Electronic health card and telematics infrastructure

Specification
TI-Messenger Specialist Service (Fachdienst)

Note: This document is non-binding.

Version:	1.1.1
Revision:	682485
Last updated:	31/07/2023
Status:	released
Classification:	public
Referencing:	gemSpec_TI-Messenger-FD

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 specification defines the requirements for production, testing and operation of the TI-Messenger specialist service product type. The specialist service enables secure ad-hoc communication between participants. The communication relationships with the TI-Messenger client and the VZD-FHIR directory result in interfaces to be offered by the TI-Messenger specialist service, which are described in this document normatively. Interfaces used by the TI-Messenger specialist service are mostly in other areas of responsibility (e.g. IDP service). These are defined in the corresponding product type specification.

1.2 Target group

The document is aimed at manufacturers of the TI-Messenger specialist service product type as well as suppliers who operate this product type [gemKPT_Betr]. All manufacturers and suppliers of TI applications using interfaces of the component or exchanging data with the product type TI-Messenger specialist service product type or processing 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

The document specifies the interfaces provided (offered) by the product type. Used interfaces, on the other hand, are described in the specification of the product type that provides this interface. Reference is made to the corresponding documents (also see annex, Section 6.5 – Referenced documents).

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

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 specialist service product as well as for the operating provider according to [gemKPT_Betr] and is to be considered as an approval criteria for both 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 identifier of an acceptance criterion is assigned by the system, e.g., the string 'ML_' followed by a number
- **Title of use case / acceptance criteria:** A title that summarises the content
- **Text/description**: Detailed description of the content. Can contain tables, illustrations and models in addition to text

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

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

Reference to open points

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

2 System overview

The TI-Messenger specialist service enables secure communication between different actors in the German healthcare system. This is based on the open and decentralised communication protocol Matrix. The Matrix standard provides RESTful APIs for the secure transfer of JSON objects between Matrix clients and other services. Secure communication between the individual actors takes place in encrypted form in rooms on the participating Matrix home servers.

The TI-Messenger specialist service consists of decentralised and central subcomponents, which must be tested during product approval and which a TI-Messenger provider MUST provide. The decentralised subcomponents are the messenger services. A messenger service consists of a Matrix home server and a messenger proxy that ensures that a federation of Matrix home servers only takes place between verified domains. Messenger services are provided to individual organisations (e.g. service provider institutions, associations) and allow use by all legitimate actors of an organisation. Furthermore, messenger services MAY provide authentication procedures that are not assigned to an organisation. These are technically no different from other messenger services. Only the associated organisation offers a necessary authentication procedure for these actors.

The communication between a TI-Messenger client and a TI-Messenger specialist service always takes place via the messenger proxy of messenger services. At the messenger proxy of a messenger service, TLS termination of connections from the TI-Messenger clients takes place first. The messenger proxy checks TI federation membership by matching it against a federation list provided by its registration service (authorisation check – Stage 1 of the client-server communication). Here, the messenger proxy checks whether the participating Matrix home servers are registered members of the federation and whether an actor is authorised to trigger requests on the Matrix home server. The messenger proxy also provides a release list for the authorisation check (Stage 2 of server-server communication). For the administration of this release list by the actors, the messenger proxy offers an interface to the TI-Messenger clients.

In addition to the decentralised messenger services, a TI-Messenger specialist service consists of the central subcomponents registration service and push gateway. The registration service enables the TI-Messenger provider to automatically provide messenger services to organisations and to enter the Matrix domain of the messenger services it provides into its organisation resource in the central VZD-FIR directory. The registration service of a TI-Messenger specialist service offers the provision of a federation list for messenger proxies of its messenger services as a further function. The push gateway is used to transmit notifications to the respective TI-Messenger clients to signal the receipt of a new message.

In the following figure, all involved components of the TI-Messenger architecture are shown in simplified form. The TI-Messenger specialist service shown in blue shows all the components described in this specification.

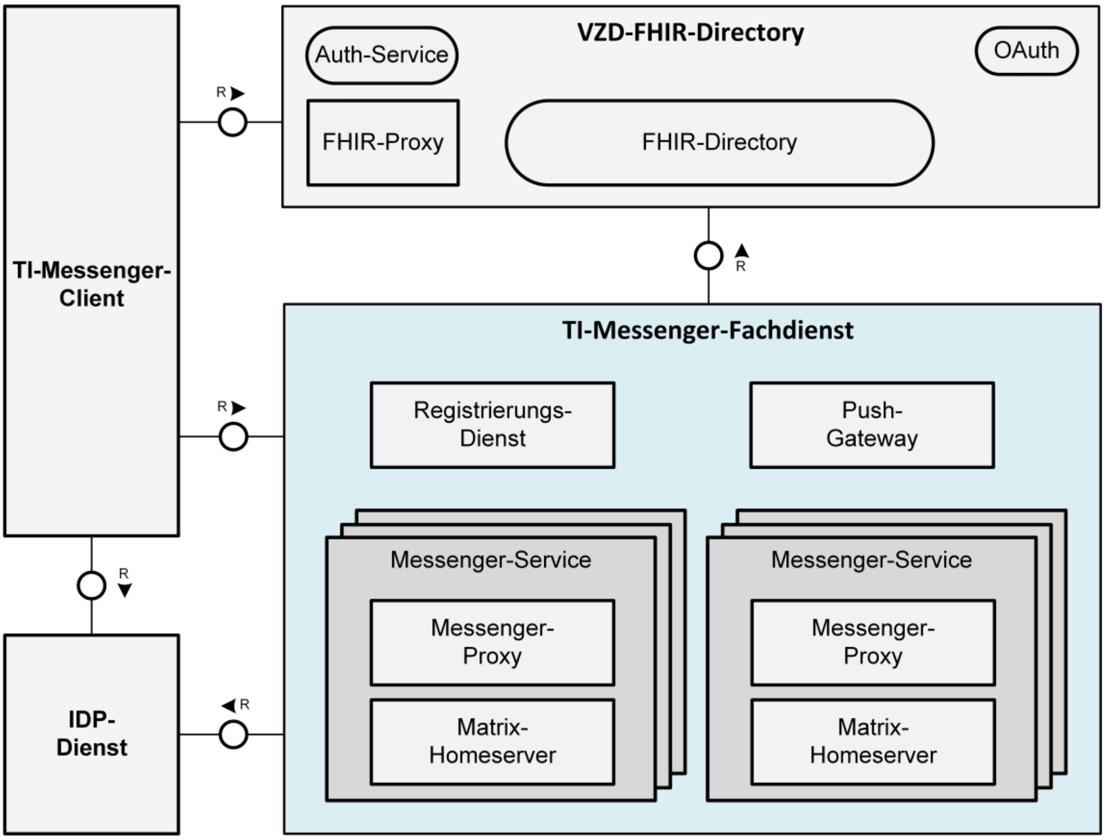

Figure 1: System overview (simplified presentation)

3 System context

The following section puts the TI-Messenger specialist service into the system context of the TI-Messenger service.

3.1 Neighbouring systems

Further systems are required for the operation of the TI-Messenger specialist service. This includes the central IDP service that performs authentications and authorisations based on SmartCard identities, as well as the VZD-FHIR directory. The figure to be found in Section 2 – System overview shows their relationship with the TI-Messenger specialist service.

The central IDP service provides an ID_TOKEN to all eligible actors in accordance with the protocol specified by the OpenID Foundation [OpenID]. These can be used as an alternative to the KIM procedure (see Section 4.2.1 – Authentication procedures for registering a messenger service) for proving possession of an SMC-B when ordering a messenger service and for authenticating service providers for write access to the FHIR directory.

The central VZD-FHIR directory forms a directory of all TI-Messenger specialist services, organisations and service providers and offers the possibility of searching for participants based on configured characteristics. Upon successful verification of an organisation, the registration service of the TI-Messenger specialist service enters the Matrix domain of the associated messenger service of the organisation into the VZD-FHIR directory. This entry allows the messenger service to participate in the federation of the TI-Messenger service. The VZD-FHIR directory trusts the Matrix host servers of the respective messenger services if the domain of the messenger service is successfully entered into the VZD-FHIR directory.

3.2 Messenger services

Through TI-Messenger providers, messenger services are provided to healthcare organisations (e.g. doctor's office, hospital, pharmacy, association, etc.). Messenger services are provided via the registration service of a TI-Messenger specialist service and MAY take place *on-premise* or centrally within data centres. Each messenger service MUST be logically assigned to an organisation. Messenger services MAY only differ by the authentication methods used for each organisation. These are defined and provided by the respective organisation and thus enable the reuse of authentication procedures already existing within the organisation. Each organisation MUST have control over user management to be able to exclude users from the TI-Messenger at any time. Actors MUST be deleted/blocked by the messenger service if the user has been deleted/blocked within the user management.

3.2.1 Authentication procedures

Messenger services MUST provide an authentication process to the actors depending on the type of organisation. For example, if systems such as Active Directory or LDAP based user directories are already available within an organisation, these MAY be used by registering the respective Matrix home server with them. If no authentication procedures are available in the organisation, TI-Messenger providers MAY provide appropriate authentication procedures. These allow authentication of actors (e.g. by username/password and a second factor) and can also be used by other systems.

The figure below illustrates the reuse of an existing authentication process by actors within an organisation through a messenger service.

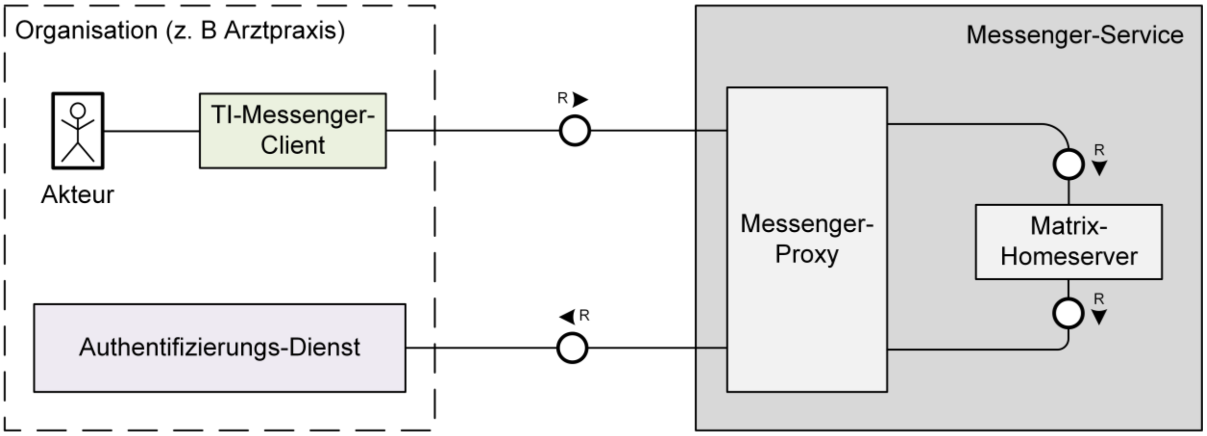

Figure 2: Example – authentication of an organisation's actors

4 General specifications

4.1 Data protection and security

To ensure data protection and security within the framework of the TI-Messenger service, the requirements to be observed for the TI-Messenger specialist service are described below. Requirements that are ensured by other system components are not further listed here.

A_22807 – Contract obligations
The TI-Messenger provider MUST contractually require customers to ensure that organisation-based TI-Messenger accounts are not given to third parties and that accounts are only created for organisation actors with whom an employment or service provider contract relationship exists. Function accounts (in conjunction with a chatbot) are excluded from the contractual obligations.
[<=]

A_22809 – Comprehensive use of TLS for manufacturers
TI-Messenger specialist service manufacturers MUST ensure that all connections between components of the TI-Messenger specialist service communicate via TLS if this communication exceeds the limits of a virtual/physical machine. A server side TLS MUST at least be used for this purpose. Unless TLS is used on both sides, the authenticity of the client side MUST be ensured with equivalent security. The specifications according to [gemSpec_Krypt] apply.
[<=**]**

A_22929 – Comprehensive use of TLS for providers
TI-Messenger providers MUST ensure that all connections between components of the TI-Messenger specialist service communicate via TLS if this communication exceeds the limits of a virtual/physical machine. A server side TLS MUST at least be used for this purpose. The specifications according to [gemSpec_Krypt] apply.
[<=]

A_22936 – Authentication procedures for actors in organisations
TI-Messenger providers MAY replicate existing authentication procedures of the organisation for authenticating actors in the "user" role. If this is the case, the provider MUST explicitly point out to the organisation and the administrators that the security of the user authentication is thus placed under the responsibility of the organisation. To this end, the provider MUST ensure that it only accepts authentication procedures that are in the hands of the organisation and whose authentication means can be managed and blocked by the organisation. The provider MUST ensure that at least two factors are used for authentication and that the safety recommendations of the BSI [BSI 2 factor] are taken into account. To prevent attacks from a distance on the 2nd factor, a procedure that is rated at least "medium" must be selected. The provider MUST ensure that at least one authentication using an OIDC authenticator is supported and that technical options are provided for the organisation so that both factors cannot be compromised by an attack vector.
[<=]

Note: A_22936 only regulates the authentication necessary to obtain a token that enables users to authenticate themselves against the messenger service.

A_23611 – Specifications for the minimum quality of passwords
The TI-Messenger service provider MUST specify the minimum quality of passwords in accordance with [BSI ORP.4] A.22 and ensure compliance with these specifications at all points where passwords are to be set as part of the configuration. Furthermore, the provider MUST instruct the service provider institution (SPI), which obtains the TI-Messenger service from it, about the necessity of compliance with the specifications from [BSI ORP.4] A8. These contain security-related requirements regarding the use and handling of passwords, but are directed at the operational business in the SPI, which cannot be controlled by the provider. In this context, passwords are understood to be both passwords and passphrases, to which the document [BSI ORP.4] is equally applicable.**[**<=**]**

A_23613 – Forced deregistration and blocking of actors
If an actor in the "User" role of an organisation's TI-Messenger service is blocked or has their active session terminated – that is, they are forcibly logged out – by an actor in the "Org Admin" role of the organisation, the TI-Messenger specialist service MUST stop forwarding messages sent to or from that actor in the "User" role with immediate effect. **[**<=**]**

A_22815 – Handling cryptographic material for OAuth
TI-Messenger providers MUST ensure that cryptographic material is safely inserted for authentication against the VZD-FHIR directory. In order to demonstrate the implementation, a review of the process for introducing the cryptographic material is required. The review includes description and execution of the process. Auditing the implementation is optional.
[<=]

A_22817 – Explicit prohibition of profiling for TI-Messenger specialist services
TI-Messenger specialist service manufacturers MUST NOT collect data for profiling purposes. This particularly concerns monitoring which actors communicate with which other actors.

Note: Pursuant to Section 331(2) of the German Social Code (SGB V), gematik may specify data that manufacturers of components and services must disclose or transmit to gematik, insofar as this data is required to fulfil gematik's legal mandate to monitor operations to ensure the security, availability and usability of the telematics infrastructure. Only personal data required for this purpose may be collected by providers and manufacturers as a time-limited exception to the profiling ban and used exclusively for that purpose.
[<=]

A_22814 – Explicit prohibition of profiling for TI-Messenger providers
TI-Messenger providers MUST NOT collect data for profiling purposes. This particularly concerns monitoring which actors communicate with which other actors.

Note: Pursuant to Section 331(2) of SGB V, gematik may specify data that providers of components and services must disclose or transmit to gematik, insofar as this data is required to fulfil gematik's legal mandate to monitor operations to ensure the security, availability and usability of the telematics infrastructure. Only personal data required for this purpose may be collected by providers and manufacturers as a time-limited exception to the profiling ban and used exclusively for that purpose.
[<=**]**

A_22813 – Logging for the purpose of troubleshooting
If logging is performed in the TI-Messenger specialist service for the purpose of troubleshooting, the specialist service MUST ensure, taking Article 25(2) of the GDPR into account, that the log data only contains personal data in accordance with the data

protection principle under Article 5 of the GDPR in the type and scope required for remedy and that the generated log data in the specialist service is deleted immediately after resolution. Unless other legal principles such as SGB V prevail, only anonymised data must be recorded.
[<=]

A_22811 – Matrix home server deletion periods
TI-Messenger specialist service manufacturers MUST ensure that their Matrix home servers offer a function that deletes events, conversation content and individual conversation-associated data (e.g. files sent) after a period of 6 months from the last activity in a room. Manufacturers MUST ensure that the time period is configurable by the actor in the "Org Admin" role. This function MUST be deactivated by the actor in the "Org Admin" role via opt-out. This function MAY be realisable via the fact that participants leave a chat room after the time limit has expired and the room is automatically deleted after all participants have left.
[<=]

A_22808 – Messenger service push notifications
TI-Messenger services MUST ensure that push gateways use external push services in a data protection compliant manner. For this purpose, the following criteria are defined, which MUST always be observed:

- All push message content that the push provider does not need to access MUST be encrypted.
- Push messages MUST be delayed by a random value of 0-10 seconds before sending in order to make timing-based profiling more difficult.
- If a target client is currently active, it should automatically listen for incoming messages and not be notified via push.
- Push messages must not contain any message content, their function is merely to inform client systems that messages are available and that synchronisation with the home server is necessary.

[<=]

A_22965 – Messenger provider push notifications
TI-Messenger providers MUST ensure that push gateways use external push services in a data protection compliant manner. For this purpose, the following criteria are defined, which MUST always be observed:

- Push notifications may only take place after the explicit consent of users (opt-in).
- Push providers must be selected to ensure respect for data subjects' rights in accordance with the GDPR.

[<=]

A_22818 – Minimise security risks of software libraries
TI-Messenger specialist service manufacturers MUST implement measures to minimise the impact of undetected vulnerabilities in used software libraries.
[<=**]**

Note on A_22818: Example measures can be found in [OWASP Proactive Control#C2]. The selected method MUST have the same effectiveness as the encapsulation according to [OWASP Proactive Control#C2 Point 4].

A_22810 – Deviations from Matrix standard
TI-Messenger specialist service manufacturers MUST document and justify any deviations from the Matrix protocol or the MUST or SHOULD recommendations of the Matrix protocol that are not described in the TI-Messenger specification.
[<=]

Note on A_22810: This only refers to actual deviations from settings of the Matrix specification and not to additional functions that build on the TI-Messenger service and are product-specific.

A_22812 – Interoperability of additional functions for the TI-Messenger specialist service
TI-Messenger specialist service manufacturers MUST ensure that all implemented functions that go beyond the normal functionality of a TI-Messenger component do not endanger product safety and ensure interoperability with other TI-Messenger products.
[<=]

A_22928 – Use of trained administrators for Org Admins
TI-Messenger providers MUST deploy personnel as administrators who have been trained and sensitised for the related tasks and topics of information security. Providers MUST technically ensure that only authorised administrators have administrative access to the messenger services to be managed.
[<=]

A_22816 – Device verification, cross-signing and SSSS for TI-Messenger specialist services
TI-Messenger manufacturers MUST ensure that the Cross-Signing and Secure Secret Storage and Sharing (SSSS) functions for device verification are supported by the specialist service. The specification regarding end-to-end encryption MUST be fully followed.
[<=**]**

4.2 Authentication

An actor in the "Org Admin" role MUST authenticate themselves against the registry service via the front end of a registration service with the identity (SMC-B) of the organisation provided by the TI-Messenger provider in order to register one or more messenger services for their organisation. To authenticate the organisation towards the registration service, the OpenID Connect or KIM procedures described in the following section MAY be used.

4.2.1 Authentication procedure for registering a messenger service

4.2.1.1 OpenID Connect

In the OpenID Connect procedure, the gematik central IDP service is required to authenticate an organisation at the registration service and to allow service providers write access to the VZD-FHIR directory via their TI-Messenger clients. For this, the registration service and the TI-Messenger clients MUST be registered at the central IDP service of gematik according to [gemSpec_IDP_FD]. These MUST trust the issued SecurityToken (ID_TOKEN) of this IDP service.

When registering the VZD-FHIR directory on the central IDP service, necessary claims for the ID_TOKEN (confirmed identification features for the actor) are defined. The provider of the TI-Messenger MUST agree on the following claims in the ID_TOKEN via an organisational process at the central IDP service:

Table 1: Content of claims for SMC-B/HBA

Service provider institutions (SMC-B)	Service providers (HBA)
• `ProfessionOID` • `idNumber` • `OrganizationName` • `acr` • `aud`	• `ProfessionOID` • `idNumber` • `given_name` • `family_name` • `acr` • `aud`

The `ProfessionOID` indicates which type of service provider (e.g. doctor, dentist, etc.) is involved. The `idNumber` contains the telematics ID for healthcare organisations and providers.

Note: Detailed explanations of the authentication procedures are described in [api-messenger] in a specific how-to.

4.2.1.2 KIM procedure

When authenticating via the KIM procedure, both the TI-Messenger provider and the organisation wishing to participate in the TI-Messenger service MUST have functioning KIM accounts. A valid SMC-B Org and a KIM installation are required to use the KIM procedure.

The actor in the "Org Admin" role is prompted in the order process to enter their KIM email address in an input mask. The `TelematicsID` and the `ProfessionOID` MUST then be retrieved for the specified KIM address in the directory service (e.g. in the LDAP VZD according to gemSpec_VZD). Subsequently, the registration service MUST check whether the `ProfessionOID` belongs to a healthcare organisation. The registration service sends the organisation a KIM message with a URL to the specified KIM address after a positive check result and requests that the actor in the "Org Admin" role read the KIM message and open the URL it contains. To ensure that the same actor who started the registration is the one calling the URL, the registration service MUST display a random six-digit code, which MUST be checked when calling the URL. In case of a negative check result, the registration service MUST display a meaningful error message. By following the link, the actor is taken back to the ordering process, enters the previously displayed code and the authentication is completed. Decoding the KIM message and entering the six-digit code proves that this is the applying healthcare organisation.

4.2.2 Preventing unauthorised registration of a messenger service

Proof of possession of an SMC-B in the course of authenticating an organisation in the registration service is a necessary criterion for the associated process to be initiated at all. However, as the proof of an SMC-B in both of the aforementioned procedures is not necessarily provided by someone who is also authorised to register a messenger service within the service provider institution, the provider MUST take measures that prevent the fulfilment of an unauthorised order.

A_23521 – Prevention of unauthorised registration
The TI-Messenger provider MUST establish an organisational or technical process to prevent the successful registration of a messenger service by an unauthorised actor.**[<=]**

Example: In order to ensure that only those orders that have been carried out willingly and with authority lead to the successful registration and commissioning of the messenger service, the provider could establish a downstream process based on the receipt of an order that provides for a postal confirmation with the SPI. This would address the body that is authorised to decide on the legitimacy of the order.

4.2.3 Authentication of actors on the messenger service

To allow actors to exchange ad-hoc messages, they MUST authenticate themselves with their messenger service. Authentication MUST take place via a process agreed between the organisation and the provider. If the actors have been successfully authenticated in their messenger service, they will receive a Matrix ACCESS_TOKEN issued by their home server, which will be used for the subsequent authentication of the TI-Messenger client.

4.2.3.1 User session management

The user session MUST be managed as described in the Matrix specification.

4.2.3.2 2-factor authentication

The TI-Messenger service MUST enforce at least 2-factor authentication to authenticate the actors. The second factor MUST meet the security recommendations of the BSI according to [BSI 2-factor] for resilience against attacks remotely, at least with medium rating. The provider MUST ensure that at least one authentication using OIDC authenticator is supported and that technical options are provided for the organisation so that both factors cannot be compromised by an attack vector.

4.3 DNS name resolution

For the name resolution of the external interfaces provided by the TI-Messenger specialist service, DNS servers are used on the internet. The agreed query record MUST be provided by the respective TI-Messenger provider and MUST be entered in public DNS servers.

If a name related to the organisation's domain is chosen when using a messenger service for an organisation, the necessary DNS records are entered on DNS servers on the internet by the organisation's administration.

4.3.1 Identifying messenger services

Each messenger service MUST be identified by a Matrix home server name consisting of a host name and an optional port. For more information, refer to [Server-Server API#Server discovery].

4.4 Test

Product testing to ensure compliance with the specification is entirely the responsibility of the suppliers/manufacturers of the TI-Messenger client. During approval, gematik focuses on the interaction of the products through E2E and IOP tests.

The independent product tests at the industrial partners include:

- Develop test environment,
- Create test case catalogue (for own product tests), and
- Perform and document product test.

The manufacturers of the TI-Messenger specialist services MUST assure that gematik can check the product tests of the industrial partners in the form of reviews of test concepts, test specifications, test cases and with the review of the test protocols (log and trace data).

Gematik promotes close cooperation and helps industrial partners to improve the quality of products. This is done by organising timely IOP tests, synchronising milestones and regular cross-industry test sessions. The test sessions include mutual IOP and E2E testing.

gematik provides a TI Messenger service reference implementation. To ensure interoperability between different TI-Messenger specialist services within the TI-Messenger service, the TI-Messenger specialist service of a TI-Messenger provider MUST be tested against the reference implementation (TI-Messenger client and TI-Messenger specialist service).

ML-124200 – Test of TI-Messenger specialist service against reference implementation
The manufacturer of the TI-Messenger specialist service MUST successfully test the specialist service against the reference implementation. The test results are to be submitted to gematik.
[<=]

For the provider approval, TI-Messenger specialist services and TI-Messenger clients MUST be provided by the TI-Messenger provider. To enable an automated test for the TI-Messenger service, the test app of the TI-Messenger client MUST also provide a test driver module internally or externally. This MUST make the functionality of the product-specific interface of the TI-Messenger client accessible from the outside via a standardised interface and allow remote access. The test driver module may process the output of the TI-Messenger client according to the technical interface, but must not corrupt the content. A detailed description of the test procedure can be found in [gemSpec_TI_Messenger-Client].

gematik tests on the basis of use cases as part of the approval process. Reference is made to the use cases from the [gemSpec_TI-Messenger service]. An attempt is made to include as many functional areas of the components of the TI-Messenger service as possible. The tests are first carried out against the reference implementation of gematik. In this step, the functionality of the TI-Messenger services approval object is checked. The IOP and E2E tests then demonstrate interoperability between the different providers. For this purpose, all already available TI-Messenger services (the test instances of individual manufacturers) are then merged and tested against each other. All providers MUST perform this IOP and E2E testing independently and on their own responsibility in advance. In case of approval problems, suppliers MUST assist in the analysis.

4.5 Operation

The operation of the specialist service is the responsibility of the TI-Messenger provider. According to the operating concept [gemKPT_Betr#Provider constellations], operation MAY also be outsourced to subcontractors or hosted on-premise. However, the coordination of the respective components and the fulfilment of the requirements remain the responsibility of the provider. The latter MAY conclude contracts in coordination with its users and service providers in order to maintain safe operation.

Requirements for performance and reporting can be found in the corresponding product and provider type profiles in the [gemSpec_Perf] and [gemKPT_Betr] documents, among others.

4.5.1 Monitoring and operational control

The TI-Messenger provider MUST provide technical and organisational support for gematik's service monitoring.

For this, it may be necessary, for example, to set up corresponding accounts on home servers. The service monitoring SHOULD not lead to any technical changes of the products.

A_23092 – TI-M organisation validation review on VZD-FHIR directory
At least every 24 hours, the TI-Messenger specialist service MUST check for all organisations with a messenger service registered with it, whether they are entered in the VZD-FHIR directory as "`active`"(Organization.active).
[<=]

A_23093 – TI-M information to users in case of deregistered organisation on VZD-FHIR directory
If the organisation is no longer "`active`" (Organisation.active) in the VZD-FHIR directory, the TI-Messenger provider MUST inform it of this.
[<=]

A_23094 – TI-M blocking of the organisation with invalid SMC-B
If the organisation is not "`active`" (Organisation.active) in the VZD FHIR directory for more than 30 calendar days, the TI-Messenger provider MUST delete the domain of this messenger service from the federation (see FHIR-VZD: I_VZD_TIM_Provider_Services, DELETE /federation/{domain}). The service MAY then only be used again after re-authentication with the SMC-B, see AF_10103.
[<=]

4.5.2 Controlled decommissioning

If, for example, the contractual relationship between the customer and the TI messenger provider expires, the TI messenger provider MUST delete the associated domain of this messenger service from the federation (see FHIR-VZD: I_VZD_TIM_Provider_Services, DELETE /federation/{domain}) and shut down the messenger service so that it can no longer be accessed.

5 Functional features

The following section provides a functional description of the TI-Messenger service in relation to its subcomponents. The TI-Messenger specialist service is the core component of the TI-Messenger service. It provides all interfaces required for communication within the TI-Messenger service.

In the following figure, the TI-Messenger specialist service is shown as a white box:

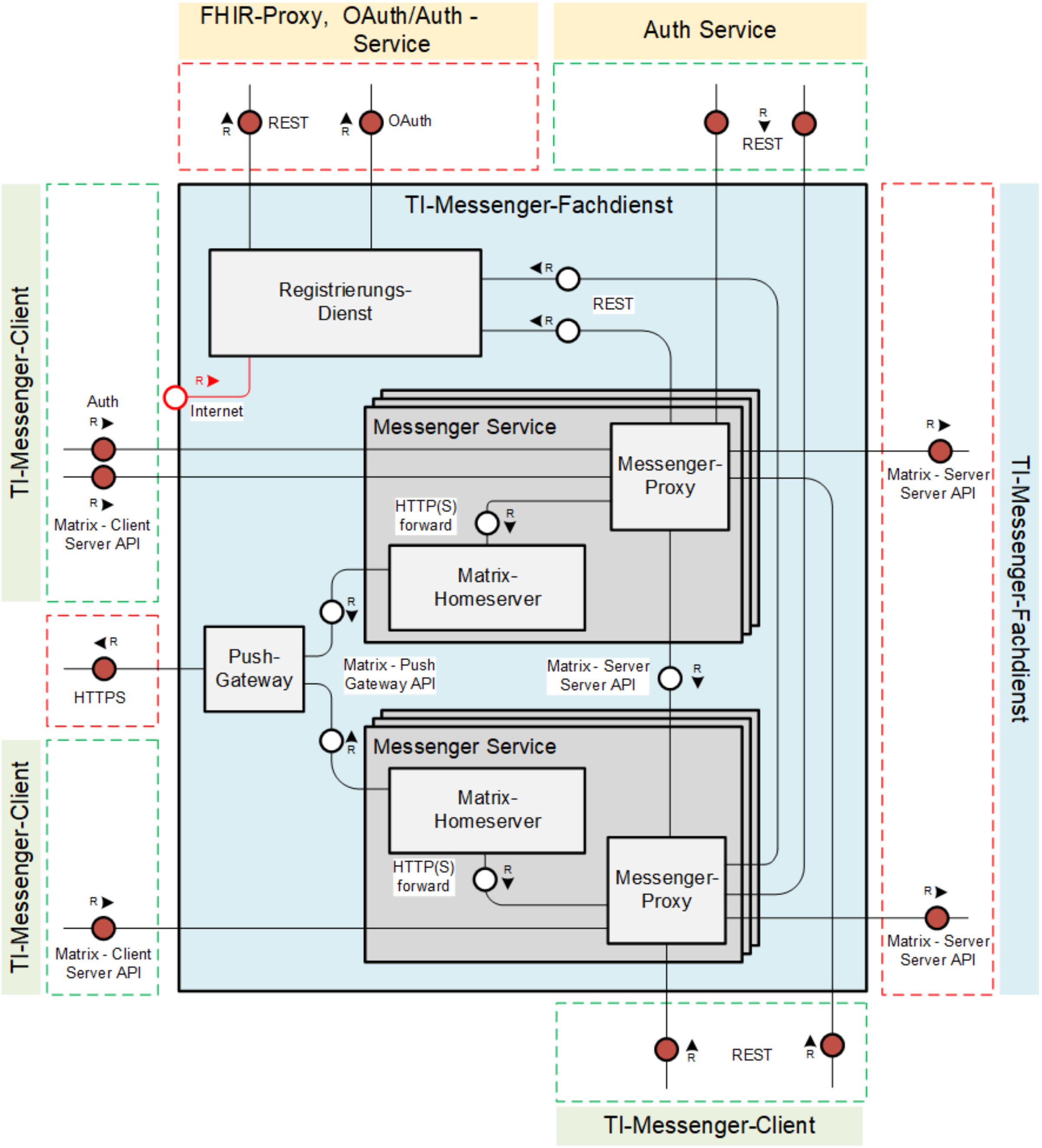

Figure 3: Functional structure of the TI-Messenger specialist service

The boxes shown in green in the figure indicate the interfaces that are called up on the TI-Messenger specialist service. Boxes shown in red show the interfaces via which the TI-Messenger specialist service uses further services of other components. One exception is communication between the TI-Messenger specialist services. Here the communication is carried out bilaterally between the specialist services of the TI federation. The line from the registration service to the internet, shown in red in the figure, indicates the interface used by the front end of the registration service or the interface used by the TI-Messenger client with Org Admin functionality to administer or issue a RegService OpenID token. This is not normatively defined by gematik. The design is the responsibility of the respective TI-Messenger provider.

5.1 Functions of the system components

In the following section, all components necessary for the operation of the TI-Messenger specialist service are described functionally.

5.1.1 Registration service

The registration service offers three interfaces. The following figure shows the interfaces provided (green) and used (red):

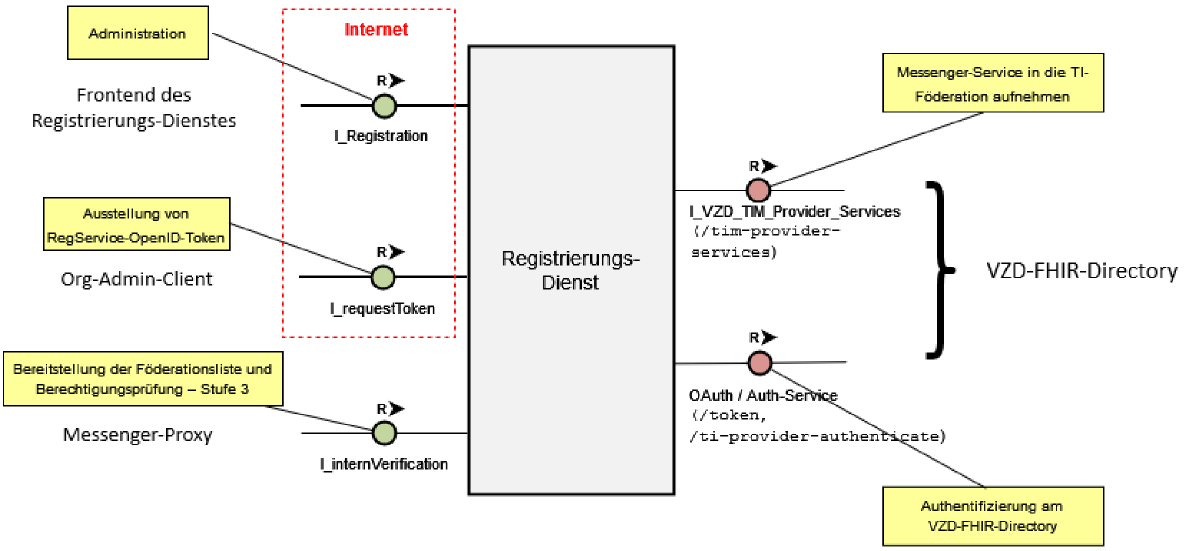
Administration
Internet
Frontend des Registrierungs-Dienstes
R
I_Registration
Ausstellung von RegService-OpenID-Token
Org-Admin-Client
R
I_requestToken
Bereitstellung der Föderationsliste und Berechtigungsprüfung – Stufe 3
Messenger-Proxy
R
I_internVerification
Registrierungs-Dienst
Messenger-Service in die TI-Föderation aufnehmen
R
I_VZD_TIM_Provider_Services
(/tim-provider-services)
VZD-FHIR-Directory
R
OAuth / Auth-Service
(/token, /ti-provider-authenticate)
Authentifizierung am VZD-FHIR-Directory

Figure 4: Overview of the interfaces at the registration service

Note: The interface `I_internalVerification` shown in the figure is an abstract internal interface at the registration service with which the messenger proxies are provided with several functionalities. The implementation of the functionalities to be provided (provision of the federation list and authorisation check – Stage 3) on the registration service can also be done via separate interfaces. The two interfaces `I_Registration` and `I_requestToken` are the interfaces that the TI-Messenger provider MUST offer on the internet. These are not normatively specified by gematik.

5.1.1.1 Interfaces

The following sections describe the interfaces that the registration service MUST provide and call.

5.1.1.1.1 I_Registration

The TI-Messenger specialist service MUST provide an interface for administration on the registration service. This is necessary to ensure an onboarding process for the registration of messenger services. The registration service MUST allow the creation of a new messenger service from a front end of the registration service. The design of the front end as well as the interface at the registration service (`I_Registration`) is left to the respective TI-Messenger provider.

5.1.1.1.2 I_requestToken

The TI-Messenger specialist service MUST provide an interface for issuing an ID_TOKEN (RegService OpenID token) on the registration service. The token is required for authentication at the FHIR proxy of the VZD-FHIR directory so that an actor in the "Org Admin" role can change organisational entries. The design of the interface at the registration service (`I_requestToken`) is left to the respective TI-Messenger provider. The registration service MUST ensure that a token is only issued to authenticated actors in the "Org Admin" role. The validity of the RegService OpenID token MUST be less than or equal to one hour.

5.1.1.1.3 Structure of the RegService OpenID token

The RegService OpenID token is a JSON web token and MUST contain the following attributes:

```
HEADER
{
  "alg": "BP256R1",
  "typ": "JWT"
  "x5c": [
     "<X.509 Sig-Cert, base64-encoded DER>" ]
}
PAYLOAD
{
  "sub": "1234567890",
  "iss": "<url of the registration service endpoint via which the token was
issued>",
  "aud": "<url of the owner-authenticate endpoint on the VZD-FHIR directory>",
  "professionOID": "<ProfessionOID of the organisation>",
  "idNummer": "<TelematicsID of the organisation>",
  "iat": "1516239022",
  "exp": "1516242622"
}
```

5.1.1.1.4 Signature of the RegService OpenID token

For the signature of the RegService OpenID token, the private key of the certificate C.FD.SIG MUST be used. The certificate is requested by means of a TI-ITSM service request. Before the certificate expires, a new one MUST be requested and the new certificate transferred to the VZD-FHIR directory.

5.1.1.1.5 I_internalVerification

The registration service MUST provide an interface for providing and updating the federation list and checking for MXID entries in the VZD-FHIR directory. The design of the interface at the registration service (`I_internalVerification`) is left to the respective TI-Messenger provider.

5.1.1.1.6 Provision and updating of the federation list

The content of the federation list, which the registration service MUST provide to the messenger proxies via the interface, is all the Matrix domain names involved in the federation. The registration service MUST query the current TI federation list on the VZD-FHIR directory. For retrieval, the `getFederationList (GET /tim-provider-services/FederationList/federationList.jws)` operation provided at the FHIR proxy of the VZD FHIR directory MUST be called. When calling the interface, a provider-accesstoken MUST be included. Optionally, the currently used version can also be included in the call. If the version is transferred, then a new federation list is only provided by the VZD-FHIR directory in the case of an outdated version. The federation list MUST be queried every hour. The check for up-to-datedness of the federation list of the registration service MUST also be performed with each request by a messenger proxy to provide the federation list via a query to the FHIR proxy of the VZD-FHIR directory, provided that the federation list held by the registration service is older than an hour. The check for up-to-datedness takes place through comparison of the versions of the federation lists. Upon receipt of a new federation list from the VZD-FHIR directory, the registration service MUST provide it to the messenger proxies to check federation membership via the `I_internalVerification` internal interface.

The registration service MUST check the up-to-datedness of the federation list on the VZD-FHIR directory regularly every hour. If the VZD-FHIR directory is not accessible within a defined response time and further(`HealthState_VZD` and `HealthStateCheck_VZD`) update attempts are unsuccessful, the registration service MUST extend its own federation list retention time to a defined value of 72 hours(`TTL_Federationlist`) and generate an incident event which can be captured by a third party system (e.g. an ITSM system). If the federation list could not be updated after further update attempts, an incident MUST be raised with the VZD-FHIR directory provider. The present federation list SHOULD continue to be used until the incident is rectified, but for a maximum of 72 hours. After the expiry of this period, the messenger proxy must no longer allow communication with other Matrix home servers until an up-to-date federation list can be retrieved from the registration service again.

Note: Keeping an up-to-date federation list makes sense from a security perspective in order to keep the time window small in which a specialised service "unknowingly" interacts with another specialised service that is no longer part of the federation. The choice of a suitable period within which working with an old list is still acceptable because it could not be updated takes into account the expected time required for recovery if the VZD is not available and is not chosen more generously than the periods granted for other communication services within the TI.

The following table defines attributes and their types that MUST be maintained at the registration service:

Table 2: Specific attributes for handling the federation list at the registration service

Attribute	Type	Description	Value range
`HealthState_VZD`	State	Type maintains health status of VZD-FHIR directory components based on their response behaviour	[healthy, unhealthy]
`HealthStateCheck_VZD`	Incrementing iterator	Type holds the amount of retries of the VZD-FHIR directory health check	0<=HealthStateCheck_VZD<=3
`Age_FederationList`	Incrementing time counter	Type keeps the current age of the federation list from the time of the last update.	min: 0s
`TTL_FederationList`	Lifetime	Type describes the upper age limit of a federation list	Constant value: 72h

The attributes described here and their use are explained in sequence diagram [gemSpec_TI_Messenger-Service#Federation List Update]. As soon as a request to update the federation list is initiated by the messenger proxy at the registration service, the registration service MUST request the current list from the FHIR proxy if the list held by the registration service is too old (`Age_FederationList`). If the registration service list is not too old, its federation list MUST be delivered to the messenger proxy. However, this only happens if the list of the registration service is more up-to-date than that of the messenger proxy. If the messenger proxy receives a current federation list, a signature check MUST be performed locally using the supplied signature certificate. The signature certificate is the first element of the `x5c` certificate list transmitted together with the federation list.

5.1.1.1.7 Authorisation check – Stage 3

The registration service MUST provide a feature that allows checking for MXID entries in the VZD-FHIR directory. For this, the registration service MUST use the operation `whereIs (GET /tim-provider-services/localization)` at the FHIR proxy of the VZD-FHIR directory.

The test succeeds 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 test was successful, the registration service MUST pass the test result to the messenger proxy.

5.1.1.1.8 I_VZD_TIM_Provider_Services

For the inclusion of a messenger service of a TI-Messenger specialist service in the TI federation of the TI-Messenger service, the registration service MUST enter the Matrix domain of an organisation transferred from the front end of the registration service by calling the operation `addTiMessengerDomain (POST /tim-provider-services/federation)` on the VZD-FHIR directory. When calling the interface, a provider-accesstoken MUST be included.

5.1.1.1.9 OAuth / Auth service

Prior authentication using OAuth2 Client Credentials Flow is required to access the registration service on the VZD-FHIR directory via the `I_VZD_TIM_Provider_Services` (`/tim-provider-services`) interface of the FHIR proxy. The necessary client credentials MUST be requested from the TI-Messenger provider for its registration service from the VZD-FHIR directory provider. The application is made via a service request in the TI-ITSM system. After successful authentication, the registration service receives a provider access token, which MUST be included when calling the `/tim-provider-services` endpoint. The authentication process consists of the successive calls:

- `POST /auth/realms/TI-Provider/protocol/openid-connect/token` (Oauth service)
- `GET /ti-provider-authenticate` (Auth service)

With the first call, the client credentials are transferred; with the second call, a TI provider access token, which was received as a return value with the first call.

5.1.1.2 Provision of an Org Admin account

The steps described in the following sections are required to provide an Org Admin account.

5.1.1.2.1 Authenticating an organisation

When authenticating an organisation, the procedures mentioned in Section 4.2.1 – Authentication procedures for registering a messenger service MAY be used. These procedures are described below:

5.1.1.2.1.1 OpenID Connect
According to the OpenID Connect standard, a PKCE code challenge MUST be performed when generating an authorisation code. For this purpose, the registration service MUST generate the PKCE code and later redeem the verifier of this challenge together with the authorisation code at the central IDP service for an ID_TOKEN. The registration service MUST automatically validate the ID_TOKEN issued by the central IDP service for a new registration request. During validation, the registration service MUST check the `ProfessionOID` contained in the ID_TOKEN against the OIDs listed in the "Tab_PKI_403-x OID definition institutions in the X.509 certificate of SMC-B" table according to [gemSpec_OID].

5.1.1.2.1.2 KIM procedure
The front end of the registration service MUST offer the actor an input mask for the KIM address to be used. At the directory service (e.g. LDAP-VZD according to [gemSpec_VZD]) the `ProfessionOID` as well as the `TelematicsID` MUST be queried using the KIM address. The determined data set MUST then be provided to the registration service. These MUST be stored with the admin account details of that organisation. The registration service MUST check the `ProfessionOID` against the OIDs listed in the "Tab_PKI_403-x OID definition institutions in the X.509 certificate of SMC-B" table according to [gemSpec_OID]. The registration service MUST then generate a KIM message with a URL leading back to the ordering process. The URL MUST consist of the FQDN of the registration service and a unique ID (UUID) according to [RFC4122]. Additionally, the email header element `X-KIM-serviceindicator: Auth;Verification;V1.0` MUST be included in the KIM message. It MUST be apparent in the KIM message that this is an authentication mail. In addition to calling up the URL, the registration service MUST also check a six-digit PIN code, which was previously displayed on the order screen and is random.

5.1.1.2.2 Creating the administration account

After successful authentication of an organisation at the registration service, an admin account for the organisation MUST be created on the registration service. This MUST use a 2-factor authentication for authenticating the actor in the "Org Admin" role and take into account the security recommendations of BSI [BSI 2-factor]. To prevent attacks from a distance on the 2nd factor, a procedure that is rated at least "medium" must be selected. The provider MUST ensure that at least one authentication using an authenticator is supported and that technical options are provided for the organisation so that both factors cannot be compromised by an attack vector. If an admin account already exists for the organisation, a new initial authentication of the organisation using the SMC-B MUST NOT be possible for this organisation and MUST NOT result in the creation of another admin account or the overwriting of the previous one.

The admin account allows an actor in the "Org Admin" role to register one or more messenger services for their organisation. The Matrix domain transferred in the registration request for a domain MUST be entered into the federation by the registration service via the interface `I_VZD_TIM_Provider_Services` according to [VZD_Provider_Services#Version 1.3.0] on the VZD FIR proxy. Likewise, the registration service MUST transfer the created Matrix domain to the front end of the registration service for access to the requested messenger service

5.1.2 Messenger service

A messenger service consists of the Matrix home server subcomponents and messenger proxy. The Matrix home server subcomponent is based on the Matrix open communication protocol. The messenger proxy serves as an inspection instance and forwards requests to the Matrix home server. The following figure shows which APIs of the Matrix specification are used in the messenger service:

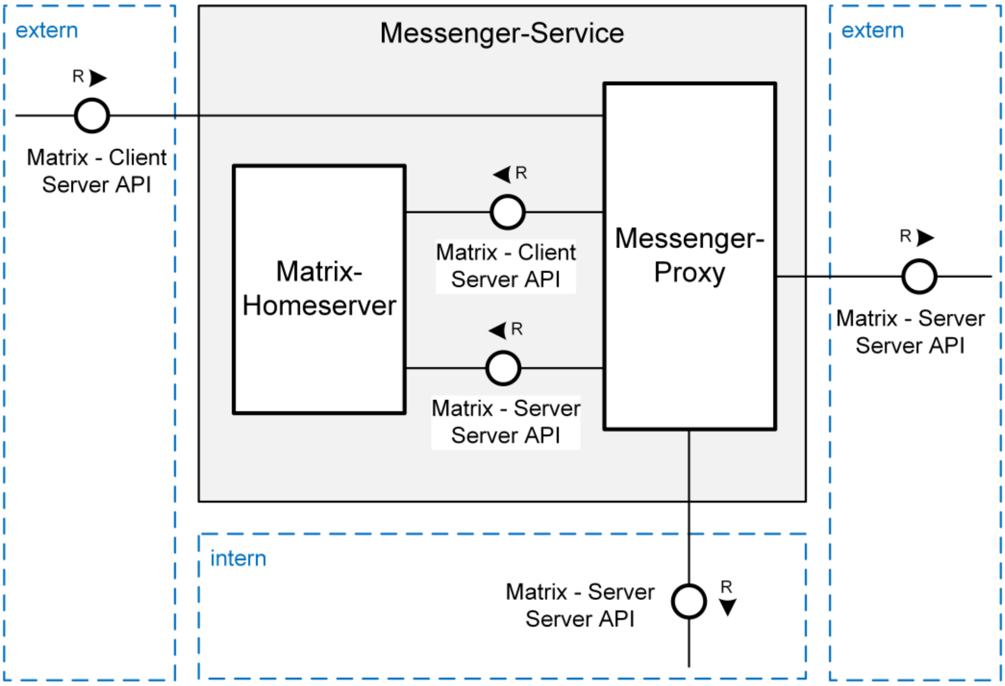
extern
Messenger-Service
extern
R
Matrix - Client Server API
R
Matrix-Homeserver
Matrix - Client Server API
Messenger-Proxy
R
Matrix - Server Server API
R
Matrix - Server Server API
intern
Matrix - Server Server API
R

Figure 5: Matrix API of messenger service

The "*Matrix API of messenger service*" figure shows the Matrix APIs to be considered (server API and client server API). These MUST be implemented in accordance with

- [Server-Server API] and
- [Client-Server API].

The client server API on the Matrix home server MUST always be called using the messenger proxy. The messenger proxy takes on the task of a reverse proxy. It forwards all calls of the TI-Messenger clients authorised by it to the Matrix home server. The communication of the Matrix home servers via the server-server API MUST also take place via the messenger proxy. Here, the proxy MUST assume the function of a forward proxy (sender side) as well as a reverse proxy (receiver side). To send push notifications, the Matrix home server MUST use the Matrix Push Gateway API of the push gateway.

In addition to acting as a proxy for forwarding all server-server API and client-server API calls to the Matrix home server, the messenger proxy acts as a control instance for checking the rights required for communication. For this, the messenger proxy MUST be used for all server-server and client-server API endpoints.

Messenger services MAY be provided decentralised or *on-premise* by a TI-Messenger provider. If several Matrix domains are operated by a TI-Messenger provider in a common messenger service, the logical separation of the Matrix domains MUST be ensured.

5.1.2.1 Messenger proxy

The messenger proxy MUST be provided for each messenger service as a forward and a reverse proxy. If several Matrix domains are operated by a TI-Messenger provider in a common messenger service, the logical separation of the Matrix domains MUST be ensured. The Matrix Server Server API (server-server communication) and Matrix Client Server API (client-server communication) related checks MAY be logically implemented in the messenger proxy. The type of implementation is left to the TI-Messenger specialist service manufacturer. The functionality of the messenger proxies is described below.

5.1.2.1.1 TLS scheduling

All requests from TI-Messenger clients and other messenger services to the Matrix home server MUST be routed via the messenger proxy (in the function of reverse proxy). TLS communication between TI-Messenger clients and the Matrix home server MUST be scheduled on the messenger proxy. The protection of the TLS communication MUST be ensured by a one-sided server authentication using an X.509 certificate.

5.1.2.1.2 Checking the used client

The messenger proxy MUST check whether the request is made by a permitted TI-Messenger client. The verification is done on the basis of the transferred parameter `client_id` of the TI-Messenger client. To check the `client_id` , it MUST be previously transmitted from the TI-Messenger client manufacturer to the TI-Messenger provider.

5.1.2.1.3 HTTP(S) forwarding

All TLS connections that are forwarded via the messenger proxy MUST be broken down by it. The communication of the Matrix home server with the internet MUST always take place via its own messenger proxy (in the function as a forward proxy). Forwarding MAY be done via both HTTP and HTTPS, but HTTP MUST NOT be used if the communication between the Matrix home server and messenger proxy uses untrusted infrastructure.

5.1.2.1.4 Interface for authentication procedure

For an organisation to use its own authentication service, the messenger proxy MUST provide an interface to connect to the organisation's authentication service. The implementation of this interface MUST be coordinated by the organisation and the respective TI-Messenger provider.

5.1.2.1.5 Federation list

The messenger proxy MUST retrieve the federation list from its responsible registration service via the internal interface `I_internalVerification`, check the signature of the federation list according to RFC7797 and store it locally. To verify the signature of the federation list, the signature certificate (public key) contained in the signature header and the X.509 root CA certificate of the TI are required. The X.509 root CA certificate MUST be stored in the messenger proxy truststore. The structure of the federation list is described in [gemSpec_VZD_FHIR_Directory#Generation and provision of the federation list].

Note: Gematik plans to provide an OCSP responder for checking the certificate status on the internet. As soon as this is available, it MUST be used additionally for the check.

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

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

```
{
  [
    {
      "name" : "RCA1",
      "CN" : "GEM.RCA1",
      "cert" : "…base64…",
      "prev” : "",
      "next" : "….base64…",
      "SKI" : "Subject key identifier as hex value"
    },
    {
      "name" : "RCA2",
      …
    },
    {
      "name" : "RCA3",
      …
    },
    …
   ]
}
```

5.1.2.1.6 Provision and administration of the release list

The messenger proxy MUST keep a release list (e.g. in the form of a lookup table). The release list is used to check whether an incoming `Invite` event is approved on the messenger proxy (see Authorisation check – Stage 2). The messenger proxy MUST implement the `I_TiMessengerContactManagement` interface as REST web service via HTTPS according to [api-messenger#TiMessengerContactManagement.yaml] version 1.0.0. It MUST also be possible for the actor to administer the release list via their TI-Messenger client. In addition, the messenger proxy MUST ensure that expired releases are removed from the release list.

5.1.2.1.7 *Exemption rules*

The messenger proxy MUST allow exemption rules to be defined. This is necessary so that requests are not rejected by the messenger proxy's authorisation check. Thus, the messenger proxy MUST allow the VZD-FHIR directory access to the `/_matrix/federation/v1/openid/userinfo` endpoint of the Matrix home servers. Further exemption rules could be defined for monitoring/reporting, for example.

5.1.2.1.8 *Implementation of check rules*

The messenger proxy MUST support the authorisation concept according to [gemSpec_TI_Messenger service#Authorisation concept]. The messenger proxy MUST check the content of the request to the Matrix home server. The type of check depends on whether it is client-server or server-server communication. The inspection rules are described below.

5.1.2.1.8.1 *Check rules for client-server communication*

The messenger proxy MUST support check rules for client-server requests. In this case, the messenger proxy must check the content of the request to the Matrix home server as follows at each `Invite` event according to [Client-Server API#Room membership].

5.1.2.1.8.1.1 Stage 1 – TI federation membership check

In this step, the messenger proxy MUST check if the Matrix domain in the `Invite` event is part of the TI federation. For this, the messenger proxy MUST check in its local federation list whether the Matrix domain is included in it. If this is not the case, then the messenger proxy MUST get an up-to-date list from its responsible registration service via the internal interface `I_internalVerification`. If the subsequent rechecking failed, the messenger proxy MUST reject the request. If the check is successful, then the messenger proxy MUST forward the `Invite` event to the inviting Matrix home server. If the check is unsuccessful, the messenger proxy MUST return the following JSON object to the TI-Messenger client:

```
Responsecode 403
{
  "errcode": "M_FORBIDDEN",
  "error": "<Matrix-Domain> could not be invited"
}
```

In the case of a successful federation test, the `Invite` event is processed by the Matrix home server. This checks whether the sender and receiver Matrix domain are the same. If this is the case, then the actors are on the same messenger service and the actor to be invited is invited to a shared chat room. If the Matrix domains of the sender and receiver do not match the Matrix domain of the messenger service, the `Invite` event is forwarded by the Matrix home server to the responsible messenger proxy of the recipient to be invited. Here, the messenger proxy MUST use the check rules of the server-server communication.

5.1.2.1.8.1.2 Further check rules for client-server communication

In addition to federation affiliation, the messenger proxy MUST support other check rules. The messenger proxy MUST check the content of the request to the Matrix home server at each `createRoom` event according to [Client-Server API#Rooms]. Here, the messenger proxy MUST check whether the "`invite`" attribute contained in the event is filled with a maximum of one element. If the check is unsuccessful, the messenger proxy MUST return the following JSON object to the TI-Messenger client:

```
Responsecode 400
{
   "errcode": "M_FORBIDDEN",
   "error": An error occurred when starting communication. Please contact your
administrator."
}
```

5.1.2.1.8.2 Check rules for server-server communication

The messenger proxy MUST support check rules for server-server requests and MUST check the content of the request for each event. For incoming server-to-server requests from other messenger proxies, the messenger proxy MUST forward these to the responsible Matrix home server, in order that the latter may perform the authentication according to [Server-Server API#Request Authentication]. The inspection rules are described below.

5.1.2.1.8.2.1 Stage 1 – TI federation membership check

In the 1st stage, the messenger proxy MUST check, for each outgoing and incoming event, whether the Matrix domain is part of the TI federation. To check the federation affiliation, the messenger proxy MUST, according to [Server-Server API#Request Authentication], check the domain contained in the Authorisation header attribute "`origin`" for incoming communication and in the Authorisation header attribute"`destination`" for outgoing communication, against the domains in its local federation list. If the check failed, then the messenger proxy MUST get an up-to-date list from its responsible registration service via the internal interface (`I_internalVerification`). If the subsequent rechecking failed, the messenger proxy MUST reject the request with the following JSON object:

```
Responsecode 403
{
   "errcode": " M_FORBIDDEN ",
   "error": "The other party could not be contacted"
}
```

If the check is successful, the messenger proxy MUST forward the event to the Matrix home server. If it is an `Invite` event, then further verification MUST be performed according to stage 2.

5.1.2.1.8.2.2 Stage 2 – Release list check

In the second step, the messenger proxy MUST check if the MXID of the inviter is present in the share list of the actor to be invited. For this, the messenger proxy MUST check by querying its release list whether there is a corresponding release for the inviter. If the check is successful, then the messenger proxy MUST forward the `Invite` event to the Matrix home server. If this is not the case, the verification MUST be done as per Stage 3.

5.1.2.1.8.2.3 Stage 3 – Check for existing VZD-FHIR directory entry

In the third step, the messenger proxy MUST check whether the MXIDs of the actors involved are included in the VZD-FHIR directory. For this, the messenger proxy MUST call the internal interface `I_internalVerification` at its responsible registration service. If the verification is successful (true), the messenger proxy MUST forward the `Invite` event to the Matrix home server. If the verification is not successful, the `Invite` event MUST be rejected.

5.1.2.2 Matrix home server

The Matrix home server MUST implement [Server-Server API] and [Client-Server API] according to the Matrix specifications in version v1.3.

The Matrix home server of a messenger service:

- MUST accept requests from its own messenger proxy and
- MUST NOT accept requests from other messenger proxies and MUST NOT be reachable by other messenger proxies.

The authentication procedures used by the Matrix home server MUST be configurable. When a new actor attempts to log in to a Matrix home server, it MUST offer all authentication methods supported for that organisation for selection. After a successful login of an actor to a Matrix home server, it provides a Matrix ACCESS_TOKEN it has created and a matrix OpenID token (see [gemSpec_TI-Messenger service#How to use the token]). In the future, the Matrix ACCESS_TOKEN will be used for every further authorisation on the Matrix home server. The issued Matrix OpenID token is used for later authentication at the Auth service of the VZD-FHIR directory to obtain a search-accesstoken for read access in the VZD-FHIR directory.

5.1.2.2.1 Server discovery

The Matrix home server MUST support server discovery according to [Server-Server API#server-discovery]. To this end, the TI-Messenger provider MUST provide the endpoint `/.well-known/matrix/` and use it to return the host name and port at which the Matrix home server can be reached.

5.1.2.2.2 Public rooms

The Matrix home server MUST allow public rooms to be created. In contrast to private rooms, end-to-end encryption MUST not be used.

5.1.2.2.3 Custom room types and custom state events

The Matrix home server MUST be able to accept the following *custom room types* as well as the following *event types* of the *custom state events* without evaluating them, rejecting them or reacting to them with an error message:

- Custom Room Types
  - `de.gematik.tim.roomtype.casereference.v1`
  - `de.gematik.tim.roomtype.default.v1`
- Custom State Events
  - `de.gematik.tim.room.casereference.v1`
  - `de.gematik.tim.room.default.v1`

- `de.gematik.tim.room.name`
- `de.gematik.tim.room.topic`

The creation of *custom room types* and *custom state events* of these *event types* MUST NOT result in the definition of a new or customised Matrix room version. Existing room definitions MUST be fully preserved according to the Default Room Version of the applicable Matrix protocol version. The *custom state event* of this *event type* MUST be compatible with its root event `(m.room.create`).

ML-123905 – Implementation of BSI specifications for server (product)
The TI-Messenger specialist service SHOULD follow the specifications of [BSI-ISI-Server].
[<=]

ML-123956 – Implementation of BSI specifications for server (provider)
The TI-Messenger provider SHOULD follow the specifications of [BSI-ISI-Server].
[<=]

ML-132863 – Accessibility of the Matrix home server
The Matrix home server can only be reached via its associated messenger proxy.
[<=]

5.1.3 Push gateway

The TI-Messenger specialist service MUST provide a push gateway, according to [Matrix Specification#Push Gateway API], for the TI-Messenger client. It is up to the TI-Messenger providers whether a push function is supported.

6 Annex A – Directories

6.1 Abbreviations

Abbreviation	Explanation
API	Application Programming Interface
CC	Common Criteria
GDPR	General Data Protection Regulation
FHIR	Fast Healthcare Interoperable Resources
HBA	Health Professional Card
HTTP	Hypertext Transfer Protocol
IDP	Identity Provider
JSON	JavaScript Object Notation
MXID	Matrix User ID
OAuth	Open Authorisation
Opt-in	Disabled with option to activate
OWASP	Open Web Application Security Project
SMC-B	Institution card (Security Module Card Type B)
SSSS	Secure Secret Storage and Sharing
TI	Telematics infrastructure
TI-ITSM	IT Service Management of TI
TI-M	TI Messenger
TLS	Transport Layer Security
VZD	Directory service

6.2 Glossary

Term	Explanation
MXID	Unique identification of a TI-Messenger user (Matrix user ID)
On-premise	The product is operated on own or leased hardware
Relying party	Trusted component that enables access to a secure application
X.509 certificate	A public key certificate according to the X.509 standard

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

6.3 List of figures

6.4 List of tables

6.5 Referenced documents

6.5.1 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
[gemGlossary]	gematik: Introduction of health card – glossary
[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_IDP_FD]	gematik: Identity Provider specification – Specialist services usage specification
[gemSpec_Krypt]	gematik: General specification Use of cryptographic algorithms in telematics infrastructure
[gemSpec_OID]	gematik: Definition of OIDs specification
[gemSpec_Perf]	gematik: Broad specification performance and quantity scaffold TI platform
[gemSpec_SST_LD_BD]	gematik: Specification log data and operating data recording
[gemSpec_TI_Messenger-Client]	gematik: TI-Messenger client specification
[gemSpec_TI_Messenger-Service]	gematik: TI-Messenger service specification
[VZD_Provider_Services]	gematik: api-vzd https://github.com/gematik/api-vzd/blob/main/src/openapi/I_VZD_TIM_Provider_Services.yaml

6.5.2 Other documents

[Source]	Publisher (publication date): Title
[BSI 2-Faktor]	BSI 2-Faktor Authentisierung für mehr Datensicherheit 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
[BSI ORP.4]	BSI ORP.4: Identitäts- und Berechtigungsmanagement (Stand Februar 2021) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2021.html
[Client-Server API]	Matrix Foundation: Matrix Specification - Client-Server API https://spec.matrix.org/v1.3/client-server-api/
[Matrix Specification]	Matrix Foundation: Matrix Specification https://spec.matrix.org/v1.3/
[OpenID]	OpenID Foundation https://openid.net/developers/specs/
[OWASP Proactive Control]	OWASP Proactive Controls https://owasp.org/www-project-proactive-controls/
[ROOT-CA]	ROOT-CA Download Punkt https://download.tsl.ti-dienste.de/ECC/ROOT-CA/
[ROOT-CA-JSON]	ROOT-CA Download Punkt als JSON-Datei https://download.tsl.ti-dienste.de/ECC/ROOT-CA/roots.json
[Server-Server API]	Matrix Foundation: Matrix Specification - Server-Server API https://spec.matrix.org/v1.3/server-server-api/