Electronic health card and telematics infrastructure

Specification
TI-Messenger Service

Note: This document is non-binding.

Version:	1.1.1
Revision:	682478
Last updated:	31/07/2023
Status:	released
Classification:	public
Referencing:	gemSpec_TI-Messenger-Service

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 the document	gematik
1.1.0	29/07/2022		Revision of the following features: – Accessibility of individual organisational units by means of function accounts – Opening of TI-Messenger for third-party systems by client-side interfaces for integration into practice management system – Quick finding of contact data by accessing the FHIR-based address book	gematik
	16/08/2022		Possibility of some kind of access control for Org Admin	gematik
1.1.1	31/07/2023		Integration of TI-Messenger Maintenance 23.1 / VZD FHIR Maintenance_23.1	gematik

Contents

1 Classification of document

1.1 Objective

This document defines the specifications for the first expansion stage of TI-Messenger. This expansion stage is defined by ad-hoc communication between healthcare organisations. Particular attention will be paid to ad hoc communication between service providers and between service provider institutions. Specifications on the user group of insured persons and requirements for health insurance organisations will be taken into account in the second stage of the TI-Messenger expansion and therefore not further considered in this document.

This document describes the system-specific solution of the TI-Messenger for the German healthcare system based on the requirements of the TI-Messenger concept paper [gemKPT_TI_Messenger]. At this point, in particular, the requirements of the concept in the form of defined use cases for the production, testing and operation of the TI-Messenger service are described. The respective use cases describe the entire process necessary for fulfilment and identification of all subcomponents necessary for implementation. Further functional specification takes place in the respective dedicated product type specification.

This specification is to be considered as a functional unit with the respective specification related to a specific product type.

1.2 Target group

For the purpose of implementation, the document is intended for manufacturers of TI-Messenger product types as well as suppliers who operate the described product types. All manufacturers and suppliers of TI applications whose interfaces use one of the TI-Messenger product types, or exchange data with the TI-Messenger product types, or process such data, must also take this document into account.

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

This document specifies the overarching requirements in the form of use cases. The functional features used for the use cases described here are further defined in the specifications of the individual TI-Messenger service product types.

The interfaces provided by the TI-Messenger service are defined in the specifications of the individual TI-Messenger service components. However, interfaces used by other product types are described in the specification of the product type that provides this interface. Reference is made to the respective documents.

The complete requirement position for the TI-Messenger service results from several specification documents. These are listed in the individual TI-Messenger product and supplier type profiles.

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 TI-Messenger service product as well as for the operating provider according to [gemKPT_Betr] and is to be considered as approval criteria for the product and the supplier.**
- The binding nature SHOULD be indicated by the keywords MUST, MUST NOT, SHOULD, SHOULD NOT, MAY, written in capital letters and corresponding to RFC 2119 [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 acceptance criteria identifier 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 secure exchange of messages between involved actors of the German healthcare sector takes place through TI-Messenger specialist services and TI-Messenger clients provided by TI-Messenger providers. Ad-hoc communication between the actors takes place via approved TI-Messenger clients. The TI-Messenger specialist service product types as well as TI-Messenger clients are provided by TI-Messenger providers approved by gematik.

A TI-Messenger specialist service consists of one or more messenger services (based on the Matrix protocol), each provided to a healthcare organisation (SMC-B owner). These only differ in the type of authentication method used. Actors involved in an organisation MAY use the messenger service provided by that organisation and replicate the authentication methods already used within that organisation. This allows seamless integration into everyday life. Actors who are not affiliated to an organisation MAY use association messenger services if they are provided by an association for their members. The existing authentication process of the association can be used here. Messenger services MAY be used with different TI-Messenger clients. For example, it is possible for both organisations to provide a messenger service to a doctor who works in a hospital and in an established practice in parallel.

The messenger services of the TI-Messenger service are merged into a TI federation to exclude unrelated messenger services. To become part of the federation of the TI-Messenger service, the respective domain of a messenger service from the TI-Messenger provider MUST be stored in the VZD-FHIR directory through the registration service of the TI-Messenger specialist service. Once this is done, its actors will have read access to the VZD-FHIR directory and, depending on the authorisation, may start communication with actors in other organisations. The communication takes place end-to-end encrypted between the TI-Messenger clients of the messenger services involved. The addressing of the actors within a messenger service is done via the Matrix user ID and is referred to as MXID in the context of the TI-Messenger service. To inform involved actors about the arrival of new messages, the TI-Messenger specialist service MUST have a push gateway at its disposal.

Note: For the purposes of the Matrix protocol, end devices – referred to as "devices" in the matrix specification – are those that have the ability to decrypt the data sent to them for the first time after it has been fully transmitted. It should be noted that "end devices" means dedicated client instances and not necessarily physical devices that are uniquely identifiable by their `device_ID` *and are created by a client the moment it is used to log on to a user account. This means that one or more end devices are subordinate to a user account, which is itself characterised by a cryptographic identity, and enables the user to receive and send end-to-end encrypted data in the first place. Only after the data has been decrypted can it be read by a user and processed by the systems they use, such as a hospital information system, in accordance with the purpose.*

The following figure shows all involved components of the TI-Messenger architecture:

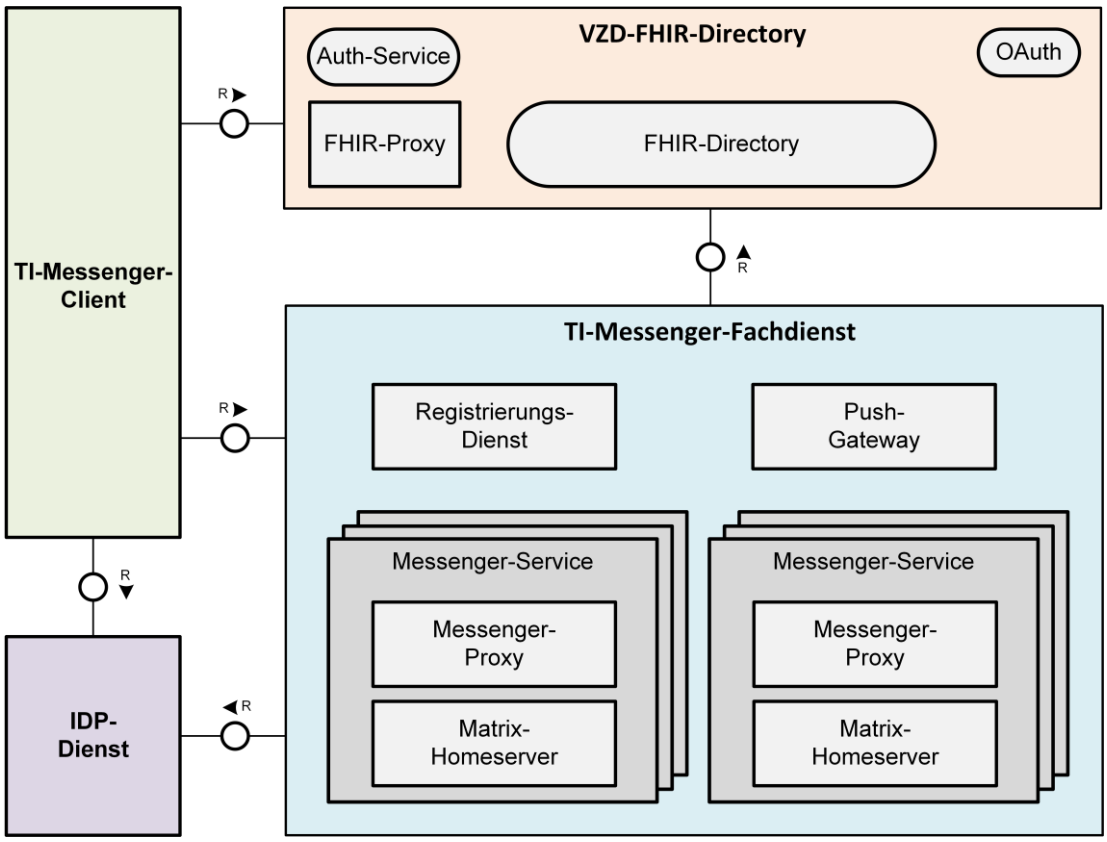

Figure 1: TI-Messenger architecture components (simplified presentation)

The TI-Messenger service is based on the open communication protocol Matrix already specified by the Matrix Foundation according to [Matrix Specification]. The specifications prepared by the Matrix Foundation describe both client-server and server-server communication as well as the API of the Matrix Push Gateway. To ensure the federal and decentralised structure of the TI-Messenger service in the German health care system and to limit the user circle, further components are required, which are described in the respective specification published by gematik.

3 System context

3.1 Actors and roles

In the context of the TI-Messenger service, different actors and roles are defined. An actor is a natural person (service provider / employee of a healthcare organisation) or a technical system (chatbot) that interacts with a TI-Messenger specialist service. Depending on the authentication process used in the messenger service of a TI-Messenger specialist service, there are different roles that an actor can take on. These roles are described below.

3.1.1 Role: "User"

The user role can be assumed by a service provider as well as by a health care worker. The authentication of the actor does not take place via an SMC-B or an HBA, but via an authentication process provided by the messenger service. For an actor in the "User" role, its MAXID can be stored in the organisation directory on the VZD-FHIR directory in order to be found for actors outside of its organisation. Chatbots for mapping function accounts also perform the "User" role and are described in more detail in Section 5.6 – Function accounts.

In this role, an actor can:

- be authenticated against a messenger service, and
- log in to a messenger service.

3.1.2 Role: "User-HBA"

The "User-HBA" role can only be assumed by a service provider. The authentication of the actor is performed through its HBA. An actor in the "User-HBA" role MAY store their MAXID in the person directory in the VZD-FHIR directory so that other actors in the "User-HBA" role who have also stored their own MAXID on the VZD-FHIR directory can contact them.

In this role, an actor can:

- authenticate themselves at the responsible IDP service,
- log in to the messenger service, and
- store their MAXID on the VZD-FHIR directory to make themselves personally available across sectors.

3.1.3 Role: Org Admin

The "Org Admin" role represents a special role in the TI-Messenger context. Service providers or employees of an organisation can assume this role after having successfully authenticated their organisation at the registration service using their SMC-B or through the KIM method (see use case AF_10103 – Authentication of an organisation at the TI-Messenger service). After successful authentication, an admin account is created at the registration service by the TI-Messenger specialist service. By logging on to the

registration service via the admin account, an actor takes on the "Org Admin" role. They MAY register messenger services for their organisation and manage entries in the VZD-FHIR directory. For the ″Org Admin" role, there is a need to use administrators who have been trained and sensitised for information security issues. It is also possible that the organisation entrusts the TI-Messenger provider with the role of ″Org Admin".

In this role, an actor can:

- Register messenger services for their organisation,
- administer the contact points of their organisation on the VZD-FHIR server and thus make them accessible across sectors,
- administer the employees of their own organisation as actors of this messenger service in the Matrix home server (user management) and set up function accounts for their organisation, and
- set up Matrix home server configurations for their organisation.

The following "*Actors and role*s" table gives an overview of the roles defined in the context of the TI-Messenger service, depending on the authentication process used by an actor. The table shows all possible user scenarios after successful authentication of an organisation at the registration service.

Table 1: Actors and roles

Which actor am I	How do I authenticate myself	Which service authenticates me	What role do I assume?
Service provider (e.g. doctors, dentists, pharmacists, psychological psychotherapists, nursing staff, midwives, employees of a health insurance fund) within the meaning of SGB V	HBA	VZD-FHIR directory via the central IDP service	User-HBA
	Organisation authentication procedures + 2nd factor	Messenger service	User
	Admin account credentials + 2nd factor	Registration service	Org Admin
Employees of a healthcare organisation who are not service providers within the meaning of SGB V.	Organisation authentication procedures + 2nd factor	Messenger service	User
	Admin account credentials + 2nd factor	Registration service	Org Admin
Designated administrator of a TI-Messenger provider	Admin account credentials + 2nd factor	Registration service	Org Admin

Which actor am I	How do I authenticate myself	Which service authenticates me	What role do I assume?
Chatbot	Organisation authentication procedures	Messenger service	User

Note:

- *For the user scenarios mentioned in the table with 2-factor authentication, the TI-Messenger provider MUST ensure that the security recommendations of the Federal Office for Information Security (BSI) according to [BSI 2-Factor] are taken into account. Here, for resilience against remote attacks, a procedure shall be chosen that is rated at least "medium".*
- *Insured persons MUST NOT currently be registered as actors on a messenger service. Only actors who can be assigned to the respective organisation by an existing contractual relationship or are in possession of an HBA are allowed to use a messenger service.*

The following illustrates the communication for incoming and outgoing messages from the perspective of an actor in the different roles in a communication matrix.

Table 2: Communication matrix

Org Admin	User	User-HBA	Type of communication
Outgoing communication to:			
x	x	x	Actors in the "user" role within their organisation
-	x	x	Actors in the "user" role outside their organisation
-	-	x	Actors in the "User-HBA" role outside their organisation
-	x	x	Actors in the "User" and "User-HBA" role by scanning a QR code
Incoming communication from:			
x	x	x	Actors in the "user" role within their organisation
-	x	-	Actors in the "user" role outside their organisation
-	-	x	Actors in the "User-HBA" role outside their organisation

Org Admin	User	User-HBA	Type of communication
-	x	x	Actors in the "User" and "User-HBA" role by scanning a QR code

3.2 Neighbouring systems

The following figure shows the neighbouring TI-Messenger service product types:

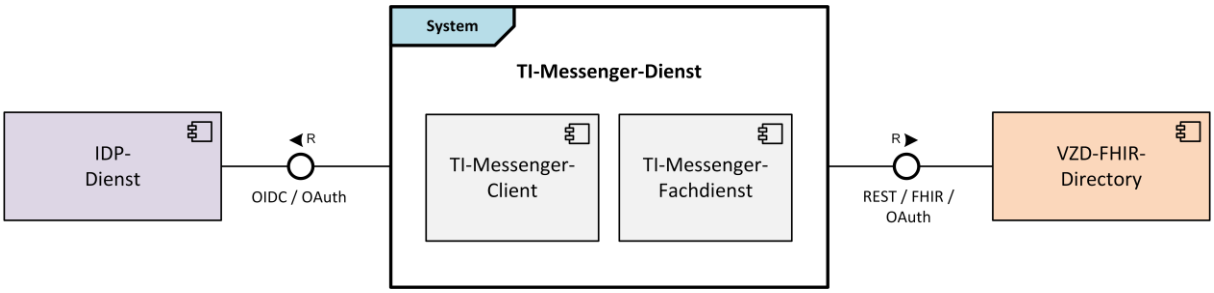

Figure 2: Related TI-Messenger service product types

The TI-Messenger service as a system consists of the TI-Messenger specialist service and TI-Messenger client components.
The TI-Messenger registration service uses the VZD FHIR directory OAuth and REST interfaces to authenticate using OAuth Client Credentials Flow to gain access to the FHIR directory. The TI-Messenger client uses the interfaces of a responsible IDP service to authenticate an actor and interfaces of the VZD-FHIR directory to find or modify, e.g., FHIR resources.

3.3 Messenger service characteristics

The messenger service is a subcomponent of the TI-Messenger professional service and is provided to organisations by the respective provider. The messenger service consists of a Matrix home server (based on the Matrix protocol) and a messenger proxy that ensures that communication with other messenger services, as part of the TI-Messenger service, only takes place within the common TI federation. The messenger services MAY offer actors different authentication procedures that do not require the possession of an SMC-B or an HBA. Messenger services MUST always be associated with organisations or associations that have control over the authentication process used.

Depending on the messenger service, there are different processes for logging into a TI-Messenger specialist service. Various authentication mechanisms can be provided by an organisation for your actors. The organisation and the TI-Messenger provider chosen by them agree on the authentication process to be used bilaterally and agree on the technical implementation of the necessary connection. It is possible, for example, to use an Active Directory (AD/LDAP) or a suitable single sign-on procedure (SSO). The provider MUST ensure that the organisation has control over the respective authentication

mechanisms and the opportunity is provided to ensure a necessary deletion or blocking of a user account.

For better understanding, various, exemplary application scenarios for the TI-Messenger are outlined below and possible forms of a messenger service are explained. There is no claim to completeness here:

3.3.1 Application example for a medical practice

The following user stories should illustrate the needs of established service providers for asynchronous ad-hoc communication:

User story 1 – Use of the TI-Messenger independent of HBA availability
As a practitioner in a medical practice, I am in direct contact with patients most of my day. A large part of the organisation in the practice and the communication with external stakeholders is therefore taken over by the practice team. As a practitioner, I would like to enable my entire practice team to use the TI-Messenger regardless of the availability of an HBA.

User story 2 – Personal accessibility as a doctor As a practitioner in a medical practice, I do not always want to be available to all other TI-Messenger users. Especially for medical enquiries from medical colleagues, I would like to be able to be found intersectorally in the user search.

User story 3 – Accessibility of my own practice for external service providers
As a practitioner in a medical practice, I would like my practice to be accessible and addressable for other TI-Messenger users as a healthcare facility. I would like to decide for myself how I map the individual structure of my practice in contact search and whether I or my practice team will be initially involved in communication.

User story 4 – Accessibility of other healthcare facilities
As a practitioner in a medical practice, I receive patients from other healthcare facilities and have questions about findings or prescriptions. Especially in the case of facilities with which I am not in regular contact, I would like to be able to establish communication even without known contact data and to reach both the right substructure of the facility (e.g. certain ward in a hospital) and the right contact person in this substructure (e.g. decision-maker on duty).

User story 5 – Making case reference in communications
As a practitioner in a medical practice, a large part of my communication with other service providers takes place with reference to a patient or case. I want to be able to manage my messages from this point of view.

User story 6 – Archiving communications
As a practitioner in a medical practice, I would like to be able to document case-related communication in my practice management system in the respective file and thus store it in a comprehensible manner.

User story 7 – Device-independent use of the TI-Messenger
As a doctor in a private practice, I primarily work in my practice management system at my stationary workplace and would like to be able to use the TI-Messenger integrated into this system. When I make home visits, I would also like to be able to access all my communications on a mobile basis and use the TI-Messenger anywhere.

User story 8 – Archivability of communications

As a doctor in a practice, I would like to be able to document case-related communication in my practice management system in the respective local file of the patient and thus store it in a comprehensible manner.

The following procedure results from the shown user stories for the establishment and administration of a TI-Messenger service:

An actor in a medical practice authenticates their organisation using the SMC-B for a registration service of a TI-Messenger provider. After successful authentication by the registration service, an administrator account is created for the organisation. After successfully logging into the registration service, the actor assumes the "Org Admin" role and registers a messenger service provided in a data centre. The provider then provides the medical practice with a messenger service with a secure authentication process. In addition, the actor in the "Org Admin" role can set up actors for their organisation on the Matrix home server (e.g. MFA, doctors). The created actors log on to the messenger service and can directly use the TI-Messenger in the ”User” role.

An actor in the "Org Admin" role sets up functional accounts for their organisation in the organisation directory on the VZD-FHIR directory to make them accessible to actors of other organisations of the TI-Messenger service. A function account is assigned to an actor of the institution (e.g. MFA), who can invite other actors to the chat room. Actors of the medical practice holding an HBA ("User-HBA"role) can additionally authenticate themselves in the TI-Messenger client using HBA and thus store their own MXID as a practitioner entry in the person directory on the VZD-FHIR directory. This also allows them to invite other HBA owners ("User-HBA"role) to a chat room or to be accessible for them.

3.3.2 Application example for a hospital

The following user stories illustrate the need for asynchronous ad-hoc communication within a hospital:

User story 1 – Simple administration of users
As an IT administrator of the hospital, I would like to be able to automate the administration of the users of my organisation in the TI-Messenger as much as possible in order to minimise the workload for the regular maintenance of user entries.

User story 2 – Easy to provide and log on to the service
As a doctor in a hospital, I would like to be able to use the existing means for logging on to the IT systems for the TI-Messenger. The registration to the service should be similar to the registrations of other IT systems I use in the hospital.

User story 3 – Ability to map the different functional areas in a clinic
As a physician in a clinic, I have queries to another department and would like to be able to reach the corresponding department or ward without knowing which other colleagues are employed or on duty there when searching for contacts.

User story 4 – Interdisciplinary teams
As a doctor in a hospital, I work in an interdisciplinary team with colleagues from other disciplines and would like to be able to exchange new laboratory findings or newly available image data on a case with colleagues.

User story 5 – Case-based communication
As a nurse on a station, I want to inform colleagues on my ward about news of a patient and share relevant information (e.g. upcoming to-dos at a shift change).

The following procedure results from the shown user stories for the establishment and administration of a TI-Messenger service within a hospital:

A hospital actor uses SMC-B to authenticate themselves with the registration service of a TI-Messenger provider. The registration service verifies the organisation's used SMC-B. If

successful, the organisation's registration service provides an administrator account. After successfully logging into the registration service, the actor assumes the "Org Admin" role and registers a messenger service for the hospital. This service is provided *on-premise* in the hospital. The messenger service uses the existing hospital authentication process (e.g. Active Directory) when registering actors on the Matrix home server. The actors of the hospital can then use the TI-Messenger service seamlessly with the existing login data, even without owning an HBA (care, therapists).

An actor in the "Org Admin" role sets up functional accounts for the departments in their hospital in the VZD-FHIR directory to make them accessible to actors outside the hospital. A chatbot is assigned to a function account, which automatically identifies the doctor on duty and loads them into the chat room.

3.3.3 Application example for pharmacies

The following user stories should illustrate pharmacy needs for asynchronous ad-hoc communication as examples:

User story 1 – Sending photos
As a pharmacist I am confronted with a defective prescription and would like to clarify the situation with the prescribing service provider. To do so, I take a picture of the prescription in question and ask my question via chat to the organisation of the issuing service provider.

User story 2 – Group chats for regular information sharing

As a pharmacist I would like to inform the service providers in a common group in close proximity to my pharmacy about the re-availability of an out-of-commerce product.

The following procedure results from the shown user stories for the establishment and administration of a TI-Messenger service within a pharmacy:

A pharmacy actor uses SMC-B to authenticate themselves with the registration service of a TI-Messenger provider. The registration service verifies the organisation's used SMC-B. If successful, the organisation's registration service provides an administrator account. After successfully logging into the registration service, the actor assumes the "Org Admin" role and registers a messenger service for the pharmacy, provided in a data centre. For the authentication of the actors in the messenger service, the responsible IDP service of the pharmacies is used, so that the actors of the pharmacies stored there can register on the TI-Messenger via OpenID-Connect.

The pharmacy becomes accessible as an organisation for other actors of the TI-Messenger by an actor in the ”Org Admin” role setting up MXIDs of actors of their pharmacy in the organisation directory on the VZD-FHIR directory. Actors of the pharmacy holding an HBA (”User-HBA” role) additionally store their own MXID as a practitioner entry in the person directory on the VZD-FHIR directory using the TI-Messenger client. This also allows them to invite other HBA owners ("User-HBA" role) to a chat room or to be accessible for them.

3.3.4 Application example for an association for HBA holders

The following user stories should illustrate association needs for asynchronous ad-hoc communication as examples:

User story 1 – Discussion of cases
As an association, I would like to give my members a platform to discuss difficult cases together.

User story 2 – Secure communication regardless of the institution in which the member is working As an association, I would like to give my members the opportunity to become personally accessible on the TI-Messenger and thus to use the service regardless of the institution in which the member is working.

The following procedure results from the shown user stories for the establishment and administration of a TI-Messenger service within an association:

The association has requested an SMC-BORG to be used for authentication on the registration service of a TI-Messenger provider. The registration service verifies the association's used SMC-B. If successful, the association's registration service provides an administrator account. After successfully logging into the registration service, the actor assumes the "Org Admin" role and registers a messenger service for the association, provided in a data centre. This service is provided to healthcare workers who are not affiliated with an organisation with access to an SMC-B.

Actors of the association in possession of an HBA (”User-HBA” role) MAY additionally save their own MXID as a practitioner entry in the person directory on the VZD-FHIR directory with the TI-Messenger client. This enables them to invite other HBA owners (”User-HBA”role) to a chat room or to be available to them.

3.4 TI-Messenger federation

Since the TI-Messenger service is based on the open and decentralised communication protocol Matrix, it MUST be ensured that only authorised Matrix home servers of a messenger service participate.

To provide access to the TI-Messenger service to all legitimate German healthcare actors, a TI-Messenger provider MUST provide its own messenger services to service provider institutions and/or organisations. In order to be able to exclude Matrix home servers not belonging to the TI-Messenger service, the domain names (also referred to as Matrix domain) of the Matrix home servers of the messenger services are summarised in a federation list. This is provided by the VZD-FHIR directory.
A prerequisite for admission to the federation is the operation of a messenger proxy as part of the messenger service, which MUST ensure that only approved TI-Messenger specialist services can enter the federation. Only Matrix home servers MUST be used for inclusion in the federation. For admission to the federation, a successful approval of the TI-Messenger provider including successful approvals for the product type TI-Messenger specialist service and TI-Messenger client must have been carried out by gematik. After successful approval, the registration service of the respective specialist service will be able to assign the Matrix domains of the respective messenger services to a corresponding organisation on the VZD-FHIR directory. Server-side bridging to other messaging protocols MUST NOT take place. To enable integration of a TI-Messenger client into existing system environments (primary systems or alternative messenger clients), client-side bidirectional exchange with third-party systems is allowed.

3.5 Authorisation concept

As described in Section 3.4 – TI-Messenger federation, the TI-Messenger federation serves to exclude non-approved Matrix home servers from the TI-Messenger service. It MUST also be possible that only the actors mentioned in Section 3.1 – Actors and roles may communicate with each other. For this purpose, the establishment of a rights concept within the TI-Messenger service is necessary.

The rights concept is based on a multi-stage test. The authorisation concept is used to prove whether an actor is entitled to interact with another actor within the TI-Messenger federation. The type of check depends on whether it is a client-server or server-server communication. The authorisation concept is described in more detail below.

3.5.1 Client-server communication

3.5.1.1 Authorisation concept – Stage 1

In this stage, it MUST be checked in the client-server communication whether the Matrix domains included in the request belong to the TI federation. Here, the messenger proxy MUST check at each `invite` event whether the Matrix domains of the invitees contained in the request from the TI-Messenger client are included in the federation list. If this is the case, the request MUST be forwarded by the messenger proxy to the Matrix home server. If this is not the case, the intended request of the actor MUST be rejected by the inviter's messenger proxy. After forwarding to the Matrix home server of the inviter, it checks whether the invited actor belongs to the same organisation. If the Matrix home server determines in the course of the above check that the invited actor does not belong to its domain, the `invite` event is directed to the messenger proxy of the Matrix home server of the actor to be invited, whereby the rules of server-server communication are to be carried out.

3.5.2 Server-server communication

3.5.2.1 Authorisation concept – Stage 1

In the 1st server-server communication stage, the messenger proxy MUST perform a check for all events to determine whether the Matrix domains contained in the event belong to the TI federation. To check the federation affiliation, the messenger proxy MUST check the domain contained in the "`origin`" attribute (for incoming communication) and the domain contained in the "`destination`" attribute (for outgoing communication) against the domains in the federation list in the Authorisation header. If the test is successful, further processing is carried out according to Stage 2.

3.5.2.2 Authorisation concept – Stage 2

In this stage, the messenger proxy of the invitee checks for a given release. This is a lookup table in which all allowed actors are stored, from which an invitation to a chat room is accepted. If an entry is available from the inviting actor, then the intended invitation of the actor MUST be allowed. If this is not the case, further verification MUST be carried out according to the third stage.

3.5.2.3 Authorisation concept – Stage 3

In the last stage, the check is carried out on the basis of the entries of the involved actors in the VZD-FHIR directory. The invitation MUST be allowed if:

- the MXID of the actor to be invited is stored in the organisation directory and its visibility in this directory is not restricted, or
- the inviting and invited actors are stored in the person directory and the invited actor has not restricted their visibility in this directory

If the check is unsuccessful, the intended invitation of the actor MUST then be rejected by the messenger proxy.

3.6 Using tokens

For the use of the TI-Messenger service, different types of tokens are used for authentication and authorisation on other services that are used in different use cases. For this reason, the following table describes the different tokens in more detail.

Table 3: Token types

Token	issued by	Description
ID_TOKEN	Central IDP service	This token is issued by the central IDP service on the basis of SmartCard identities and contains the associated identity data (`TelematicsID`, `ProfessionOID`, etc.). The registration service uses this token to check the contained `ProfessionOID` for a valid institution type for an SMC-B and to enter the contained `TelematicsID` into the federation list within the scope of a messenger service order. The VZD-FHIR directory uses this token to determine for which resource (identified by the `TelematicsID`) an owner-accesstoken is issued.
Matrix ACCESS_TOKEN	Matrix home server	After successfully logging in to the Matrix home server, an access token is issued by the Matrix home server. In the context of the TI-Messenger service, the access token issued by the Matrix home server is referred to as the Matrix ACCESS_TOKEN. This token MUST be securely stored in the local storage of the TI-Messenger client. This token will be used every time you interact with the issuing Matrix home server to authorise the TI-Messenger client to use specific services of the server. It is linked to the session of the respective TI-Messenger client.

Token	issued by	Description
Matrix OpenID token	Matrix home server	The Matrix OpenID token is a third-party token issued by a Matrix home server according to [Client-Server API#OpenID] if required for an actor. In the context of the TI-Messenger service, the third-party token is called the Matrix OpenID token. The Matrix OpenID token is required to verify a messenger service and search FHIR resources in the VZD-FHIR directory. For this purpose, the Matrix OpenID token in the Auth service of the directory service will be replaced against the search access token required on the FHIR proxy for further processing. The originally issued Matrix OpenID token will no longer be needed. To verify the validity of the Matrix OpenID token, the Auth service calls the Userinfo endpoint on the respective Matrix home server.
RegService OpenID token	Registration service	The RegService OpenID token is a JSON web token issued by a registration service on demand for an actor in the role "Org Admin". The RegService OpenID token is required for processing FHIR resources in the VZD-FHIR directory. For this purpose, the RegService OpenID token in the Auth service of the directory service will be replaced against the owner-accesstoken required on the FHIR proxy for further processing.
ti-provider-accesstoken / provider-accesstoken	OAuth / Auth service of the VZD-FHIR directory	The provider-accesstoken is provided to the registration service by the OAuth service and the provider-accesstoken by the Auth service of the VZD-FHIR directory. A provider-accesstoken is required, for example, if the registration service of a TI-Messenger specialist service, after providing a new messenger service for an organisation, creates a new federation list entry for this organisation or the registration service wants to query a federation list from the FHIR proxy. For this purpose, in the first step, the registration service transfers agreed client credentials to the OAuth service of the VZD-FHIR directory and receives the provider-accesstoken after successful verification of these credentials. The ti-provider-accesstoken is then passed to the Auth service of the VZD-FHIR directory and upon successful verification by the VZD-FHIR directory, a provider-accesstoken is issued.

Token	issued by	Description
search-accesstoken	Auth service of the VZD-FHIR directory	The search-accesstoken is provided to a legitimate actor by the Auth service of the VZD-FHIR directory. This is required to search in the VZD-FHIR directory and ensures that only authorised actors can trigger a search in the VZD-FHIR directory. For this purpose, the Matrix OpenID token issued by the Matrix home server is transferred to the Auth service of the VZD-FHIR directory. In this case, this serves as proof that an actor is registered with a messenger service belonging to the TI federation. Only then will the authentication service of the VZD-FHIR directory provide a search-accesstoken. In the following search, it must be included in the VZD-FHIR directory call. The check is performed by the FHIR proxy.
owner-access token	Auth service of the VZD-FHIR directory	The owner-accesstoken is provided to a legitimate actor by the Auth service of the VZD-FHIR directory. This is required by an actor in the "User-HBA" role to manage their FHIR resource in the person directory and by an actor in the "Org-Admin" role to add the organisational resources in the VZD-FHIR directory. It serves as evidence that the intended changes may be carried out by an actor. For authentication, the respective actor MUST use the central IDP service. The ID_TOKEN issued by the IDP is checked by the authentication service of the VZD-FHIR directory. If successful, the owner-accesstoken is issued by the Auth service.

4 System breakdown

As shown in Section 2 – System overview, several components are involved in the implementation of the TI-Messenger service functionalities, which are provided by different providers. In the following, the respective involved TI-Messenger service components are further described.

The following figure shows all components involved in the TI-Messenger architecture with their interfaces.

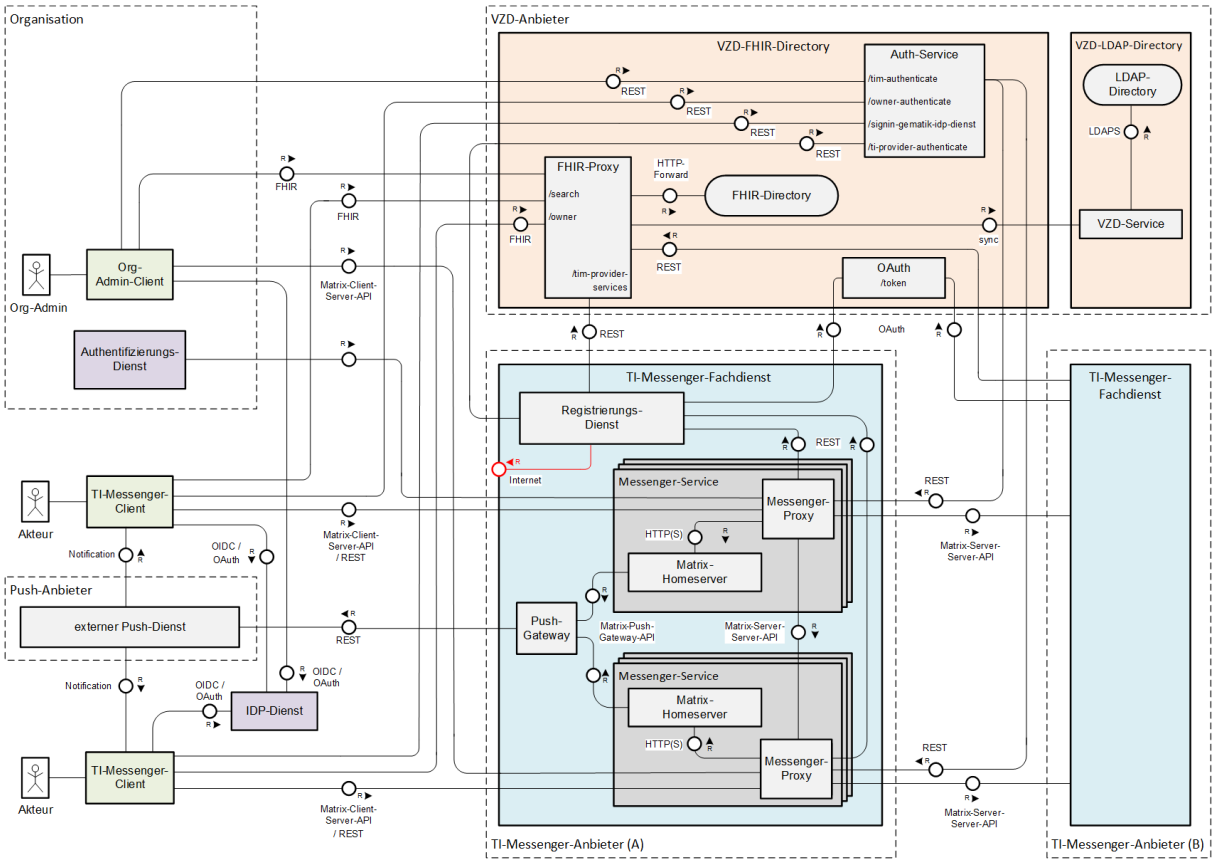

Figure 3: TI-Messenger architecture components and their interfaces

The interface on the registration service shown in red in the figure is not specified by gematik. It offers an actor in the "Org-Admin" role the possibility to administer messenger services for their organisation. With this interface, it is left to the TI-Messenger specialist service manufacturer to implement it in a suitable form. gematik only specifies basic functions to be provided.

Note: Further information on the interaction of the components can be found in Section 6 – Use cases.

4.1 IDP service

An IDP service issues JSON WebTokens (JWT) for attested identities. It is responsible for identifying the actors for the specialist service. This means that specialist services MUST not implement the verification of the actors themselves, but MAY assume that the owner of the "ID_TOKEN" presented to them has already been identified and authenticated. Application front ends can be accessed through the authentication of the actor at the IDP service (on presentation of the issued ID_TOKEN) to the data offered by the specialist services.

In the first expansion stage of the TI-Messenger service, the central IDP service specified by gematik must be used. Other possible formulations are "competent IDP", "competent IDP service" or "an IDP service". This makes it possible to safely identify the actors using the identification tools provided to them (SMC-B/HBA). The identification of the actor is ensured using a smart card and the evaluation of the authentication certificate (from the smart card) passed by the Authenticator module to the IDP service. The authenticator is operated on decentralised hardware in Windows system environments together with the primary system. The Authenticator module for the central IDP service is provided by gematik [gematik Authenticator]. Manufacturers MAY develop their own authenticator solutions.

If other approved IDP services become available in the future, these MAY also be used for the authentication of actors. In the following, the term IDP service is used, which means the central IDP service in the first expansion stage.

4.2 VZD-FHIR directory

The VZD-FHIR directory is a central directory of TI that enables the Germany-wide search of organisations and actors of the TI-Messenger service. The VZD-FIR directory is based on the FHIR standard for exchanging defined information objects (FHIR resources).

The directory service offers two directory types that can be searched. The organisation directory (*Healthcare Service*) and the person directory (*PractitionerRole*) are used to search for organisational entries. In the organisation directory, all resources related to an organisation that are maintained by an actor in the "Org Admin" role of the organisation are stored. The personal directory provides actors in the "User-HBA" role with the option to configure all FHIR entries belonging to their *PractitionerRole*. To search for FHIR entries, FHIR interfaces are accessed through the TI-Messenger clients on the VZD-FHIR directory. When using the interfaces, the TI-Messenger client MUST authenticate itself against the VZD-FHIR directory. For authentication, access tokens (search-accesstoken and owner-accesstoken) described in Section 73.6 – Using tokens are used. The following table shows the two directory types depending on the respective identity and the resulting permissions.

Table 4: Directory types – rights concept

Directory type	FHIR resource	Identity	Role	Permissions
	HealthcareService	SMC-B	Org Admin	Read and write access

Directory type	FHIR resource	Identity	Role	Permissions
Organisation directory		-	User	Read access
		-	User-HBA	Read access
Person directory	PractitionerRole	HBA	User-HBA	Read and write access
		-	User	Read access

In addition to providing directory types, the VZD-FHIR directory also enables cross-sectoral communication. For this purpose, the Matrix domain of a messenger service is included in the TI federation through an entry in the VZD-FHIR directory by the registration service. To register the Matrix domain, the registry service calls a REST interface on the VZD-FHIR directory, secured by OAuth2 Client Credentials Flow. This allows TI-Messenger providers to include and manage their operated messenger services in the TI-Messenger federation.

In general, the VZD-FHIR directory consists of several subcomponents (FHIR proxy, Auth service, Oauth service and FHIR directory) needed to map all functional features. The subcomponents are described below. Further information about the VZD-FHIR directory can be found in [api-vzd].

4.2.1 FHIR proxy

The FHIR proxy is a subcomponent of the VZD-FHIR directory. All queries to the FHIR directory are processed via the FHIR proxy. The FHIR proxy provides the following three interfaces, which are called by the TI-Messenger clients as well as the registration service:

- `/search` (FHIR interface to the search)
- `/owner` (FHIR interface to maintain own entries)
- `/tim-provider-services` (REST interface for maintaining own TIM provider entries)

When calling the interfaces, a corresponding access-token MUST be handed over. If authentication is successful, the FHIR proxy will forward the requests to the FHIR directory.

4.2.2 Auth service

The Auth service subcomponent issues TI-Messenger clients and the registration service of a TI-Messenger specialist service with the access-tokens required to call the FHIR interfaces on the FHIR proxy. The following REST interfaces:

- `/tim-authenticate`,
- `/owner-authenticate`,
- `/signin-gematik-idp-service` and
- `/ti-provider-authenticate`

are used here. The `/tim-authenticate` interface expects a matrix OpenID token, whereas the `/owner-authenticate` interface requires the RegService OpenID token issued by a registration service. Alternatively, authentication by means of a smartcard can be carried out at the central IDP service of gematik and the authorisation code received can be transferred to the `/signin-gematik-idp-service` interface. The `/ti-provider-authenticate` interface expects a ti-provider-accesstoken, which was previously issued by the OAuth service of the VZD-FHIR directory.

4.2.3 OAuth

The OAuth subcomponent issues a temporary ti-provider-accesstoken for the OAuth2 Client Credentials Flow to the Registration Service via the `/token` endpoint. Before the registration service can call the `/token` endpoint on the OAuth service, the TI-Messenger provider MUST first request client credentials from the VZD provider, which MUST be transferred when calling the endpoint.

4.2.4 FHIR directory

The FHIR directory subcomponent provides the central directory of FHIR resources.

4.3 TI-Messenger specialist service

The TI-Messenger specialist service is the central component of the TI-Messenger service for ad-hoc communication between several actors. The specialist service provides all the necessary interfaces for communication with the TI-Messenger clients. For interdisciplinary communication, all messages are sent to the TI-Messenger specialist services listed in the TI federation. It MUST be ensured that the organisation can identify actors at any time and that organisations can exclude actors from the TI-Messenger service at any time. Therefore, control over the identities must lie with the organisation. A delegation, e.g., to a service provider, is permitted. Any TI-Messenger specialist service provider MUST operate a registration service, push gateway and one or more messenger services. The individual components are described below.

Note: The components are to be understood as logical services, which ultimately MUST implement the functions described in the specification. The actual implementation or separation of these services may be variable by the product manufacturers as long as all requirements for functionality, security and interoperability are always met and complied with.

4.3.1 Registration service

The registration service is a component that MUST be implemented by the manufacturer of the TI-Messenger specialist service. Through this, the Matrix domains of the TI-Messenger specialist services participating in the federation of TI-Messenger must be entered in the VZD-FHIR directory. The Matrix domain SHOULD be entered automatically. Likewise, the accounting MAY be performed via the registration service. This is not normatively defined by gematik.

To ensure a user-friendly onboarding process, the registration service MUST enable the provision of a messenger service via a front end (hereinafter also referred to as the front end of the registration service). For this, the organisation MUST authenticate itself to the

registration service. Authentication MAY be done either via OpenID Connect or via an existing KIM address of the organisation. When authenticating via OpenID Connect, an ID_TOKEN issued by the central IDP service is validated at the registration service. When authenticating using the organisation's existing KIM address, the registration service sends a KIM message to the organisation and verifies the organisation by confirming a URL contained in the KIM message. After successfully authenticating an organisation, an administration account is created in the registration service for an actor in the "Org Admin" role. This allows an actor in the "Org Admin" role to register one or more messenger services for their organisation. To do so, the front end of the registration service MUST be registered for the central IDP service. Before creating a new messenger service, the registration service MUST check if the requested domain name is available and add it to the TI-Messenger federation.

In addition to registering new messenger services, the registration service serves as the middleware between TI-Messenger services and the VZD-FHIR directory and stores an up-to-date list of all verified domains (federation list) so that they can be retrieved by the messenger proxies of the TI-Messenger specialist service (see Section 3.5 – Authorisation concept – Stage 1). Another feature of the registration service is checking for entries in the VZD-FHIR directory. This also serves the messenger proxy for checking permissions when contacting other actors (see Section 3.5 – Authorisation concept – Stage 3). In addition, the registration service issues ID_TOKENs (RegService OpenID tokens), which are used for the authorisation to change organisational entries in the VZD-FHIR directory.

4.3.2 Push gateway

Each provider of a TI-Messenger specialist service MUST provide a push gateway to signal the receipt of new messages to its registered actors. The push gateway must be implemented according to the Matrix foundation specification [Push Gateway API]. This forwards the notification to push services on the internet.

4.3.3 Messenger service

A messenger service consists of a messenger proxy and a Matrix home server implemented according to the Matrix foundation specification. Messenger services only differ by the authentication methods supported in each case. It is necessary that messenger services can be scaled up with increasing load scales. A healthcare organisation is logically assigned to a messenger service. More information on securing the messenger service components can be found in the specification of the TI-Messenger specialist service [gemSpec_TI-Messenger-FD]. The components are described below.

4.3.3.1 Messenger proxy

The messenger proxy as an inspection instance of all incoming and outgoing requests to the messenger service is responsible for regulating calls according to the Matrix Client Server API and Matrix Server API. The check rules to be implemented in each case differ and are described in more detail below. The following figure shows the checks to be performed depending on the intended communication.

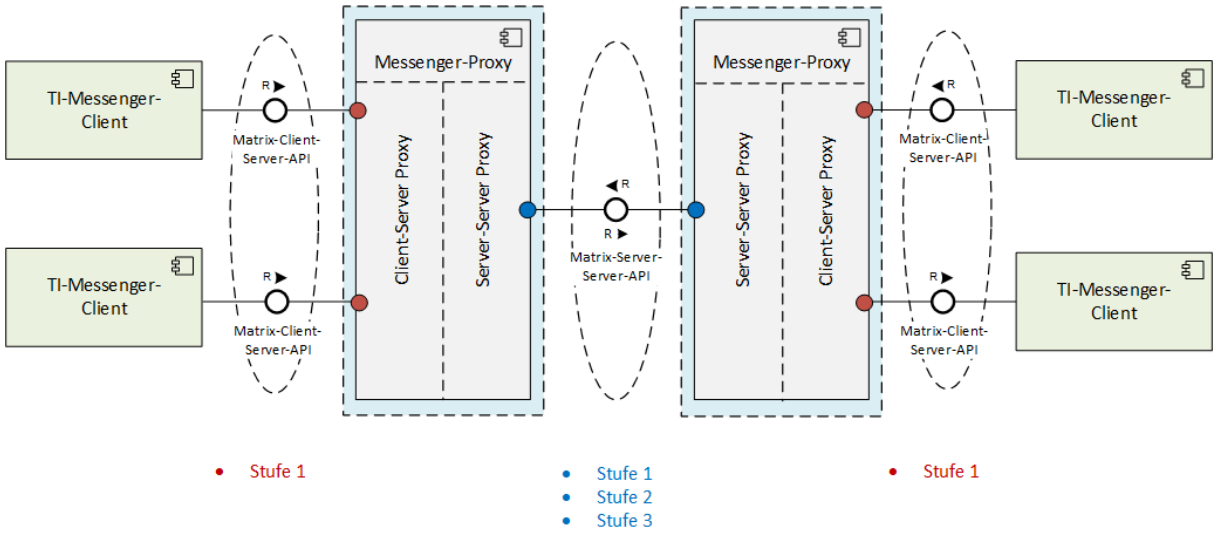

Figure 4: Representation of authorisation check in messenger proxy

4.3.3.1.1 Client-server proxy

In its function as a client-server proxy, the messenger proxy checks incoming `Invite` and `createRoom` events of the TI-Messenger clients (shown in red in the illustration) and thus functions as a reverse proxy (see the illustration shown in Section 2 – System overview for an overview or Section 4 – System breakdown for a detailed view). For each `Invite` event, the messenger proxy MUST check whether the Matrix domains contained in the request belong to the TI federation (see Section 3.5.1 – Client-server communication – Stage 1 as well as Section 8.3 – Stages of the authorisation check). After successful verification, the event is forwarded to the Matrix home server of the inviter. The Matrix home server checks whether the involved actors are registered on the same Matrix home server. If this is not the case, the `invite` event is sent to the responsible messenger proxy of the person to be invited, whereby the rules of the server-server communication are to be carried out.

The messenger proxy MUST also check each `createRoom` event. Here, the messenger proxy MUST check whether the "`invite`" attribute contained in the event is filled with a maximum of one element. If this is not the case, then the messenger proxy MUST reject the connection with an error message.

4.3.3.1.2 Server-server proxy

In its function as a server-server proxy, the messenger proxy checks all outgoing and incoming events. Thus, the server-server proxy acts as both a forward and a reverse proxy. In contrast to the client-server proxy, the server-server proxy checks the domain affiliation for each event. This rules out the possibility of communicating with a messenger service that no longer belongs to the federation. In the function as a server-server proxy, all stages MUST be checked by the messenger proxy according to Section 3.5.2 – Server-server communication of the authorisation concept (shown in blue in the illustration). If none of the three stages have been successfully checked, the messenger proxy MUST reject the connection. In addition, the server-server proxy MUST also allow other legitimate requests that go beyond the authorisation concept. For example, requests from the VZD-FHIR directory to a Matrix home server so that it can verify a Matrix OpenID token to be checked.

4.3.3.1.3 Further specifications

The messenger proxy MUST provide a release list. This is used to check authorisations when contacting other actors (see Section 3.5 – Authorisation concept – Stage 2). The messenger proxy MUST also provide an interface with which TI-Messenger clients can store permissions in the release list.

The messenger proxy MUST check the signature of the received file after receiving a new federation list from the registration service and use it only after successful verification.

The messenger proxy component MUST be provided separately for each messenger service. It is not mandatory to implement these checks related to the Matrix-Server-Server API and Matrix-Client-Server API by separate components. The type of implementation is left to the TI-Messenger specialist service manufacturer.

When using the messenger service for an organisation, the messenger proxy also serves as an interface for connecting the organisation's authentication service to the target Matrix home server.

4.3.3.2 Matrix home server

For the operation of the TI-Messenger service, the TI-Messenger provider MUST operate at least one Matrix home server according to the Matrix Foundation specification in the intersectoral TI federation. All Matrix home servers used in the federation MUST meet the requirements of the Matrix Foundation specification. Ad-hoc communication between the actors and other user interactions (e.g. start of new rooms, etc.) takes place via the Matrix home server.

4.4 TI-Messenger Client specification

A TI-Messenger client is a mobile or stationary application. This is based on the specification defined by the Matrix Foundation and allows ad-hoc communication of actors via the TI-Messenger service. In the context of the TI-Messenger service, a distinction is made between two forms of the TI-Messenger client. These result from the respective roles of the actors, which are further described below.

For the realisation of use cases that are exclusively executed by an administrator of the organisation (see Section 6 – Use cases, use cases assigned to the "Org Admin" actor), a TI-Messenger provider MUST offer a TI-Messenger client with administration functions (also referred to as Org Admin client). This extended functionality MAY also be integrated into the TI-Messenger client for actors. TI-Messenger clients for actors (actors in the user/user-HBA role) support the functionalities defined by the Matrix specification as well as the queries in the VZD-FHIR directory. The required minimum functional scope to be provided is described in [gemSpec_TI-Messenger client].

5 General specifications

5.1 Data protection and security

The TI-Messenger service builds on universal use of transport encryption by means of TLS (according to the [gemSpec_Krypt] specifications), additional modern end-to-end encryption of chat content by means of OLM/MEGOLM and a decentralised call architecture by means of federated Matrix home servers.

The requirements for securing the TI-Messenger consist of component-related requirements, which are housed in the respective documents in separate sections, function-related requirements, which can be found within the framework of the respective functional descriptions and complementary cross-requirements, which come from other specifications and are assigned to the profiles.

5.2 Standards used

5.2.1 Matrix

For the TI-Messenger service, the open communication protocol of the Matrix Foundation is used. As part of the specification, the server-server (according to [Server API]) and the client-server protocol (according to [Client Server API]) are reused. For the communication of the Matrix home servers in the federation, the API according to [Server-Server API] is used. The TI-Messenger client implements the API of the Matrix-Client-Server protocol when communicating with the Matrix home servers. For notifying actors about incoming messages, a push gateway is used, which is re-used according to [Push Gateway API]. In the communication, REST web services are called via HTTPS (JSON objects).

The Matrix protocol allows you to define a custom room type for a chat room during its creation using a type initialisation in the `/createRoom` endpoint in order to use special room properties *(room state*) for this *custom room type*. In addition, the Matrix protocol allows the properties of a chat room to be extended or changed with *state events*. Typical *state events* that define a *room state* and that are defined by the Matrix protocol are, for example, `m.room.name` or `m.room.topic`. The Matrix protocol also allows the use of *custom state events*. The present specification already defines the first *custom room types* and *custom state events* with *event types* and *event content* defined by gematik. In the context of the TI-Messenger, this allows for more specific and thus more structured and directed communication than would be possible with standard Matrix chat rooms. Specifically, definitions are introduced for the case reference (referencing treatment cases in the medical care context) of chats as well as for internal and intersectoral communication. For case-related as well as federated and intersectoral communication, it is intended to store defined FHIR objects as payload in the *event content* of a *custom state event*.

Note: In the present specification, the productive use of custom room types and custom state events is not currently required, as the necessary preconditions for productive use on the part of the Matrix protocol have not yet been completely fulfilled.

5.2.2 OpenID-Connect

The VZD-FHIR directory, registration service and TI-Messenger clients use an ID_TOKEN as authentication in the form of a JSON web token (JWT) according to [OpenID].

5.2.3 FHIR

The TI-Messenger clients use the FHIR interfaces of the FHIR proxy subcomponent of the VZD-FHIR directory in accordance with the FHIR [FHIR] standard using a RESTful API.

5.3 Authentication and Authorisation

5.3.1 Authentication of actors on the messenger service

Authentication procedures provided by the respective Matrix home server are used for the authentication of actors. This allows, for example, hospitals to use their own user administration (e.g. Active Directory) or associations to use their own identity servers (IDP service). The organisation coordinates which authentication method is used with the respective TI-Messenger provider. User management is carried out by authorised employees in the respective organisation (actors in the "Org Admin" role). The administration of the authentication methods used MUST be under the control of the respective organisation.

5.3.2 VZD-FHIR directory authentication

Authentication for read and write access to the FHIR directory is performed using identity tokens. The respective verification of the identity tokens takes place at the FHIR proxy of the VZD-FHIR directory. The authentication of the components registration service and TI-Messenger client is further described below**.**

5.3.2.1 Registration service

Authentication of the registration service for the use of the `I_VZD_TIM_Provider_Services` interface on the VZD-FHIR directory is performed using OAuth on the OAuth/Auth service on the VZD-FHIR directory. After successful authentication with agreed client credentials, a provider-accesstoken is issued to the registration service.

The TI-Messenger provider obtains the client credentials by using a service of the TI-ITSM system to request the credentials. Requesting the credentials also serves to establish a trust relationship between the registration service and the VZD-FHIR directory, as the registration service issues RegService OpenID tokens that are used for authorisation to modify organisational entries in the FHIR directory. Trust between the VZD-FHIR directory and the TI-Messenger provider registration services is established by the TI-Messenger provider handing over the signature certificate used to sign the RegService OpenID token when requesting the client credentials and can thus be taken into account by the VZD-FHIR directory during token verification. The TI-Messenger provider receives the signature certificate by means of a TI-ITSM service request for TI component PKI certificates (`C.FD.Sig` with application identifier `oid_tim`). A RegService OpenID token with the organisation's `TelematicsID` is issued after an actor in the organisation's "Org Admin" role has successfully logged in.

5.3.2.2 TI-Messenger Client specification

TI-Messenger clients MUST authenticate themselves against the authentication service of the VZD-FHIR directory using an ID_TOKEN or the Matrix OpenID token. The Matrix OpenID token of the Matrix home server is trusted if the issuing Matrix home server has been entered as the Matrix domain of a verified organisation resource in the VZD-FHIR directory. The Auth service of the VZD-FHIR directory issues a search-accesstoken after successful verification of the respective Matrix-OpenID token. The ID_TOKEN is trusted if the issuing IDP service is registered with the VZD-FHIR directory and the token can be thus validated by the Auth service. After successful verification of the ID_TOKEN by the Auth service of the VZD-FHIR directory, an owner-accesstoken is issued.

5.3.3 Authorisation on the messenger service

When a Matrix ACCESS_TOKEN is handed over, TI-Messenger clients gain access to the messenger service of an organisation registered in the federation. This is issued by the Matrix home server after an actor has been successfully authenticated. The Matrix ACCESS_TOKEN MUST be securely stored on the end device.

5.3.4 VZD FHIR directory authorisation

5.3.4.1 Registration service

For write access of the registration service, the registration service authorises itself to the FHIR proxy of the VZD FHIR directory with a provider-accesstoken issued by the Auth service of the VZD FHIR directory.

5.3.4.2 TI-Messenger Client specification

For read access authorisation, TI-Messenger clients will use a search-accesstoken issued by the Auth service of the VZD-FHIR directory against the FHIR proxy of the VZD-FHIR directory. For write access, TI-Messenger clients use the owner access token issued by the Auth service of the VZD FHIR directory.

5.4 VZD-FHIR Directory rights concept

The following section describes how read and write access by the TI-Messenger clients and the registration service on the VZD-FHIR directory takes place.

5.4.1 Read access

5.4.1.1 Registration service

The TI-Messenger specialist services will be able to retrieve the federation list from the FHIR proxy of the VZD-FHIR directory by means of their registration service. For this purpose, the `/tim-provider-services` interface must be opened on the FHIR proxy of the VZD-FHIR directory under presentation of the provider-accesstoken.

5.4.1.2 TI-Messenger clients

By calling the `/search` interface on the FHIR proxy of the VZD-FHIR directory, a TI-Messenger client can place a search query to the FHIR directory under presentation of

the search-accesstoken. The search results depend on the registered FHIR resources and their visibility.

5.4.2 Write access

5.4.2.1 Registration service

The TI-Messenger specialist services will be able to integrate messenger services into the TI federation through their registration service. For this purpose, the `/tim-provider-services` interface must be opened on the FHIR proxy of the VZD-FHIR directory under presentation of the provider-accesstoken.

5.4.2.2 TI-Messenger clients

By calling the `/owner` interface on the FHIR proxy of the VZD-FHIR directory, an actor receives write access to the FHIR directory under presentation of the owner-accesstoken. The following table describes the FHIR resource to be changed depending on the identity of an actor used (also see the "Directory types – rights concept" table).

Table 5: Write access – VZD-FHIR resources

Role	Identity	FHIR resource	Description
Org Admin	SMC-B (represented by a RegService OpenID token)	HealthcareService	An actor in the role "Org Admin" can edit FHIR resources on behalf of the organisation in the organisation directory of the VZD-FHIR directory using a TI-Messenger client with administration function and, after authentication, using a RegService OpenID token, for example, to enter a new endpoint under a *HealthcareService*. The RegService OpenID token is obtained by the actor in the "Org Admin" role after successful login to the registration service by calling the `I_requestToken` interface provided by the provider.
User-HBA	HBA	PractitionerRole	The use of an HBA enables an actor in the "User-HBA" role to extend their existing FHIR resource *PractitionerRole* to include an endpoint in the person directory with the help of a TI-Messenger client in order to become writeable for other service providers or in order to write to other service providers.

5.5 User management

Due to the large number of participants, convenient user management is required within the TI-Messenger service. This section describes the roles required for user management and the user directories used for them.

The prerequisite for using the TI-Messenger service is that an actor can authenticate themselves using an authentication process on the Matrix home server of their organisation and a user account has been created on the Matrix home server. The user account on the Matrix home server is provided by either the actor in the "Org Admin" role of their organisation or registered by the actor themselves on the Matrix home server. When creating the user account, the MXID of the actor is generated and the display name of the actor is defined (see gemSpec_TI-Messenger-Client#Other functions). After creating the user account on the Matrix home server, the MXID of the actor is stored in the user directory of the Matrix home server. All MXIDs stored in the user directory of the Matrix home server can then be found and reached by other players in their organisation. If the actor is to be found from outside the organisation, they MUST be stored in the organisation directory in the VZD-FHIR directory with their MXID. The inclusion of the MXID of an actor in the organisation directory MUST be done by the actor in the "Org Admin" role. The prerequisite is the existence of a healthcare service resource of the organisation. The MXIDs are stored in Endpoint resources assigned to the HealthcareService resource. A healthcare service resource of an organisation is set up by the actor in the "Org Admin" role. If you want to find an actor without belonging to an organisation, your MXID MUST be stored in the personal directory of the VZD-FHIR directory. A prerequisite for this is the possession of an HBA.

The following table provides a summary of user management.

Table 6: User management overview depending on role

Role	Client	Administration	Where
Org Admin	TI-Messenger client with administration functions (Org-Admin client)	• Create user account • Manage user account	Matrix home server (user directory)
		• Create HealthcareService resource • Create endpoint of a HealthcareService resource • Manage HealthcareService resource endpoint	VZD-FHIR directory
User	TI-Messenger client	• Create user account	Matrix home server (user directory)
User-HBA	TI-Messenger client	• Create endpoint of a PractitionerRole resource • Manage PractitionerRole resource endpoint	VZD-FHIR directory (person directory)

5.6 Function accounts

Healthcare facilities have very different structures and want to be able to flexibly map their own structures in terms of accessibility. Therefore, the TI-Messenger service requires accounts that make it possible to reach actors below the structure. The questioning actor does not need to know the exact internal structure of the organisation. These special accounts are referred to as function accounts in the following.
A function account is to be created as an *endpoint* resource (with the"`payloadTyp: TI-Messenger chat`") of a *HealthcareService of* an organisation. The *HealthcareService* forms a structure (e.g. ward in a hospital) of the organisation in the FHIR directory. For the accessibility of this structure, the MXID in URI format of a chatbot or an actor (who represents the organisation) is stored in the "`address`" attribute of the endpoint resource. Thus, the created structure of the organisation can be found by an actor via the function account and its stored name (*Endpoint.name*) in the VZD-FHIR directory.

5.6.1 Chatbot

Chatbots are special actors (see Section 3.1 – Actors and roles) that can be invited for a structure of an organisation by an actor who initiates communication. Chatbots MAY complete the communication in a fully automated manner (e.g. schedule an appointment) or associate individuals in the organisation with the chat (e.g. issue a prescription). Examples of chatbots can be found under [Matrix Bots]. If chatbots appear as communication participants of the TI-Messenger, they MUST be marked as chatbot in the respective chat.

The following is an example of a possible assignment for the mapping of function accounts with the help of chatbots and an actor representing the organisation.
The chatbot MAY automate actor requests (e.g. appointment requests, medication decision) or, if necessary, invite assigned and available actors into the chat room. The actors available to the chatbot (stored in the column Actor Blue) must be defined in the configuration of the chatbot. In the final example, an actor (natural person) is stored as an endpoint and represents the organisation in the chat.

Table 7: Function accounts example

Department	Function account	Endpoint.address	Actor (MXID)	Display name
Cardiology	Laboratory_Cardiology	@MXID_Bot01:<domain>.de	@MXID_01:<domain>.de @MXID_02:<domain>.de	Reception_Cardiology (Chatbot) Dennert, Maltilde Fritsche, Sarah
Neurology	Ambulance_Neurology	@MXID_Bot02:<domain>.de	@MXID_03:<domain>.de	Ambulance_Neurology (Chatbot) Gotsch, Gerd

Department	Function account	Endpoint.address	Actor (MXID)	Display name
Radiology	Reception_Radiology	@MXID_04:<domain>.de	-	Fruechtl, Wilfried

The following shows the interaction of an external actor with a function account.

Process:

1. Precondition:
   - Organisation has a TI-Messenger client with administration function and a messenger service
   - Chatbots are available and can be managed by the actor in the "Org Admin" role

2. Configuration of function accounts:
   - The actor in the "Org Admin" role creates a function account (organisation-related MXID) as an *endpoint* of the desired *HealthcareService* of the organisation and assigns a chatbot to this MXID
   - The actor in the "Org Admin" role assigns responsible actors of the organisation (personal MXIDs) to the chatbot
   - Actors are assigned to individual requests within a function account (e.g. appointment requests, medication decision) through the configuration in the chatbot

Alternative: The actor in the "Org Admin" role creates a function account (organisation-related MXID) as an *endpoint* of the desired *HealthcareService* of the organisation and deposits the MXID of an actor at this endpoint.

3. Example process (see "*Interaction with a chatbot*" figure):
   1. An actor searches for an organisation and/or substructure of this organisation (e.g. the Department of Cardiology in a hospital)
   2. The actor opens a chat room with the function account of the Department of Cardiology
   3.
      a. The cardiology function account chatbot enters the room
      b. The chatbot MAY automate the request from the actor (e.g. appointment request, referral to physician, etc.)
   4. The actor responds to the chatbot
   5. Depending on the request, the chatbot invites the assigned and available actors to the chat room
   6.
      a. Invited actors enter the chat room with their display name
      b. Invited actors communicate with the actor

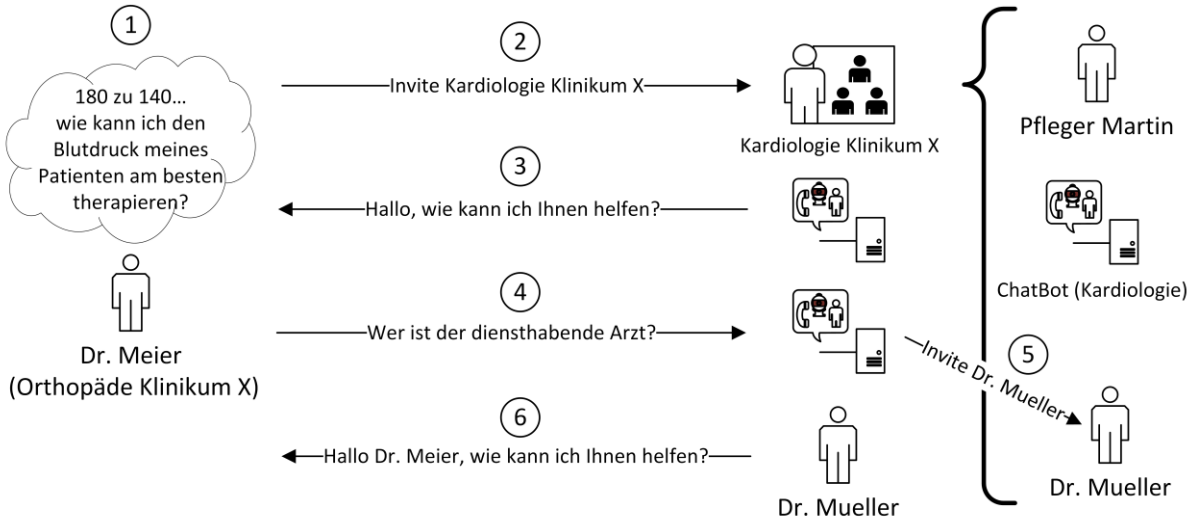

Figure 5: Example of interaction with a chatbot

5.7 Test

The TI-Messenger provider MUST provide and operate a reference instance and at least one test instance of the TI-Messenger specialist service and TI-Messenger client. The reference instance has the same version as the production environment and can be used by other manufacturers for testing and development against the approved version. Furthermore, the reference instance is used to reproduce current errors/problems from the production environment. Access to the reference instance MUST be guaranteed for the system for error analysis.
The test instance serves the manufacturers in the development of new TI-Messenger

clients and TI-Messenger specialist services versions, the IOP tests between the different TI-Messenger providers and is also used by gematik for approval.
The TI-Messenger provider MUST coordinate the different users of the reference instance and the test instance (manage a test / usage plan). If required (development of different versions, high utilisation by other manufacturers or through gematik), the TI-Messenger provider MUST also provide and operate several test instances with the same or different versions.

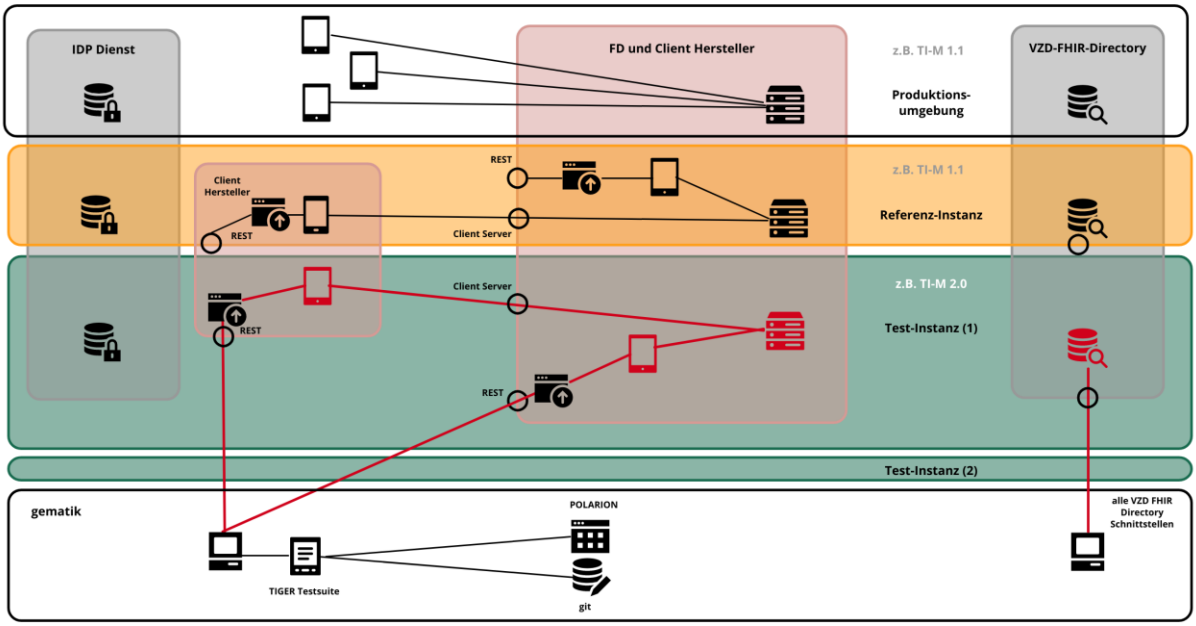

Figure 6: TI-Messenger service instances

Note: In principle, it is possible to carry out a CC certification for the entire product or product components and thus replace other types and categories of tests that check the safety-related suitability as well as product appraisals.

5.8 Operation

The TI-Messenger provider is responsible for the following products during operation:

- TI-Messenger specialist service(s),
- TI-Messenger client(s) for actors and
- TI-Messenger clients with administration functions (Org Admin client) incl. Authenticator (module).

The TI-Messenger provider MUST provide at least one TI-Messenger specialist service, at least one TI-Messenger client for actors and at least one Org Admin client (the clients integrated in each case or in a TI-Messenger client).

A_23658 – Product verification within the scope of controlled commissioning
The product MUST fulfil the functionality, safety and interoperability requirements according to the respective product type profile in the production environment. The evidence for this MUST be provided accordingly and as part of the controlled commissioning concept.
[<=]

Note: The requirement [A_22658] is a supplement for the productive environment and does not replace the upstream test procedures of the products in the reference environment.

The TI-Messenger provider MAY also offer several TI-Messenger clients and several TI-Messenger specialist services. The actual operation can be outsourced according to [gemKPT_Betr#provider constellations].

The TI-Messenger provider MUST offer its users and organisations a helpdesk corresponding to [gemKPT_Betr] that also takes on disruptions to all responsible TI-Messenger clients and TI-Messenger specialist services.

According to the operating concept [gemKPT_Betr], the TI-Messenger provider is a participant in TI-ITSM (IT service management of TI) with all associated rights and obligations.

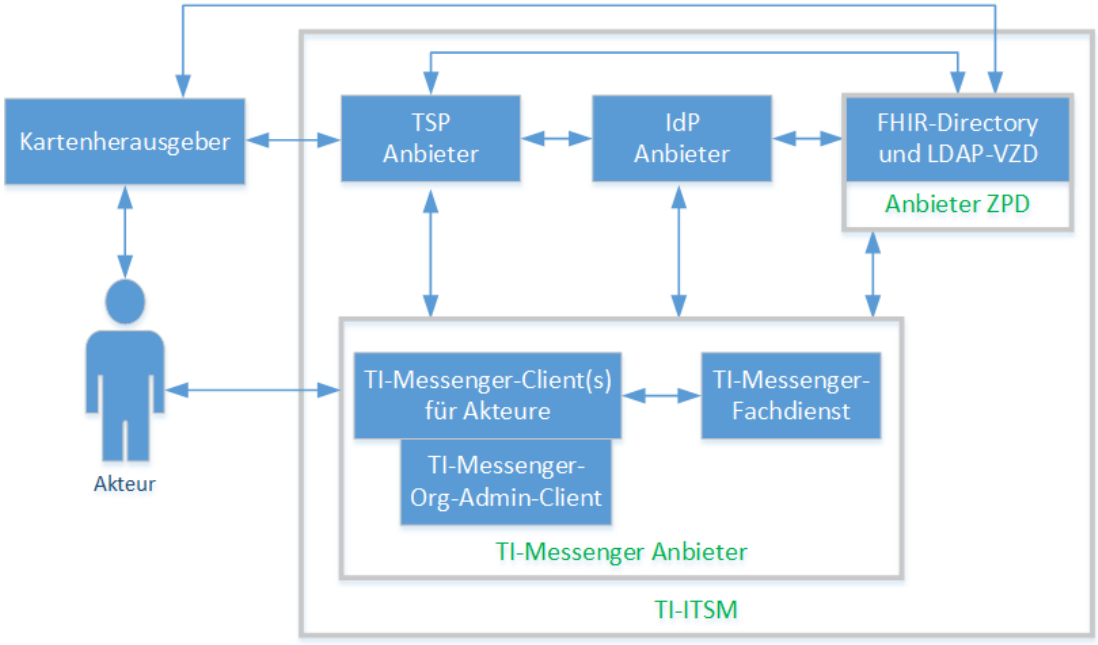

Figure 7: Excerpt – TI-Messenger provider in TI-ITSM

Note: The illustration shows the organisational communication relationships in the foreground of the TI-ITSM system between the respective entities. The products of the TI-Messenger provider can be approved individually, but are offered in a bundle in the interests of the user with a SPOC for the respective components by the respective provider.

6 Use cases

The use cases described below are specific to the TI-Messenger service and therefore differ in part from the Matrix client-server API. The same applies to use cases based on the Matrix server protocol ([server-server API]). This means that all use cases implemented according to the Matrix client-server protocol are not listed here. Instead, the Matrix client-server API is referenced here ([Client-Server API]).

In the context of the TI-Messenger service, actors take on different roles (see Section *3.1 – Actors and roles)*. Depending on the role played by an actor, different use cases are triggered. For the "Org Admin and User/User-HBA" roles, this is shown in the following figures.

Role: Org Admin

An actor in the "Org Admin" role MAY be a service provider / commissioned employee in an organisation or an appointed administrator of the TI-Messenger provider. For their administrative activities, this actor triggers the following use cases using an unlocked SMC-B in the context of the TI-Messenger service.

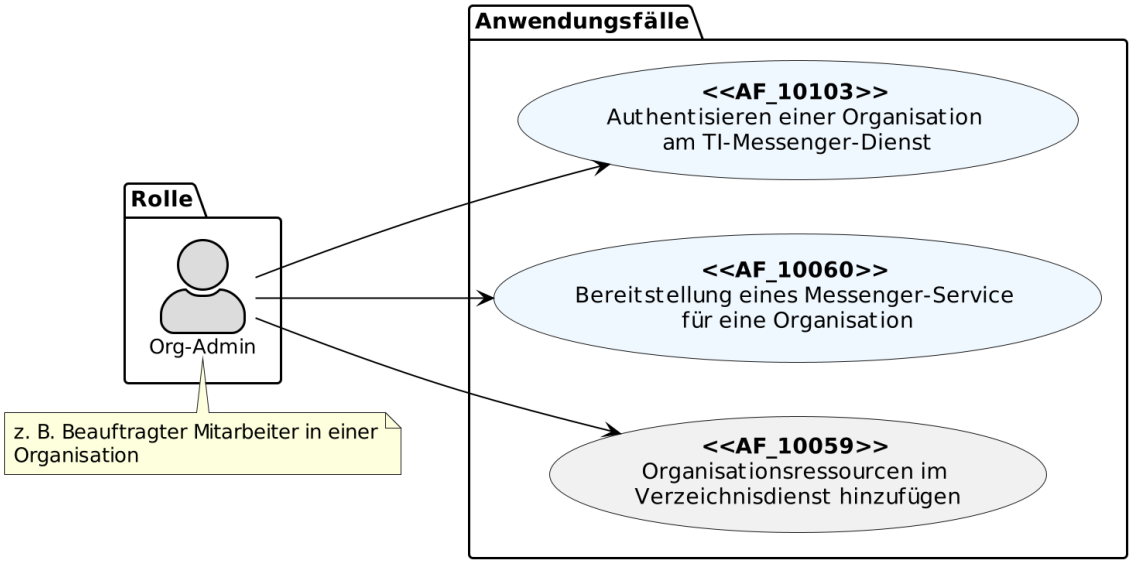

Figure 8: Org Admin – overview of use cases

The use case AF_10060 – Provision of a messenger service for an organisation requires successful authentication of the organisation by the use case AF_10103 – Authentication of an organisation on the TI-Messenger service. If multiple messenger services are required by one organisation (e.g. in the hospital environment), the use case may be executed multiple times. The colour assignment is intended to indicate a functional relationship between the individual use cases.

Another task of the actor in the "Org Admin" role, which is no longer shown here in a use case, is the setting up of function accounts and user management.

Role: User/User-HBA

An actor in the "User/User-HBA" role MAY trigger the following use cases.

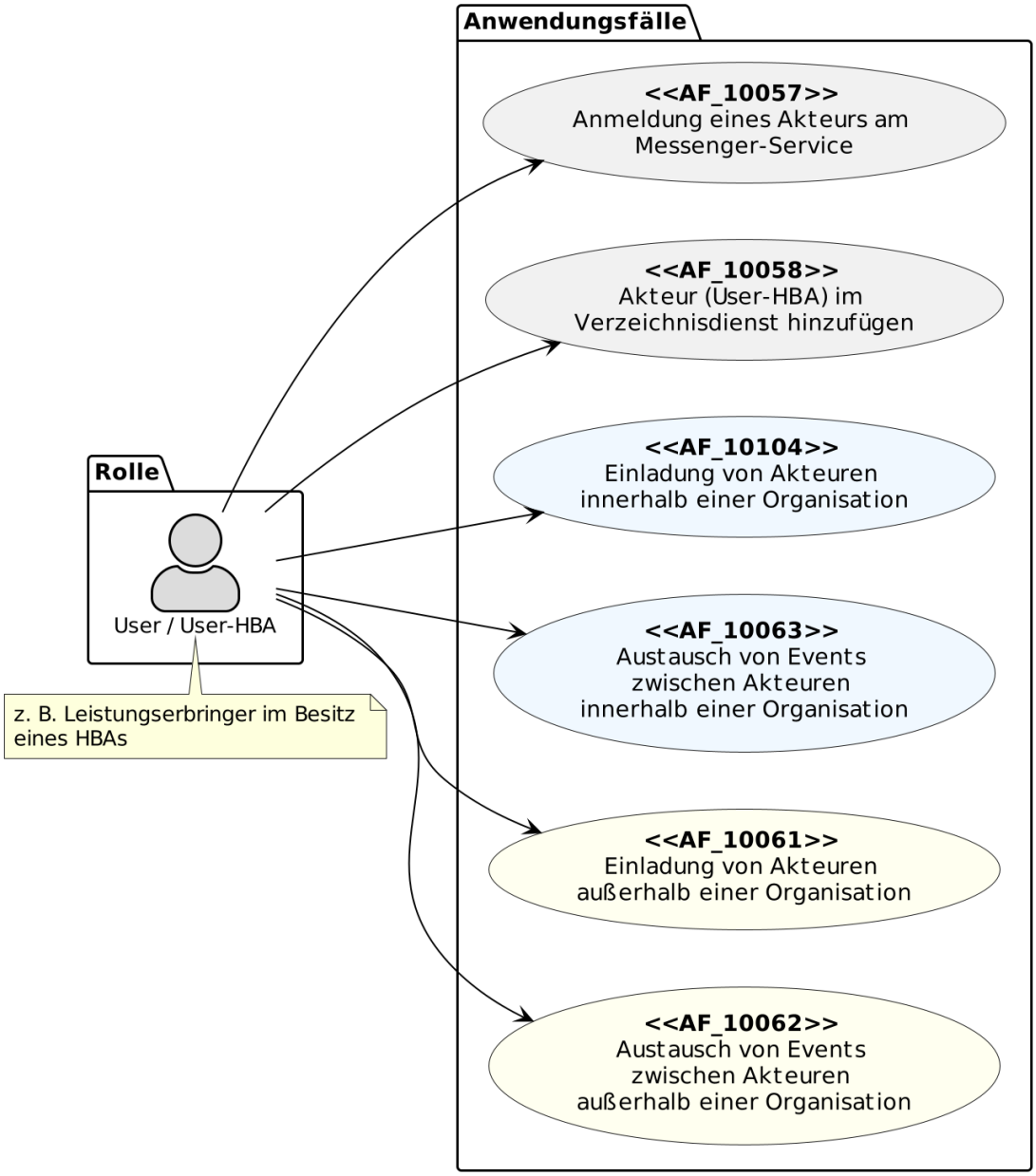

Figure 9: User/User HBA – Overview of use cases

The use case AF_10058 – Add actor (User-HBA) in the directory service MAY only be executed by an actor in the "User-HBA" role. All other shown use cases MAY be executed by the actors in the "User/User-HBA" role. The colour assignment is intended to indicate a functional relationship between the individual use cases.

Note: In the following use cases, reference is made to procedures that can be found in Annex B. For better readability, the runtime views shown in the respective use cases can also be called up as PlantUML source in [api-messenger] sub `src/plantuml` and in diagram form under `/images/diagrams`.

6.1 AF – Authentication of an organisation on the TI-Messenger service

AF_10103-01 – Authentication of an organisation on the TI-Messenger service
With this use case, an actor, in the "Org Admin" role, authenticates their organisation with a TI-Messenger provider. For the authentication of an organisation, the TI-Messenger specialist service provides an interface on its registration service. It is used for authentication via the front end of the registration service. The authentication of the organisation is carried out individually and subject to use by an actor in the "Org Admin" role. Authentication MUST demonstrate possession of a valid SMC-B as only healthcare organisations are eligible to receive a messenger service. One of the following methods MUST be used as proof.

For the verification of the organisation,

- Procedure 1: an unlocked SMC-B MUST be used for authentication at the central IDP service or
- Procedure 2: a KIM message MUST be sent to the address of the organisation with the unlocked SMC-B.

As evidence to check for a valid organisation, the registration service MUST check in both procedures whether the `ProfessionOID` belongs to a healthcare organisation. If the organisation is successfully verified, an administrator account for the organisation is created at the registration service. This allows an administrator to register messenger services and their organisation to participate in the TI-Messenger service.

Table 8: AF – Authentication of an organisation on the TI-Messenger service

AF_10103	**Authentication of an organisation on the TI-Messenger service**
Actor	Representative of an organisation in the "Org Admin" role
Trigger	An organisation of the German healthcare system wants to participate in the TI-Messenger service and needs permission to register a messenger service
Components	• Front end of the registration service, • Authenticator (optional for procedure 2), • Connector, • eHealth card terminal with inserted SMC-B, • Registration service, • Central IDP service (optional for procedure 2) • KIM client module and mail client (optional for procedure 1)

AF_10103	Authentication of an organisation on the TI-Messenger service
Precondition	1. The actor can access the registration service via a front end of the registration service for communication. 2. Verification of the organisation: • Procedure 1: The actor can use the Authenticator as well as the registration service front end used, which is registered with the central IDP service. • Procedure 2: The TI-Messenger provider has an SMC-B Org and a KIM address as well as an eHealth card terminal and a connector with TI access. The actor has an SMC-B and a KIM address as well as an eHealth card terminal and a connector with TI access. 3. The SMC-B inserted in the eHealth card terminal is enabled.
Input data	Identity of the organisation, SMC-B, alternatively KIM address
Result	The organisation has been verified at the registration service of the TI-Messenger specialist service
Output data	Admin account, status
Acceptance criteria	ML-128757, ML-128759, ML-128758, ML-129853, ML-132446

In the runtime view, the interactions between the components used by the use case are shown. For the authentication of an organisation, the central IDP service of TI is used in the runtime view.

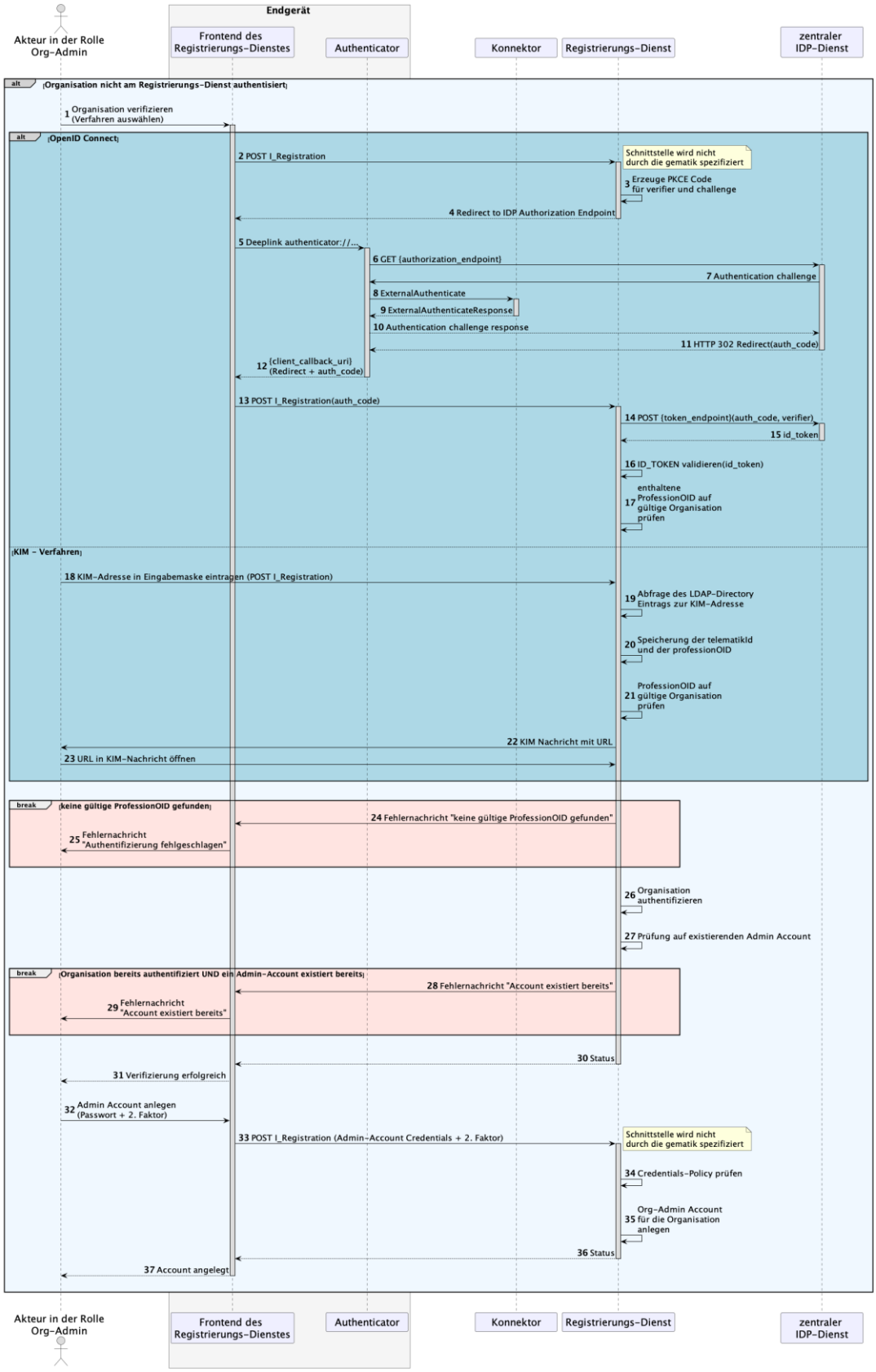

Figure 10: Runtime view – Authentication of an organisation on the TI-Messenger service [<=]

Acceptance criteria for use case: Authentication of an organisation on the TI-Messenger service (AF_1103)

AF_10103 – Verification of the organisation as an actor in the Org Admin role
Only one actor in the "Org Admin" role may authenticate their organisation towards the TI-Messenger specialist service.
[<=]

AF_10103 – Organisation has been successfully verified
The organisation was successfully verified at the TI-Messenger specialist service with an identity of a healthcare organisation
[<=]

AF_10103 – ID tokens were issued and handed over
ID_TOKEN issued by the IDP service is valid and is available to the registration service front end.
[<=]

AF_10103 – Administrator account created
An Administrator Account for the organisation has been successfully created at the registration service.
[<=]

AF_10103 – TI-M Raw data recording and delivery
The raw data was successfully recorded in accordance with the raw data definition according to [gemSpec_TI-Messenger-FD#Operation] for the TI-Messenger specialist service and sent to the defined interface of the raw data recording.**[**=]

6.2 AF – Provision of messenger service to an organisation

AF_10060-01 – Provision of a messenger service to an organisation
This use case provides an organisation previously authenticated to the registration service with a messenger service for that organisation through an actor in the "Org Admin" role. The request to provide a messenger service is made by the actor in the "Org Admin" role on the front end of the registration service. They MUST first log on to the registration service with the organisation's admin account. For timely adaptation of the TI-Messenger service, a fast delivery of messenger services MUST be ensured. TI-Messenger providers are obliged to establish processes so that messenger services can be provided to organisations quickly and, if necessary, automatically. After successful delivery of a Messenger service, it is included in the federation of the TI-Messenger service. If multiple messenger services are required for an organisation, this use case MAY be executed multiple times.

Table 9: AF – Provision of messenger service to an organisation

AF_10060	Provision of messenger service to an organisation
Actor	Representative of an organisation in the "Org Admin" role
Trigger	An organisation of the German healthcare system wants to participate in the TI-Messenger service and needs to provide one or more messenger services

AF_10060	Provision of messenger service to an organisation
Components	• Front end of the registration service, • Registration service, • VZD-FHIR directory, • Messenger service.
Precondition	1. There is a contractual relationship with a TI-Messenger provider. 2. The operator has a front end of the registration service for communication with the registration service. 3. The used front end of the registration service is registered with the central IDP service. 4. The organisation is successfully authenticated with the registration service and an admin account exists. 5. The registration service can authenticate itself with the VZD-FHIR directory server for write access with OAuth2.
Input data	Admin account, identity of organisation (SMC-B)
Result	1. The messenger service for the organisation has been created. 2. The Matrix domain of the new messenger service was entered as an endpoint in the VZD-FHIR directory and included in the federation.
Output data	New messenger service for the organisation, status
Acceptance criteria	ML-123648, ML-123649, ML-123650, ML-132585

In the runtime view, the interactions between the components used by the use case are shown. For the use case, successful authentication of the organisation is required with the help of the use case AF_10103 – Authentication of an organisation on the TI-Messenger service. The messenger service component for the organisation is created later in the course of the use case.

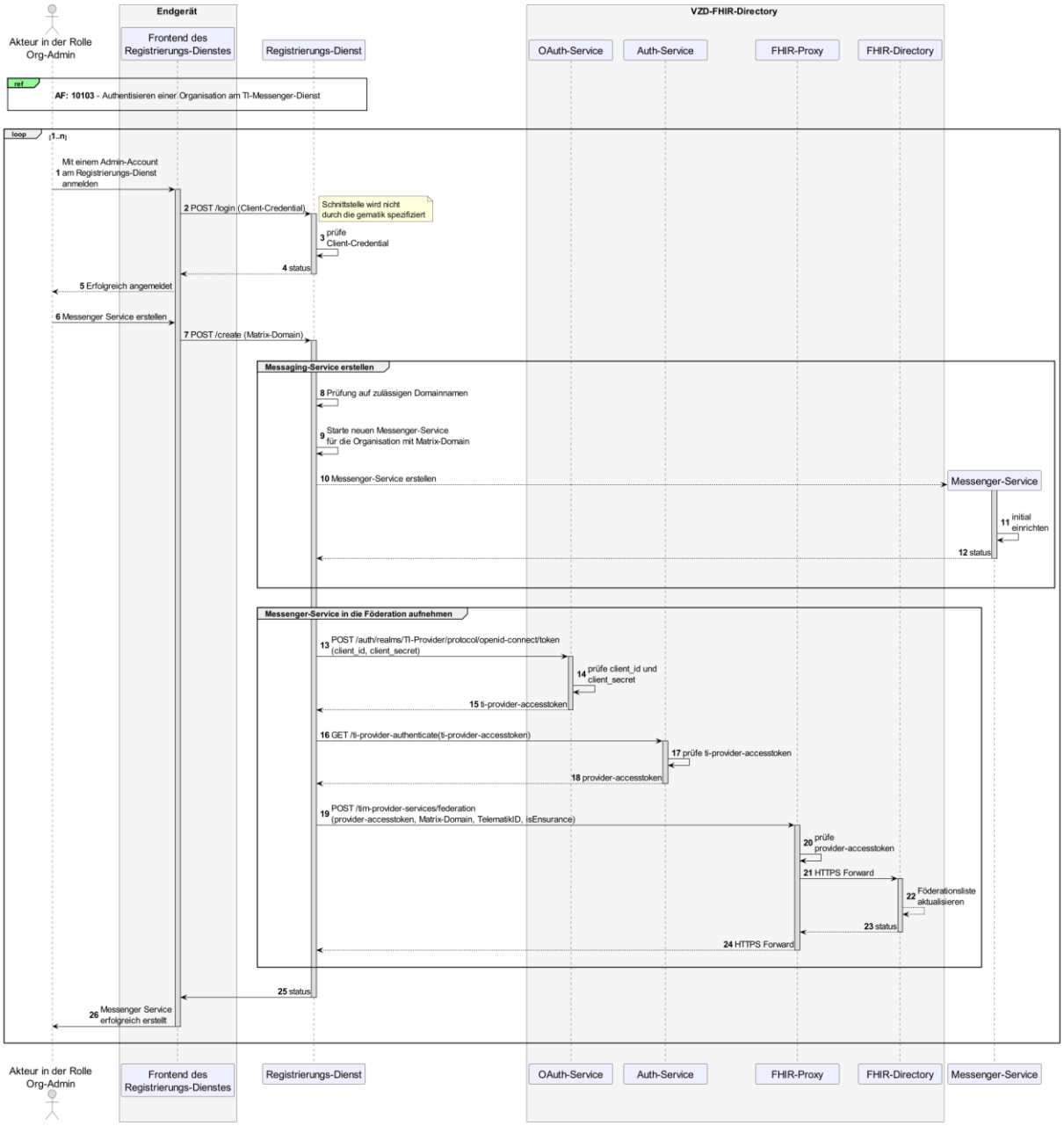

Figure 11: Runtime view – Provision of a messenger service to an organisation

[<=]

Acceptance criteria for use case: Provision of messenger service to an organisation (AF_10060)

AF_10060 – Provide messenger service only as actor in the Org Admin role

Only one actor in the "Org Admin" role can provide a messenger service.
[<=]

AF_10060 – Messenger service created

A new messenger service was created with the selected domain identifier.
[<=]

AF_10060 – Messenger service exists in VZD-FHIR directory
A new entry in the VZD-FHIR directory was created for the generated messenger service
[<=]

AF_10060 – TI-M Raw data recording and delivery
The raw data was successfully recorded in accordance with the raw data definition according to [gemSpec_TI-Messenger-FD#Operation] for the TI-Messenger specialist service and sent to the defined interface of the raw data recording.
[<=]

6.3 AF – Add organisation resources to directory service

AF_10059-01 – Add organisation resources to directory service
With this use case, an actor in the "Org Admin" role makes actors of their organisation discoverable and reachable by other actors in the TI-Messenger service. For this purpose, *endpoint* resources with their respective MXID are stored in the organisation directory (*HealthcareService*) of the VZD-FHIR directory. Organisations MAY administer multiple FHIR resources per organisation and thus structure detailed communication processes in an organisational and thematic way (see [gemSpec_VZD_FHIR_Directory]).

Table 10: AF – Add organisation resources to directory service

AF_10059	Add organisation resources to directory service
Actor	Representative of an organisation in the "Org Admin" role
Trigger	The administrator of the organisation (Org Admin) wants to make their organisation accessible by storing the MXIDs of the actors of the organisation in the VZD-FHIR directory.
Components	• TI-Messenger client (with advanced Org Admin functionality), • TI-Messenger registration service, • Auth service, • FHIR proxy, • FHIR directory.
Preconditions	1. A messenger service was provided to the organisation and there is an organisation entry in the FHIR directory. 2. The organisation administrator has a TI-Messenger client (with advanced Org Admin functionality). 3. A trust relationship exists between the TI-Messenger registration service and the VZD-FHIR directory (transfer of the certificate) 4. The administrator of the organisation has been authenticated by the registration service.

AF_10059	Add organisation resources to directory service
Input data	Org Admin credentials, second factor (*), FHIR organisational resources
Result	FHIR organisation resources updated, status
Output data	Updated VZD-FHIR directory records
Acceptance criteria	ML-123626, ML-132586, ML-138468

(*) Note: With regard to the second factor mentioned in the table under "Input data", the security recommendations of the Federal Office for Information Security (BSI) according to [BSI 2-Factor] MUST be taken into account. Here, for resilience against remote attacks, a procedure shall be chosen that is rated at least "medium".

In the runtime view, the interactions between the components used by the use case are shown. This is a **simplified runtime view** in which, for example, TLS scheduling on the FHIR proxy was not considered for the sake of clarity.

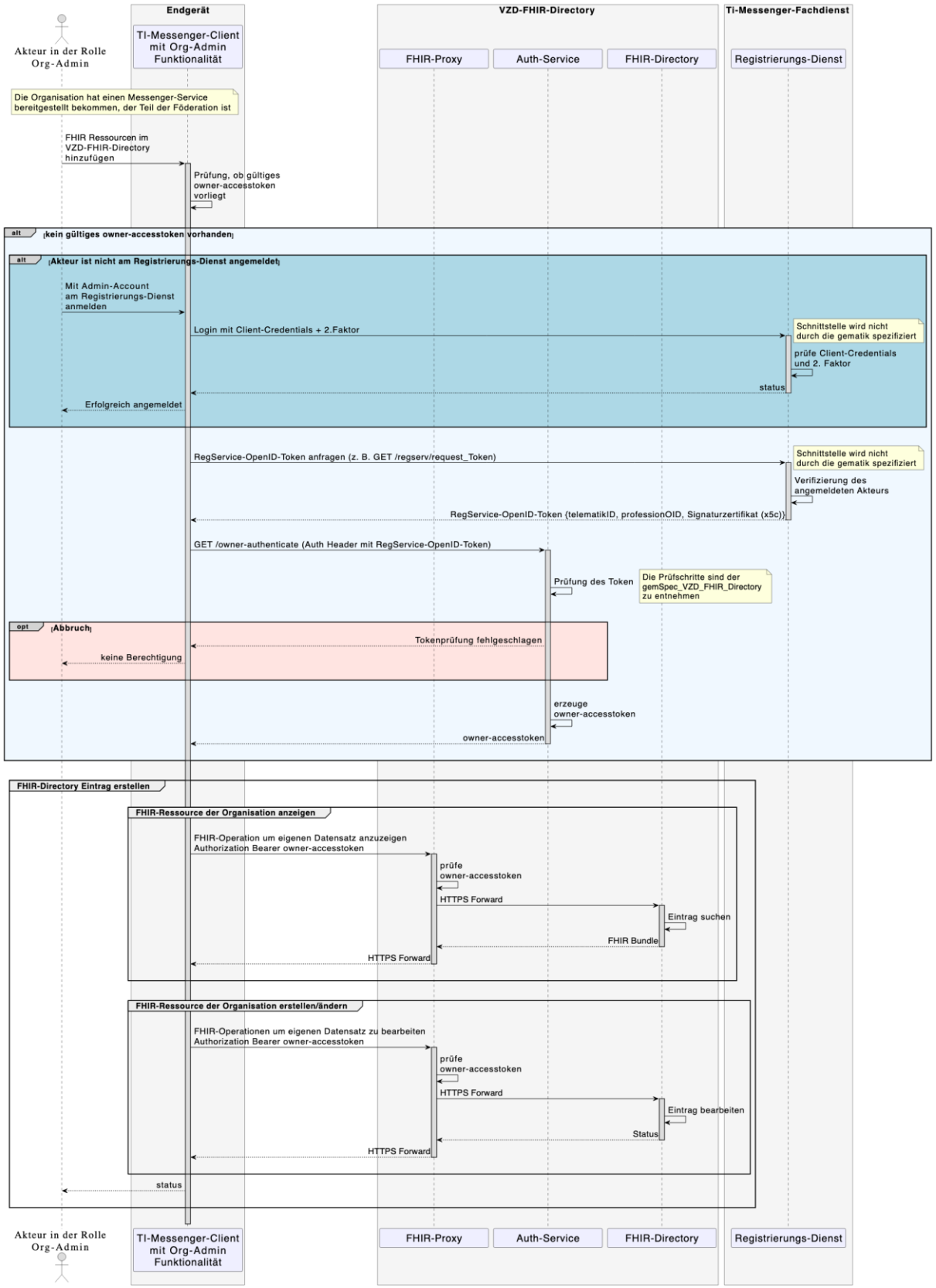

Figure 12: Runtime view – Add organisation resources to directory service

[<=]

Acceptance criteria for use case: Add organisation resources in directory service (AF_10059)

AF_10059 – Changes for own organisation FHIR records only
The actor in the "Org Admin" role may only change FHIR resources of their own organisation (including substructures). Access to non-affiliated FHIR resources MUST be prevented.
[<=]

AF_10059 – TI-M Raw data recording and delivery
The raw data was successfully recorded in accordance with the raw data definition according to [gemSpec_TI-Messenger-FD#Operation] for the TI-Messenger specialist service and sent to the defined interface of the raw data recording.
[<=]

AF_10059 – Add organisation resources in VZD-FHIR directory
After successful authentication at the registration service as an administrator of an organisation, the actor in the role "Org Admin" can have a RegService OpenID token issued and exchange it for an owner-accesstoken at the VZD-FHIR directory. With the owner-accesstoken, the actor can enter the MXID of an actor of their organisation below the *HealthcareService* resources into an *endpoint* or create new *HealthcareService* resources for the organisation. The actor in the "Org Admin" role is informed about the success of the operation.
[<=]

6.4 AF – Login of an actor to the messenger service

AF_10057 – Login of an actor to the messenger service
With this use case, an actor logs in to a messenger service responsible for the TI federation and registers their TI-Messenger client as the end device. The actor MUST be able to enter the Matrix domain of the desired messenger service directly into the TI-Messenger client. The input MAY be automated or supported by other tools such as a QR code scan. The authentication is performed according to the specifications of the respective organisation. After the successful login of an actor to the messenger service, the services offered by it MAY be used.

Table 11: AF – Login of an actor to the messenger service

AF_10057	**Login of an actor to the messenger service**
Actor	Service provider, employee of an organisation in the "User/User-HBA" role
Trigger	An actor wants to register with a messenger service with their TI-Messenger client.

AF_10057	Login of an actor to the messenger service
Components	• TI-Messenger client, • Messenger proxy, • Messenger home server, • FHIR proxy, • FHIR directory.
Preconditions	1. The actor has a TI-Messenger client supported by the provider. 2. The actor knows the messenger service URL or the URL is already configured in their TI-Messenger client. 3. The actor can identify themselves through an authentication process supported by the Matrix home server. If a separate authentication procedure is used by the organisation, a connection to the Matrix home server MUST have been made. 4. The Matrix home server used is integrated into the federation (valid messenger service).
Input data	URL of the Matrix home server
Result	A TI-Messenger account was created for an actor in the "User/User-HBA" role.
Output data	`Matrix-ACCESS_TOKEN`, `MXID`, `device_id` status
Acceptance criteria	ML-123571, ML-123576, ML-123575, ML-129870, ML-132587

In the runtime view, the interactions between the components used by the use case are shown. This describes the process of an actor logging in to a messenger service. If an actor is not yet registered on a matrix home server, then the actor is first registered with the operation `POST /_matrix/client/register`. The registration procedure is similar to the login procedure.

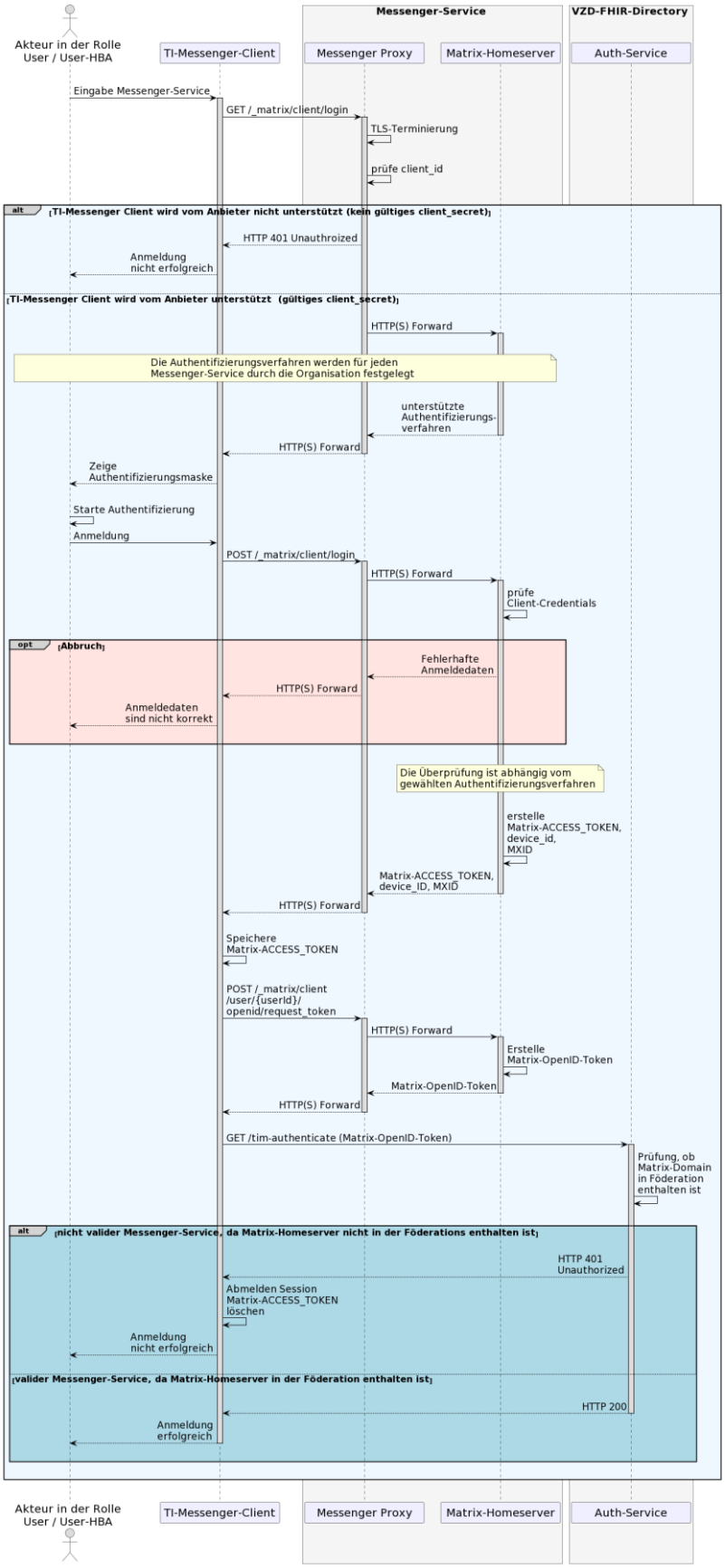

Figure 13: Runtime view – Login of an actor to the messenger service

[<=]

Acceptance criteria for use case: Login of an actor to the messenger service (AF_10057)

AF_10057 – Actor can successfully log in to a valid messenger service
An actor successfully logged in to a valid messenger service and successfully authenticated themselves using an approved authentication process. It MUST be ensured that it is not possible to log on to messenger services that are not part of the federation.
[<=]

AF_10057 – Messenger service issues an access token to TI-Messenger client
After successful login, the messenger service issued a Matrix ACCESS_TOKEN to the TI-Messenger client.
[<=]

AF_10057 – Storage of access token through TI-Messenger client
The TI-Messenger client stores the Matrix ACCESS_TOKEN given to it for use in the following use cases.
[<=]

AF_10057 – Actor cannot log in to an invalid messenger service
An actor cannot log into a public Matrix home server that is not integrated into the TI federation.
[<=]

AF_10057 – TI-M Raw data recording and delivery
The raw data was successfully recorded in accordance with the raw data definition according to [gemSpec_TI-Messenger-FD#Operation] for the TI-Messenger specialist service and sent to the defined interface of the raw data recording.
[<=]

6.5 AF – Add actor (user-HBA) in directory service

AF_10058-01 – Add actor (user-HBA) in directory service
With this use case, an actor in the "User-HBA" role can be found and reached by other actors of other messenger services. For this purpose, FHIR resources with their respective MXID are stored in the person directory (*PractitionerRole*) of the VZD-FHIR directory. In addition, it is possible to limit visibility for other actors. This use case CAN be directly combined with the initial login process of an actor to the messenger service (see use case: AF_10057 – Login of an actor to the messenger service). For this purpose, the actor in the "User-HBA" role is asked by the TI-Messenger client during the login process whether they have an HBA.

Table 12: AF – Add actor (user-HBA) in directory service

AF_10058	**Add actor (user-HBA) in directory service**
Actor	Service provider, a healthcare organisation employee in the "User-HBA" role

AF_10058	Add actor (user-HBA) in directory service
Trigger	An actor in the "User-HBA" role wants to be accessible in the person directory by storing their MXID in their Practitioner record in the VZD-FHIR directory.
Components	• TI-Messenger client, • Authenticator, • Central IDP service, • FHIR proxy, • Auth service, • FHIR directory.
Preconditions	1. The actor is logged in to a valid messenger service. 2. The actor has an approved TI-Messenger client. 3. The VZD-FHIR directory is registered with the central IDP service. 4. The actor can authenticate themselves using the central IDP service.
Input data	HBA, FHIR-Practitioner resources
Result	FHIR Practitioner resources updated, status
Output data	Updated Practitioner record
Acceptance criteria	ML-123612, ML-123611, ML-132588

In the runtime view, the interactions between the components used by the use case are shown. This is a **simplified runtime view** in which, for example, TLS scheduling on the FHIR proxy was not considered for the sake of clarity.

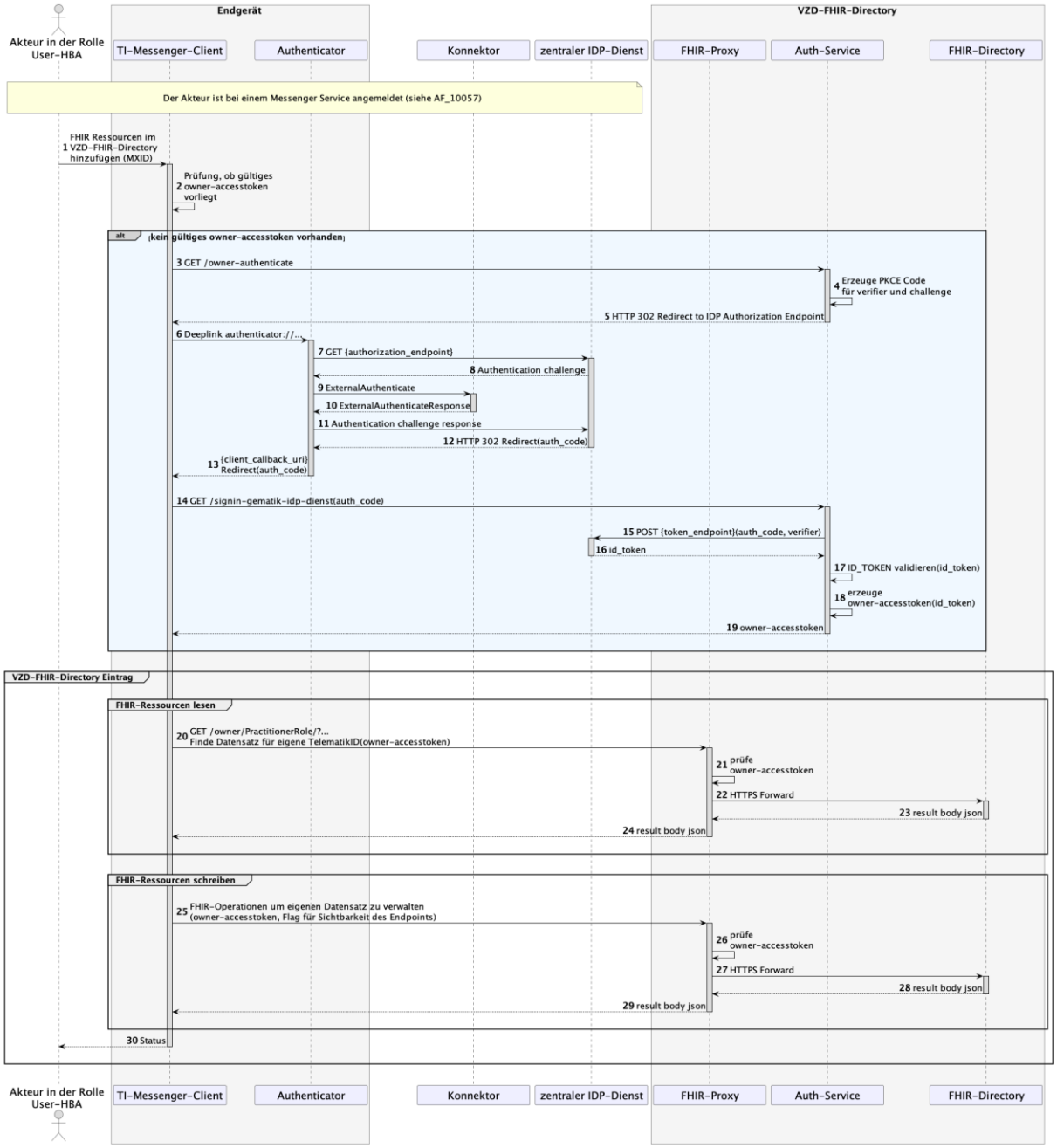

Figure 14: Runtime view – Add actor (user-HBA) in directory service

[<=]

Acceptance criteria for use case: Add actor (User-HBA) in directory service (AF_10058)

AF_10058 – Add actor as Practitioner
The MXID was included in the Practitioner FHIR record and the actor was informed about the success.
[<=]

AF_10058 – MXID entry for own Practitioner FHIR record only
The actor in the "User-HBA" role may only change their own FHIR resources.
[<=**]**

AF_10058 – TI-M Raw data recording and delivery
The raw data was successfully recorded in accordance with the raw data definition according to [gemSpec_TI-Messenger-FD#Operation] for the TI-Messenger specialist service and sent to the defined interface of the raw data recording.
[<=]

6.6 AF – Check federation affiliation of a messenger service

AF_10064-01 – Check federation affiliation of a messenger service
This use case checks whether a messenger service belongs to the TI-Messenger federation according to the criteria for stage 1 of client-server and server-server communication defined in Section 3.5 – Authorisation concept and applies to all use cases that need to check the Matrix domain of a messenger service. To check whether the Matrix domain belongs to the TI-Messenger federation, the messenger proxy uses a federation list that is provided by the registration service of its TI-Messenger specialist service. The storage time of the messenger proxy federation list is limited. The update of the federation list takes place as described in Annex 8.2 – Update of the federation list.

Table 13: Check federation affiliation of a messenger service

AF_10064	Check federation affiliation of a messenger service
Actor	-
Trigger	The messenger proxy receives or sends a Matrix event and MUST check the MXIDs included in the request for domain membership to the TI-Messenger federation.
Components	• Messenger proxy, • Matrix home server.
Preconditions	None
Input data	Matrix event
Result	The messenger proxy uses the federation list to determine whether the Matrix domain of the other messenger service is part of the TI-Messenger federation.
Output data	Status of the Matrix home server and forwarding
Acceptance criteria	ML-123672, ML-123891, ML-132589, ML-137902

In the runtime view, the interactions between the components used by the use case are shown. The triggering Matrix event on the messenger proxy is not shown in the following figure. The updating of the federation list is adequately described in Annex 8.2 – Update of the federation list.

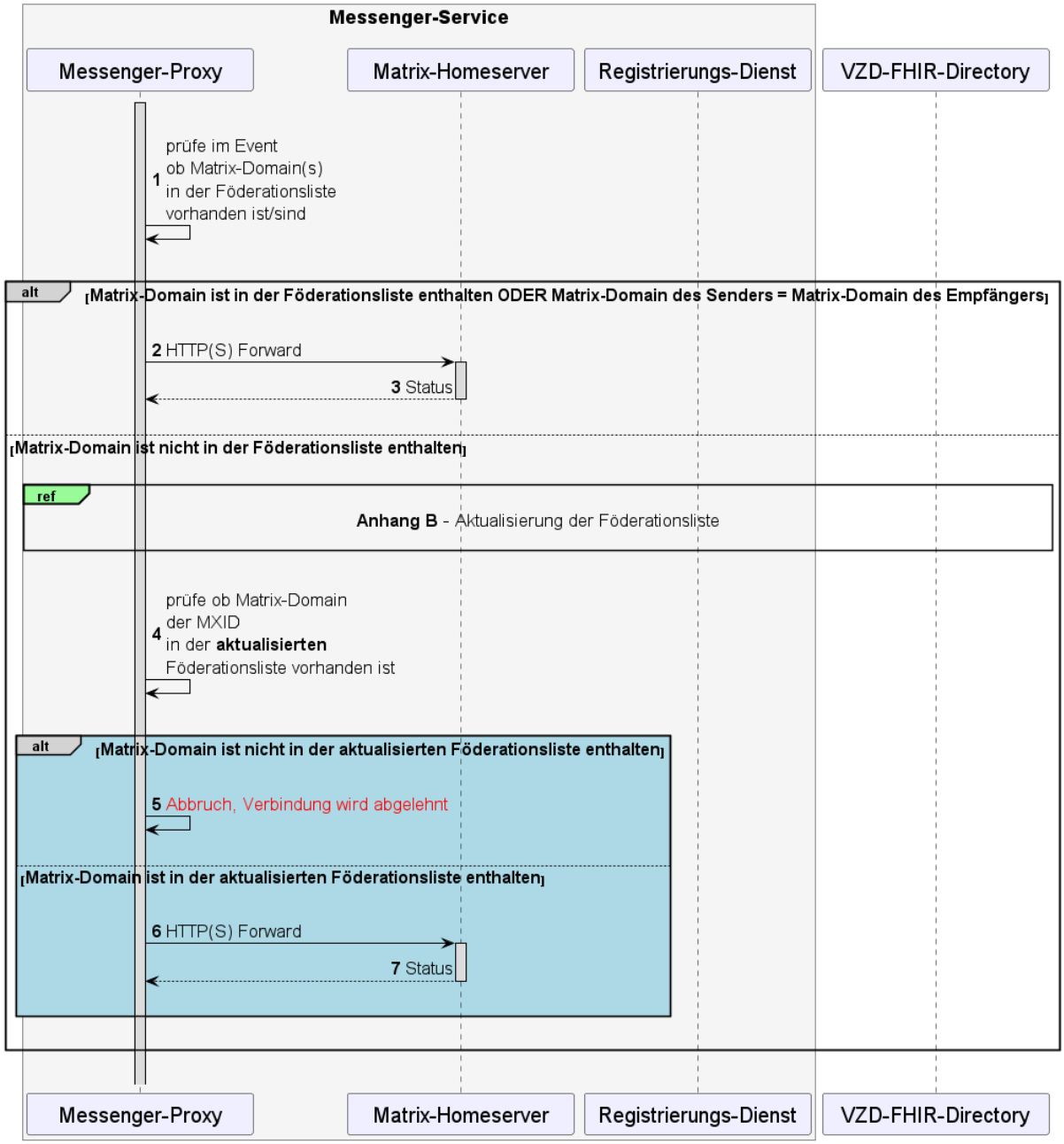

Figure 15: Runtime view – Check federation affiliation of a messenger service

[<=]

Acceptance criteria for use case: Check federation affiliation of a messenger service (AF_10064)

AF_10064 – Get federation list from VZD-FHIR directory

The registration service of the TI-Messenger specialist service MUST successfully retrieve the federation list from the FHIR proxy of the VZD-FHIR directory.

[<=]

AF_10064 – Matrix domain part of the federation list & up-to-dateness check
It MUST be ensured that the registration service checks the federation list for up-to-dateness before an updated list can be retrieved by the messenger proxy. It MUST also be ensured that the messenger proxy actually checks whether the Matrix domain of the other messenger service is part of the federation list.
[<=]

AF_10064 – TI-M Raw data recording and delivery
The raw data was successfully recorded in accordance with the raw data definition according to [gemSpec_TI-Messenger-FD#Operation] for the TI-Messenger specialist service and sent to the defined interface of the raw data recording.
[<=**]**

AF_10064 – Up-to-dateness – messenger proxy federation list
It MUST be ensured that the messenger proxy's federation list is up-to-date. For this, the messenger proxy MUST request an up-to-date list from the registration service at a fixed interval of once per hour.
[<=]

6.7 AF – Invitation of actors within an organisation

AF_10104-01 – Invitation of actors within an organisation
In this use case, an actor belonging to a common organisation is invited to a room to carry out actions. To search for actors within a common organisation, a TI-Messenger client searches its organisation's user directory on the Matrix home server. In this use case, the messenger proxy checks whether the Matrix domains contained in the `Invite` event are part of the TI federation in accordance with Section 3.5 – Authorisation concept of client-server communication. If this is the case, it is forwarded to the Matrix home server of the inviter. The latter checks whether the involved actors are registered with it. If this is not the case, the invited actor is not an actor within the organisation and the `Invite` event is forwarded for external delivery. The use case AF_10061 – Invitation of actors outside an organisation shows the resulting course of events.

Table 14: Invitation of actors within an organisation

AF_10104	Invitation of actors within an organisation
Actor	Service provider, employee of a healthcare organisation in the "User/User-HBA" role
Trigger	Actor A wants to invite actor B of their organisation to a shared space.
Components	• TI-Messenger client A + B, • Messenger proxy, • Matrix home server, • Push gateway.

AF_10104	Invitation of actors within an organisation
Preconditions	1. The actors are logged in to the same messenger service. 2. Each actor has an approved TI-Messenger client. 3. A chat room has been set up by the inviter.
Input data	`Invite event`
Result	Actor A and actor B are both in a shared chat room. Optionally, a notification is made to actor B about the invitation to the chat room.
Output data	Status
Acceptance criteria	ML-123896, ML-129415, ML-129414, ML-132590

In the runtime view, the interactions between the components used by the use case are shown. The chat room used for future communication has already been created by the inviting actor. Therefore, in this application example, a `/_matrix/client/v3/rooms/{roomId}/invite` event is checked at the messenger proxy. The following illustration only shows the invitation between two actors. Other actors can be invited regardless of this runtime view (Note: group messaging). For simplified presentation, it is assumed that the TI-Messenger clients of the involved actors are online. It is also assumed that both actors are registered on the same Matrix home server.

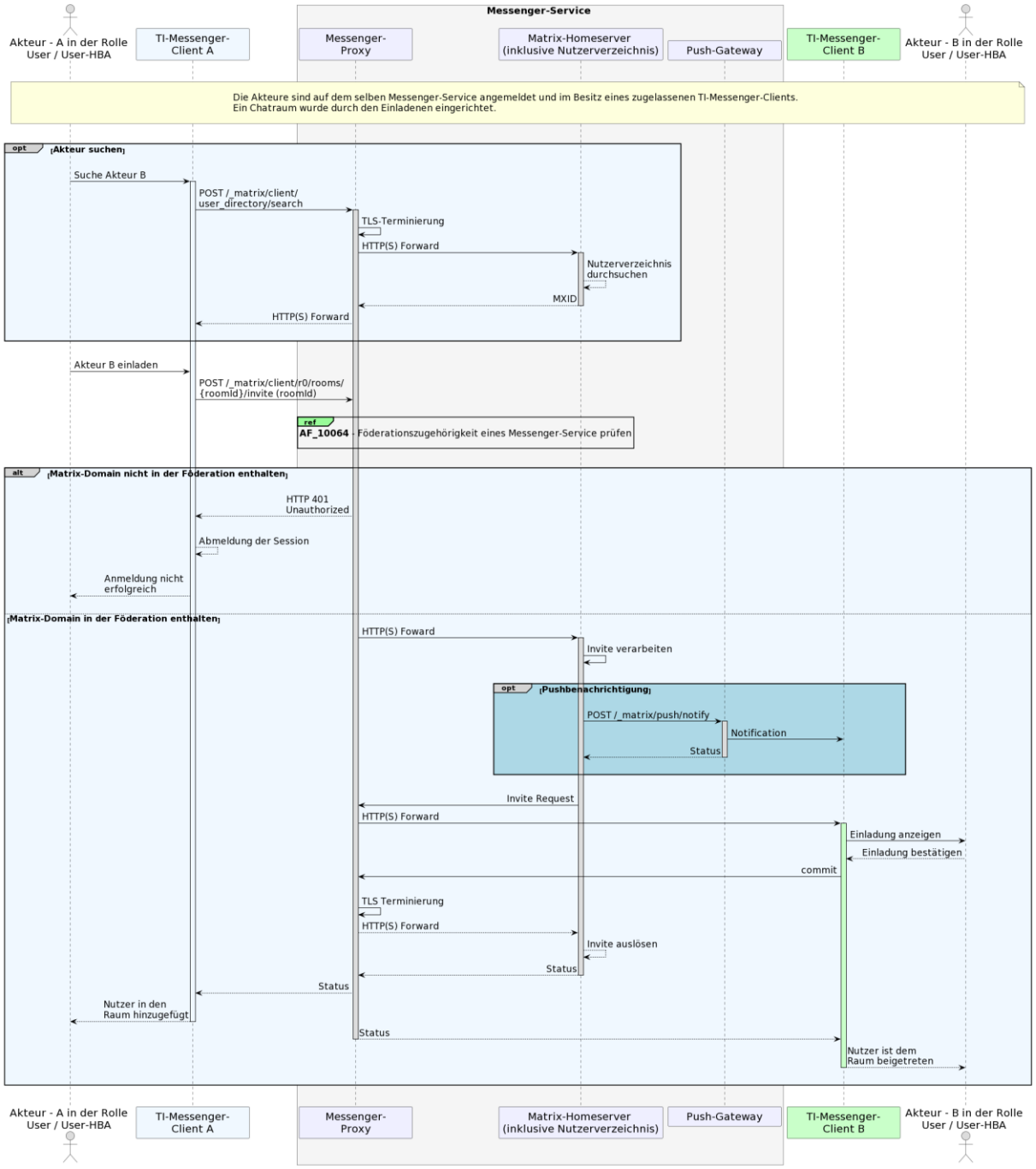

Figure 16: Invitation of actors within an organisation

[<=]

Acceptance criteria for use case: Invitation of actors within an organisation (AF_10104)

AF_10104 – Search Matrix home server for actors

The TI-Messenger client displays a list of all actors of a Matrix home server.
[<=]

AF_10104 – Messenger proxy checks TI federation affiliation
The messenger proxy rejects the `Invite event` if the Matrix domain is not part of the TI federation.
[<=]

AF_10104 – Actors have joined the chat room
All chat parties are successfully present in the chat room.
[<=]

AF_10104 – TI-M Raw data recording and delivery
The raw data was successfully recorded in accordance with the raw data definition according to [gemSpec_TI-Messenger-FD#Operation] for the TI-Messenger specialist service and sent to the defined interface of the raw data recording.**[**=]

6.8 AF – Exchange of events between actors within an organisation

AF_10063 – Exchange of events between actors within an organisation
This use case allows actors who are in a common space within a messenger service to exchange messages and execute other actions (events) defined by the Matrix specification.

Table 15: Exchange of events between actors within an organisation

AF_10063	**Exchange of events between actors within an organisation**
Actor	Service provider, employee of a healthcare organisation in the "User/User-HBA" role
Trigger	All Matrix events performed within an organisation's messenger service
Components	• TI-Messenger client A + B, • Messenger proxy, • Matrix home server, • Push gateway.
Preconditions	1. The actors are logged in to the same messenger service. 2. Each actor has an approved TI-Messenger client. 3. The participants have joined a common space.
Input data	Matrix event
Result	Matrix event was successfully processed
Output data	Dependent on the Matrix event
Acceptance criteria	ML-123669, ML-123670, ML-132591

In the runtime view, the interactions between the components used by the use case are shown. This is a **simplified runtime view** in which, for example, TLS scheduling on the messenger proxy was not considered for the sake of clarity. The line displayed in red in the figure symbolises the communication history of the triggering Matrix request. For simplified presentation, it is assumed that the TI-Messenger clients of the involved actors are online.

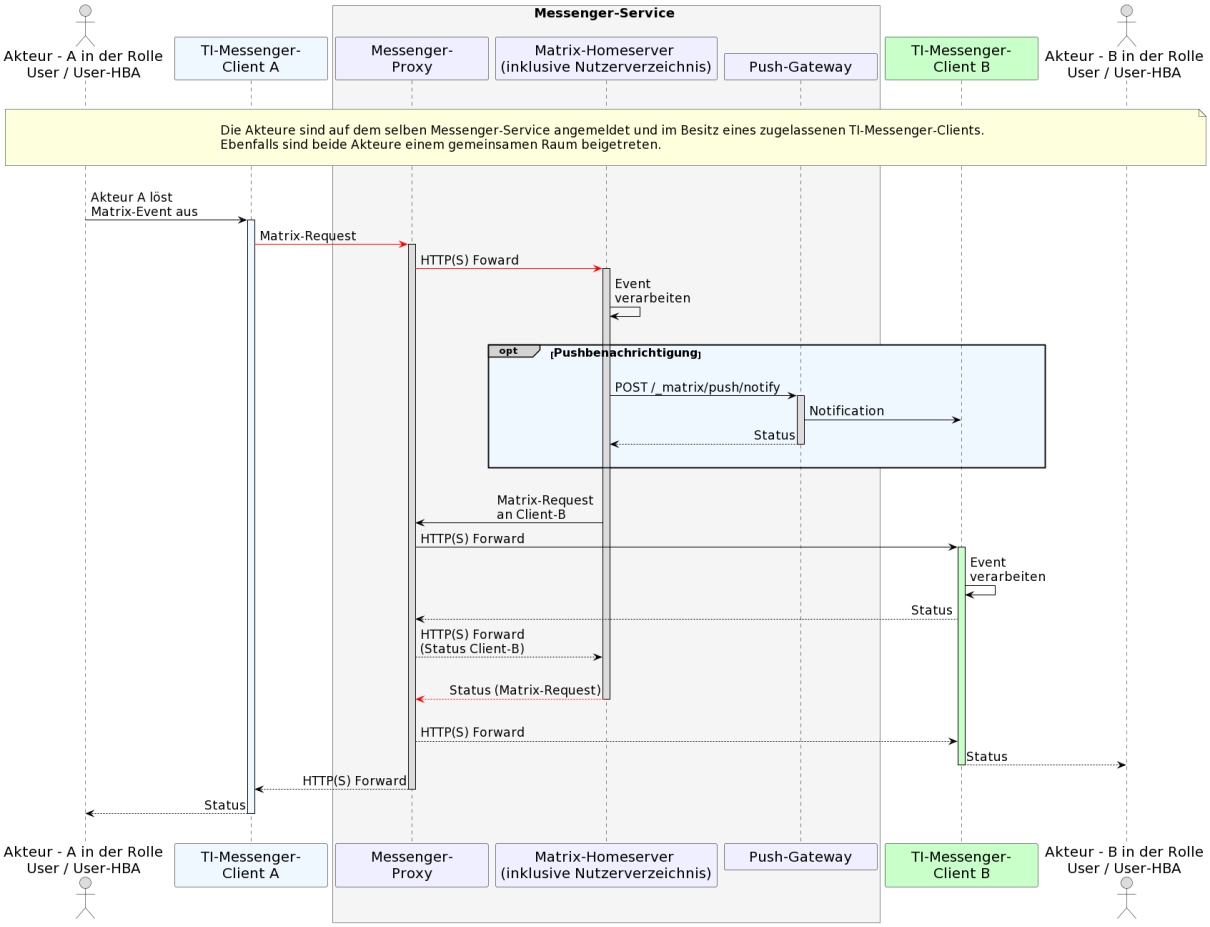

Figure 17: Runtime view – Exchange of events between actors within an organisation

[<=]

Acceptance criteria for use case: Exchange of events between actors within an organisation (AF_10063)

AF_10063 – Chat message processing
A chat message from TI-Messenger client A to TI-Messenger client B was successfully processed by the Matrix home server.
[<=]

AF_10063 – Triggering a notification
The Matrix home server triggers a notification of the TI-Messenger client from the receiver via the push gateway of the TI-Messenger provider connected to the TI-Messenger client.
[<=]

AF_10063 – TI-M Raw data recording and delivery
The raw data was successfully recorded in accordance with the raw data definition according to [gemSpec_TI-Messenger-FD#Operation] for the TI-Messenger specialist service and sent to the defined interface of the raw data recording.
[<=]

6.9 AF – Invitation of actors outside an organisation

AF_10061-01 – Invitation of actors outside an organisation
In this use case, an actor outside an organisation is invited. The VZD-FHIR directory can be used to search for actors outside the organisation. If the MXID of the sought actor does not exist there, there MUST be the possibility of enabling contact in other ways as well. At a minimum, making contact by means of a QR code scan MUST be offered. Other options for entering the MXID (e.g. manual entry) are permitted. In contrast to an invitation of actors within an organisation (see AF_10104 – Invitation of actors within an organisation), in this use case the messenger proxy additionally checks the server-server communication criteria defined in Section 3.5 – Authorisation concept (stage 1-3).

Table 16: AF – Invitation of actors outside an organisation

AF_10061	**Invitation of actors outside an organisation**
Actor	Service provider, employee of an organisation in the "User/User-HBA" role
Trigger	Actor A wants to set up a shared chat room with actor B outside an organisation.
Components	• TI-Messenger client A + B, • Messenger proxy A + B, • Matrix home server A + B, • VZD-FHIR directory, • Push gateway B.
Preconditions	1. The actors have an approved TI-Messenger client. 2. The actors know the URL of their messenger service or the URL is already configured in their TI-Messenger clients. 3. The actors are logged in to the messenger service. 4. The messenger services used are components of the TI-Messenger federation.
Input data	`Invite event`
Result	Actor A and actor B are both in a shared chat room. Optionally, a notification is made to actor B about the invitation to the chat room.
Output data	Status
Acceptance criteria	ML-123654, ML-123663, ML-132864, ML-132592

In the runtime view, the interactions between the components used by the use case are

shown. This is a **simplified runtime view** in which, for example, TLS scheduling on the messenger proxy was not considered for the sake of clarity. Also, for a simplified presentation it was omitted to show any necessary update of the federation list from its own registration service. The retrieval of the federation list is adequately described in Annex 8.2 – Update of the federation list. The individual check steps that the messenger proxy carries out for the defined criteria (Stage 2-3) of server-server communication can be found in Annex 8.3 – Stages of the authorisation check. For simplified presentation, it is assumed that the TI-Messenger clients of the involved actors are online. In this runtime view, actor A immediately invites actor B into a shared chat room.

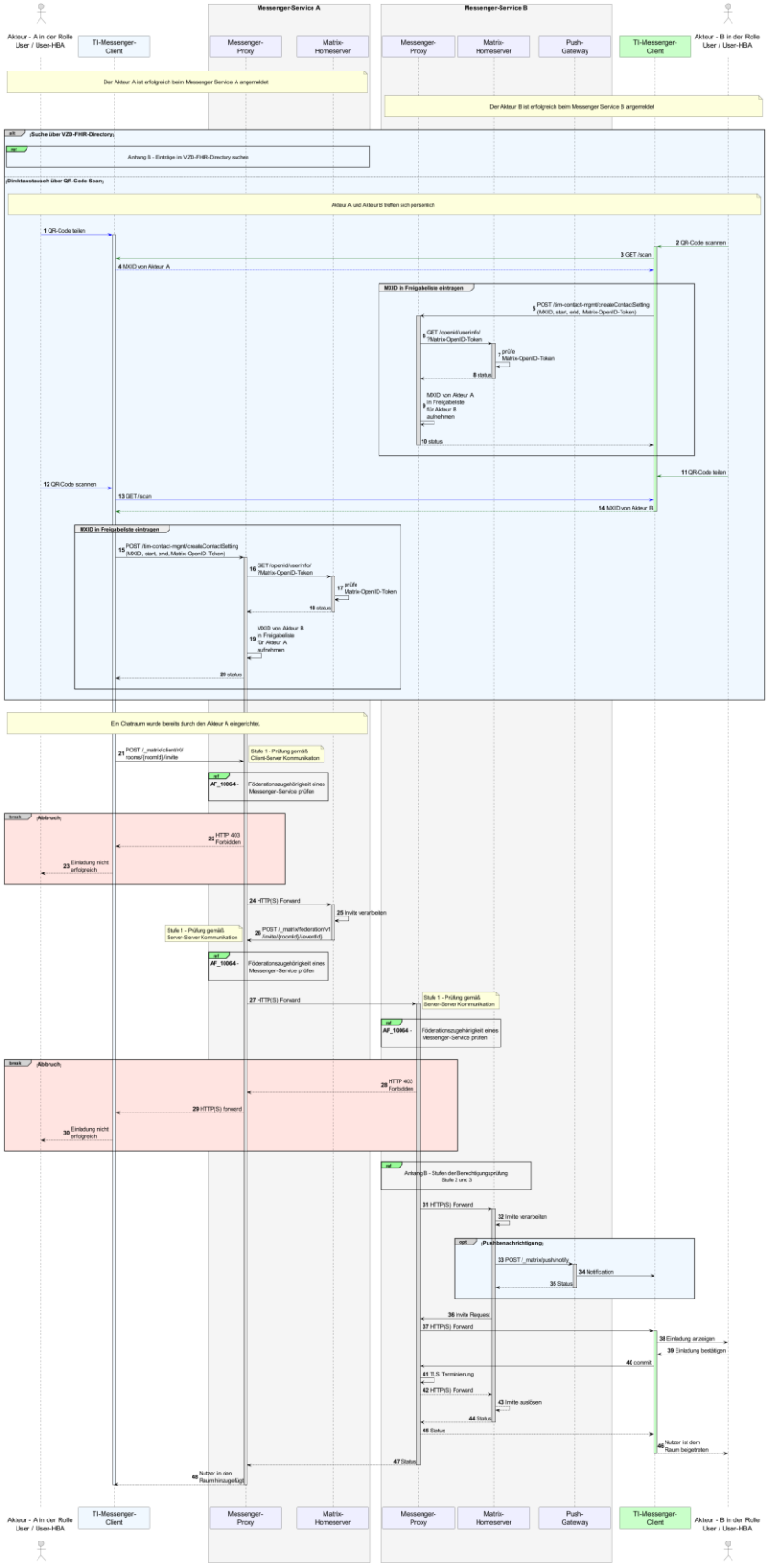

Figure 18: Runtime view – Invitation of actors outside an organisation

[<=]

Acceptance criteria for use case: Invitation of actors outside an organisation (AF_10061)

AF_10061 – VZD-FHIR directory search
A messenger client can successfully search for a chat partner in the VZD-FHIR directory.
[<=]

AF_10061 – Actors have joined the chat room
All chat parties are successfully present in the chat room.
[<=]

AF_10061 – Permission check of all stages
The authorisation check of Stages 1-3 has been taken into account.
[<=]

AF_10061 – TI-M Raw data recording and delivery
The raw data was successfully recorded in accordance with the raw data definition according to [gemSpec_TI-Messenger-FD#Operation] for the TI-Messenger specialist service and sent to the defined interface of the raw data recording.
[<=]

6.10 AF – Exchange of events between actors outside an organisation

AF_10062-01 – Exchange of events between actors outside an organisation
In this use case, actors in a common space can exchange messages and execute other actions specified by the Matrix specification. This use case requires a successful `Invite` event for one or more involved actors. However, the check for domain affiliation takes place with every event of the server-server communication. In this use case, the involved actors are distributed in a shared chat room and across different messenger services.

Table 17: AF – Exchange of events between actors outside an organisation

AF_10062	Exchange of events between actors outside an organisation
Actor	Service provider, employee of a healthcare organisation in the "User/User-HBA" role
Trigger	All Matrix events run between messenger services of different organisations.
Components	• TI-Messenger client A + B, • Messenger proxy A + B, • Matrix home server A + B, • Push gateway B.
Preconditions	1. Both actors are participants in a common space. 2. The messenger proxies have a current federation list.
Input data	Matrix event
Result	Matrix event was successfully processed
Output data	Dependent on the Matrix event, status
Acceptance criteria	ML-123665, ML-123666, ML-123667, ML-123668, ML-132593

In the runtime view, the interactions between the components used by the use case are shown. This is a **simplified runtime view** in which, for example, TLS scheduling on the messenger proxy was not considered for the sake of clarity. In the use case, only two actors are assumed to be involved. The necessary interactions during the federation list check, by the messenger proxy, were omitted in this runtime view. For a detailed description of this check, reference is made to the use case AF_10064 – Check federation affiliation of a messenger service. The line displayed in red in the figure symbolises the communication history of the triggering Matrix request. For simplified presentation, it is assumed that the TI-Messenger clients of the involved actors are online.

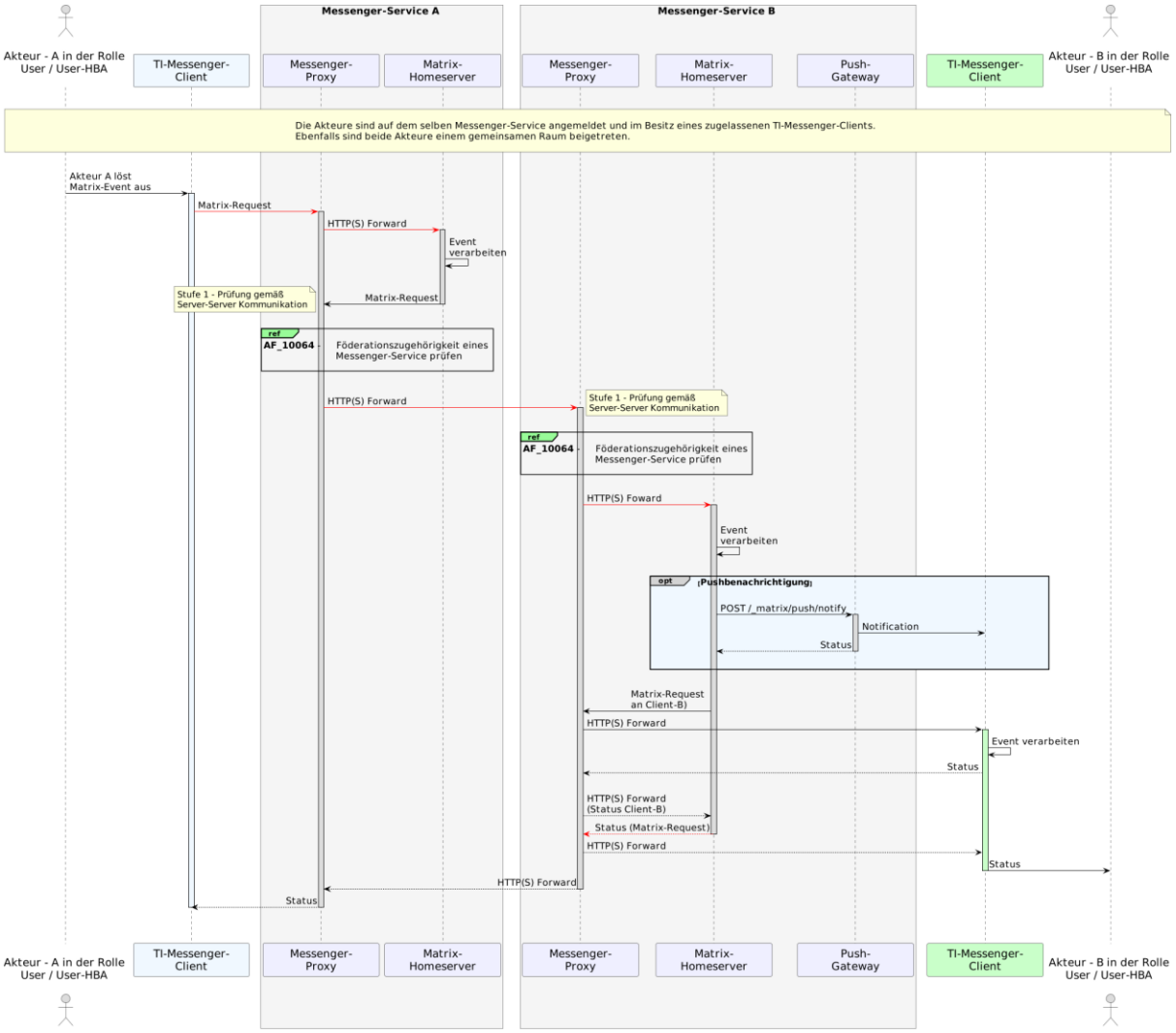

Figure 19: Runtime view – Exchange of events between actors outside an organisation

[<=]

Acceptance criteria for use case: Exchange of messages between actors outside an organisation (AF_10062)

AF_10062 – Sender messenger proxy checks recipient's domain

The sender's messenger proxy checks the recipient's domain for affiliation with the TI-Messenger federation.

[<=]

AF_10062 – Recipient's messenger proxy checks sender's domain

The recipient's messenger proxy checks the sender's domain for affiliation with the TI-Messenger federation.

[<=]

AF_10062 – Triggering a notification

The recipient's Matrix home server triggers a notification from the messenger client via its push gateway.

[<=]

AF_10062 – Message is displayed
The message is displayed to the recipient in the shared space.
[<=]

AF_10062 – TI-M Raw data recording and delivery
The raw data was successfully recorded in accordance with the raw data definition according to [gemSpec_TI-Messenger-FD#Operation] for the TI-Messenger specialist service and sent to the defined interface of the raw data recording.
[<=]

7 Annex A – Directories

7.1 Abbreviations

Abbreviation	Explanation
AD	Active Directory
AF	Use case
AZPD	Central Platform Services Provider
FHIR	Fast Healthcare Interoperable Resources
HBA	Health Professional Card
HTTP	Hypertext Transfer Protocol
IDP	Identity Provider
JSON	JavaScript Object Notation
JWT	JSON Web Token
LDAP	Lightweight Directory Access Protocol
SP	Service provider
MXID	Matrix User ID
OAuth	Open Authorisation
PTA	Pharmaceutical Technical Assistant
REST	Representational State Transfer
SMC-B	Institution card (Security Module Card Type B)
SMC-B ORG	Security Module Card for Organisations
SPOC	Single Point of Contact
SSO	Single Sign-On
TI	Telematics infrastructure

Abbreviation	Explanation
TI-ITSM	IT Service Management of TI
TI-M	TI Messenger
TSP	Trust Service Provider
VZD	Directory service

7.2 Glossary

Term	Explanation
MXID	Unique identification of a TI-Messenger participant (Matrix User ID)
On-premise	The product is operated on own or leased hardware
Third-party	Third-party provider providing additional services or components

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
[api-messenger]	gematik: api-ti-messenger https://github.com/gematik/api-ti-messenger/
[api-vzd]	gematik: Directory service of the telematics infrastructure https://github.com/gematik/api-vzd
[gemKPT_Betr]	gematik: Operating concept online productive operation
[gemKPT_TI_Messenger]	gematik: TI-Messenger concept paper
[gemSpec_IDP_Service]	gematik: Identity provider service specification
[gemSpec_TI-Messenger-FD]	gematik: Specification TI-Messenger specialist service
[gemSpec_VZD_FHIR_Directory]	gematik: FHIR Directory specification directory service

7.5.2 Other documents

[Source]	Publisher (publication date): Title
[BSI 2-factor]	BSI 2-factor authentication for more data security https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/Bewertung-2FA-Verfahren/bewertung-2fa-verfahren_node.html
[Server-Server API]	Matrix Foundation: Matrix Specification – Client-Server API https://spec.matrix.org/v1.3/client-server-api/
[FHIR]	HL7 FHIR Dokumentation https://www.hl7.org/fhir/documentation.html
[gematik Authenticator]	gematik Authenticator https://cloud.gematik.de/index.php/s/23ebxa75z3s7zGt?path=%2Fv2.1.0

[Source]	Publisher (publication date): Title
[Matrix Bots]	Matrix Bot Implementierungen https://matrix.org/bots/
[Matrix Specification]	Matrix Foundation: Matrix Specification https://spec.matrix.org/v1.3/
[OpenID]	OpenID Foundation https://openid.net/developers/specs/
[Push Gateway API]	Matrix Foundation: Matrix Specification - Push Gateway API https://spec.matrix.org/v1.3/push-gateway-api/
[RFC 8225]	IETF https://datatracker.ietf.org/doc/html/rfc8225
[Server-Server API]	Matrix Foundation: Matrix Specification - Server-Server API https://spec.matrix.org/v1.3/server-server-api/

8 Annex B – Procedures

8.1 Search entries in the VZD-FHIR directory

The following figure describes how an actor searches for *HealthcareService* and *PractitionerRole* resources in the VZD-FHIR directory. This requires a successful login of the actor to a messenger service. The shown procedure displays all communication relationships that are necessary in principle. Further information on the procedure can be found in [gemSpec_VZD_FHIR_Directory]. Access to the endpoint `/_matrix/federation/v1/openid/userinfo` MUST be enabled for the Matrix OpenID token check.

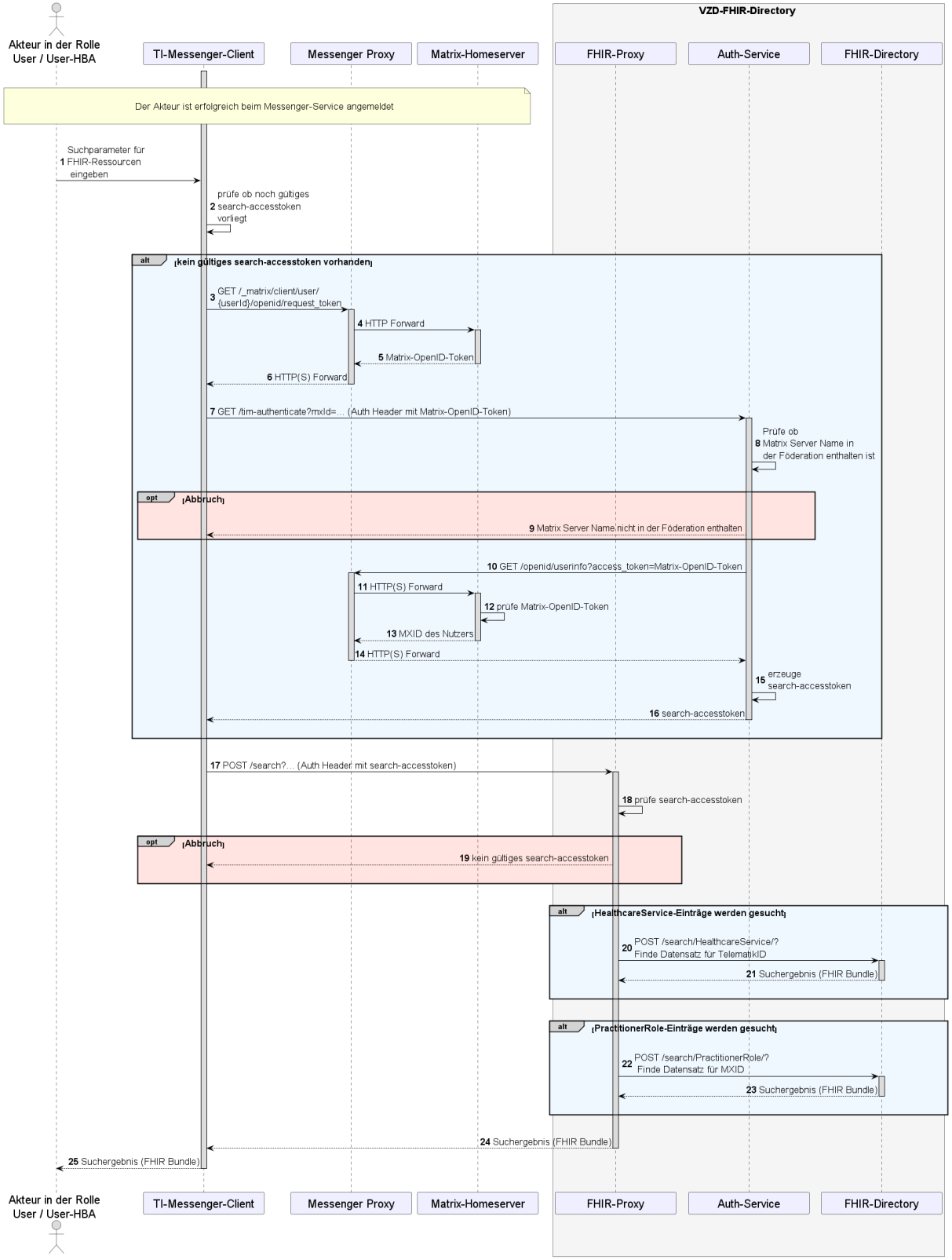

Figure 20: Runtime view – Search entries in the VZD-FHIR directory

8.2 Update of the federation list

The following figure describes how the messenger proxy updates its locally maintained federation list. To update the federation list, the messenger proxy MUST request it from the registration service of its TI-Messenger specialist service. The frequency of requesting a new list is determined by the provider; the aim should be to have a federation list as up-to-date as possible. Here, the messenger proxy transfers the saved version of the federation list to the registration service. If the version matches, no new federation list will be provided by the registration service for the messenger proxy. If the version is larger than the one passed by the messenger proxy, an updated federation list is provided by the registration service. Each time a messenger proxy requests an up-to-date federation list from the registration service, the registration service MUST ensure the up-to-datedness of the list delivered by it by overwriting the version of the federation list stored by it with a more current version obtained from the FHIR proxy, if necessary. A download of the federation list is only necessary if a newer version exists on the FHIR proxy. The structure of the federation list is described in [gemSpec_VZD_FHIR_Directory]. After retrieving the federation list from the registration service, through the messenger proxy, the latter MUST check the signature of the federation list.

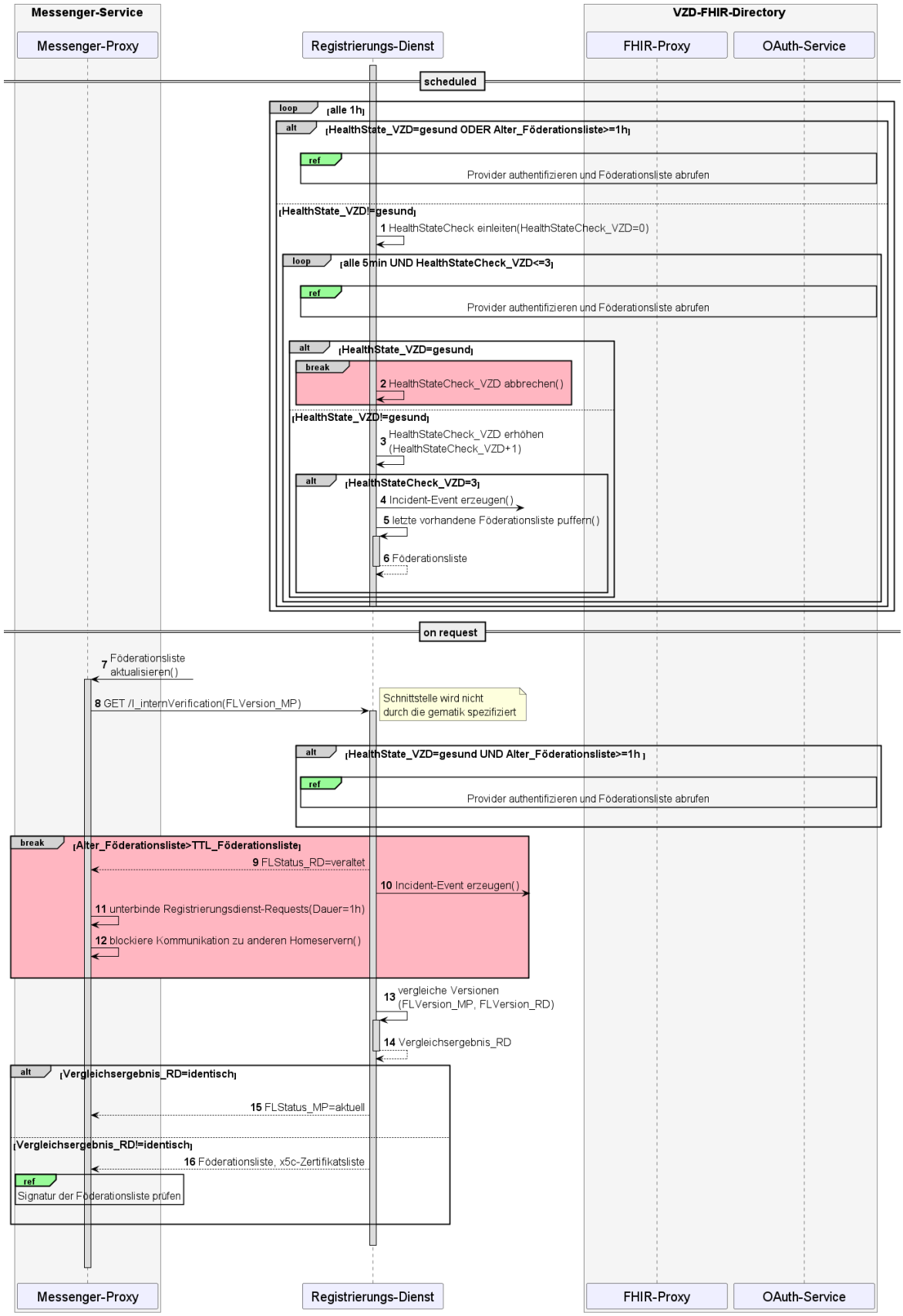

Figure 21: Runtime view – Update of the federation list

The sequence diagram "Authenticate provider and retrieve federation list" referenced in the figure "Runtime view – Update of the federation list":

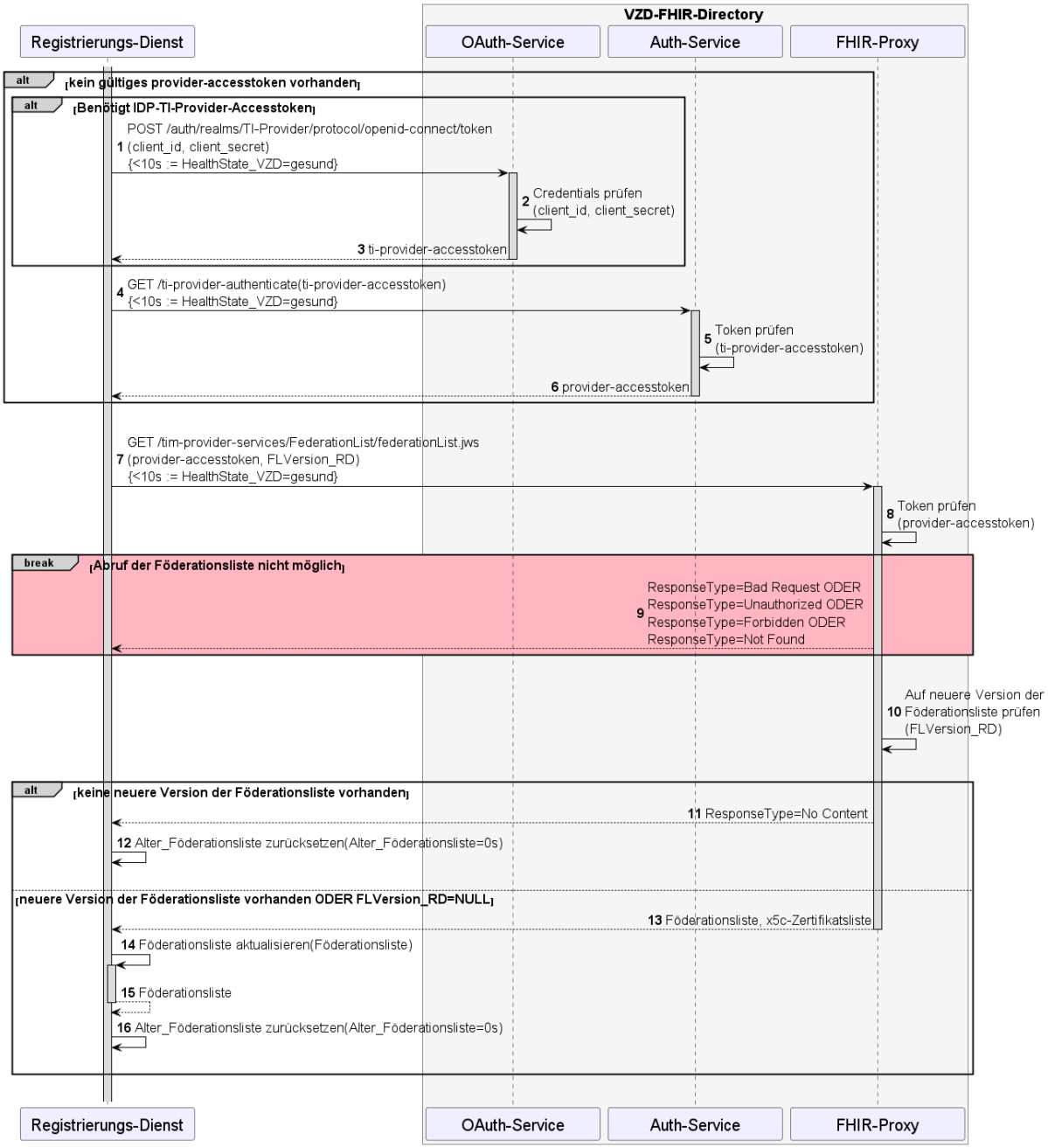

Figure 22: Authenticate provider and retrieve federation list

The sequence diagram "Check federation list signature" referenced in the figure "Runtime view – Update of the federation list":

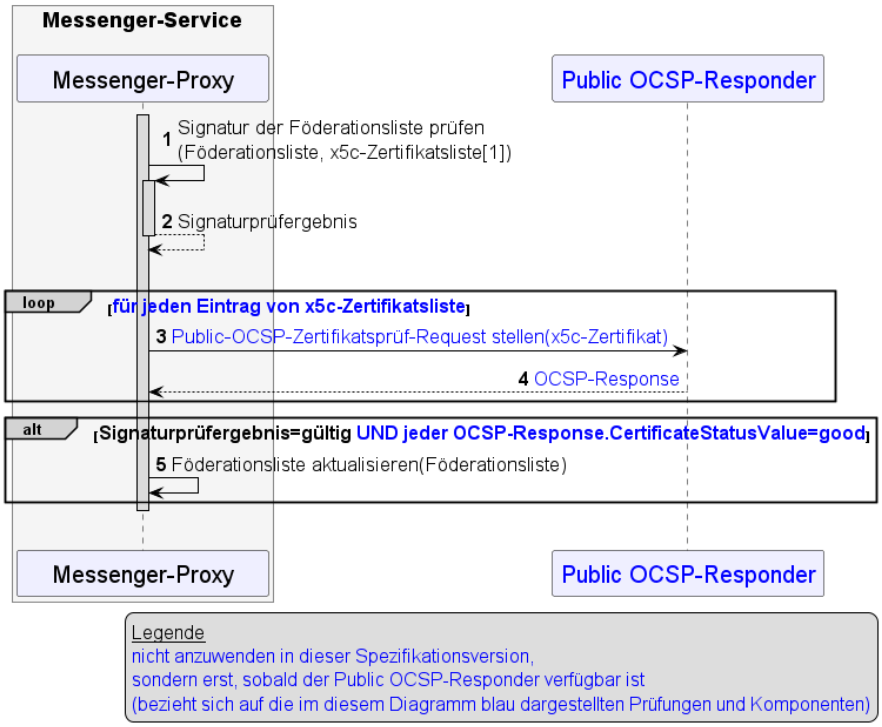

Figure 23: Checking the signature of the federation list

8.3 Stages of the authorisation check

The following figure describes how to check the entitlement of incoming and outgoing Matrix events on the messenger proxy. The authorisation concept is based on a three-stage check, which is described in Sections 3.5.1 – Client-server communication and 3.5.2 – Server-server communication. The mention of necessary authentications is omitted here.

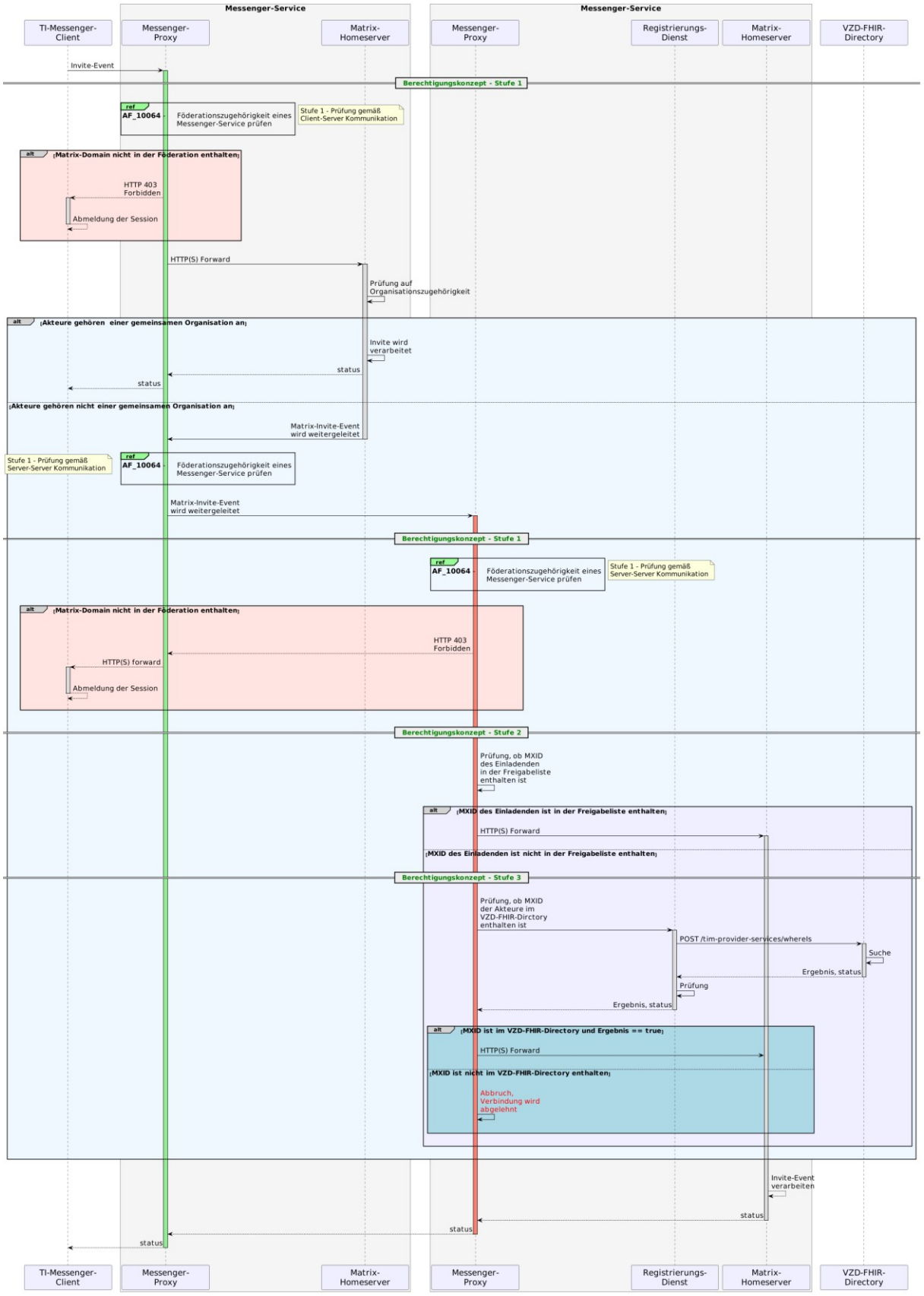

Figure 24: Runtime view – Authorisation check stages