

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation TI-Messenger Pro

Version: 1.~~0.2~~1.0 CC
Revision: 1~~73943~~397370
Stand: ~~12.03~~14.10.2025
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich Entwurf
Referenzierung: gemSpec_TI-M_Pro

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	13.11.2024		initiale Erstellung	gematik
1.0.1	09.12.2024		Update TI-Messenger_24_2-1	gematik
1.0.2	12.03.2025		Einarbeitung Patch TI-Messenger_25_1-2	gematik
<u>1.1.0 CC</u>	<u>14.10.205</u>		<u>Einarbeitung TI-Messenger 25 3 - zur Abstimmung freigegeben</u>	<u>gematik</u>

Inhaltsverzeichnis

1 Einordnung des Dokumentes	5
1.1 Zielsetzung	5
1.2 Zielgruppe	5
1.3 Geltungsbereich	5
1.4 Abgrenzungen	5
1.5 Methodik	6
2 Systemüberblick	7
2.1 Akteure und Rollen	7
2.1.1 Akteur: Chatbot	7
2.1.2 Rolle: "Org Admin"	7
2.1.3 Rolle: "User HBA"	7
2.2 Nachbarsysteme	8
2.2.1 VZD-FHIR-Directory	8
2.3 Zugriffstoken	8
3 Zerlegung des Produkttyps	10
3.1 TI-M-Client-Pro	10
3.1.1 Ausprägungen nach Nutzergruppen	10
3.1.1.1 TI-M-Client-Pro für Akteure in der Rolle "Org Admin" (Org Admin-Client)	10
3.1.2 Ausprägungen nach Plattform	10
3.1.2.1 TI-M-Client als Web-Anwendung	10
3.1.3 Matrix-Spezifikation	11
3.1.3.1 Weitere Ergänzungen/Einschränkungen zur Matrix-Spezifikation	11
3.1.4 VZD-FHIR-Directory	11
3.1.4.1 Schreibzugriff	11
3.1.5 Sichtbarkeit	12
3.2 TI-M-FD-Pro	12
3.2.1 Registrierungs-Dienst	12
3.2.1.1 I_requestToken	12
3.2.1.1.1 RegService-OpenID-Token	13
3.2.2 Messenger-Service	13
3.2.3 Matrix-Spezifikation	14
3.2.3.1 Weitere Ergänzungen/Einschränkungen zur Matrix-Spezifikation	14
4 Übergreifende Festlegungen	15
4.1 Datenschutz und Sicherheit	15
4.2 Betrieb	16
5 Funktionsmerkmale	17
5.1 Anwendungsfälle	17

5.1.1 Organisationsressourcen im Verzeichnisdienst hinzufügen	17
5.1.2 Akteur (User-HBA) im Verzeichnisdienst hinzufügen	20
5.1.3 FHIR-VZD-Sichtbarkeit für Versicherte setzen	21
5.1.4 Anmeldung eines Akteurs am Messenger-Service	24
5.1.5 Einladung von Akteuren innerhalb einer Organisation	27
5.2 Funktionsaccounts	29
5.2.1 Chatbot	29
5.3 Berechtigungsmanagement – Anpassungen	30
5.3.1 Akteursspezifische Berechtigungskonfiguration	30
5.4 Management von Akteuren und Rollen	31
5.5 Unterbindung der Versichertenkommunikation beim Verlassen eines Raumes	32
6 Anhang A – Verzeichnisse	33
6.1 Abkürzungen	33
6.2 Glossar	33
6.3 Abbildungsverzeichnis	33
6.4 Tabellenverzeichnis	34
6.5 Referenzierte Dokumente	34
6.5.1 Dokumente der gematik	34
6.5.2 Weitere Dokumente	35
1 Einordnung des Dokumentes	6
1.1 Zielsetzung	6
1.2 Zielgruppe	6
1.3 Geltungsbereich	6
1.4 Abgrenzungen	6
1.5 Methodik	7
2 Systemüberblick	8
2.1 Akteure und Rollen	8
2.1.1 Akteur: Chatbot	8
2.1.2 Rolle: "Org-Admin"	8
2.1.3 Rolle: "User-HBA"	8
2.2 Nachbarsysteme	9
2.2.1 VZD-FHIR-Directory	9
2.3 Zugriffstoken	9
3 Zerlegung des Produkttyps	11
3.1 TI-M Client Pro	11
3.1.1 Ausprägungen nach Nutzergruppen	11
3.1.1.1 TI-M Client Pro für Akteure in der Rolle "Org-Admin" (Org-Admin-Client)	11
3.1.2 Ausprägungen nach Plattform	11

3.1.2.1 TI-M Client als Web-Anwendung.....	11
3.1.3 Matrix Spezifikation	12
3.1.3.1 Weitere Ergänzungen/Einschränkungen zur Matrix-Spezifikation	12
3.1.4 VZD-FHIR-Directory	12
Schreibzugriff	12
3.1.5 Sichtbarkeit.....	13
3.2 TI-M FD Pro	14
3.2.1 Registrierungs-Dienst	14
3.2.1.1 I_requestToken.....	14
3.2.1.1.1 RegService-OpenID-Token.....	14
3.2.2 Messenger-Service	15
3.2.3 Matrix Spezifikation	15
3.2.3.1 Weitere Ergänzungen/Einschränkungen zur Matrix-Spezifikation	15
4 Übergreifende Festlegungen	17
4.1 Datenschutz und Sicherheit.....	17
4.2 Betrieb.....	18
5 Funktionsmerkmale	20
5.1 Anwendungsfälle	20
5.1.1 Organisationsressourcen im Verzeichnisdienst hinzufügen	20
5.1.2 Akteur (User-HBA) im Verzeichnisdienst hinzufügen	23
5.1.3 ice.....	26
5.1.4 Einladung von Akteuren innerhalb einer Organisation	32
5.2 Funktionsaccounts.....	35
5.2.1 Chatbot	36
5.3 Berechtigungsmanagement - Anpassungen.....	37
5.3.1 Akteursspezifische Berechtigungskonfiguration	37
5.4 Management von Akteuren und Rollen	38
5.5 Löschen von Inhalten – Anpassungen	39
5.5.1 Serverseitiges Löschen	39
5.6 Matrix-Events	39
6 Anhang A – Verzeichnisse	41
6.1 Abkürzungen	41
6.2 Glossar	41
6.3 Abbildungsverzeichnis.....	41
6.4 Tabellenverzeichnis	42
6.5 Referenzierte Dokumente	43
6.5.1 Dokumente der gematik.....	43
6.5.2 Weitere Dokumente.....	43

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Zulassung der Produkttypen TI-M Client Pro und TI-M FD Pro. Dieses Dokument erweitert die Basisspezifikation [gemSpec_TI-M_Basis] um die für die genannten Produkttypen notwendigen Anpassungen. Für die Produkte gelten weiterhin die in der Basisspezifikation beschriebenen Funktionalitäten, sofern Sie nicht in diesem Dokument erweitert oder eingeschränkt werden.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller von TI-M Client Pro, an Hersteller von TI-M FD Pro und an Anbieter, welche die beschriebenen Produkttypen betreiben und diese Institutionen des Gesundheitswesens und ihren Akteuren (z. B. Sachbearbeitern bei Kostenträgern, Pflegern in Krankenhäusern, etc.) zur Verfügung stellen.

1.3 Geltungsbereich

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

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzungen

Spezifiziert werden in diesem Dokument die vom Produkttyp bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang 6).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten. Diese sind in den Produkttypsteckbriefen der Produkttypen TI-M_Client_Pro und TI-M_FD_Pro verzeichnet.

1.5 Methodik

Anwendungsfälle und Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID, Anforderungen zusätzlich durch die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen.“ die Phrase „DARF NICHT“ semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen „Eine leere Liste DARF KEIN Element besitzen.“ verwendet. Die Schlüsselworte werden außerdem um Pronomen in Großbuchstaben ergänzt, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

Anwendungsfälle und Anforderungen werden im Dokument wie folgt dargestellt:

<AF-ID> - <Titel des Anwendungsfalles>

Text / Beschreibung

[<=]

bzw.

<AFO-ID> - <Titel der Afo>

Text / Beschreibung

[<=]

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

2 Systemüberblick

2.1 Akteure und Rollen

Aufbauend auf der Beschreibung in der Basisspezifikation des TI-Messengers, wird die Liste der Akteure und Rollen für den TI-Messenger Pro um Nutzer im Besitz eines Heilberufsausweises (HBA) sowie automatisierte Systeme, kurz Chatbots, erweitert. Die folgende Tabelle ist eine Ergänzung zur Tabelle aus der Basisspezifikation.

Tabelle 1: Akteure und Rollen

Welcher Akteur bin ich	Wie authentisiere ich mich	Welcher Dienst authentifiziert mich	Welche Rolle nehme ich ein
Chatbot	Authentifizierungsverfahren der Organisation	Messenger-Service	User
Nutzer des TI-Messengers mit Heilberufsausweis (HBA)	HBA	zentraler IDP-Dienst	User-HBA

Im Folgenden werden die neuen bzw. erweiterten Akteure und Rollen beschrieben. Das alle Rollen und Akteure betreffende User Management wird in Kapitel 5.4- Management von Akteuren und Rollen behandelt.

2.1.1 Akteur: Chatbot

Chatbots können ebenso wie natürliche Personen Teilnehmer von Chaträumen sein, in welchen sie dann bestimmte Funktionen (z. B. Archivierung) übernehmen. Zu diesem Zweck müssen sie sich gleichermaßen authentisieren.

Chatbots, die als Teilnehmer in einem Chatraum auftreten, sind so wie menschliche Akteure an ihrem jeweiligen Client durch eine kryptographische Identität und das verwendete "Gerät" (Device) gekennzeichnet, auf deren Grundlage Ende-zu-Ende-Verschlüsselung und Authentizitätsprüfung stattfinden.

2.1.2 Rolle: "Org-Admin"

Der Org-Admin im Kontext von TI-M Pro erhält zusätzlich die Fähigkeit Einträge im VZD-FHIR-Directory für seine Organisation zu verwalten.

2.1.3 Rolle: "User-HBA"

Der TI-M Pro führt die Rolle "User-HBA" ein auf Grundlage der Rolle "User" gemäß [gemSpec_TI-M_Basis]. Einem Akteur in der Rolle "User-HBA" stehen somit die gleichen Funktionalitäten wie einem Akteur in der Rolle "User" zur Verfügung. Zusätzlich kann der

Akteur diese Rolle einnehmen, wenn er sich mit seinem Heilberufsausweis (HBA) gegenüber dem zentralen IDP-Dienst der gematik authentisiert. In dieser Rolle stehen dem Akteur zusätzliche Funktionen zur Verfügung, die im Anwendungsfall 5.1.2: Akteur (User-HBA) im Verzeichnisdienst hinzufügen beschrieben werden.

2.2 Nachbarsysteme

2.2.1 VZD-FHIR-Directory

Beim VZD-FHIR-Directory gibt es gegenüber der Basisspezifikation die folgenden Anpassungen.

- Nach der Authentisierung wird für die Akteure in der Rolle "User" ein individueller search-accesstoken bereitgestellt.
- Für die Suche der Akteure in der Rolle wurde ein eigener Endpunkt bereitgestellt
- Für die Authentisierung der Akteure in der Rolle "User-HBA" und in der Rolle "Org-Admin" wird ein eigener Authentisierungsendpunkt `/owner-authenticate` bereitgestellt.

2.3 Zugriffstoken

Für die Nutzung des TI-Messengers kommen unterschiedliche Arten von Token zur Authentisierung und Autorisierung an weiteren Diensten zum Einsatz, die in verschiedenen Anwendungsfällen verwendet werden. Die folgende Tabelle listet die für den TI-M Pro neu hinzukommenden Token und beschreibt ihre Verwendung. Die folgende Tabelle ist eine Ergänzung zur Tabelle aus der Basisspezifikation.

Tabelle 2: Arten von Token

Token	ausgestellt vom	Beschreibung
RegService-OpenID-Token	Registrierungs-Dienst	<p>Bei dem RegService-OpenID-Token handelt es sich um ein JSON-Web-Token, welches von einem Registrierungs-Dienst bei Bedarf für einen Akteur in der Rolle "Org-Admin" ausgestellt wird.</p> <p>Das RegService-OpenID-Token wird für die Bearbeitung der FHIR-Ressourcen im VZD-FHIR-Directory benötigt. Hierfür wird das RegService-OpenID-Token im Auth-Service des Verzeichnisdienstes gegen ein owner-accesstoken ersetzt, welches am FHIR-Proxy für die weitere Verarbeitung benötigt wird.</p>
owner-accesstoken	Auth-Service des VZD-FHIR-Directory	<p>Das owner-accesstoken wird einem berechtigten Akteur durch den Auth-Service des VZD-FHIR-Directory bereitgestellt. Das Token beinhaltet u.a. die Telematik-ID der FHIR-Ressource, für die der Akteur die Rechte zur Verwaltung erhält. Mit dem</p>

		owner-accesstoken können die entsprechenden Endpunkte zur Bearbeitung der FHIR-Ressource aufgerufen werden.
--	--	---

3 Zerlegung des Produkttyps

3.1 TI-M Client Pro

3.1.1 Ausprägungen nach Nutzergruppen

3.1.1.1 TI-M Client Pro für Akteure in der Rolle "Org-Admin" (Org-Admin-Client)

Der Org-Admin-Client für TI-M Pro erhält zusätzlich die Funktionalität im Namen der Organisation FHIR-Ressourcen im VZD-FHIR-Directory hinzuzufügen/zu verwalten (siehe ~~5.1.1.1 Organisationsressourcen im Verzeichnisdienst hinzufügen~~). Für die Authentisierung kann der Org-Admin ein Token vom Registrierungsdienst verwenden, welches im Kapitel ~~3.2.1.1 I_requestToken~~ beschrieben wird.

A_27147 --Erweiterte Administration von Benutzeraccounts

Der Org-Admin-Client MUSS folgende Verwaltungsaktionen, bezogen auf die Nutzer von Messenger-Services, die durch die eigene Organisation verwaltet werden, unterstützen:

- Direktes oder indirektes (provisioniertes) Anlegen eines Nutzers
- Zurücksetzen der Login Credentials

[<=]

3.1.2 Ausprägungen nach Plattform

Der TI-M Client Pro kann auch als Web-Anwendung zur Nutzung in einem Browser zur Verfügung gestellt werden. Für diese Ausprägung gelten die im folgenden Kapitel gesondert aufgeführten Anforderungen.

3.1.2.1 TI-M Client als Web-Anwendung

A_25507 --Abmeldung statt Sperre bei Web-Clients

Ein browserbasierter TI-M Client Pro MUSS anstelle einer App-Sperre über eine Funktion zur automatischen Abmeldung verfügen, die nach einer bestimmten Zeit der Inaktivität ausgelöst wird.[<=]

A_25508 --Dauer der Inaktivität für automatische Abmeldung

Die Dauer der Inaktivität, nach der ein browserbasierter TI-M Client Pro automatisch abmeldet, MUSS durch den Akteur konfigurierbar und standardmäßig auf eine Stunde eingestellt sein.[<=]

A_26282 --Automatische Abmeldung bei geschlossenem Client

Die automatische Abmeldung des browserbasierten TI-M Client Pro MUSS auch dann wirksam sein, wenn der Client zum Zeitpunkt der Auslösung nicht geöffnet ist.[<=]

A_25536 --Abschottung von Inhalten in Web-Clients

Web-Clients MÜSSEN sicherstellen, dass sensible Daten im Browser (z. B. OLM-Keys, ACCESS_TOKEN) nicht durch andere Anwendungen, die ebenfalls im Browser ausgeführt werden, ausgelesen werden können.[<=]

3.1.3 Matrix Spezifikation

3.1.3.1 Weitere Ergänzungen/Einschränkungen zur Matrix-Spezifikation

A_25325—01 -Erzeugung Öffentlicher Räume-Client

Der TI-M Client Pro MUSS ~~dem Akteur erlauben Räume Anzulegen von öffentlich, in denen Räumen durch den Akteur unterstützten~~ die Join Rule auf public gesetzt ist. [\leq]

Hinweis: Der TI-M Client Pro kann dem Akteur erlauben, die Verschlüsselung beim Anlegen eines öffentlichen Raumes zu deaktivieren.

A_25324-01 -Deaktivierung der Verschlüsselung beim Anlegen von Räumen

Der TI-M Client Pro MUSS sicherstellen, dass unverschlüsselte Räume nur angelegt werden können wenn mindestens eine der folgenden Einstellungen gewählt wurde:

- Join Rule: public, restricted oder knock restricted
- History Visibility: world_readable

[\leq]

A_25562-01 -Hinweis auf Öffentlichkeit eines Raums

Der TI-M Client Pro MUSS Räume durch geeignete UI-Elemente kennzeichnen wenn mindestens eine der folgenden Einstellungen gewählt wurde:

- Join Rule: public
- History Visibility: world_readable
- Verschlüsselung: inaktiv

[\leq]

A_26347 --Hinweis vor Einladung weiterer Chatteilnehmer

Der TI-M Client Pro SOLL dem Nutzer vor Einladung weiterer Teilnehmer in einen Raum einen Hinweis anzeigen, der darauf hinweist, dass nur entsprechend legitimierte Nutzer (bspw. bei Versicherten deren Stellvertreter) eingeladen werden dürfen. [\leq]

3.1.4 VZD-FHIR-Directory

A_26172-01 --Schnittstelle für die VZD-FHIR-Directory Suche

Der TI-M Client Pro MUSS für die Suche im VZD-FHIR-Directory die Schnittstelle `/search` verwenden. [\leq]

3.1.4.1 Schreibzugriff

Für den Schreibzugriff nutzen TI-M Clients Pro ein owner-accesstoken, welches vom Auth-Service des VZD-FHIR-Directory ausgestellt wurde. Um ein gültiges owner-accesstoken zu erhalten, muss ein Akteur in der Rolle "User-HBA" sich mit seinem HBA gegenüber dem zentralen IDP-Dienst der gematik authentisieren.

Eine Besonderheit bietet sich dem Akteur in der Rolle "Org-Admin", da dieser sich bei der Registrierung seiner Organisation bereits mit der SM(C)-B der Organisation authentisiert hat und somit die Möglichkeit bekommt, beim zuständigen Registrierungs-Dienst einen RegService-OpenID-Token anzufragen, welcher anschließend am `/owner-authenticate` Endpunkt gegen ein owner-accesstoken eingetauscht werden kann.

Durch den Aufruf der Schnittstelle `/owner` am FHIR-Proxy des VZD-FHIR-Directory erhält ein Akteur unter Vorlage des `owner-accesstoken` Schreibzugriffe auf das FHIR-Directory. In der folgenden Tabelle wird die zu verändernde FHIR-Ressource in Abhängigkeit zu der verwendeten Identität eines Akteurs beschrieben.

Tabelle 3: Schreibzugriff - VZD-FHIR-Ressourcen

Rolle	Identität	FHIR-Ressource	Beschreibung
Org-Admin	SM(C)-B (stellvertretend durch einen RegService-OpenID-Token)	HealthcareService	Ein Akteur in der Rolle "Org-Admin" kann mit Hilfe des Org-Admin Clients und nach Authentisierung mit einem RegService-OpenID-Token, FHIR-Ressourcen im Namen der Organisation im Organisationsverzeichnis des VZD-FHIR-Directory bearbeiten, um zum Beispiel einen neuen Endpunkt unterhalb eines <i>HealthcareService</i> zu hinterlegen. Das RegService-OpenID-Token erhält der Akteur in der Rolle "Org-Admin" nach erfolgreicher Anmeldung am Registrierungs-Dienst durch Aufruf der vom Anbieter bereitgestellten Schnittstelle <code>I_requestToken</code> .
User-HBA	HBA	PractitionerRole	Ein Akteur in der Rolle "User-HBA" kann, nachdem er sich mit seinem HBA gegenüber dem zentralen IDP-Dienst der gematik authentisiert hat, das Attribut <i>PractitionerRole.endpoint</i> modifizieren, um dort die eigene Erreichbarkeit über TI-M (<i>connectionType</i> Code = "tim") inkl. MXID sowie Informationen zur eigenen Sichtbarkeit zu hinterlegen.

3.1.5 Sichtbarkeit

Akteure in der Rolle "User-HBA" ~~und~~ sowie Akteure in der Rolle "Org-Admin" können die Sichtbarkeit ihrer hinterlegten Informationen an einem Endpoint im VZD-FHIR Directory ~~für Akteure in konfigurieren. Wird der Rolle "Endpoint als zu Versicherter"~~¹ ~~konfigurieren (siehe 5.1.3.1 Practitioner FHIR VZD Sbergen markiert, dann wird dieser nichtbarkeit für Versichert mehr Teil der Ergebnismenge setzen)-in, sofern Akteuren in der Rolle "Org Admin" können die gleiVersichen-Einstellungen für die Endpoints vornehmen, die sie stellvertretend für ihre Organisation verwalten (siehe 5.1.3.2 Organizrter"~~¹ ~~eine Suche am VZD FHIR Directory absetzen. Details zur Administration FHIR VZD der Sichtbarkeit für Versicherte setzen) sind der Spezifikation [gemSpec_VZD_FHIR_Directory] zu entnehmen.~~

¹ Rolle "Versicherter" definiert in [gemSpec_TI-M_ePA]

3.2 TI-M FD Pro

3.2.1 Registrierungs-Dienst

Der Registrierungs-Dienst darf Akteuren in der Rolle "Org-Admin" einen RegService-OpenID-Token ausstellen, welcher die Telematik-ID der SM(C)-B enthält, die bei der Anlage des Org-Admin Accounts verwendet wurde. Dieses Token kann der Org-Admin-Client anschließend beim VZD-FHIR-Directory gegen ein owner-accesstoken eintauschen, um Zugriff auf die eigenen Ressourcen im VZD-FHIR-Directory zu erlangen.

3.2.1.1 I_requestToken

Über die Schnittstelle I_requestToken stellt der Registrierungs-Dienst RegService-OpenID-Token aus. Das Token wird für die Authentifizierung am FHIR-Proxy des VZD-FHIR-Directory benötigt, damit ein Akteur in der Rolle "Org-Admin" Organisationseinträge ändern kann. Die Ausgestaltung der Schnittstelle am Registrierungs-Dienst (I_requestToken) ist dem jeweiligen TI-Messenger-Anbieter überlassen. Das Token muss signiert werden, damit das VZD-FHIR-Directory dem Aussteller vertraut. Hierzu ist ein Zertifikat über einen TI-ITSM Service Request zu beantragen, welches im Anschluss für die Signatur genutzt werden kann.

A_25566 --I_requestToken

Der TI-M Fachdienst Pro MUSS die Schnittstelle I_requestToken für die Ausstellung eines ID_TOKENS (RegService-OpenID-Token) am Registrierungs-Dienst bereitstellen. [≤=]

A_25567 --Authentifizierte Akteure

Der Registrierungs-Dienst MUSS sicherstellen, dass nur für authentifizierte Akteure in der Rolle "Org-Admin" ein RegService-OpenID-Token ausgestellt wird. [≤=]

A_25572 --Zertifikatsablauf

Bevor das Signaturzertifikat für den RegService-OpenID-Token abläuft, MUSS vom TI-Messenger-Anbieter ein neues beantragt werden und das neue Signaturzertifikat an das VZD-FHIR-Directory übermittelt werden. [≤=]

3.2.1.1.1 RegService-OpenID-Token

A_25564 ~~01~~ -Aufbau des RegService-OpenID-Token

Das RegService-OpenID-Token ist ein JSON-Web-Token und MUSS folgende Attribute enthalten:

```

HEADER
{
  "alg": "BP256R1",
  "typ": "JWT"[SEP],
  "x5c": [[SEP] "<X.509 Sig-Cert, base64-encoded DER>" ]
}
PAYLOAD
{
  "sub": "1234567890",
  "iss": "<URL des Registrierungs-Dienst-Endpunkts, über den das Token
ausgestellt wurde>",
  "aud": "<URL des owner-authenticate-Endpunkts am VZD-FHIR-Directory>",
  "professionOID": "<ProfessionOID der Organisation>",[SEP]
  "idNummer": "<TelematikID der Organisation>",
  "iat": "1516239022",
  "exp": "1516242622"
}

```

[<=]

A_25571 --Signatur RegService-OpenID-Token

Für die Signatur des RegService-OpenID-Token MUSS der private Schlüssel des Signaturzertifikats C.FD.SIG verwendet werden.[<=]

A_25568 --Gültigkeitsdauer RegService-OpenID-Token

Die Gültigkeitsdauer des RegService-OpenID-Tokens DARF NICHT mehr als eine Stunde betragen.[<=]

3.2.2 Messenger-Service

Damit ein Akteur in der Rolle "User" den TI-M Client Pro nutzen kann, um die MXID eines Versicherten mit Hilfe von vorliegenden Stammdaten (KVNR und IK-Nummer) herzuleiten, ist es notwendig aus einer IK-Nummer den zugehörigen Servernamen abzuleiten.

Zur Durchsetzung des Berechtigungskonzeptes im Client ist es zusätzlich nötig für eine gegebene MXID festzustellen ob es sich um einen Versicherten handelt oder nicht. Hierfür muss der zugehörige Homeserver gegen die Föderationsliste abgeglichen werden.

Die oben genannten Operationen werden durch die Schnittstelle [api-messenger/src/openapi/TiMessengerInformation.yaml] am Messenger-Proxy bereitgestellt.

A_26445-01 --TiMessengerInformation Schnittstelle

Der Messenger-Proxy Pro SOLL eine Schnittstelle auf Basis von [api-messenger/src/openapi/TiMessengerInformation.yaml] implementieren.[<=]

3.2.3 Matrix Spezifikation**3.2.3.1 Weitere Ergänzungen/Einschränkungen zur Matrix-Spezifikation****A_26515—8166 -Externe Einladungen zu Öffentlichen Räumen beitreten**

Der TI-M FD MUSS für Räume mit der Join Rule public sicherstellen, dass nur ~~N~~invites an Nutzer ~~dem zugelassen werden, die ihren Account auf demselben Homeserver haben, auf dem der Raum erstellt wurde.~~[<=]

A_26515-01 -Zutrittsbeschränkung für öffentliche Räume

Der TI-M FD MUSS in Räumen mit der Join Rule public sicherstellen, dass nur solche Nutzer dem Raum beitreten können, die ihren Account auf demselben Homeserver haben, auf dem der Raum erstellt wurde.[<=]

A_28271 -Nachträgliches Erzeugen öffentlicher Räume

Der TI-M FD MUSS Anfragen am Endpunkt/rooms/{roomId}/state/{eventType}/{stateKey} mit HTTP 400 undM_INVALID_ROOM_STATE ablehnen wenn alle der folgenden Bedingungen zutreffen:

- die Anfrage setzt die Join Rule im Raum auf public und
- es befinden sich Versicherte im Raum (egal in welchem Membership-Status).

[<=]

A_26518 --Öffentliche Räume Client-API Auth

Der TI-M FD MUSS Requests zu den Endpunkten

- `/_matrix/client/v3/directory/list/room/{roomId}`¹
- `/_matrix/client/v3/publicRooms`²

nur authentifizierten Akteuren erlauben.

¹ [Client-Server API/#get_matrixclientv3directorylistroomroomid]

² [Client-Server API/#get_matrixclientv3publicrooms][<=]

Hinweis: Erfolgt ein Zugriff von einem unauthentifzierten Akteur soll sich der Fachdienst wie bei allen anderen Endpunkten der Client-Server-API verhalten. [Client-Server-API/#using-access-tokens]

A_26520 –Öffentliche Räume Server-API

Der TI-M FD MUSS Requests zum Endpunkt `/_matrix/federation/v1/publicRooms` mit einer HTTP 403 Response ablehnen.[<=]

4 Übergreifende Festlegungen

4.1 Datenschutz und Sicherheit

Zur Sicherstellung des Datenschutzes und der Sicherheit im Rahmen des TI-Messenger-Dienstes werden im Folgenden zu erfüllende Anforderungen an den TI-Messenger-Fachdienst und den TI-Messenger-Client, beziehungsweise deren Hersteller und Anbieter beschrieben. Anforderungen, die durch andere Systemkomponenten zu erfüllen sind, werden hier nicht aufgeführt.

Hinweis: Clients und Server im Sinne der folgenden Anforderung sind alle Komponenten des TI-Messenger-Dienstes, die miteinander kommunizieren, wobei der Client der Initiator einer Verbindung zu einem Server ist, der eine Ressource zur Verfügung stellt. Wenn TI-Messenger-Clients und TI-Messenger-Fachdienste gemeint sind, werden diese auch explizit als TI-Messenger-Clients und TI-Messenger-Fachdienste bezeichnet.

A_25544 --Nutzung des TI-Messenger-Clients durch Drittsysteme

Um eine nahtlose Integration in z.B. Primär- (PVS, ZPVS, KIS, AVS etc.) oder Archivsysteme zu ermöglichen, KANN der TI-M Client Pro eine Schnittstelle zum Zugriff auf Daten durch Drittsysteme anbieten. [≤]

A_25545 --Information über Nutzung des TI-Messenger-Clients durch Drittsysteme

Bietet der TI-M Client Pro eine Schnittstelle zur Nutzung durch Drittsysteme, z.B. Primär- (PVS, ZPVS, KIS, AVS etc.) oder Archivsysteme an, MUSS er sicherstellen, dass Akteure bei Verwendung einer solchen Funktion geeignet darüber informiert werden, dass sie Daten aus dem geschützten Bereich des Clients hinausbewegen. Geeignet bedeutet dabei, dass darüber zumindest einmalig informiert wird, welche Daten in welches Drittsystem weitergeleitet werden. [≤]

A_25509 --Verhinderung von Bildschirmaufnahmen

Der TI-M Client Pro für mobile Szenarien MUSS die Anfertigung von Bildschirmaufnahmen standardmäßig verhindern. [≤]

Hinweis: Der Client kann die Anfertigung von Bildschirmaufnahmen nach Konfiguration durch den Akteur erlauben.

A_25510 --Warnung vor mangelndem Schutz von Bildschirmaufnahmen

Wurde die Verhinderung von Bildschirmaufnahmen durch den Akteur deaktiviert, so MUSS der TI-M Client Pro für mobile Szenarien den Akteur bei Anfertigung von Bildschirmaufnahmen darüber informieren, dass diese nicht durch den Client geschützt sind und sich daraus Risiken ergeben können. [≤]

A_25506 --Nachnutzung der Sperre übergeordneter Systeme

Der TI-M-Client Pro KANN eine vorhandene Sperre des übergeordneten Systems nachnutzen, um auf eine eigene App-Sperre zu verzichten. Im Fall von eigenständigen Clients kann dies eine Sperre des Betriebssystems sein, bei integrierten Clients die von KIS, PVS, AVS und ähnlichen. [≤]

A_25505 --Prüfung auf konforme Sperre des übergeordneten Systems

Wird der TI-M Client, der kein Web-Client ist, ohne aktive App-Sperre verwendet, MUSS er regelmäßig und wenigstens beim Öffnen prüfen, ob eine konforme Sperre im übergeordneten System (z.B. Betriebssystem, KIS, PVS, AVS etc.) aktiviert ist und bei negativem Prüfergebnis eine dedizierte App-Sperre aktivieren. [≤]

4.2 Betrieb

Im Betrieb verantwortet ein Anbieter des TI-Messengers das Produkt:

- TI-M Fachdienst Pro
- TI-Messenger Client für Akteure (inkl. Org-Admin)

A_26397 --TI-Messenger Anbieter - Produktverantwortung (Pro)

Jeder Anbieter eines TI-Messenger Fachdienstes Pro, MUSS für Organisationen, die einen Messenger-Service vom Anbieter erhalten, sowohl den TI-M Client für Akteure in der Rolle "User" als auch den TI-M Client für Akteure in der Rolle "Org-Admin" (Org-Admin-Client) anbieten.【<=】

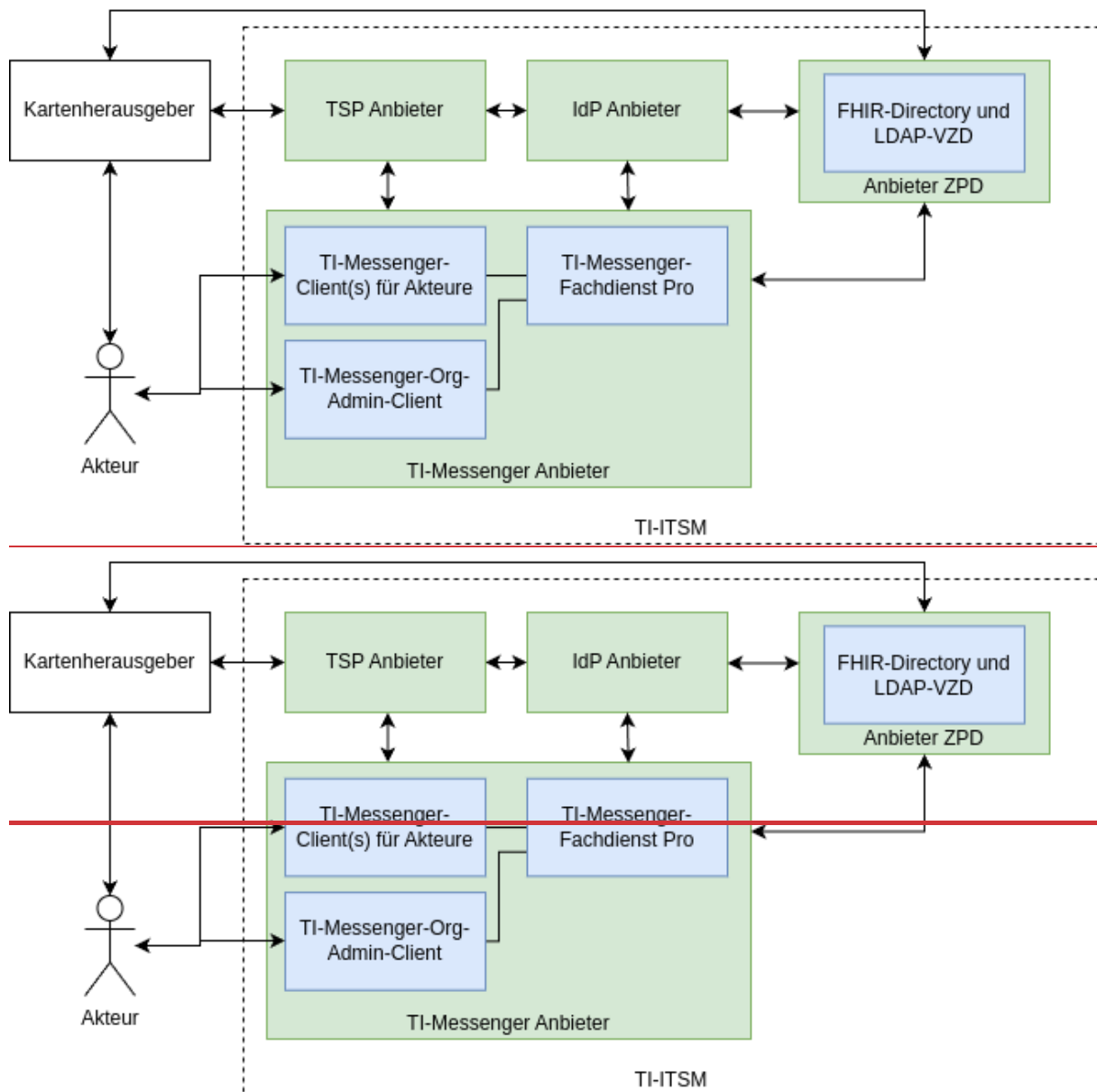


Abbildung 1: Betriebsmodell TI-M Pro

Hinweis zur Abbildung: -Die Abbildung bildet die organisatorischen Kommunikationsbeziehungen aus Sicht des TI-ITSM-Systems zwischen den jeweiligen Entitäten/Anbieterrollen ab.

5 Funktionsmerkmale

5.1 Anwendungsfälle

5.1.1 Organisationsressourcen im Verzeichnisdienst hinzufügen

AF_10059-02 --Organisationsressourcen im Verzeichnisdienst hinzufügen

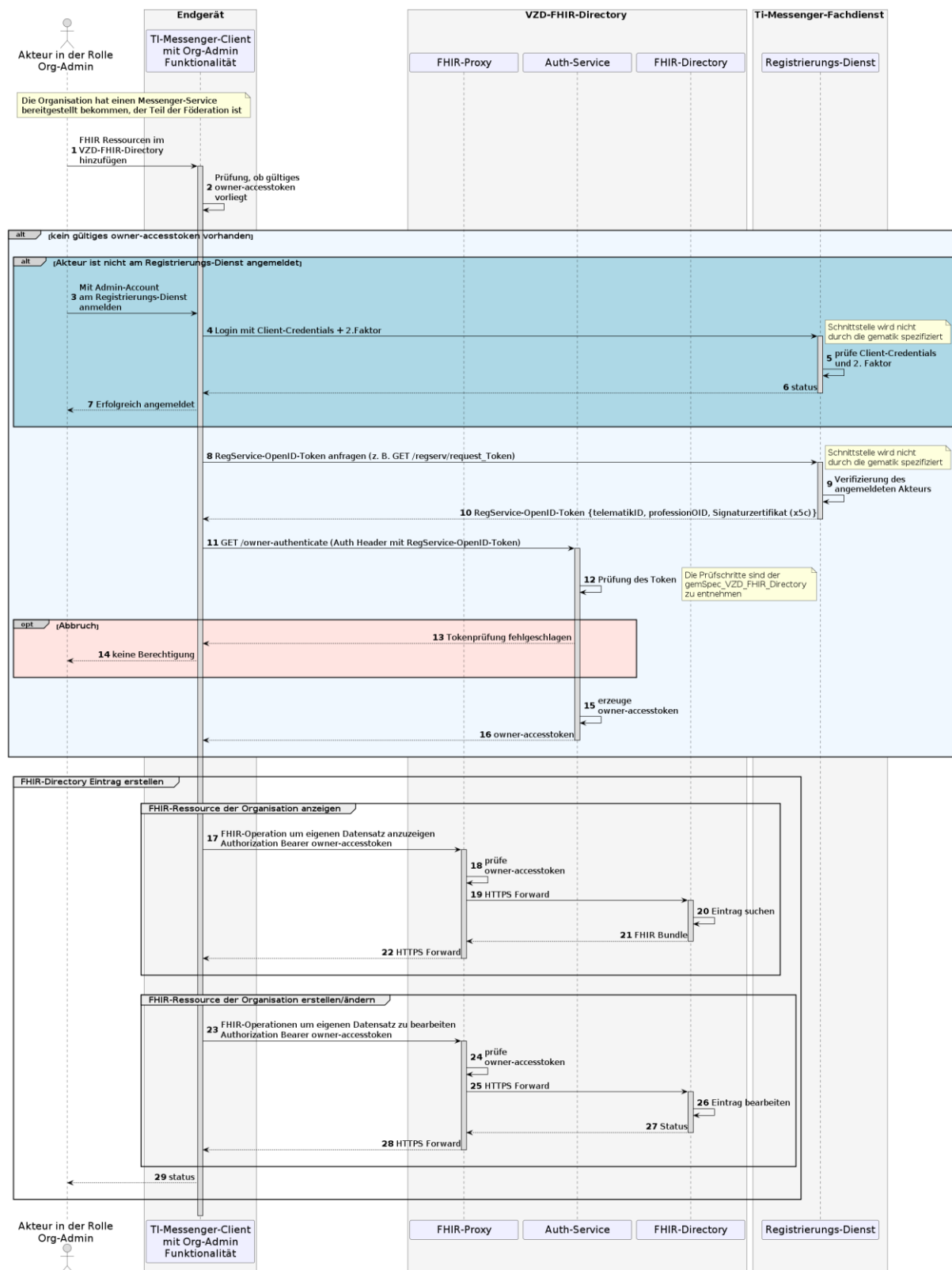
Mit diesem Anwendungsfall macht ein Akteur in der Rolle "Org-Admin" Akteure seiner Organisation im TI-M Dienst für andere Akteure auffindbar und erreichbar. Dafür werden *Endpoint*-Ressourcen mit ihrer jeweiligen MXID im Organisationsverzeichnis (*HealthcareService*) des VZD-FHIR-Directory hinterlegt. Organisationen können mehrere FHIR-Ressourcen administrieren und somit eingehende Kommunikationsprozesse organisatorisch und thematisch strukturieren (siehe [gemSpec_VZD_FHIR_Directory]).

Tabelle 4: AF - Organisationsressourcen im Verzeichnisdienst hinzufügen

AF_10059	Organisationsressourcen im Verzeichnisdienst hinzufügen
Akteur-	Beauftragter Mitarbeiter einer Organisation in der Rolle "Org-Admin"
Auslöser	Der Akteur in der Rolle "Org-Admin" möchte seine Organisation erreichbar machen, indem die MXIDs der Akteure der Organisation im VZD-FHIR-Directory hinterlegt werden.
Komponenten	<ul style="list-style-type: none">• Org-Admin-Client• TI-Messenger Registrierungs-Dienst• Auth-Service• FHIR-Proxy• FHIR-Directory
Vorbedingungen	<ol style="list-style-type: none">1. Für die Organisation wurde ein Messenger-Service bereitgestellt und es existiert ein Eintrag der Organisation im FHIR-Directory.2. Der Administrator der Organisation verfügt über einen Org-Admin-Client3. Es existiert eine Vertrauensbeziehung zwischen dem Registrierungs-Dienst und dem VZD-FHIR-Directory (Übergabe des Zertifikates).4. Der Administrator der Organisation wurde vom Registrierungs-Dienst authentifiziert.
Eingangsdaten	Org-Admin-Credentials, FHIR-Organisations-Ressourcen

Ergebnis	FHIR-Organisations-Ressourcen aktualisiert, Status
Ausgangsdaten	Aktualisierte VZD-FHIR-Directory-Datensätze

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es sich um eine **vereinfachte Laufzeitansicht**, in der zum Beispiel die TLS-Terminierung am FHIR-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde.



5.1.2 Akteur (User-HBA) im Verzeichnisdienst hinzufügen

AF_10058-02 --Akteur (User-HBA) im Verzeichnisdienst hinzufügen

Mit diesem Anwendungsfall wird ein Akteur in der Rolle "User-HBA" für Akteure anderer Messenger-Services auffindbar und erreichbar gemacht. Dafür werden FHIR-Ressourcen mit ihrer jeweiligen MXID des Akteurs im Personenverzeichnis (*PractitionerRole*) des VZD-FHIR-Directory hinterlegt. Um diesen Anwendungsfall ausführen zu können ist der Besitz eines HBA notwendig.

Tabelle 5: AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen

AF_10058	Akteur (User-HBA) im Verzeichnisdienst hinzufügen
Akteur-	Akteur in der Rolle "User-HBA"
Auslöser	Ein Akteur in der Rolle "User-HBA" möchte sich im Personenverzeichnis erreichbar machen, indem er seine MXID in seinen Practitioner-Datensatz im VZD-FHIR-Directory hinterlegt.
Komponenten	<ul style="list-style-type: none"> • TI-Messenger-Client • Authenticator • zentraler IDP-Dienst • FHIR-Proxy • Auth-Service • FHIR-Directory
Vorbedingungen	<ol style="list-style-type: none"> 1. Der Akteur ist bei einem gültigen Messenger-Service angemeldet. 2. Der Akteur verfügt über einen zugelassenen TI-Messenger-Client. 3. Das VZD-FHIR-Directory ist beim zentralen IDP-Dienst registriert. 4. Der Akteur kann sich mit dem HBA am zentralen IDP-Dienst authentisieren.
Eingangsdaten	HBA, FHIR-Practitioner-Ressourcen
Ergebnis	FHIR-Practitioner-Ressourcen aktualisiert, Status
Ausgangsdaten	aktualisierter Practitioner-Datensatz

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es sich um eine **vereinfachte Laufzeitansicht** in der zum Beispiel die TLS-Terminierung am FHIR-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde. Darüber hinaus kann bei Nutzung NFC-fähiger HBAs und Endgeräte die Signatur der IDP Challenge auch ohne Konnektor direkt im Endgerät implementiert werden.

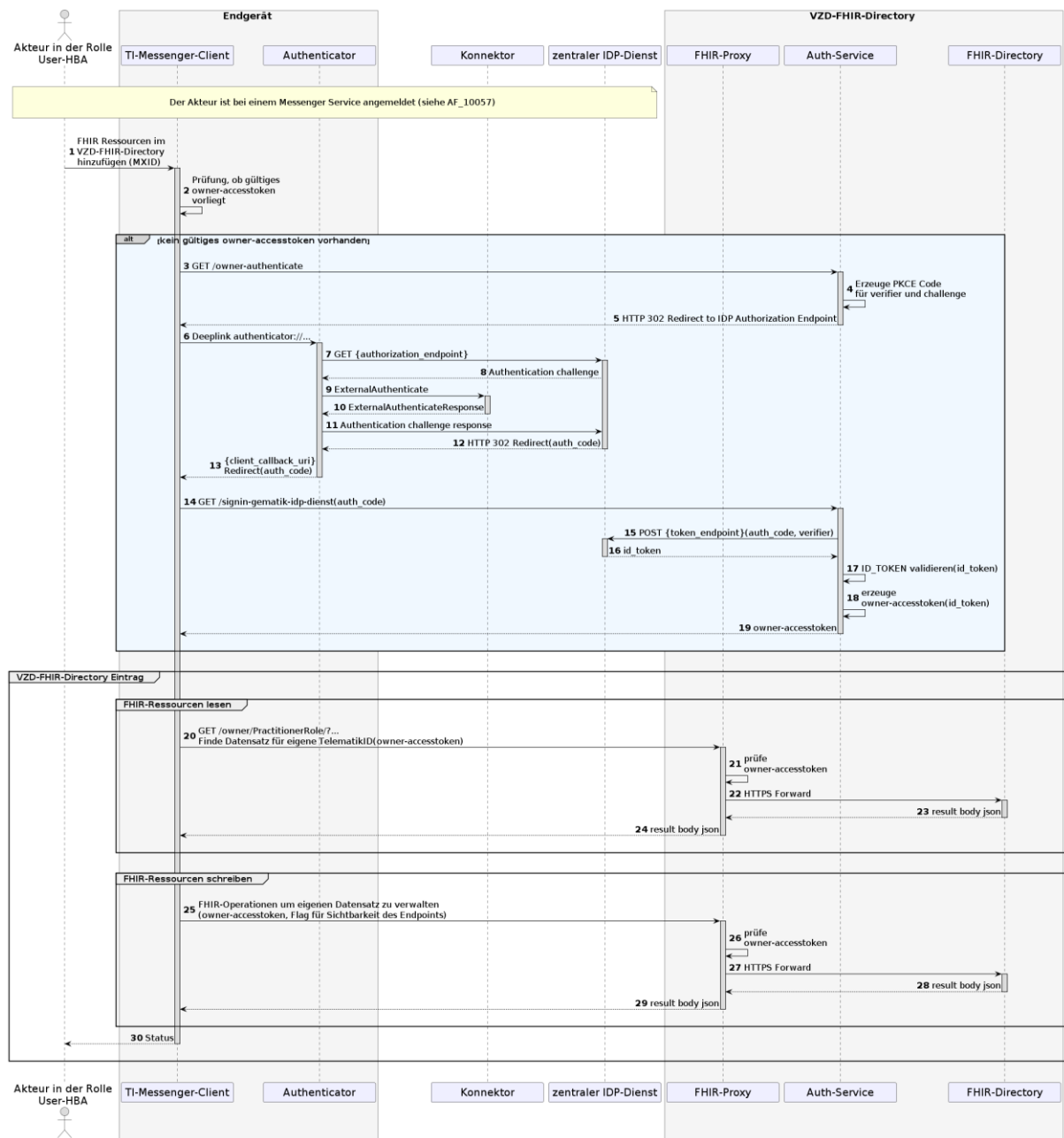


Abbildung 3: Laufzeitsicht - Akteur (User-HBA) im Verzeichnisdienst hinzufügen

[<=]

5.1.3 FHIR-VZD-Sichtbarkeit für Versicherte setzen

AF_10376-Practitioner-FHIR-VZD-Sichtbarkeit für Versicherte setzen

Mit diesem Anwendungsfall kann ein Akteur in der Rolle "User-HBA" die Sichtbarkeit seiner Endpoint Einträge im VZD-FHIR-Directory verwalten. Möchte der Akteur verhindern, dass Akteure in der Rolle "Versicherter" seine MXID über die Suche finden können, dann kann er dies am Endpunkt konfigurieren oder im umgekehrten Fall wieder zurücknehmen.

~~Tabelle 6: Practitioner – FHIR-VZD_m_MeSichtbarkeit für Versicherte setzen~~

Attribute	Bemerkung
Akteur	Akteur in der Rolle "User-HBA"
Auslöser	Ein Akteur in der Rolle "User-HBA" möchte, seinen Endpunkt im VZD-FHIR-Directory für Versicherte nicht sichtbar (a) bzw. sichtbar (b) schalten.
Komponenten	<ul style="list-style-type: none"> • TI-Messenger-Client • FHIR-Proxy • FHIR-Directory
Vorbedingungen	<ol style="list-style-type: none"> 1. Der Akteur ist bei einem zugelassenen TI-Messenger-Client angemeldet. 2. Der Akteur hat durch erfolgreiche Anmeldung mit seinem HBA die Rolle "User-HBA" eingenommen und ein gültiges owner-accesstoken liegt vor. 3. Die seinem Practitioner-Eintrag zugehörigen Endpoints aus dem VZD-FHIR-Directory liegen dem Client vor.
Eingangsdaten	FHIR-Endpoint mit neuer endpointVisibility
Ergebnis	Der Eintrag ist in der Suche für Akteure in der Rolle "Versicherter" nicht sichtbar (a) bzw. sichtbar (b).
Ausgangsdaten	FHIR-Endpoint mit aktualisierter endpointVisibility

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es sich um eine **vereinfachte Laufzeitansicht**, in der zum Beispiel die TLS-Terminierung am FHIR-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde.

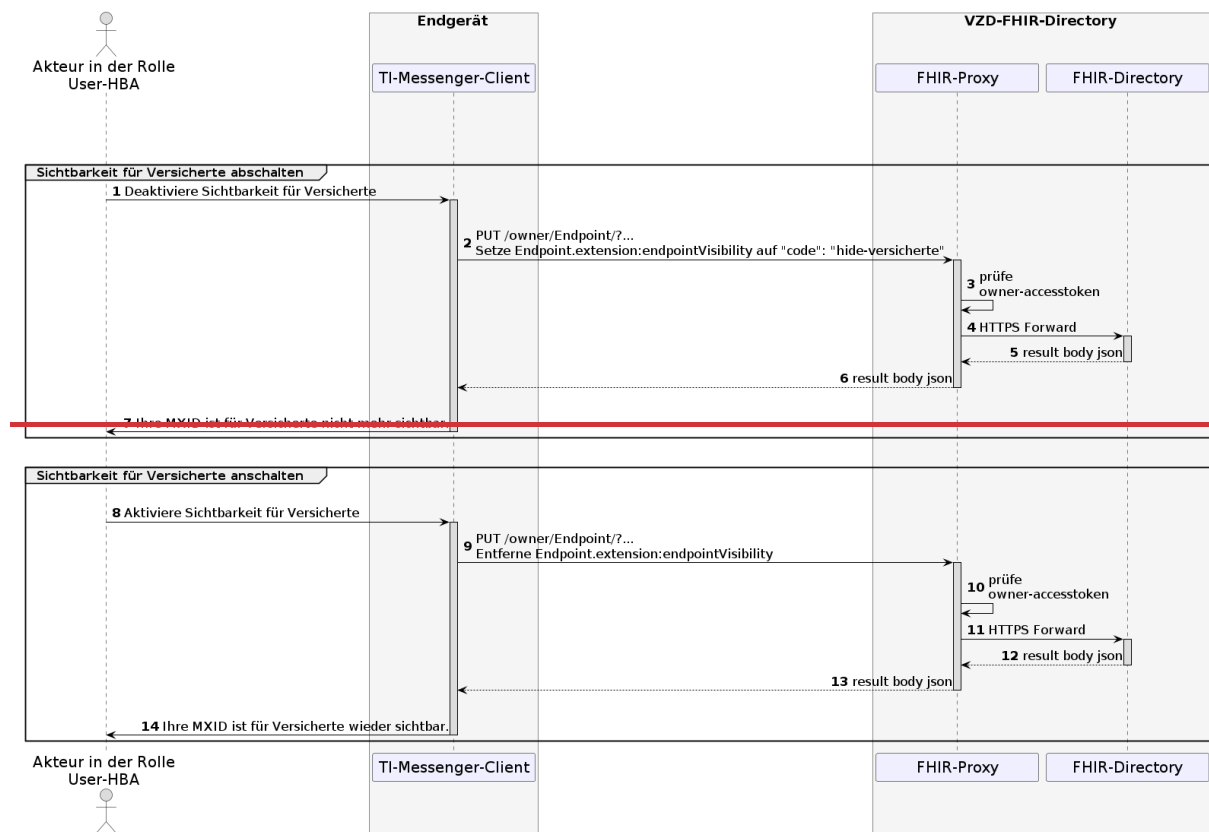


Abbildung 4: Laufzeitsicht — Practitioner — FHIR-er-SerVZD-Sichtbarkeit für Versicherte setzen

{<=>}

5.1.3 ice

AF_10377 — Organization — FHIR-VZD-Sichtbarkeit für Versicherte setzen

Mit diesem Anwendungsfall kann ein Akteur in der Rolle "Org-Admin" die Sichtbarkeit der Endpoint Einträge der Organisation, die er vertritt, im VZD-FHIR-Directory verwalten. Möchte der Akteur verhindern, dass Akteure in der Rolle "Versicherter" eine für die Organisation hinterlegte MXID über die Suche finden können, dann kann er dies am Endpunkt konfigurieren oder im umgekehrten Fall wieder zurücknehmen.

Tabelle 7: Organization — FHIR-VZD-Sichtbarkeit für Versicherte setzen

Attribute	Bemerkung
Akteur-	Akteur in der Rolle "Org-Admin"
Auslöser-	Ein Akteur in der Rolle "Org-Admin" möchte einen Endpunkt im VZD-FHIR-Directory für Versicherte nicht sichtbar (a) bzw. sichtbar (b) schalten.
Komponenten-	<ul style="list-style-type: none"> ◆ Org-Admin-Client ◆ FHIR-Proxy

	• FHIR-Directory
Vorbedingungen	1. Der Akteur ist bei einem zugelassenen Org-Admin-Client angemeldet. 2. Der Akteur hat erfolgreich ein RegService-OpenID-Token gegen ein owneraccess-token für seine Organisation eingetauscht 3. Die seinem Organization-Eintrag zugehörigen Endpoints aus dem VZD-FHIR-Directory liegen dem Client vor.
Eingangsdaten	FHIR-Endpoint mit neuer endpointVisibility
Ergebnis	Der Eintrag ist in der Suche für Akteure in der Rolle "Versicherter" nicht sichtbar (a) bzw. sichtbar (b).
Ausgangsdaten	FHIR-Endpoint mit aktualisierter endpointVisibility

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es sich um eine **vereinfachte Laufzeitsicht**, in der zum Beispiel die TLS-Terminierung am FHIR-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde.

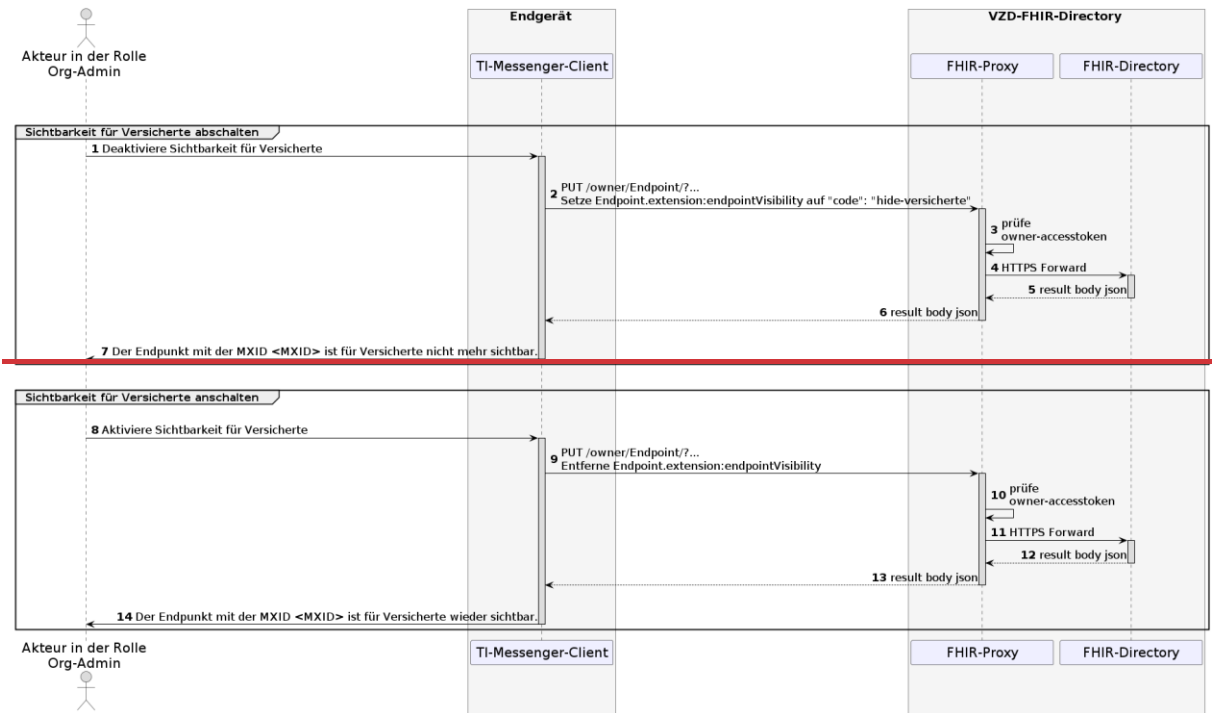


Abbildung 5: Laufzeitsicht – Organization – FHIR-VZD Sichtbarkeit für Versicherte setzen
[<=]

5.1.4 Anmeldung eines Akteurs am Messenger-Service

AF_10057-04 --Anmeldung eines Akteurs am Messenger-Service

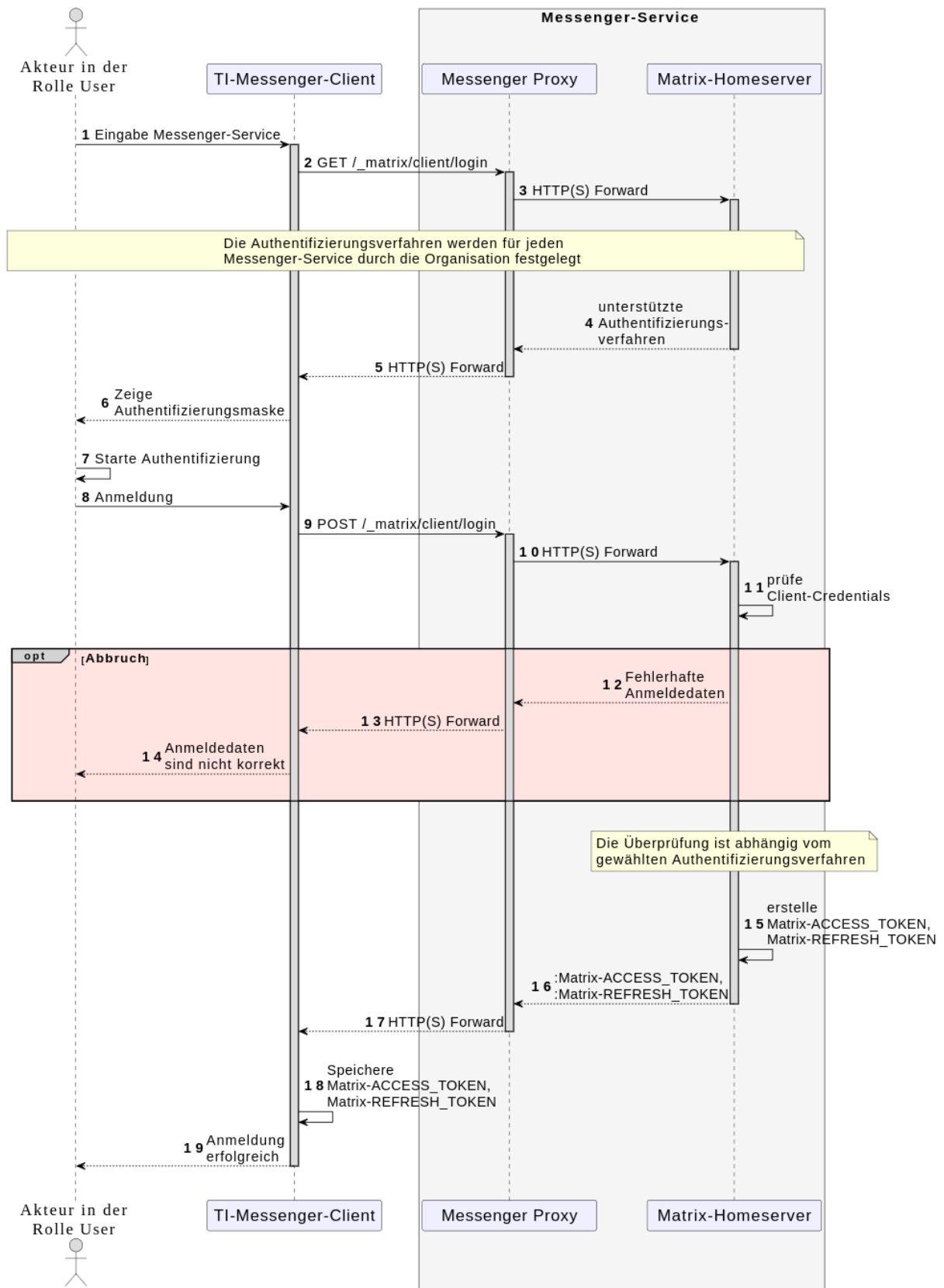
Mit diesem Anwendungsfall meldet sich ein Akteur an einen in der TI-Föderation zuständigen Messenger-Service an und registriert seinen TI-M Client als Endgerät. Der TI-M Client kann die Auswahl der Matrix-Domain des gewünschten Messenger-Service automatisieren oder durch andere Hilfsmittel wie z. B. QR-Codes unterstützen. Erfolgt dies nicht, so muss der TI-M Client dem Akteur die freie Eingabe der Matrix-Domain ermöglichen.

Tabelle 6: AF - Anmeldung eines Akteurs am Messenger-Service

AF_10057	Anmeldung eines Akteurs am Messenger-Service
Akteur-	Akteur in der Rolle "User"
Auslöser	Ein Akteur möchte sich mit seinem TI-M Client bei einem Messenger-Service anmelden.
Komponenten	<ul style="list-style-type: none"> • TI-M Client • Messenger-Proxy • Matrix-Homeserver
Vorbedingungen	<ol style="list-style-type: none"> 1. Der Akteur verfügt über einen vom Anbieter unterstützen TI-M Client. 2. Der Akteur kennt die URL des Messenger-Services oder die URL ist bereits in seinem TI-M Client konfiguriert. 3. Der Akteur kann sich durch ein beim Matrix-Homeserver unterstütztes Authentisierungsverfahren identifizieren. Wird durch die Organisation ein eigenes Authentifizierungsverfahren verwendet, MUSS eine Anbindung an den Matrix-Homeserver erfolgt sein. <i>Hinweis: Bei dem zweiten Faktor muss es sich nicht um für die Nutzer individuelle Faktoren handeln. Dieses schließt die gemeinsame Nutzung der SMC-B oder des HSM-B der LEI oder des KTR durch Angehörige dieser Institution als zweiten Faktor mit ein.</i> 4. Der verwendete Matrix-Homeserver ist in die Föderation integriert (valider Messenger-Service).
Eingangsdaten	URL des Matrix-Homeservers
Ergebnis	Ein Akteur hat sich erfolgreich an einem gültigen Messenger-Service angemeldet und mit einem zugelassenen Authentifizierungsverfahren erfolgreich authentisiert.
Ausgangsdaten	Matrix-ACCESS_TOKEN, Matrix-REFRESH_TOKEN, MXID, device_id Status

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. In dieser wird der Prozess einer Anmeldung eines Akteurs an einem Messenger-Service dargestellt. Sollte ein Akteur noch nicht an einem Matrix-Homeserver registriert sein, dann wird zunächst eine Registrierung des

Akteurs mit der Operation `POST /_matrix/client/register` durchgeführt. Der Ablauf der Registrierung ist analog dem des Login-Verfahrens.



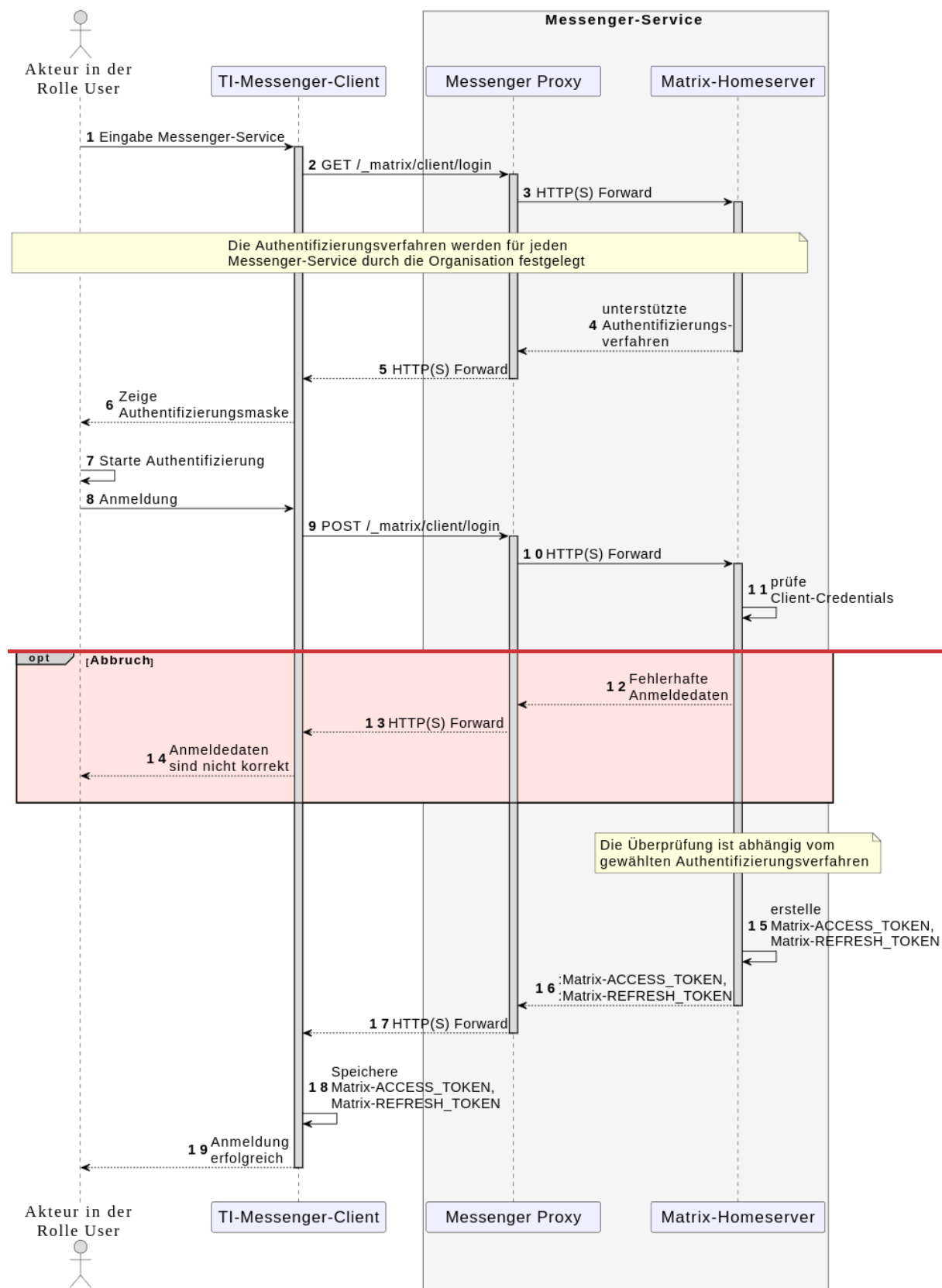


Abbildung 4: Laufzeitsicht - Anmeldung eines Akteurs am Messenger-Service

[<=]

5.1.55.1.4 Einladung von Akteuren innerhalb einer Organisation

AF_10104-03 --Einladung von Akteuren innerhalb einer Organisation

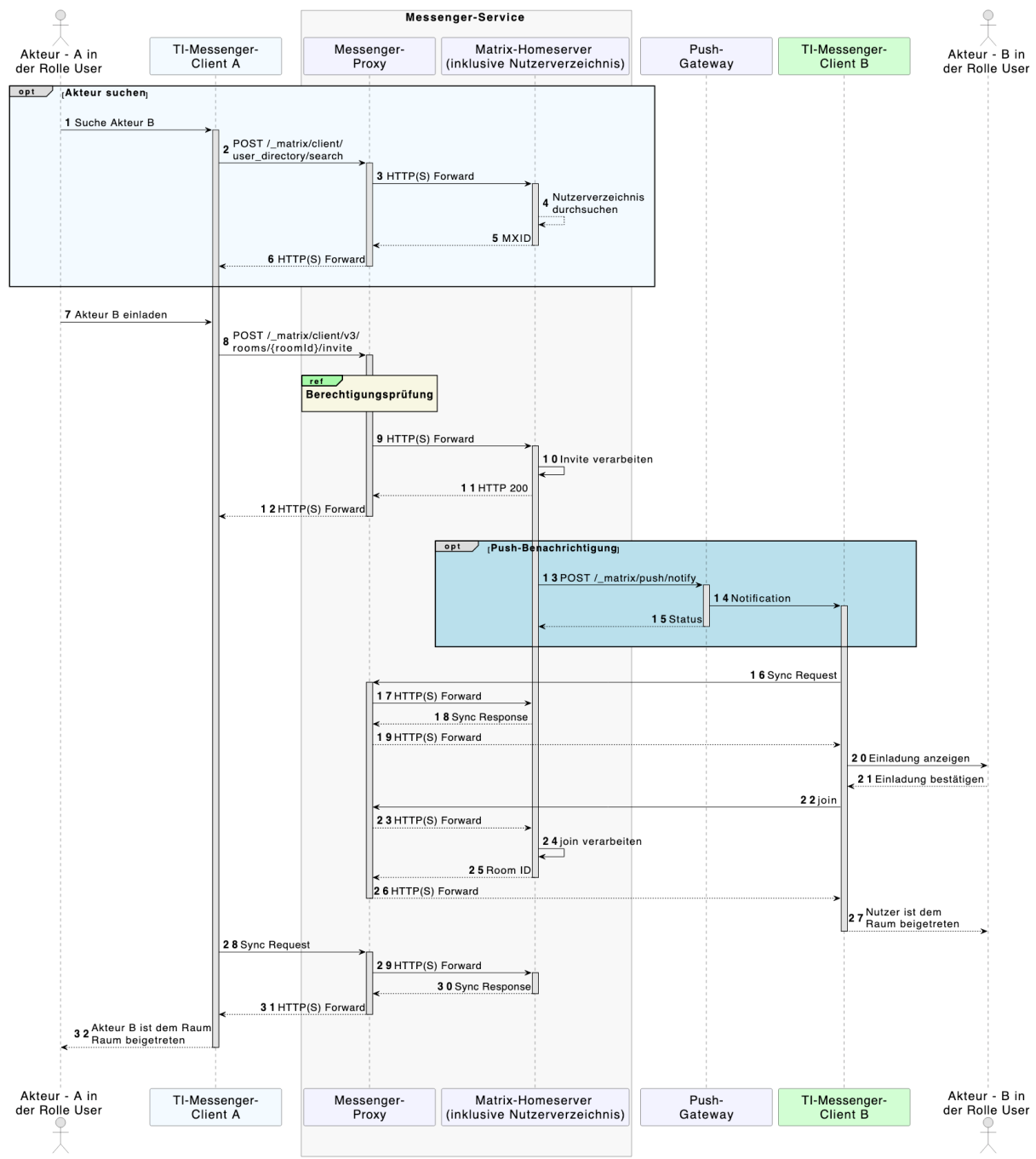
In diesem Anwendungsfall wird ein Akteur, der zu einer gemeinsamen Organisation gehört, in einen Raum eingeladen, um Aktionen auszuführen. Für die Suche nach Akteuren innerhalb einer gemeinsamen Organisation durchsucht ein TI-M Client das Nutzerverzeichnis seiner Organisation auf dem Matrix-Homeserver. Anschließend wird die Einladung vom Einladenden an den Messenger-Proxy übermittelt. Dieser prüft, ob die beteiligten Akteure bei ihm registriert sind. Ist dies der Fall, erfolgt die Weiterleitung an den Matrix-Homeserver der Akteure. Ist dies nicht der Fall, handelt es sich bei dem einzuladenden Akteur nicht um einen Akteur innerhalb der Organisation und die Einladung wird für die externe Zustellung weitergeleitet.

Tabelle 7: Einladung von Akteuren innerhalb einer Organisation

AF_10104	Einladung von Akteuren innerhalb einer Organisation
Akteur	Akteur in der Rolle "User"
Auslöser	Akteur A möchte Akteur B seiner Organisation in einen gemeinsamen Raum einladen.
Komponenten	<ul style="list-style-type: none"> • TI-Messenger Client A + B • Messenger-Proxy • Matrix-Homeserver • Push-Gateway
Vorbedingungen	<ol style="list-style-type: none"> 1. Die Akteure sind am selben Messenger-Service angemeldet. 2. Jeder Akteur hat einen zugelassenen TI-M Client. 3. Einladender ist Mitglied des Chatraums, in den eingeladen wird. 4. Einladender verfügt in diesem Chatraum über einen hinreichenden Powerlevel, um einen Teilnehmer einladen zu können.
Eingangsdaten	Invite-Event
Ergebnis	<p>Akteur A und Akteur B sind beide im Chatraum, zu dem die Einladung ausgesprochen wurde.</p> <p>Optional erfolgt eine Benachrichtigung an Akteur B über die Einladung in den Chatraum. (Hat Akteur B den Akteur A auf seine BlockedUser-Liste gesetzt, dann erfolgt keine Benachrichtigung.)</p>
Ausgangsdaten	Status

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Der für die zukünftige Kommunikation genutzte Chatraum wurde durch den einladenden Akteur bereits erstellt. Daher wird in

diesem Anwendungsbeispiel ein `/_matrix/client/v3/rooms/{roomId}/invite` Event am Messenger-Proxy geprüft. Die folgende Darstellung zeigt lediglich die Einladung zwischen zwei Akteuren. Weitere Akteure können unabhängig von dieser Laufzeitsicht eingeladen werden (Hinweis: Group-Messaging).



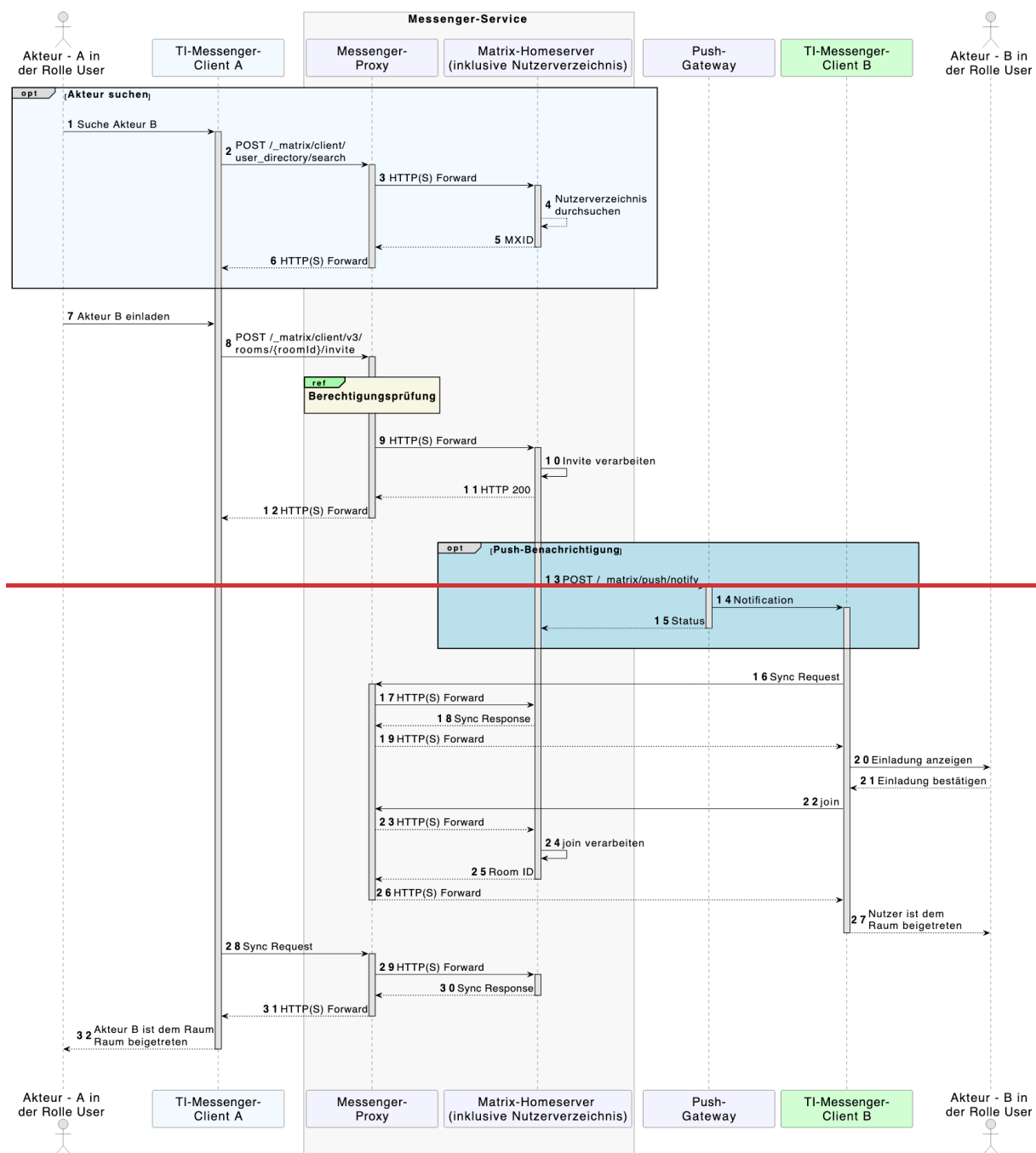


Abbildung 5: Einladung von Akteuren innerhalb einer Organisation

[<=]

5.2 Funktionsaccounts

Einrichtungen im Gesundheitswesen sind sehr unterschiedlich strukturiert und wollen hinsichtlich ihrer Erreichbarkeit flexibel eigene Strukturen abbilden können. Daher sind beim TI-M Dienst Accounts notwendig, die es ermöglichen, Akteure unterhalb der Struktur erreichbar zu machen. Der anfragende Akteur muss dann nicht die genaue

interne Struktur der Organisation kennen. Diese speziellen Accounts werden im folgenden als Funktionsaccounts bezeichnet.

Folgende Beispielszenarien können umgesetzt werden:

- Die Credentials für einen Funktionsaccount werden an mehrere Mitarbeiter verteilt und somit können alle stellvertretend für die Organisation antworten.
- Hinter dem Funktionsaccount verbirgt sich ein Automatismus, der z.B. den diensthabenden Arzt in den Chatraum hinzuholt.
- Hinter dem Funktionsaccount verbirgt sich ein Automatismus, der selbstständig Antworten generiert.

Ein Funktionsaccount ist als eine *Endpoint*-Ressource eines *HealthcareService* einer Organisation anzulegen. Somit kann der Funktionsaccount unterhalb der Organisationsstruktur von einem Akteur gefunden und kontaktiert werden.

A_26523 --Funktionsaccount als Endpunkt

Der Org-Admin-Client MUSS einen Funktionsaccount als *Endpoint*-Ressource mit dem "payloadTyp: *TI-Messenger chat*"-eines *HealthcareService* einer Organisation anlegen. [\leq]

A_26524 --Funktionsaccount Address

Der Org-Admin-Client MUSS das *address* Attribut der *Endpoint*-Ressource mit der MXID des Funktionsaccounts im URI Format befüllen. [\leq]

A_26525 --Funktionsaccount Name

Der Org-Admin-Client MUSS das *name* Attribut der *Endpoint*-Ressource mit dem Displaynamen des Funktionsaccounts befüllen. [\leq]

A_25546 --ConnectionType persönlicher Funktionsaccount

Der Org-Admin-Client MUSS für einen Funktionsaccount, der von einer oder mehreren natürlichen Personen betreut wird, an der *Endpoint*-Ressource den Code des *EndpointDirectoryConnectionType* auf "tim-fa" setzen. [\leq]

5.2.1 Chatbot

Chatbots sind spezielle Akteure, die stellvertretend für eine Person oder Organisation die Kommunikation mit einem Akteur führen. Chatbots können die Kommunikation vollständig automatisiert abschließen (z. B. Terminvergabe) oder in der Organisation hinterlegte natürliche Personen dem Chat hinzuziehen (z. B. Ausstellen eines Rezeptes). Treten Chatbots als Kommunikationsteilnehmer des TI-Messengers auf, so sind diese im jeweiligen Chat als Chatbot zu kennzeichnen. Ein Beispiel für eine Kommunikation ist unter [api-messenger/docs/anwendungsfalle/COM-chatbot.adoc] hinterlegt.

A_25547 --ConnectionType Funktionsaccount Chatbot

Der Org-Admin-Client MUSS für einen Funktionsaccount, der von einem automatisierten System abgebildet wird, an der *Endpoint*-Ressource den Code des *EndpointDirectoryConnectionType* auf "tim-bot" setzen. [\leq]

A_25553 --Displayname Chatbot

Wird ein Akteur durch einen Chatbot realisiert, MUSS folgende Bildungsregel für den Displaynamen auf dem Homeserver verwendet werden: <Name des Funktionsaccounts> (Chatbot). [\leq]

5.3 Berechtigungsmanagement - Anpassungen

5.3.1 Akteursspezifische Berechtigungskonfiguration

Für die Akteure des TI-M Pro wird die Möglichkeit geschaffen, bestimmte Nutzergruppen in der Berechtigungskonfiguration nutzen zu können. Als erste Benutzergruppe wird die Gruppe der Versicherten eingeführt. Die Zuordnung einer MXID zu dieser Gruppe kann über die Schnittstelle [api-messenger/src/openapi/TiMessengerInformation.yaml] erfolgen. Die folgende Abbildung zeigt beispielhaft die Verwendung der Gruppe anhand einer UI.

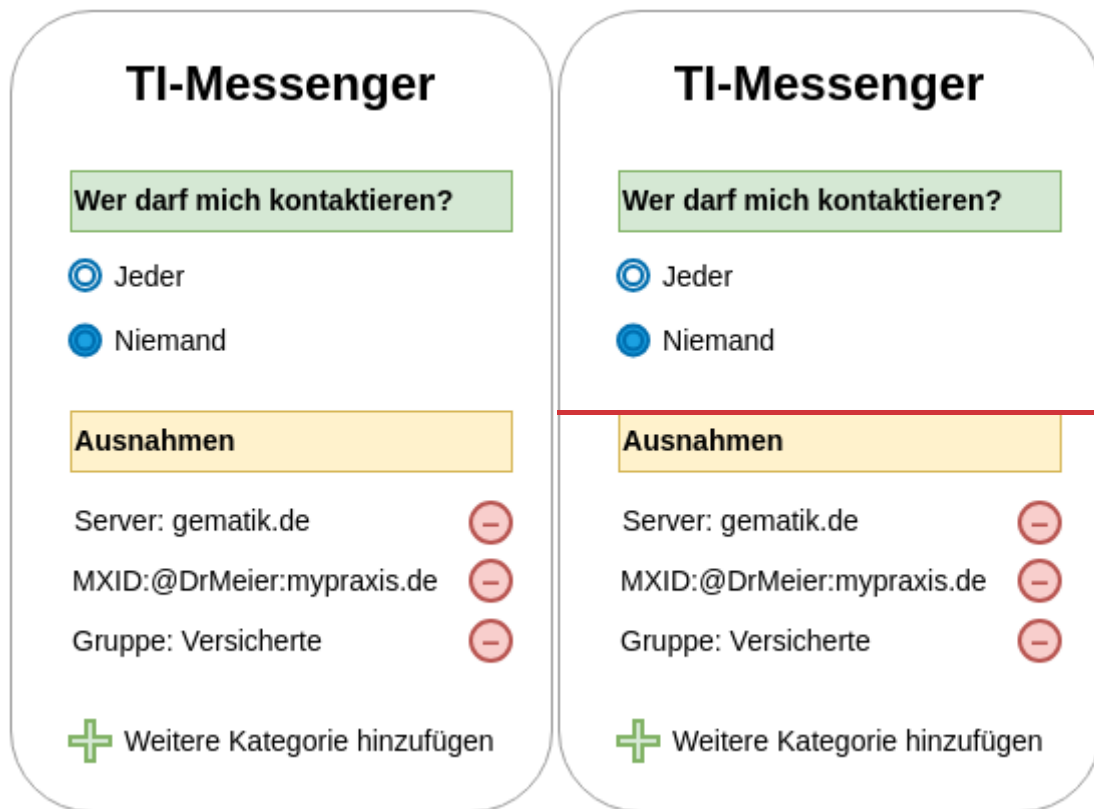


Abbildung 6: Beispielhaftes UI zum Setzen der Berechtigungen

Um die Berechtigung auf Gruppenebene nutzen zu können, wird für die Berechtigungskonfiguration für den TI-M Pro der folgende Namespace und das folgende Schema definiert.-

A_26389 --Event Type für Berechtigungskonfiguration

Der TI-M Client Pro MUSS für die Ablage der Berechtigungskonfiguration in den Accountdaten des Matrix-Homeservers

`de.gematik.tim.account.permissionconfig.pro.v1-`als Event Type verwenden. [<=]

A_26390 --Schema der Berechtigungskonfiguration

Die Daten der Berechtigungskonfiguration MÜSSEN dem JSON-Schema [api-messenger/src/schema/TI-M_Pro/permissionConfig_V1.json] entsprechen. [<=]

5.4 Management von Akteuren und Rollen

Aufgrund der Vielzahl an Teilnehmern wird eine komfortable Benutzerverwaltung innerhalb des TI-Messenger-Dienstes benötigt. In diesem Kapitel werden die für das User Management notwendigen Rollen und Nutzer-Verzeichnisse beschrieben.

Voraussetzung für die Nutzung des TI-Messenger-Dienstes ist zunächst, dass sich ein Akteur über ein Authentifizierungsverfahren am Matrix-Homeserver seiner Organisation authentifizieren kann und ein Nutzer-Account auf dem Matrix-Homeserver angelegt wurde. Der Nutzer-Account auf dem Matrix-Homeserver wird vom Akteur in der Rolle "Org-Admin" seiner Organisation bereitgestellt. Alternativ ist auch eine automatisierte Provisionierung möglich.

Bei der Erstellung des Nutzer-Accounts wird die MXID des Akteurs erzeugt sowie der Displayname des Akteurs festgelegt. Nach der Erstellung des Nutzer-Accounts am Matrix-Homeserver wird die MXID des Akteurs im User-Directory des Matrix-Homeservers hinterlegt. Alle im User-Directory des Matrix-Homeservers hinterlegten MXIDs sind anschließend durch andere Akteure seiner Organisation auffindbar und erreichbar. Soll der Akteur auch von außerhalb der Organisation auffindbar werden, so muss dieser mit seiner MXID in das Organisationsverzeichnis im VZD-FHIR-Directory hinterlegt werden. Das Hinterlegen der MXID eines Akteurs in das Organisationsverzeichnis muss durch den Akteur in der Rolle "Org-Admin" erfolgen. Voraussetzung ist das Vorhandensein einer HealthcareService-Ressource der Organisation. Die MXIDs werden in Endpoint-Ressourcen hinterlegt, die der HealthcareService-Ressource zugeordnet sind. Die Einrichtung einer HealthcareService-Ressource einer Organisation erfolgt durch den Akteur in der Rolle "Org-Admin". Möchte ein Akteur ohne Zugehörigkeit zu einer Organisation gefunden werden, so muss seine MXID in das Personenverzeichnis des VZD-FHIR-Directory hinterlegt werden. Voraussetzung hierfür ist der Besitz eines HBAs.

Die folgende Tabelle zeigt einen zusammenfassenden Überblick der Benutzerverwaltung.

Tabelle 8: Überblick der Benutzerverwaltung in Abhängigkeit der Rolle

Rolle	Client	Administration	Wo
Org-Admin	TI-Messenger Client mit Administrationsfunktionen (Org-Admin-Client)	<ul style="list-style-type: none"> Nutzer-Account anlegen Nutzer-Account verwalten 	Matrix-Homeserver (User Directory)
		<ul style="list-style-type: none"> HealthcareService-Ressource anlegen Endpoint einer HealthcareService-Ressource anlegen Endpoint einer HealthcareService-Ressource verwalten 	VZD-FHIR-Directory (Organisationsverzeichnisse)
User	TI-Messenger Client	<ul style="list-style-type: none"> Nutzer-Account anlegen 	Matrix-Homeserver (User Directory)

Hinweis: Der TI-M Fachdienst Anbieter kann eine automatisierte Provisionierung von Nutzer-Accounts umsetzen. Details eines entsprechenden Verfahrens werden von der gematik nicht spezifiziert und obliegen dem Anbieter.

5.5 UnterbindLöschen von Inhalten – Anpassung-der-Versen

Dieses Kapitel ergänzt das gleichertenkommunikation-beim-Verlassen-eines-Raumenamige Kapitel aus [gemSpec TI-M Basis] mit Regelungen für TI-M Pro Fachdienste und Clients.

5.5.1 Serverseitiges Löschen

5.5.6 Matrix-Events

A_26463—Sperrungitarbeiter des Gesundheitswesens sind ihren Organisationen und **der-weien Regeln unterführenden-Kommunik**geordnet. Für diese Organisation-**nach Verlassen des Raumes**

Der Anbieter MUSS die Organisation, welche den TI-Messenger-Dienst von ihm bezieht, darüber informieren wiederum gelten gesetzliche Vorgaben zur Datenhaltung, die eine automatische serverseitige Löschung nötig machen können. Beispiele hierfür sind DSGVO Art. 17 und SGB 5 § 304. TI-M Pro Fachdienste dürfen Matrix-Events daher bei Bedarf auch ohne Einwilligung der Raumteilnehmer löschen.

Die Löschoption selbst darf dabei allerdings nur server-lokal und ohne direkte Auswirkung auf die Föderation erfolgen damit Löschkonfigurationen auf unterschiedlichen Servern nicht interferieren, dass-Leist. Eine serverlokale Löschung schließt z. B. die Verwendungserbring von Redactions oder das Kicken der vor-dem-Nutzer anderer HomeserverVerlassen aus.

Die konkrete Ausgestaltung eines-Raumes, in dem-r automatischen serverseitigen Löschfunktion wird darüber hinausausschließlich-Versicherte durch die Spezifikation nicht näher vorgegeben. Hier gibt es verbleiben, diesenschiedene Möglichkeiten. so zu konfigurieren,könnten z. B. Nutzer des eigenen Homeservers aus Räumen entfernt werden und diese Räume samt der zugehörigen Events dass-eine-weinn aus der Datenbank des Servers gelöscht werden. Alternativ wäre auch ein fortlaufende Kommunikation-unters Löschen von veralteten Events aus der den-atenbank des SerVers möglichert, wobei der Raum selbst bestehen unterbundenbleibt. Homeserver wird. Diese e Synapse bieten hierfür Konfigurierbare Message Retention kann z. B. durch Entfernen dPolicies an.

Damit Inhalte nicht unerwartet verloren gehen, müssen Nutzer Versiüber etwaige automatische-enters aus-dem-Raum-oder die-Einstell Löschfunktionen informiert werden. Die konkrete Form dieser Information bleibt dabei dem Anbieter überlassen. So könnten einzelne Räumlöschung-entsprechender-Poen z. B. über Server Notices angekündigt wer-Levels im Raum erfolgen.[-=>]

Hinweis: Die Unterbindden. Alternativ wäre es auch denkbar, dass nur einmalig über feste Löschintervalle informiert wird.

A 28340 -Lokale Beschränkung der automatischen serverseitigen Löschung der weiterführenden-Kommunikavon Events

~~Implementieren TI-M Pro Fachdienste Funktionen zum automatischen Löschen~~
~~Versicherten erfolgte Matrix-Events, so MUSS die Löschung serverlokal unter Erhalt der~~
~~zuvor in den jeweiligen Räumen ohne direkten Einfluss auf die Föderation erfolgen. [<=]~~

A 28341 -Information über ~~ausgetau~~tomatischten Nachrichten, sodass Versicherte **serverseitige Löschung von Events**

~~Nutzen TI-M Pro Anbieter Funktionen versorgungsrelevante Infor~~ zur automatischen
~~serverseitigen Löschung von mationen nicht verloren gehen-rix-Events, so MÜSSEN sie~~
~~ihre Nutzer vorab darüber informieren. [<=]~~

6 Anhang A – Verzeichnisse

6.1 Abkürzungen

Tabelle 9: Im Dokument verwendete Abkürzungen

Kürzel	Erläuterung
API	Application Programming Interface
ePA	elektronische Patientenakte
FD	Fachdienst
IdP	Identity Provider
KIM	Kommunikation im Medizinwesen
TLS	Transport Layer Security
VZD	Verzeichnisdienst

6.2 Glossar

Tabelle 10: Im Dokument verwendete Begriffe

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

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

6.3 Abbildungsverzeichnis

Abbildung 1: Betriebsmodell TI-M Pro	16
Abbildung 2: Laufzeitsicht – Organisationsressourcen im Verzeichnisdienst hinzufügen ..	19
Abbildung 3: Laufzeitsicht – Akteur (User-HBA) im Verzeichnisdienst hinzufügen	21
Abbildung 4: Laufzeitsicht – Practitioner – FHIR-VZD-Sichtbarkeit für Versicherte setzen	23

Abbildung 5: Laufzeitsicht – Organization – FHIR VZD-Sichtbarkeit für Versicherte setzen	24
Abbildung 6: Laufzeitsicht – Anmeldung eines Akteurs am Messenger-Service	26
Abbildung 7: Einladung von Akteuren innerhalb einer Organisation	28
Abbildung 8: Beispielhaftes UI zum Setzen der Berechtigungen	30
Abbildung 1: Betriebsmodell TI-M Pro	19
Abbildung 2: Laufzeitsicht - Organisationsressourcen im Verzeichnisdienst hinzufügen	22
Abbildung 3: Laufzeitsicht - Akteur (User-HBA) im Verzeichnisdienst hinzufügen	24
Abbildung 4: Laufzeitsicht - Anmeldung eines Akteurs am Messenger-Service	31
Abbildung 5: Einladung von Akteuren innerhalb einer Organisation	35
Abbildung 6: Beispielhaftes UI zum Setzen der Berechtigungen	37

6.4 Tabellenverzeichnis

Tabelle 1: Akteure und Rollen	7
Tabelle 2: Arten von Token	8
Tabelle 3: Schreibzugriff – VZD-FHIR-Ressourcen	11
Tabelle 4: AF – Organisationsressourcen im Verzeichnisdienst hinzufügen	17
Tabelle 5: AF – Akteur (User-HBA) im Verzeichnisdienst hinzufügen	20
Tabelle 6: Practitioner – FHIR VZD-Sichtbarkeit für Versicherte setzen	22
Tabelle 7: Organization – FHIR VZD-Sichtbarkeit für Versicherte setzen	23
Tabelle 8: AF – Anmeldung eines Akteurs am Messenger-Service	25
Tabelle 9: Einladung von Akteuren innerhalb einer Organisation	27
Tabelle 10: Überblick der Benutzerverwaltung in Abhängigkeit der Rolle	31
Tabelle 11: Im Dokument verwendete Abkürzungen	33
Tabelle 12: Im Dokument verwendete Begriffe	33
Tabelle 13: Referenzierte Dokumente der gematik	34
Tabelle 14: Weitere Dokumente	35

Tabelle 1: Akteure und Rollen	8
Tabelle 2: Arten von Token	9
Tabelle 3: Schreibzugriff - VZD-FHIR-Ressourcen	13
Tabelle 4: AF - Organisationsressourcen im Verzeichnisdienst hinzufügen	20
Tabelle 5: AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen	23
Tabelle 6: AF - Anmeldung eines Akteurs am Messenger-Service	28

Tabelle 7: Einladung von Akteuren innerhalb einer Organisation	32
Tabelle 8: Überblick der Benutzerverwaltung in Abhängigkeit der Rolle	38
Tabelle 9: Im Dokument verwendete Abkürzungen	41
Tabelle 10: Im Dokument verwendete Begriffe	41
Tabelle 11: Referenzierte Dokumente der gematik	43
Tabelle 12: Weitere Dokumente	43

6.5 Referenzierte Dokumente

6.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur.

Tabelle 11: Referenzierte Dokumente der gematik

[Quelle]	Herausgeber: Titel
[api-messenger]	gematik: Implementierungsleitfaden zum TI-Messenger https://github.com/gematik/api-ti-messenger
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar
[gemSpec_SST_LD_BD]	gematik: Spezifikation Logdaten- u. Betriebsdatenerfassung
[gemSpec_TI-M_Basis]	gematik: Spezifikation TI-Messenger (Basis)
[gemSpec_TI-M_ePA]	gematik: Spezifikation TI-Messenger (ePA)
[gemSpec_VZD_FHIR_Directory]	gematik: Spezifikation Verzeichnisdienst FHIR-Directory

6.5.2 Weitere Dokumente

Tabelle 12: Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[Client-Server API]	Matrix Foundation: Matrix Specification - Client-Server API https://spec.matrix.org/v1.11/client-server-api/
[RFC2119]	IETF: Key words for use in RFCs to Indicate Requirement Levels https://datatracker.ietf.org/doc/html/rfc2119

[Server-Server API]	Matrix Foundation: Matrix Specification - Server-Server API https://spec.matrix.org/v1.11/server-server-api
---------------------	--