2ZTQzYzRiY2FmMmQ5ODM2MTI4NWE3NGY2NDEzY2M4MTBiMz
hhY2FmMTliMDc3ZTAzZDIyN2MiLCJ0ZWxlbWF0aWtJRCI6IjEtMWFydnRzdC10ZXN0LXRwM
DYtMDEiLCJpc0luc3VyYW5jZSI6ZmFsc2V9LHsiZG9tYWluIjoiOWZmNDE0NDNlNGUwZDI0Y
zZkMGNiOGQwYWU2YTEzNWRkYzc3ZjUxZGViMmZmNDI4OWViMjkyZGZkZDY3NjcxMyIsIn
RlbGVtYXRpa0lEIjoiMS0xYXJ2dHN0LXRlc3QtdHAwNi0wMiIsImlzSW5zdXJhbmNlIjpmYWxz
ZX0seyJkb21haW4iOiJjNjYwYTMyN2QwNWMzNjNlZWFlN2ZhN2M0MWRkODY2ZmEzMzJm
N2M2OTdiODllZThjMWU5YWNjNzA5ODRjOTFlIiwidGVsZW1hdGlrSUQiOiJ0cDA2YXJ2dHN0L
XRlc3QtdHAwNi0wMyIsImlzSW5zdXJhbmNlIjpmYWxzZX0seyJkb21haW4iOiI0ZjlhZDY1NTli
YjkzZjg2NTgwM2FjM2Q2YzgyMDhhNWFlNTIxZGMwMzdmYWVjYWU4YzVmMTVkMGJlMDlm
MzhhIiwidGVsZW1hdGlrSUQiOiIxLTFhcnZ0c3QtdGVzdC10cDA2LTA0IiwiaXNJbnN1cmFuY2
UiOmZhbHNlfSx7ImRvbWFpbiI6IjM1OTdjOWZkYTdiYWNiZGI5MGQ4ZTlkYTVkMDU5YWU0
NzI5MjQ1OGEyODkxYmZlN2ViYzk4MjQ5YzRjN2EzOWMiLCJ0ZWxlbWF0aWtJRCI6IjEtMWFy
dnRzdC10ZXN0LXRwMDYtMDUiLCJpc0luc3VyYW5jZSI6ZmFsc2V9LHsiZG9tYWluIjoiZDk4N
TFmMjNjMWRkYjFjMDlmNjcxOGQ3OWE3MDFjYzQwOTVjMjJiMjA0NGU3MWY3ODE4OGIwY
TRjZjNlOWJkZSIsInRlbGVtYXRpa0lEIjoiMS0xYXJ2dHN0LXRlc3QtdHAwNjA2IiwiaXNJbnN1c
mFuY2UiOmZhbHNlfSx7ImRvbWFpbiI6IjE4MjQzMGIxNmQ0NjdjNzMxYzMxYjgwYzNiYTg5Z
TMwMzEzYWZjNTdkOTJlZThlY2FlMDQyNDRmZGU4ZDI2ODgiLCJ0ZWxlbWF0aWtJRCI6IjEt
MWFydnRzdC10ZXN0LXRwMDciLCJpc0luc3VyYW5jZSI6ZmFsc2V9XX0.T3oRi_f5LT9C70eo
LWkLLxHalpq5VUx6zAJb9FrSNPFzKpR8SPD3C342mpCGfrEvEc51bTtxxqmFBwve9lLYSg
```

ML-123677 – Measures against manipulation of the federation list (VZD-FHIR directory, security assessment)
The security assessment of the VZD-FHIR directory describes suitable measures against manipulation of the federation list. **[**<=]

4.2.4 Localisation of an MXID (operation whereIs)

The operation checks which part of the directory (organisation, person) contains an MXID and returns the check result. The MXID is passed to the operation in URL form.
For this operation to be performant, the entire FHIR database must not be searched when the operation is called. This can be ensured, for example, by a performance-optimised table with the MXIDs and associated result.

The authentication of the client is carried out for operation whereIs according to Section 4.2.1.4 FHIRDirectoryTIMProviderAPI interface.

The FHIR proxy MUST provide the localisation of an MXID via operation whereIs on a performant basis. To do this, the FHIR proxy must update the required data for the performance response of the whereIs operation whenever a change is made to the endpoint entries (the MXID in it). The FHIR proxy MUST NOT search the original FHIR data to perform the whereIs operation.

4.3 General requirements

4.3.1 Security and data protection

The following specifications also apply to the FHIR-VZD.

TIP1-A_5546-01 – VZD, integrity & authenticity protection
The provider of the VZD MUST implement the integrity and authenticity of the data stored in the VZD in accordance with the guidelines of the Federal Office for Information Security for general directory services, [BSI APP.2.1]. **[<=]**

TIP1-A_5548 - VZD, logging of change operations
The VZD MUST log changes to directory service entries and must keep them available for 6 months.
[<=]

6 months is the maximum depth of proof without coming into the realm of data retention.

TIP1-A_5549 – VZD, No reading profiling
The VZD MUST NOT store or log search requests.
[<=]

TIP1-A_5550 – VZD, no copies of deleted data
The VZD MUST NOT store copies of deleted data.
[<=]

TIP1-A_5551 – VZD, securing against data loss
The VZD provider MUST secure the service against data loss.
[<=]

TIP1-A_5552 – VZD, limitation of search results
The VZD MUST limit the results list of a search query to 100 search results.
[<=]

The 100 search results refer to the FHIR resources HealthcareService and PractitionerRole respectively. All referenced resources included by search parameter "_include" are not counted when limiting the search results.

The bundle in the FHIR search result MUST always contain all referenced resources included by "_include" for each FHIR HealthcareService or PractitionerRole resource included and thus represent a complete package of the included resources.

TIP1-A_5553 – VZD, storing private keys securely
The VZD MUST store its private keys securely and prevent them from being read out in order to prevent manipulation.
[<=]

TIP1-A_5554-01 – VZD, storing registration data securely
The VZD MUST ensure the integrity and authenticity of the stored registration data. **[<=]**

TIP1-A_5556 – VZD, error logging
The VZD MUST log locally and remotely detected errors in its local memory.
[<=]

TIP1-A_5558 – VZD, secure storage of the TSL
The VZD MUST securely store the contents of the TSL in a local trust store and keep it locally accessible for X.509 certificate checks.
[<=]

The X.509 root CA certificate MUST be stored in the FHIR VZD trust store for certificate checks.

The FHIR VZD MUST check weekly whether new X.509 root CA versions exist and cross certificates are available. If this is the case, the FHIR VZD MUST import these new root versions into its trust store.

After creating a new root version of the X.509 root CA of TI, its self-signed certificate and cross-certificates are saved to the download point according to [ROOT-CA]. On an automated basis, the FHIR VZD can monitor the availability of new versions from there. In addition, the following download point can be used under [ROOT-CA-JSON]. The current root certificates including their cross-certificates are maintained there. As a rule, a new root version is generated every two years. The file size of the downloaded JSON file can be used as a hash function. For example, you can use the curl tool to use the HTTP method HEAD to find out whether the local copy of the JSON file is still up to date. The JSON file is an array in which associative arrays are listed as elements. These elements each contain a root certificate including cross certificates for the chronologically preceding and the subsequent root certificate. I.e., cryptographically, this is a double-chained list.

The sub-CA certificates are stored on the download point according to [Sub-CA].

4.3.2 Operation

The VZD-FHIR directory is operationally regarded as another service component in the sense of further development of the directory service. This service component, apart from the interfaces, can be developed and deployed independently of the VZD-LDAP directory. From a user point of view, it is not so much the internal logical structure of directory services that is relevant, but the availability of interfaces and the data contained in the directory.

The VZD-FHIR directory MUST fulfil the processing times under load from Tab_VZD_FHIR_Perf under the peak load parallel for all functions.

Table 6: Tab_VZD_FHIR_Perf

Interface operation	Load specifications Peak load [1/sec]	Processing time specifications Mean value [msec]	Processing time specifications 99% quantile [msec]
FHIR interface for TI-Messenger users (/search)	1000	1000	1250
FHIR interface for owners (/owner)	20	1000	1250

Interface operation	Load specifications Peak load [1/sec]	Processing time specifications Mean value [msec]	Processing time specifications 99% quantile [msec]
Interface I_VZD_TIM_Provider_Services (/tim-provider-services)			
- getFederationList	1	1000	1250
- whereIs	50	1000	1250
- addTiMessengerDomain	1	1000	1250
- getTiMessengerDomain	1	1000	1250
- updateTiMessengerDomain	1	1000	1250
- deleteTiMessengerDomain	1	1000	1250
- checkTiMessengerDomains	1	1000	1250

5 Use cases

5.1 TI-Messenger user searches for entries in the FHIR directory

AF_10036 – User searches for entries in FHIR directory

Attributes	**Remark**
Description	Users can search on the FHIR directory for HealthcareServiceDirectory and PractitionerRoleDirectory entries. This requires authentication at the Auth service. Here the authentication with TI-Messenger clients is described. If there is no valid sitim access token from the Auth service in the TI-Messenger client, a Matrix OpenID token is queried by the TI-Messenger client at the Matrix home server and the /tim-authenticate endpoint of the Auth service is called with the Matrix OpenID token in the Auth header. The Auth service checks the Matrix OpenID token handed over from the TI-Messenger client. The matrix_server_name specified in the Matrix OpenID token MUST be included in the TI-Messenger federation list. The Auth service calls the operation GET/openid/userinfo with the Matrix OpenID token as a parameter on the Matrix home server and receives the MXID of the TI-Messenger user in the response. This completes the authentication of the user. The Auth service creates a search-accesstoken and sends it to the TI-Messenger client. The TI-Messenger client sends a GETRequest to the endpoint /search of the FHIR proxy according to FHIR specification. The authentication header contains the search-accesstoken. The GET request according to the FHIR specification is forwarded from the FHIR proxy to the FHIR directory via http Forward. The FHIR proxy receives a response from the FHIR directory with the found entries as json data. The response is sent to the TI-Messenger client.
Precondition	The user is registered at their home server.
Post-condition	The TI-Messenger client has received all entries found.

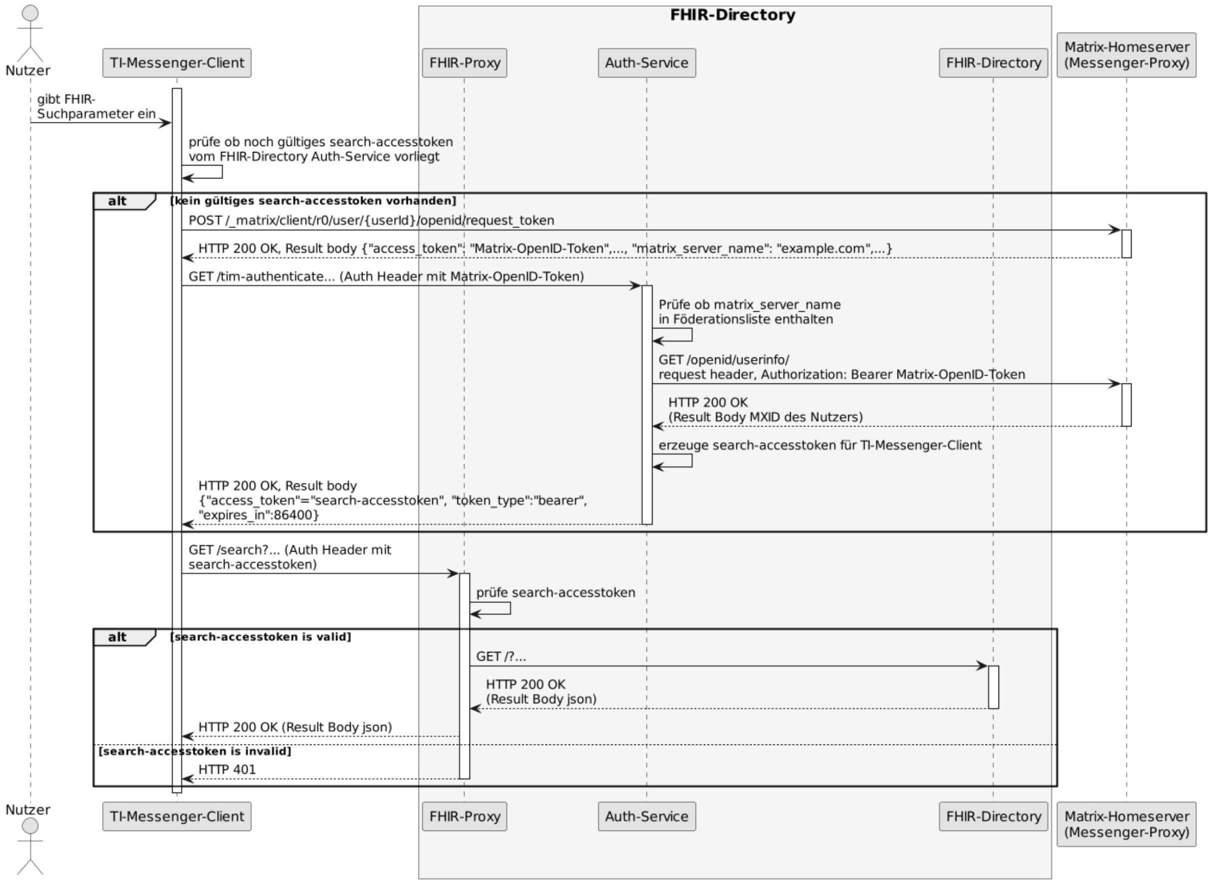
FHIR-Directory
Nutzer
TI-Messenger-Client
FHIR-Proxy
Auth-Service
FHIR-Directory
Matrix-Homeserver (Messenger-Proxy)
gibt FHIR-Suchparameter ein
prüfe ob noch gültiges search-accesstoken vom FHIR-Directory Auth-Service vorliegt
alt
[kein gültiges search-accesstoken vorhanden]
POST /_matrix/client/r0/user/{userId}/openid/request_token
HTTP 200 OK, Result body {"access_token": "Matrix-OpenID-Token",..., "matrix_server_name": "example.com",...}
GET /tim-authenticate... (Auth Header mit Matrix-OpenID-Token)
Prüfe ob matrix_server_name in Föderationsliste enthalten
GET /openid/userinfo/ request header, Authorization: Bearer Matrix-OpenID-Token
HTTP 200 OK (Result Body MXID des Nutzers)
erzeuge search-accesstoken für TI-Messenger-Client
HTTP 200 OK, Result body {"access_token"="search-accesstoken", "token_type":"bearer", "expires_in":86400}
GET /search?... (Auth Header mit search-accesstoken)
prüfe search-accesstoken
alt
[search-accesstoken is valid]
GET /?...
HTTP 200 OK (Result Body json)
HTTP 200 OK (Result Body json)
[search-accesstoken is invalid]
HTTP 401
Nutzer
TI-Messenger-Client
FHIR-Proxy
Auth-Service
FHIR-Directory
Matrix-Homeserver (Messenger-Proxy)

Figure 3: Sequence diagram /search

[<=]

Acceptance criteria for use case AF_10036 User searches for OrganizationDirectory and PractitionerDirectory entries in the VZD-FHIR directory

ML-123485 – Authentication at the endpoint /search (VZD-FHIR directory, security assessment)
At the /search endpoint of the FHIR proxy, authentication may only succeed for requests that contain a valid search-accesstoken in the Authentication header issued by the Auth service.**[<=]**

5.2 Owner changes their entry in the FHIR directory

AF_10037 – Change entries in VZD-FHIR directory

Attributes	Remark
Description	Organisations can customise their entry in the VZD-FHIR directory to their own structures. For example, service providers can add the TI-Messenger address in their entry. As like before, the basic entry of an organisation or a service provider is created by the card issuer. The organisation MAY create its own FHIR resources linked to the basic entry to map the structure of the organisation. For example, hospitals can map their departments as HealthcareService entries that are linked to the organisation entry. If the Org Admin or SP does not have a valid owner accesstoken from the VZD-FHIR directory in the client, authentication by means of OIDC must be performed at an IDP of the TI-IDP federation. After successful authentication, the telematics ID of the service provider or organisation confirmed by the IDP is known at the Auth service. For the calling of FHIR operations by the client, the Auth service issues an owner-accesstoken to the client that also contains the telematics ID of the SP or organisation.
Precondition	The organisation or service provider already has a basic entry in the VZD-FHIR directory. An authenticator app of the IDP is available to confirm the organisation identity or service provider identity for an IDP of the TI-IDP federation.

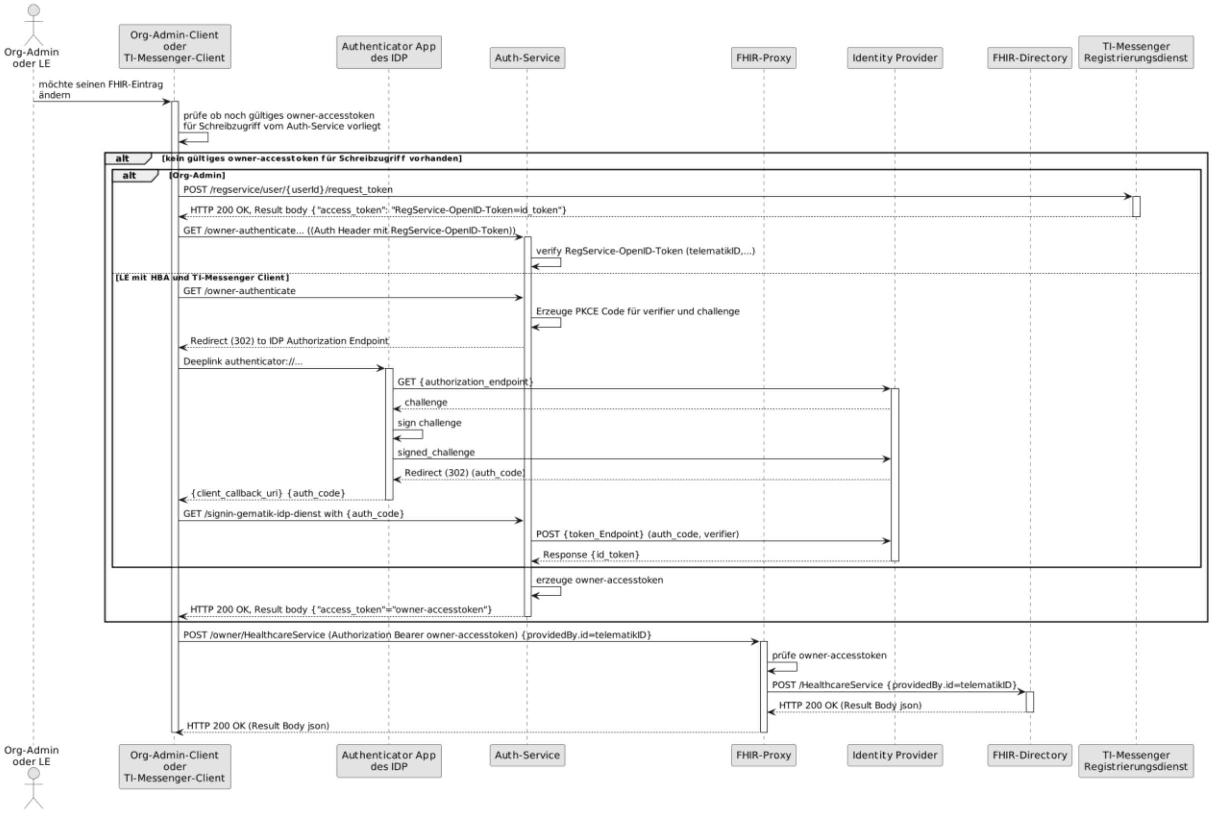
Org-Admin
oder LE
Org-Admin-Client
oder
TI-Messenger-Client
Authenticator App
des IDP
Auth-Service
FHIR-Proxy
Identity Provider
FHIR-Directory
TI-Messenger
Registrierungsdienst
möchte seinen FHIR-Eintrag
ändern
prüfe ob noch gültiges owner-accesstoken
für Schreibzugriff vom Auth-Service vorliegt
alt
[kein gültiges owner-accesstoken für Schreibzugriff vorhanden]
alt
[Org-Admin]
POST /regservice/user/{userId}/request_token
HTTP 200 OK, Result body {"access_token": "RegService-OpenID-Token=id_token"}
GET /owner-authenticate... ((Auth Header mit RegService-OpenID-Token))
verify RegService-OpenID-Token (telematikID,...)
[LE mit HBA und TI-Messenger Client]
GET /owner-authenticate
Erzeuge PKCE Code für verifier und challenge
Redirect (302) to IDP Authorization Endpoint
Deeplink authenticator://...
GET {authorization_endpoint}
challenge
sign challenge
signed_challenge
Redirect (302) (auth_code)
{client_callback_uri} {auth_code}
GET /signin-gematik-idp-dienst with {auth_code}
POST {token_Endpoint} (auth_code, verifier)
Response {id_token}
erzeuge owner-accesstoken
HTTP 200 OK, Result body {"access_token"="owner-accesstoken"}
POST /owner/HealthcareService (Authorization Bearer owner-accesstoken) {providedBy.id=telematikID}
prüfe owner-accesstoken
POST /HealthcareService {providedBy.id=telematikID}
HTTP 200 OK (Result Body json)
HTTP 200 OK (Result Body json)
Org-Admin
oder LE
Org-Admin-Client
oder
TI-Messenger-Client
Authenticator App
des IDP
Auth-Service
FHIR-Proxy
Identity Provider
FHIR-Directory
TI-Messenger
Registrierungsdienst

Figure 4: Sequence diagram VZD-FHIR directory Change of own OrganizationDirectory or PractitionerDirectory entries

[<=]

An Org Admin account can only be created at the registration service if an organisation has been successfully authenticated. To do this, the FHIR directory must trust the registration services of all TI-Messenger providers and check the required data (telematicsID, certificate type, technical role) in the id_token of the registration service.

Trust in the registration services of the TI-Messenger providers is established when the TI-Messenger provider registers with the FHIR directory for the I_VZD_TIM_Provider_Services interface (see also Section 4.2.1.4 FHIRDirectoryTIMProviderAPI interface).

- When the TI-Messenger provider is registered, the signature certificate used to sign the id_token is stored in the FHIR directory.
- This signature certificate is checked against the signature certificate used during the token check (see acceptance criterion ML-136890).

The owner-accesstoken is queried according to the context /client/relevant IDP via the corresponding URL.
Currently only the gematik-IDP is supported and therefore the corresponding URL /signin-gematik-idp-dienst

After successful verification, the FHIR directory issues and returns an owner-accesstoken.
If the Auth service of the VZD-FHIR directory is called without a token, it must perform authentication according to OpenID Connect.
The Auth service must support the authentication according to OpenID Connect also for

accesses by Org-Admins (SMC-B/organisation) – in addition to the authentication with RegService OpenID token.

Acceptance criteria for use case AF_10037 Change OrganizationDirectory entries in VZD-FHIR directory

ML-123873 – Authentication at the endpoint /owner (VZD-FHIR directory, security assessment)
At the FHIR proxy endpoint /owner, authentication may only be successful for users who have a valid access token from the VZD-FHIR directory.
[<=]

ML-123874 – Change entries with own telematics ID only (VZD-FHIR directory)
The access token used for authentication contains the telematics ID of the user. Only the (PractitionerDirectory or OrganizationDirectory) entry with its own telematics ID may be changed. Only those attributes that are not synchronised by the VZD-LDAP directory may be changed.
[<=]

ML-138040 – Self-created HealthcareDirectory entries MUST be linked to one's own basic entry (VZD-FHIR directory)
All FHIR entries created by the owner themselves MUST be linked to their own basic entry providedBy. If the link is not correct, the FHIR proxy MUST reject creating or modifying the HealthcareDirectory entry with the error message (HTTP 422 Unprocessable Entity). **[**<=**]**

ML-136899 – AF_10037 IDP service ID-TOKEN check (VZD-FHIR directory)
The ID_TOKEN check is based on information from the IDP Discovery document of the IDP service.
The URL of the download point on the internet is: "https://idp.app.ti-dienste.de/.well-known/openid-configuration".
The Discovery document must have been read in before the tests for the current environment (RU/TU/PU) are carried out.

Optional and mandatory from FHIR VZD 1.2:

- Verification of the signature of the Discovery document: The VZD-FHIR directory must be able to mathematically check the signature of the Discovery document and trace it back to a temporally valid C.FD.SIG certificate with the role OID oid_idpd, which was issued by a CA of the component PKI known to it.
- Verification of the signature certificate against the X.509 root CA certificate of the TI.
- OCSP verification of the signature certificate.
- Regular loading of the Discovery document: The VZD-FHIR directory must regularly load the Discovery document from its download point every 24 hours and, after its successful check, use the data it contains to check ID_TOKEN.

The ID_TOKEN issued by the IDP service must be checked by the VZD-FHIR directory according to the following criteria:

- Validation of the structure of the ID_TOKENs prescribed in [RFC7519 # section-7.1] in accordance with [RFC7519 # section-7.2].

- Decryption of the encrypted ID_TOKEN according to the procedure provided for this transmission with the "token_key" selected by the VZD-FHIR directory. Unencrypted ID_TOKENs are invalid and must be rejected.
- Verification of the signature of the ID_TOKEN against the public key of the token endpoint PUK_IDP_SIG. The VZD-FHIR directory must take the public key PUK_IDP_SIG from the Discovery document of the IDP service beforehand.
    - Algorithm: "alg": Must match a permitted value from the IDP service's Discovery document, attribute "id_token_signing_alg_values_supported". E.g. "BP256R1"
    - Reaction in case of invalid or missing signature of the "ID_TOKEN": The VZD-FHIR directory must abort all operations associated with the ID_TOKEN if the ID_TOKEN is not signed or its signature is incorrect.
- The VZD-FHIR directory must ensure that the period of use of the token is between the values of the attributes iat and exp supplied in the token.
- Telematics ID check: The ID_Token must contain a telematics ID in the idNumber attribute. ID_Tokens with empty attribute idNumber must be rejected.
- The VZD-FHIR directory must reject ID_TOKENs if the values carried forward in an attribute do not correspond to the schematically expected data type of the attribute.

Optional and mandatory from FHIR VZD 1.2:

- The VZD-FHIR directory must check the claim "aud" of the ID_TOKEN against its client-id registered with the IDP service. Only if these match is the check considered positively validated.
- The VZD-FHIR directory must compare the attributes transmitted in the ID_TOKEN with those agreed with the IDP service at registration and must abort all operations related to the ID_TOKEN if the ID_TOKEN is missing claims necessary for processing or if personal attributes other than those agreed with the IDP service are present.
    - Note: Unexpected person-related attributes are as per the table: [gemSpec_IDP_FD#TAB_IDP_DIENST_0005] the claims given_name, family_name and organizationName
- Optional: If the VZD-FHIR directory has set a nonce parameter in the authorisation request to the IDP service, then the ID token issued by the IDP service contains exactly this value as a claim. The VZD-FHIR directory must then check whether the nonce value passed in the authorisation request matches that in the ID token.

[<=]

ML-136890 – AF_10037 TIM registration service id_token check (VZD-FHIR directory)
The id_token issued by the registration service must be checked by the VZD-FHIR directory:

- Validation of the structure of the id_tokens prescribed in [RFC7519 # section-7.1] in accordance with [RFC7519 # section-7.2].
- Verification of signature of the id_token according to RFC7515 (the certificate used must originate from the TI's component PKI)

  - Certificate type: C.FD.SIG
  - technical role: oid_tim
- The telematicsID must be contained in the token attribute idNumber.

Optional and mandatory from FHIR VZD 1.2:

- Verification of the id_token signature certificate (or its hash) against the signature certificate provided when requesting the credentials for the I_VZD_TIM_Provider_Services interface.
  - OCSP verification of the id_token signature certificate
  - Check of algorithm: "alg": "ES256"
  - Verification of the signature certificate against the X.509 root CA certificate of the TI.
- Check of the temporal validity of the id_token for access to the VZD-FHIR directory: The VZD-FHIR directory must ensure that the period of use of the token is between the values of the attributes iat and exp supplied in the token.
- The VZD-FHIR directory must compare the attributes transmitted in the id_token with those agreed with the registration service and must abort all operations related to the id_token if the id_token is missing claims necessary for processing or if personal attributes other than those agreed with the IDP service are present.
  - Note: Unexpected person-related attributes are as per the table: [gemSpec_IDP_FD#TAB_IDP_DIENST_0005] the claims given_name, family_name and organizationName
- Audience: "aud": URL of the interface e.g. "https://fhir-directory.vzd.ti-dienste.de/owner-authenticate"
- The telematicsID from the token attribute idNumber must be contained in the federation list and the federation list entry must have been entered by the same TIM provider that issued the token.

[<=]

ML-136887 – AF_10037 TI provider access token check (VZD-FHIR directory)
The TI provider access tokens must be checked by the VZD-FHIR directory for the /tim-provider-services endpoint:

- Validation of the structure of the ACCESS_TOKENs prescribed in [RFC7519 # section-7.1] in accordance with [RFC7519 # section-7.2].
- Ensuring the correct signature of the token according to RFC7515:
  - Certificate type: C.FD.SIG
  - technical role: oid_vzd_ti
  - OCSP verification of the signature certificate: No
- Temporal validity: The VZD-FHIR directory must ensure that the period of use of the token is between the values of the attributes iat and exp supplied in the token.
- The telematicsID must be contained in the token "sub" claim.

Optional and mandatory from FHIR VZD 1.2:

- The VZD-FHIR directory must compare the attributes transmitted in the ACCESS_TOKEN with those agreed and must abort all operations related to the

ACCESS_TOKEN if the ACCESS_TOKEN is missing claims necessary for processing or if personal attributes other than those agreed are present.

  - Check of audience "aud" from the token (must correspond to the /tim-provider-services interface, e.g. https://fhir-directory. [vzd.ti-dienste.de/tim-provider-services)](vzd.ti-dienste.de/tim-provider-services)
  - Note: Unexpected person-related attributes are as per the table: [gemSpec_IDP_FD#TAB_IDP_DIENST_0005] the claims given_name, family_name and organizationName
- Ensuring the correct signature of the token according to RFC7515:
  - Check of algorithm: "alg": "ES256"

[<=]

5.3 Use cases of the TI-Messenger provider in the VZD-FHIR directory

AF_10048-01 – Use cases of the TI-Messenger provider in the VZD-FHIR directory

Attributes	Remark
Description	For the operation of a TI-Messenger specialist service, it is necessary to know all the Matrix domains involved in the federation in order to be able to exclude Matrix domains not involved in the federation. Domains are stored in the VZD-FHIR directory in endpoint entries. The endpoint entries of a TI-Messenger provider are linked to its OrganizationDirectory entry. The TI-Messenger provider manages its entries in the VZD-FHIR directory itself. For this purpose, the TI-Messenger provider requests client credentials for the use of the I_VZD_TIM_Provider_Services interface for its registration service. With the credentials, the registration service receives a ti-provider-accesstoken from the VZD TI provider OAuth server. It exchanges this for a provider-accesstoken from the VZD-FHIR directory Auth service, which is used for authentication at the interface. After successful authentication, the registration service can use the FHIR operations to manage its own OrganizationDirectory entry and endpoint entries. In order to obtain all the Matrix domain names involved in the federation, operation GET /FederationList is called. Optionally, the known version can be specified in the request. As a result, the registration service receives a list of hashes of the domain names involved in the federation or no list if no newer version exists. The hashes of domain names are used to prevent every TI-Messenger provider from knowing all domain names in plain text.
Precondition	The registration service of the TI-Messenger provider is already registered as a user of the VZD-FHIR directory and has received TI provider OAuth Client Credentials (client_id and client_secret) for the environments RU, TU and PU.

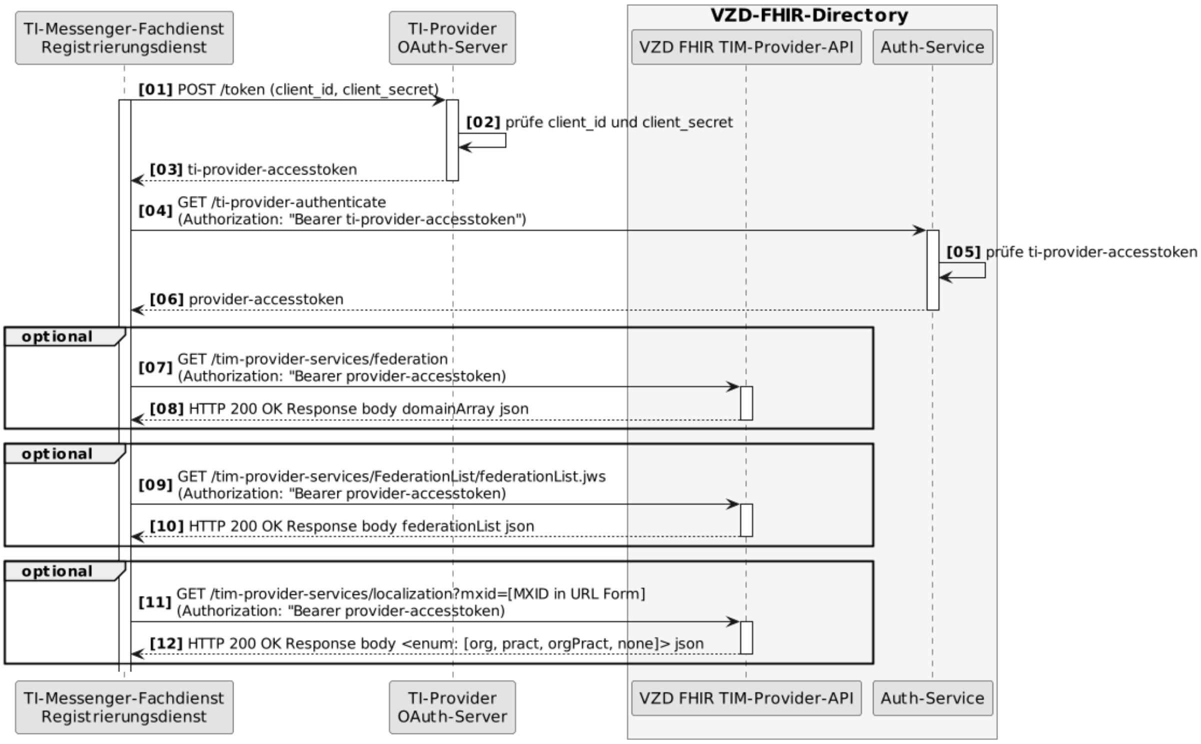
TI-Messenger-Fachdienst Registrierungsdienst
TI-Provider OAuth-Server
VZD-FHIR-Directory
VZD FHIR TIM-Provider-API
Auth-Service
[01] POST /token (client_id, client_secret)
[02] prüfe client_id und client_secret
[03] ti-provider-accesstoken
[04] GET /ti-provider-authenticate (Authorization: "Bearer ti-provider-accesstoken")
[05] prüfe ti-provider-accesstoken
[06] provider-accesstoken
optional
[07] GET /tim-provider-services/federation (Authorization: "Bearer provider-accesstoken)
[08] HTTP 200 OK Response body domainArray json
optional
[09] GET /tim-provider-services/FederationList/federationList.jws (Authorization: "Bearer provider-accesstoken)
[10] HTTP 200 OK Response body federationList json
optional
[11] GET /tim-provider-services/localization?mxid=[MXID in URL Form] (Authorization: "Bearer provider-accesstoken)
[12] HTTP 200 OK Response body <enum: [org, pract, orgPract, none]> json

Figure 5: VZD-FHIR-Directory_Sequence-Diagram_TI-Messenger-Provider-Services

[<=]

ML-123881 – Authentication at the I_VZD_TIM_Provider_Services interface (VZD-FHIR directory, security assessment)

At the I_VZD_TIM_Provider_Services interface, the authentication may only be successful for clients who have a valid provider access token from the OAuth server of the VZD provider.
[<=]

5.4 Compare entries with the VZD-LDAP directory

AF_10047-01 – Compare entries with the VZD-LDAP directory

Attributes	Remark
Description	The FHIR proxy regularly updates the entries in the VZD-LDAP directory that have changed since the last update at a configurable interval. As this is an internal directory service interface, it does not specify how the interface is to be implemented. The transfer of data MUST be done TLS-encrypted in an internal network of the directory service. All changed entries since the last update are queried by the FHIR proxy from the VZD-LDAP directory and updated according to [VZD-FHIR-Directory_Mapping_LDAP_to_FHIR]. Deleted entries in the VZD-LDAP directory must also be detected and deleted in the VZD-FHIR directory. In the VZD-FHIR directory, the value of Organization.active or PractitionerDirectory.active is set to "active" during synchronisation from the VZD-LDAP directory according to the LDAP base entry attribute.

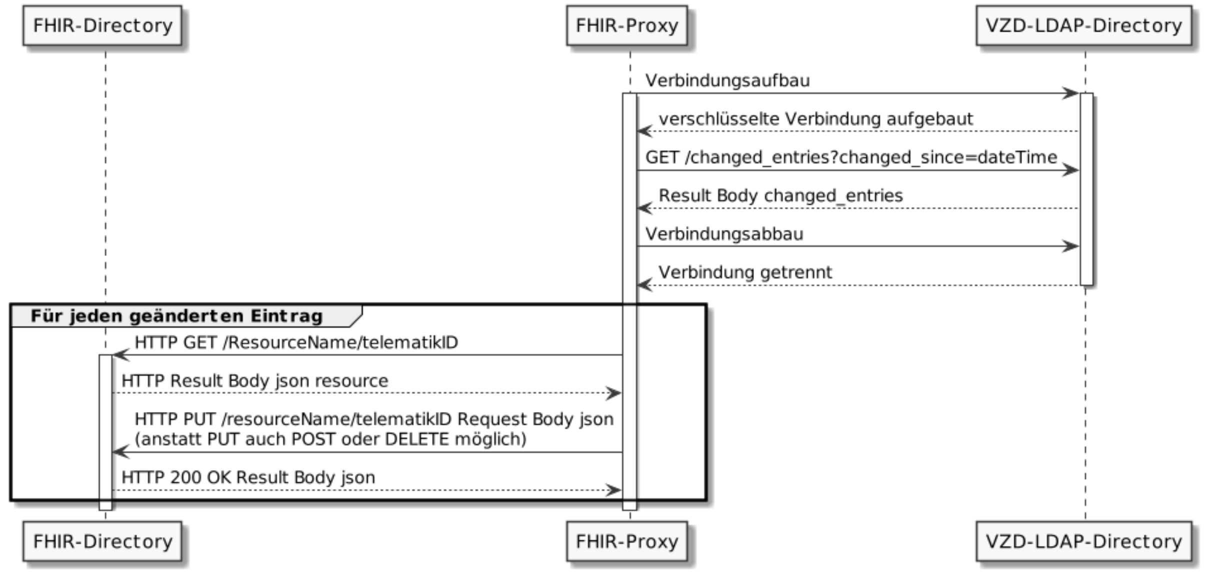
FHIR-Directory
FHIR-Proxy
VZD-LDAP-Directory
Verbindungsaufbau
verschlüsselte Verbindung aufgebaut
GET /changed_entries?changed_since=dateTime
Result Body changed_entries
Verbindungsabbau
Verbindung getrennt
Für jeden geänderten Eintrag
HTTP GET /ResourceName/telematikID
HTTP Result Body json resource
HTTP PUT /resourceName/telematikID Request Body json
(anstatt PUT auch POST oder DELETE möglich)
HTTP 200 OK Result Body json
FHIR-Directory
FHIR-Proxy
VZD-LDAP-Directory

Figure 6: VZD-FHIR directory, updating basic entries

[<=]

ML-134278 – Synchronisation of VZD-LDAP directory with FHIR directory (VZD-FHIR directory)

The VZD FHIR proxy must ensure that after a configurable interval, the entries changed in the VZD-LDAP directory since the last update have been synchronised into the VZD-FHIR directory.

[<=]

6 Distribution view

The VZD-FHIR directory initially supports the TI-Messenger application, but will in future also support other applications such as ePA and KIM in their subsequent versions as well as previously unknown specialist applications and new user groups. It is therefore necessary that the VZD-FHIR directory can scale with the number of user accesses and store application-specific resources.

The FHIR proxy MUST be able to operate in multiple instances that implement the interfaces towards the internet for queries of TI-Messenger users and changes by owners. Load balancing of client requests is done via DNS by entering an A and an AAAA resource record for each instance of the FHIR proxy for the RU, TU and PU FQDNs of the interfaces in DNS. FHIR proxy instances are added or removed depending on the load.

The FHIR proxy is also the HTTP load balancer for read access to FHIR directory instances. An instance is implemented for write access. The databases of the read access instances are synchronised with the write access database.

Another component implements the updating of the base entries in the FHIR directory with the changed data from the VZD-LDAP directory. In addition, this component implements the I_VZD_TIM_Provider_Services interface.

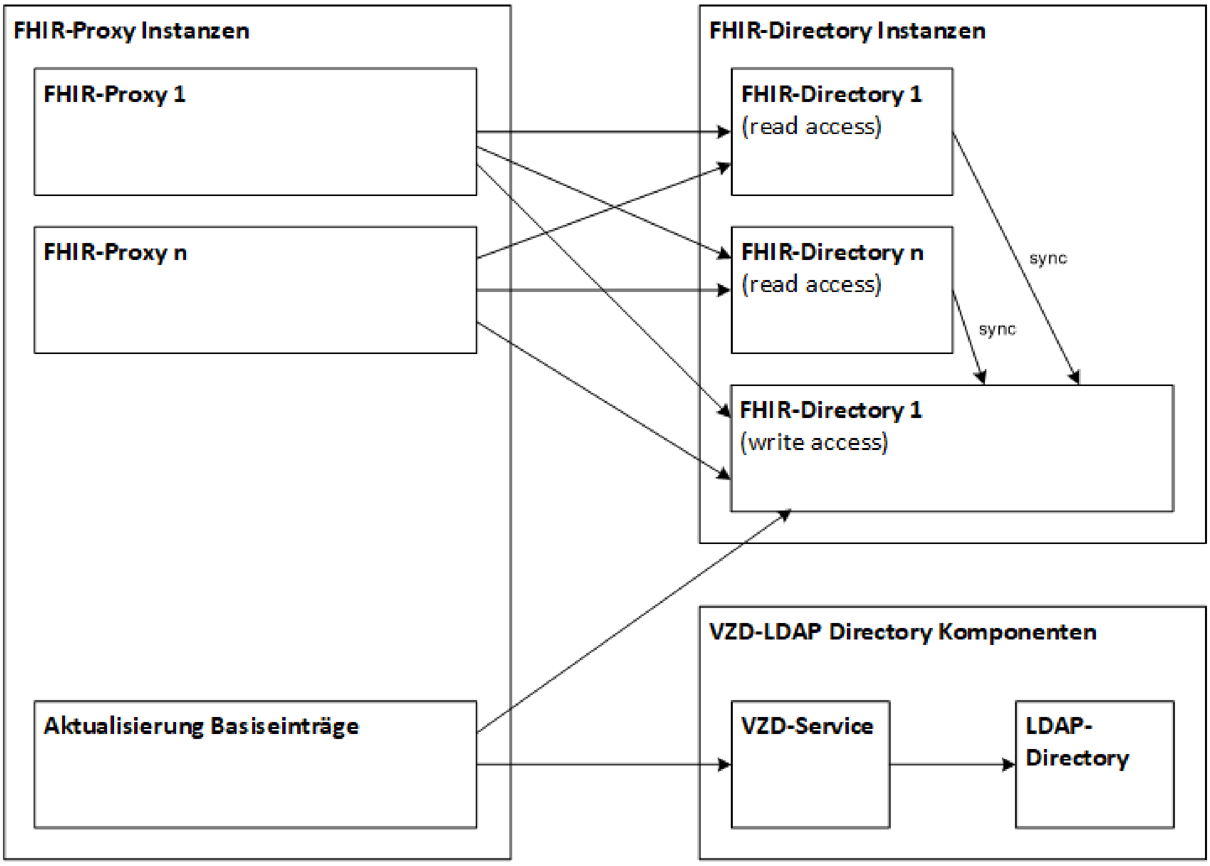

Figure 7: VZD-FHIR directory distribution view

7 Annex A – Directories

7.1 Abbreviations

Abbreviation	Explanation
AF	Use case
DNS	Domain Name System
FHIR	Fast Healthcare Interoperable Resources
FQDN	Full Qualified Domain Name
LDAP	Lightweight Directory Access Protocol
OWASP	Open Web Application Security Project
PU	Production environment
RU	Reference environment
SHA	Secure Hash Algorithm
TLS	Transport Layer Security
TI	Telematics infrastructure
TIM	TI-Messenger (only use abbreviation in attributes, parameters or URLs)
TU	Test environment
VZD	Directory service

7.2 Glossary

Term	Explanation
Functional feature	The term describes a function or also individual sub-functions of the TI forming a logical unit within the framework of the functional breakdown of the system.

The glossary is made available as an independent document (see [gemGlossary]).

7.3 List of figures

7.4 List of tables

7.5 Referenced documents

7.5.1 gematik documents

The following table contains the names of the gematik documents on telematics infrastructure referenced in this document. The version-related state of development of these concepts and specifications is defined per release in a document map; the version and status of the referenced documents are therefore not listed in the table below. Their respective valid version numbers for this document are included in the current document map published by gematik, in which the present version is listed.

[Source]	Published by: Title
[gemGlossary]	gematik: Introduction of health card – glossary
[gemSpec_VZD]	gematik: Directory service specification
[gemSpec_Krypt]	gematik: General specification Use of cryptographic algorithms in telematics infrastructure

[Source]	Published by: Title
[gemKPT_Betr]	gematik: Operating concept online productive operation
[VZD-FHIR-Directory_Mapping_LDAP_to_FHIR]	gematik: VZD mapping LDAP to FHIR resources https://github.com/gematik/api-vzd/blob/23456d9ef61263185edfbcaabf09086ba7b26a20/docs/LDAP2FHIR_Sync.adoc
[Simplifier-FHIR-VZD]	gematik: FHIR VZD data model https://simplifier.net/vzd-fhir-directory

7.5.2 Other documents

[Source]	Publisher (publication date): Title
[CAB-Forum]	Trusted certificate issuer (root CAs) list for applications on the 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
[Sub-CA]	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/

7.6 Data model versioning

The following versions of the data model resources (https://simplifier.net/vzd-fhir-directory/) are relevant for the present specification:

- de.gematik.fhir.directory/0.10.1