

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation TI-Messenger Pro

Version:	1. 1 2.0_CC
Revision:	1 4372421685359
Stand:	25.11.20 2510.08.2026
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_TI-M_Pro

Dokumentinformationen

Gender-Hinweis

Aus Gründen der besseren Lesbarkeit wird in diesem Dokument überwiegend die männliche Form verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

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
1.1.0	25.11.2025		Einarbeitung TI-Messenger_25_3	gematik
1.1.1	03.03.2025		Einarbeitung TI-Messenger_26_1 (HotFix)	gematik
1.2.0	10.08.2026		Einarbeitung TI-Messenger_26_2	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes	7
1.1 Zielsetzung	7
1.2 Zielgruppe	7
1.3 Geltungsbereich	7
1.4 Abgrenzungen	7
1.5 Methodik	8
2 Systemüberblick	9
2.1 Akteure und Rollen	9
2.1.1 Akteur: Chatbot	9
2.1.2 Rolle: "Org Admin"	9
2.1.3 Rolle: "User HBA"	9
2.2 Nachbarsysteme	10
2.2.1 VZD-FHIR-Directory	10
2.3 Zugriffstoken	10
3 Zerlegung des Produkttyps	12
3.1 TI-M Client Pro	12
3.1.1 Ausprägungen nach Nutzergruppen	12
3.1.1.1 TI-M Client Pro für Akteure in der Rolle "Org Admin" (Org Admin-Client)	12
3.1.2 Ausprägungen nach Plattform	12
3.1.2.1 TI-M Client als Web-Anwendung	12
3.1.3 Matrix-Spezifikation	13
3.1.3.1 Ergänzungen zum Erstellen von / Verhalten in Räumen	13
3.1.4 VZD-FHIR-Directory	13
3.1.4.1 Schreibzugriff	14
3.1.5 Sichtbarkeit	14
3.2 TI-M FD-Pro	15
3.2.1 Registrierungs-Dienst	15
3.2.1.1 I_requestToken	15
3.2.1.1.1 RegService-OpenID-Token	16
3.2.2 Messenger-Service	16
3.2.3 Matrix-Spezifikation	17
3.2.3.1 Weitere Ergänzungen/Einschränkungen zur Matrix-Spezifikation	17
4 Übergreifende Festlegungen	27
4.1 Datenschutz und Sicherheit	27
4.2 Betrieb	28
5 Funktionsmerkmale	30
5.1 Anwendungsfälle	30
5.1.1 Organisationsressourcen im Verzeichnisdienst hinzufügen	31

5.1.2 Akteur (User-HBA) im Verzeichnisdienst hinzufügen	35
5.1.3 Anmeldung eines Akteurs am Messenger Service	37
5.1.4 Einladung von Akteuren innerhalb einer Organisation	41
5.2 Funktionsaccounts	44
5.2.1 Chatbot	46
5.3 Berechtigungsmanagement – Anpassungen	46
5.3.1 Akteursspezifische Berechtigungskonfiguration	46
5.4 Management von Akteuren und Rollen	48
5.5 Löschen von Inhalten – Anpassungen	50
5.5.1 Serverseitiges Löschen	50
5.5.1.1 Matrix Events	50
6 Anhang A – Verzeichnisse	57
6.1 Abkürzungen	57
6.2 Glossar	57
6.3 Abbildungsverzeichnis	57
6.4 Tabellenverzeichnis	58
6.5 Referenzierte Dokumente	59
6.5.1 Dokumente der gematik	59
6.5.2 Weitere Dokumente	60
1 Einordnung des Dokumentes	7
1.1 Zielsetzung	7
1.2 Zielgruppe	7
1.3 Geltungsbereich	7
1.4 Abgrenzungen	7
1.5 Methodik	8
2 Systemüberblick	9
2.1 Akteure und Rollen	9
2.1.1 Akteur: Chatbot	9
2.1.2 Rolle: "Org-Admin"	9
2.1.3 Rolle: "User-HBA"	9
2.2 Nachbarsysteme	10
2.2.1 VZD-FHIR-Directory	10
2.3 Zugriffstoken	10
3 Zerlegung des Produkttyps	12
3.1 TI-M Client Pro	12
3.1.1 Ausprägungen nach Nutzergruppen	12
3.1.1.1 TI-M Client Pro für Akteure in der Rolle "Org-Admin" (Org-Admin-Client)	12
3.1.2 Ausprägungen nach Plattform	12
3.1.2.1 TI-M Client als Web-Anwendung	12
3.1.3 Matrix Spezifikation	13
3.1.3.1 Ergänzungen zum Erstellen von / Verhalten in Räumen	13

3.1.4 VZD-FHIR-Directory	13
3.1.4.1 Schreibzugriff	14
3.1.5 Sichtbarkeit	14
3.2 TI-M FD Pro	15
3.2.1 Registrierungs-Dienst	15
3.2.1.1 <i>I_requestToken</i>	15
3.2.1.1.1 RegService-OpenID-Token	16
3.2.2 Messenger-Service	16
3.2.3 Matrix Spezifikation	17
3.2.3.1 <i>Weitere Ergänzungen/Einschränkungen zur Matrix-Spezifikation</i>	17
3.3 TI-M Pro Headless Client	17
3.3.1 Sicherheit	19
3.3.1.1 <i>Betriebliche Sicherheitsaspekte</i>	19
3.3.1.2 <i>Absicherung der Headless-Client API</i>	20
3.3.1.3 <i>Kryptografische Sicherheit</i>	20
3.3.1.4 <i>Logging, Audit und Nachvollziehbarkeit</i>	21
3.3.1.5 <i>Sicherheitsvorfälle und Incident Handling</i>	21
3.3.2 Test	22
3.3.2.1 <i>Testvorgehen</i>	22
3.3.3 Betrieb	22
3.3.3.1 <i>Anbieter</i>	22
3.3.3.2 <i>Client</i>	24
3.3.4 Produkt und Anbieterkonstellationen	25
4 Übergreifende Festlegungen	27
4.1 Datenschutz und Sicherheit	27
4.2 Betrieb	28
5 Funktionsmerkmale	30
5.1 Anwendungsfälle	30
5.1.1 Institutionsidentitäten verwalten	30
5.1.2 Organisationsressourcen im Verzeichnisdienst hinzufügen	31
5.1.3 Akteur (User-HBA) im Verzeichnisdienst hinzufügen	35
5.1.4 Anmeldung eines Akteurs am Messenger-Service	37
5.1.5 Einladung von Akteuren innerhalb einer Organisation	41
5.2 Organisationsressourcen im Verzeichnisdienst	44
5.2.1 Akteur	45
5.2.2 Funktionsaccount	45
5.2.3 (Chat)bot	46
5.3 Berechtigungsmanagement - Anpassungen	46
5.3.1 Akteursspezifische Berechtigungskonfiguration	46
5.4 Management von Akteuren und Rollen	48
5.4.1 Zusätzliche Attribute in den User Profilen	49
5.5 Löschen von Inhalten – Anpassungen	50
5.5.1 Serverseitiges Löschen	50
5.5.1.1 <i>Matrix-Events</i>	50
5.6 Strukturierte Daten – Anpassungen	51
5.6.1 Austausch von FHIR-Ressourcen	51

5.7 Organisationsspezifische Raumnamen	53
6 Anhang A – Verzeichnisse	57
6.1 Abkürzungen	57
6.2 Glossar	57
6.3 Abbildungsverzeichnis.....	57
6.4 Tabellenverzeichnis	58
6.5 Referenzierte Dokumente.....	59
6.5.1 Dokumente der gematik.....	59
6.5.2 Weitere Dokumente.....	60

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 5.1.23- 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	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. 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.

Token	ausgestellt vom	Beschreibung
owner-accesstoken	Auth-Service des VZD-FHIR-Directory	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 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 [5.1.1.2 - 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

[<=]

A_30032 -weitere Organisationen

Der Org-Admin-Client SOLL die Verwaltung mehrere Organisations-Entitäten([5.1.1.1 - Institutionsidentitäten verwalten](#)) unterstützen und diese dem Org-Admin bei der Verwaltung von FHIR-VZD Ressourcen zur Auswahl anbieten.[<=]

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 Ergänzungen zum Erstellen von / Verhalten in Räumen

A_25325-02A_25325-01 -Erzeugung öffentlicher Räume

Der TI-M Client Pro MUSS dem Akteur erlauben Räume anzulegen, in denen **sowohl** die Join Rule **als auch die Room Directory Visibility** auf `public` gesetzt ist. In diesem Fall MUSS `m.federate = false` im `creation_content` gesetzt werden. [≤]

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

A_25324-02A_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:~~

- die Join Rule ~~auf~~ `public`, ~~restricted oder knock_restricted~~

und die History Visibility ~~auf~~ `world_readable` oder `shared` gesetzt sind. [≤]

Um zu verhindern, dass Akteure sensible Inhalte unbeabsichtigt mit falschen Empfängern teilen ist es notwendig diese dafür zu sensibilisieren, dass sie sich gerade in einem Raum befinden, in dem viele Personengruppen Zugriff auf die Inhalte haben. Dies trifft vor allem auf Räume zu in denen es keine Zugriffsbeschränkung gibt, die unverschlüsselt sind oder in denen die Historie von allen gelesen werden kann. Die Hersteller und Anbieter sind angehalten die Akteure durch die UI auf diesen Zustand hinzuweisen wodurch sich die folgende Afo ergibt.

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

[≤]

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. [≤]

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. [≤]

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" sowie Akteure in der Rolle "Org-Admin" können die Sichtbarkeit ihrer hinterlegten Informationen an einem Endpoint im VZD-FHIR Directory konfigurieren. Wird der Endpunkt als zu verbergen markiert, dann wird dieser nicht

mehr Teil der Ergebnismenge sein, sofern Akteuren in der Rolle "Versicherter"¹ eine Suche am VZD_FHIR_Directory absetzen. Details zur Administration der Sichtbarkeit 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_30016 -Token für jede SM(C)-B Identität

Der TI-M Fachdienst Pro SOLL über die Schnittstelle I_request Token anbieten für jede über [5.1.1-1- Institutionenidentitäten verwalten](#) registrierte Identität einen RegService-OpenID-Token bereitzustellen. [<=]

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"
  "x5c": [ [SEP] "<X.509 Sig-Cert, base64-encoded DER>" ]
}
PAYLOAD
{
  "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>",
  "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_26515-01 -Zutrittsbeschränkung für öffentliche Räume

Der TI-M FD MUSS in Räumen mit der Join Rule `public` sicherstellen, dass diese immer mit `m.federate=false` erzeugt werden. [`<=`]

A_28755 -Zutrittsbeschränkung für historische öffentliche Räume

Ist in einem Raum, die Join Rule `public` gesetzt, ohne dass gleichzeitig `m.federate=false` gesetzt ist, so MUSS der TI-M FD 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 und `M_INVALID_ROOM_STATE` ablehnen wenn die Anfrage die Join Rule im Raum auf `public` setzt.
[`<=`]

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 unauthentifizierten 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~~

~~3.3 Der TI-M FD MUSS Requests zum Endpunkt~~

~~`/_matrix/federation/v1/publicRooms` mit einer HTTP 403 Response ablehnen.[`<=`]~~

3.4 TI-M Pro Headless Client

Der TI-M Pro Headless Client ist eine Unterausprägung des TI-M Pro Client, die dazu dient eine verbesserte Integration und Nutzbarkeit von TI-Messenger Pro Clients in medizinischen Informationssystemen und Backend-Systemen der gesetzlichen Krankenversicherungen zu ermöglichen. Im Unterschied zum TI-M Pro Client kann der Headless Client nicht direkt über eine grafische Oberfläche bedient werden.

A_28650 -Keine grafische Oberfläche

Der TI-M Pro Headless Client DARF Endanwendern KEINE grafische Benutzeroberfläche anbieten. [`<=`]

Stattdessen verfügt der Headless Client über eine Schnittstelle, die sogenannte *Headless-Client-API*, die von anderen Systemen angesprochen werden kann. Diese API ist zur direkten Integration in das verwendende System im Sinne eines Moduls bzw. einer Bibliothek gedacht. Sie darf daher nicht als Netzwerkschnittstelle ausgestaltet werden.

A_28653 -Headless-Client-API

Der TI-M Pro Headless Client MUSS eine Schnittstelle zur Verwendung durch integrierende Systeme anbieten. [<=]

A_28854 -Headless-Clients Fehlercodes

Der Headless-Client MUSS die Fehlercodes der Matrix Client-Server Schnittstelle und die Fehlercodes aus der TI-Messenger Spezifikation an das integrierende System weiterreichen. [<=]

A_28651 -Keine Netzwerkschnittstelle

Die Schnittstelle für integrierende Systeme am TI-M Pro Headless Client DARF KEINE Netzwerkschnittstelle sein, egal ob lokal oder öffentlich. [<=]

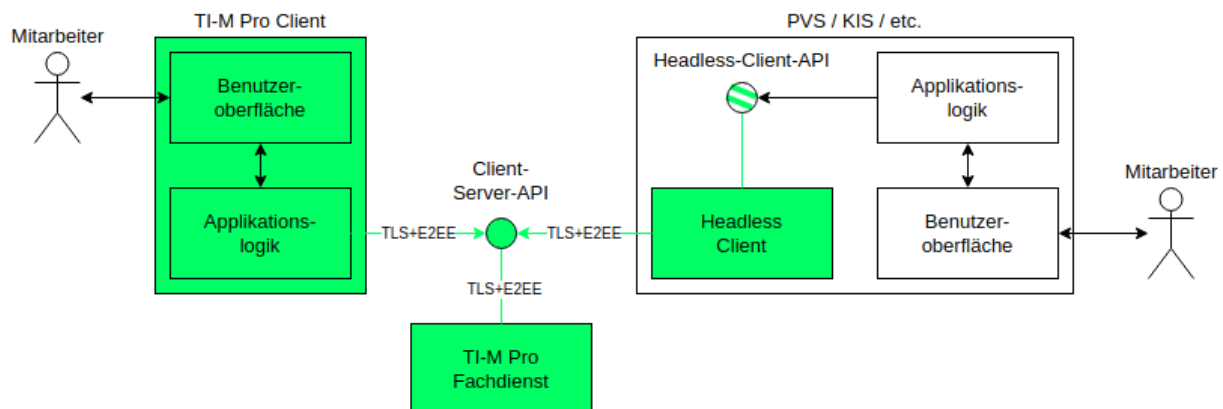


Abbildung 1: Übersicht Headless Client Architektur. Farbig: von der gematik (teil-)regulierte Komponenten.

Unabhängig von den Vorgaben für die Headless-Client-API darf das integrierende System selbst Netzwerkschnittstellen bereitstellen, über welche die Headless-Client-API direkt oder indirekt angesprochen wird.

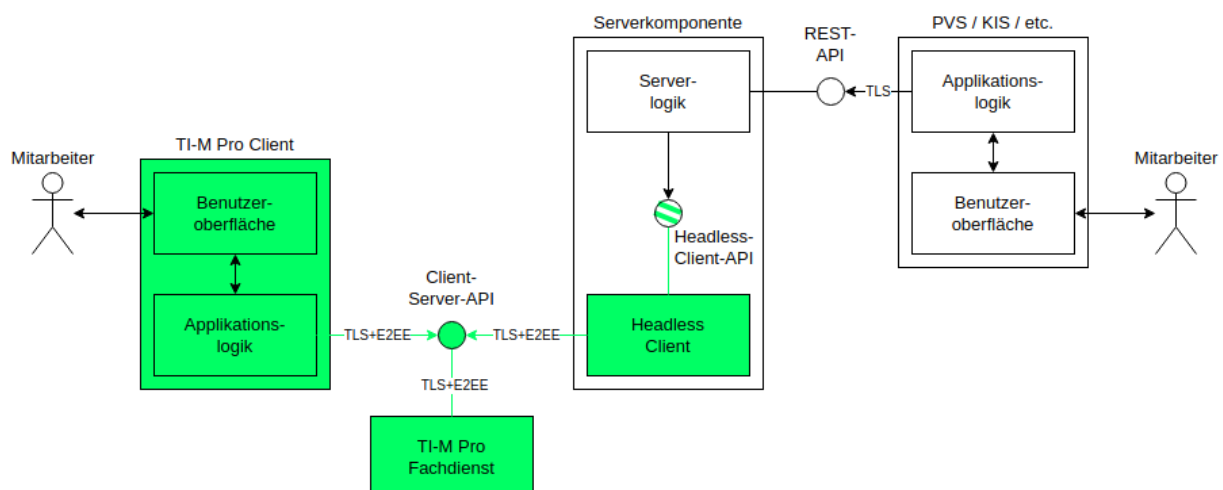


Abbildung 2: Beispiel für Integration des Headless Client in eine Serverkomponente mit Netzwerkschnittstelle. Farbig: von der gematik (teil-)regulierte Komponenten.

Nachrichtenschlüssel müssen sicher im Headless Client verwahrt werden und dürfen nicht über die Headless-Client-API ausgeleitet werden. Das bedeutet der Headless Client bildet

den Endpunkt der Ende-zu-Ende-Verschlüsselung (E2EE) im Sinne des Matrix-Protokolls. Nähere Details zu diesem Punkt finden sich im nachfolgenden Unterkapitel [3.3.1-Sicherheit](#).

Weitere Einzelheiten der Headless-Client-API (wie z. B. konkrete Technologien, Interfaces oder Methoden) werden von der gematik nicht vorgegeben. Diese Aspekte liegen stattdessen in der Hoheit der Hersteller. Des Weiteren ergibt sich aus der Verwendung der Headless-Client-API keine Zulassungspflicht für das integrierende System.

Für die Authentifizierung des Headless Clients am Fachdienst werden die Mechanismen aus TI-M Pro wiederverwendet. Dabei kann das integrierende System die Anmeldung am Fachdienst über die Headless-Client-API steuern. Da der Headless Client direkt in das verwendende System integriert wird, gibt es am Headless Client selbst jedoch keine Anmelde-mechanismen. Diese Mechanismen werden stattdessen im integrierenden System umgesetzt. Anbieter können dadurch bei Bedarf auch eine Trennung zwischen den vom Headless Client verwendeten Accounts am Fachdienst und den von Mitarbeitern verwendeten Accounts am integrierenden System realisieren. So wäre es z. B. denkbar, dass jeder Mitarbeiter einen eigenen Account am integrierenden System hat, der Headless Client aber nur einen einzigen Matrix-Account am Fachdienst benutzt. Nach außen könnten alle Mitarbeiter dadurch unter derselben Matrix-ID kommunizieren. Alternativ könnte der Headless Client aber auch so integriert sein, dass sich Mitarbeiter direkt mit ihren personalisierten Matrix-Accounts anmelden.

3.4.1 Sicherheit

Dieses Kapitel legt die sicherheitstechnischen Ziele, Grundannahmen und Abgrenzungen für den Headless Client fest. Es beschreibt Maßnahmen zum Schutz sicherheitsrelevanter Funktionen, Daten und Zustände. Die Sicherheitsanforderungen adressieren ausschließlich den Betrieb des Headless Client als Bestandteil eines Systems (zum Beispiel PVS). Andere Betriebsformen oder Ausführungsumgebungen des Headless Clients sind nicht Gegenstand dieser Spezifikation und werden durch die gematik nicht abgesichert.

Ziel der Sicherheitsanforderungen ist es, den Headless Client so auszugestalten, dass sicherheitskritische Funktionen ausschließlich innerhalb eines definierten und kontrollierten Sicherheitskontextes ausgeführt werden. Dabei sollen insbesondere Risiken aus Fehlbedienung, fehlerhafter Integration, unzureichend abgesicherten Schnittstellen sowie aus unbeabsichtigten Implementierungsfehlern systematisch begrenzt werden.

3.4.1.1 Betriebliche Sicherheitsaspekte

Ziel ist es, sicherzustellen, dass der Headless Client ausschließlich innerhalb einer definierten, kontrollierten und vertrauenswürdigen Betriebsumgebung eingesetzt wird und dass sicherheitsrelevante Funktionen nur unter klar geregelten betrieblichen Voraussetzungen ausgeführt werden. Ein wesentliches Element des sicheren Betriebs ist zudem die Kontrolle der eingesetzten Softwareversionen des konkret ausgelieferten Softwareartefakts. Der Hersteller des Headless Clients kontrolliert seine Softwareversion durch die Freigabe einer signierten Version, die technische Signierung des Artefakts sowie die Dokumentation der Freigabe. Die Ausgestaltung der digitalen Signatur erfolgt herstellereigenspezifisch, die dafür verwendeten Zertifikate stammen vom Hersteller selbst.

A_28703 -Ausführungsumgebung

Der TI-M Pro Headless Client MUSS innerhalb einer geschützten Ausführungsumgebung betrieben werden, die eine wirksame Trennung gegenüber anderen Komponenten, Modulen und Erweiterungen gewährleistet. Eine geschützte Ausführungsumgebung ist eine Umgebung, in der mindestens die Prozess- und Zugriffskontrolle durch das

Betriebssystem gewährleistet ist, ausschließlich freigegebene Softwareversionen des TI-Messenger Headless Client ausgeführt werden und keine nicht autorisierten Manipulations- oder Debug-Mechanismen aktiv sind. Es müssen technische und organisatorische Maßnahmen umgesetzt werden, um den Headless Client gegenüber anderen Organisationseinheiten abzugrenzen und den Zugang zu kontrollieren. Der Schutz vor Kompromitierung der zugrunde liegenden Plattform oder vor privilegierten Administratoren ist nicht Bestandteil dieses Sicherheitskonzepts. [<=]

A_28704 -Ansteuerung

Der TI-M Pro Headless Client MUSS als eigenständiges Modul implementiert sein und DARF im produktiven Betrieb ausschließlich über vorgesehene lokale Funktionsaufrufe angesteuert werden. [<=]

A_28727 -Hinweis des Anbieters

Der Anbieter MUSS in der technischen Dokumentation explizit und nachvollziehbar darauf hinweisen, dass der TI-M Pro Headless Client in der Produktivversion ausschließlich über vorgesehene lokale Funktionsaufrufe angesteuert werden darf. [<=]

A_28707 -Freigegebene Version ausführen

Der Anbieter des TI-M Pro Headless Clients MUSS sicherstellen, dass die Verwendung des Headless Clients auf signierte, geprüfte und freigegebene Versionen beschränkt ist. Der Integrator MUSS einerein kryptografische Offline-Prüfung (Signaturprüfung) gegen einen lokal hinterlegten Vertrauensanker beim Laden des Artefakts durchführen (soweit dies technisch möglich ist) und MUSS die Ausführung verweigern, wenn ein Verifikationsfehler auftritt. Ein Vertrauensanker kann eine definierte Zertifikatskette sein. [<=]

3.4.1.2 Absicherung der Headless-Client API

Die Schnittstellen des Headless Clients stellen sicherheitskritische Einstiegspunkte dar, über die Funktionen mit Auswirkungen auf Vertraulichkeit, Integrität und korrekte Nutzung sensibler Daten ausgelöst werden können. Daher müssen diese Schnittstellen so gestaltet und abgesichert sein, dass missbräuchliche, fehlerhafte oder unvollständige Aufrufe erkannt und vor Ausführung unterbunden werden. Ziel ist es, sicherzustellen, dass sämtliche über die Schnittstellen ausgelöste Funktionsaufrufe ausschließlich in zulässiger, kontrollierter und sicherheitskonformer Weise erfolgen.

A_28699 -Prüfung von Funktionsaufrufen

Der TI-M Pro Headless Client MUSS sicherstellen, dass Funktionsaufrufe nur ausgeführt werden, wenn die angegebenen Parameter konsistent und für die angeforderte Funktion technisch zulässig sind. [<=]

3.4.1.3 Kryptografische Sicherheit

Dieses Unterkapitel beschreibt die Sicherheitsziele zum Schutz kryptografischer Schlüssel, Ende-zu-Ende Verschlüsselung (E2EE) sowie temporärer kryptischer Sitzungszustände. Ziel ist es, sicherzustellen, dass kryptografisches Material ausschließlich innerhalb des Sicherheitskontextes des Headless Clients verarbeitet wird.

Das Vorgehen zur Integration des Headless Clients mit einem Virens Scanner ist identisch zum Vorgehen beim TI-M Client Pro. Der Headless Client kann Dateien vor dem Download von einer fachdienstseitigen Schnittstelle auf Schadsoftware prüfen lassen und nur bei erfolgreicher Prüfung über die Headless-Client-API zugänglich machen. Es gelten hierbei die Anforderungen aus TI-M Basis.

A_28710 -Verschlüsselte Kommunikation

Der TI-M Pro Headless Client MUSS der alleinige kryptografische Endpunkt für die Ende-zu-Ende verschlüsselte Kommunikation sein. [≤]

A_28713 -Schutzmechanismen

Der Anbieter des TI-M Pro Headless Clients MUSS sicherstellen, dass sicherheitsrelevante Prüf- und Schutzmechanismen des Headless Clients im Produktivbetrieb nicht modifiziert, umgangen oder außer Kraft gesetzt werden. [≤]

A_28715 -Kryptografische Isolation

Das TI-M Pro Headless Client MUSS sicherstellen, dass kryptografisches Schlüsselmaterial, interne E2EE-Zustände und andere sicherheitsrelevante Laufzeitinformationen weder ausgelesen, manipuliert oder rekonstruiert werden können. Im Produktbetrieb dürfen keine detaillierten Exception-Dumps erzeugt oder persistiert werden, die Rückschlüsse auf kryptografische Schlüssel oder E2EE-Zustände des Headless Clients zulassen. [≤]

A_28734 -Absicherung integrierender Netzwerkschnittstellen

Der Anbieter TI-Messenger Pro MUSS in den bereitgestellten Komponenten, Referenzarchitekturen und Integrationsvorgaben sicherstellen, dass Daten, die über seine Funktionsaufrufe zur Weiterverarbeitung bereitgestellt werden, ausschließlich über TLS-gesicherte und dem aktuellen Stand der Technik entsprechende Netzwerkschnittstellen des integrierenden Systems übertragen werden. Der Anbieter MUSS in seiner technischen Dokumentation und im Betriebshandbuch für Org-Admins explizit und nachvollziehbar darauf hinweisen. [≤]

3.4.1.4 Logging, Audit und Nachvollziehbarkeit

Ziel ist es, sicherheitsrelevante Entscheidungen, Zustandsänderungen und erkannte Fehl- und Missbrauchssituationen nachvollziehbar zu erfassen, ohne dabei selbst neue Sicherheitsrisiken zu erzeugen.

A_28720 -Protokolle

Der TI-M Pro Headless Client MUSS sicherstellen, dass sicherheitsrelevante Protokolle und Ereignisdaten unverändert und zeitlich korrekt erzeugt werden. Zu den sicherheitsrelevanten Ereignissen zählen insbesondere: Entscheidungen über die Ablehnung von Funktionsaufrufen, erkannte Fehl- oder Missbrauchssituation sowie sicherheitsrelevante Zustands- oder Konfigurationsänderungen. [≤]

A_28728 -Integrität von Audit-Logs

Der Anbieter MUSS in der technischen Dokumentation explizit und nachvollziehbar darauf hinweisen, dass die Erzeugung und Weitergabe von Audit-Logs durch den Headless Client nicht durch externe Konfigurationen oder von externen Komponenten, Modulen und Erweiterungen deaktiviert, unterdrückt oder manipuliert werden dürfen. [≤]

3.4.1.5 Sicherheitsvorfälle und Incident Handling

Das Incident Handling umfasst nicht nur die Erkennung, sondern auch die Unterstützung angemessener Reaktionsmaßnahmen, wie etwa die temporäre Einschränkung von Funktionen, die kontrollierte Deaktivierung des Headless Clients oder die Übergabe relevanter Informationen an übergeordnete Sicherheits- und Betriebsprozesse.

A_28721 -Erkannter Vorfall und Risikominimierung

Der TI-M Pro Headless Client MUSS bei erkannter Manipulation oder sonstigen sicherheitsrelevanten Abweichungen geeignete Maßnahmen zur Risikominimierung ergreifen und Funktionen einschränken oder den Betrieb mit einer aussagekräftigen

Rückmeldung kontrolliert beenden. Erkannte Manipulationen können zum Beispiel unzulässige Änderungen sicherheitsrelevanter Parameter, inkonsistente Sicherheitszustände, unerwartete Wechsel sicherheitsrelevanter Flags, nicht erlaubte Aufrufreihenfolgen oder das Replay von Transaktions-IDs sein. Zur Verhinderung von Reverse-Engineering sollten Funktionen nur generische Fehlermeldungen und keine technischen Details zum Fehler nach extern weitergeben. Der Headless Client MUSS sicherheitsrelevante Regelverletzungen protokollieren, insbesondere unzulässige oder abgelehnte Funktionsaufrufe, Verstöße gegen definierte Kontexte und Berechtigungsregeln, erkannte Anomalien im Aufrufverhalten und sicherheitsrelevante Zustandsinkonsistenzen. [<=]

3.4.2 Test

Dieses Kapitel ergänzt das gleichnamige Kapitel aus [gemSpec_TI-M_Basis] mit Regelungen für den TI-M Headless Client.

3.4.2.1 Testvorgehen

Der TI-M Headless Client benötigt ebenfalls eine Testtreiberschnittstelle. Diese Testtreiberschnittstelle wurde in der Übersicht "Headless Client Architektur" nicht dargestellt wird aber für die Zulassung der TI-M Headless Clients benötigt. Das Testtreiber-Module kann für die Zulassung isoliert von der späteren Lösung betrieben werden. Die Zulassung beschränkt sich ausschließlich auf den TI-M Client, das dahinter liegendem System wird nicht betrachtet. Durch den Wegfall der grafische Benutzeroberfläche werden bei der Zulassung des TI-M Headless Clients keine "Look and Feel" Workshops und keine manuellen Tests durchgeführt.

A_28678 -Tests des TI-M Pro Headless Clients gegen die Referenzimplementierung

Der TI-M Client MUSS erfolgreich mit einem Fachdienst (eigener Fachdienst, ein Partner Fachdienst oder ein zusätzlichen Fachdienst einer Referenzimplementierungs-Instanz) gegen eine eigene Instanz und gegen eine Referenzimplementierungs-Instanz getestet werden. Das Ergebnis dieser Tests wird als Eingangskriterium für die Zulassung herangezogen. Die Eingangskriterien für die Zulassung sind in der Verfahrensbeschreibung festgelegt. Die Testergebnisse (Serenity Report) MÜSSEN der gematik vorgelegt werden. [<=]

3.4.3 Betrieb

Durch die Einführung eines neuen Produkttypen, dem TI-Messenger Pro Headless Client braucht es eine klare Verantwortung im Betrieb. Die Verantwortung wird dem Anbieter TI-Messenger Pro zugeordnet und erweitert damit sein Portfolio an möglichen Produkten welche dieser anbieten kann.

3.4.3.1 Anbieter

A_28679 -Betriebliche Verantwortung Anbieter TI-M Pro Headless Client

Der Anbieter TI-Messenger Pro MUSS die betriebliche Verantwortung für das Produkt TI-Messenger Headless Client übernehmen, sofern er dieses Produkt anbietet. [<=]

Ein On-Premise-Betrieb ist weiterhin möglich, vorausgesetzt, dass dieser mit dem Anbieter abgestimmt wird. Dabei ist sicherzustellen, dass alle Anforderungen – sowohl unmittelbar als auch mittelbar – durch geeignete Maßnahmen erfüllt werden können.

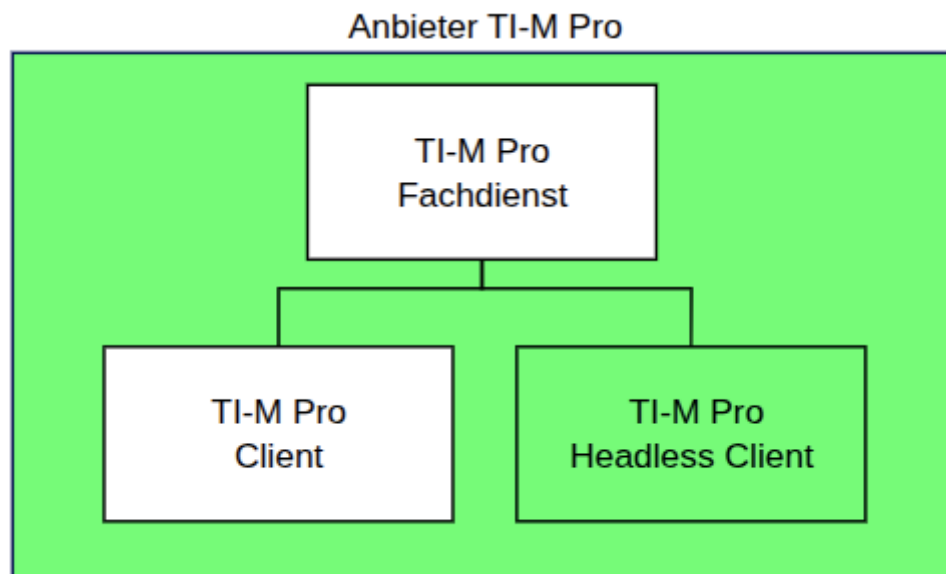


Abbildung 3: Verantwortung im Betrieb für den Anbieter TI-Messenger Pro (farbig: neue/angepasste Anteile)

Damit die gematik in der Rolle des Gesamtverantwortlichen für die TI (GTI) ihrer Pflicht nachkommt, braucht es definierte Governance-Prozesse zur Integration von neuen Komponenten in der TI. Dies erstreckt sich auf den laufenden Betrieb als auch die Außerbetriebnahme.

A_28683 -TI-M Pro Headless Client (un-)mittelbares Bridging-Verbot

Der Anbieter TI-Messenger Pro DARF NICHT den TI-M Pro Headless Client un- oder mittelbar dafür nutzen um ein Bridging in andere Messenger-Systeme durchzuführen.[<=]

A_28725 -TI-M Pro Headless Client Integrationsbeschränkung

Der Anbieter TI-Messenger Pro MUSS sicherstellen, dass der TI-M Pro Headless Client ausschließlich in Systeme von Organisationen des Gesundheitswesens integriert wird, die berechtigt sind, einen TI-Messenger zu bestellen und zu nutzen. Der Anbieter MUSS sicherstellen, dass die über den TI-M Pro Headless Client verarbeiteten medizinischen Daten ausschließlich zur Gesundheitsversorgung bzw. zu deren Organisation genutzt werden.

Hinweis: Bei Mehrzwecksystemen, wie z.B. im PKV-Bereich, sind technisch-organisatorische Maßnahmen umzusetzen um den TI-Messenger Pro Headless Client gegenüber anderen Organisationseinheiten in den jeweiligen Systemen vor unbefugten Zugriffen zu schützen.

Wie beim TI-M Pro Client werden die Informationen am jeweiligen Fachdienst gesammelt und konsolidiert an die gematik weitergeleitet. Die Verpflichtung beim Anbieter TI-M Pro zum bereits für TI-M Pro bestehenden Monitoring wird analog auf das neue Produkt TI-M Pro Headless Client ausgeweitet.

[<=]

A_28681 -TI-M Pro Headless Client Integrationsbeschreibung Betriebshandbuch

Der Anbieter TI-Messenger Pro MUSS die Integration in jedes verschiedene System in seinem Betriebshandbuch grob in der Architektur beschreiben. Dabei MUSS jedes System

in welches der Headless Client integriert wurde, einzeln benannt und mit dem jeweils verantwortlichen Hersteller verknüpft werden.

Hinweis: Die Benennung eines solchen Systems in welches der Headless Client integriert wurde, kann z.B. so aussehen (das folgende Beispiel ist fiktiv):

- 1) E-Rezept-App, verantwortlicher Hersteller: gematik GmbH
- 2) Titus, verantwortlicher Hersteller: gematik GmbH
- 3) ...

Hinweis: Bei Mehrzwecksystemen, wie z.B. im PKV-Bereich, sind technisch-organisatorische Maßnahmen umzusetzen um den TI-Messenger Pro Headless Client gegenüber anderen Organisationseinheiten in den jeweiligen Systemen vor unbefugten Zugriffen zu schützen. [<=]

A_28682 -TI-M Pro Headless Client Integrationsbeschreibung Aktualisierung Betriebshandbuch

Der Anbieter TI-Messenger Pro MUSS spätestens halbjährlich beginnend ab Zulassungserteilung die Systeme in welche der TI-M Pro Headless Client integriert wurde auf Aktualität prüfen und das Betriebshandbuch dahingehend aktualisieren. [<=]

A_28849 -TI-M Pro Headless Client Integrationsfreigabe

Der Anbieter TI-Messenger Pro MUSS vor der Integration des TI-Messenger Headless Clients die Freigabe durch den GTI über einen betrieblichen Change einholen. Der Anbieter MUSS dabei nachweisen, dass alle Rahmenbedingungen dafür erfüllt sind. [<=]

A_28850 -TI-M Pro Headless Client Integrationsänderungen

Der Anbieter MUSS eine Freigabe durch den GTI einholen, wenn wesentliche Änderungen an einer bestehenden Integration des TI-M Pro Headless Clients vorgenommen werden. Als wesentliche Änderungen gelten insbesondere aber nicht ausschließlich die Integration in ein neues System, Änderungen der Systemarchitektur, die die Sicherheit oder Zweckbindung betreffen könnten, Änderungen im Rollen- und Berechtigungskonzept sowie neue Nutzergruppen oder Anwendungsfälle. [<=]

A_28685 -TI-M Pro Headless Client kontrollierte Inbetriebnahme

Der Anbieter TI-Messenger Pro MUSS für die initiale Inbetriebnahme des TI-M Pro Headless Client eine Inbetriebnahme entsprechend der Vorgaben von [gemKPT_Inbetriebnahme_TI-Messenger_Pro] durchführen. [<=]

A_28733 -TI-M Pro Headless Client Einsatzkontext

Der Anbieter TI-Messenger Pro MUSS sicherstellen, dass der TI-M Pro Headless Client ausschließlich in Systemen von Organisationen des Gesundheitswesens betrieben wird, die berechtigt sind, einen TI-Messenger zu bestellen und zu nutzen. Der Anbieter MUSS sicherstellen, dass die über den TI-M Pro Headless Client verarbeiteten medizinischen Daten ausschließlich zur Gesundheitsversorgung bzw. zu deren Organisation genutzt werden. [<=]

3.4.3.2 Client

Um auch während des dezentralen Betriebs bei den jeweiligen Anbietern aussagefähig zur aktuellen Betriebslage zu sein braucht die gematik zuverlässige Daten aus dem Produktivbetrieb.

A_28693 -TI-M Pro Headless Client Ereignisdaten

Der TI-M Pro Headless Client MUSS auf Produkttyp- und Produktversionsebene gegenüber dem TI-M Pro Fachdienst eindeutig identifizierbar sein. [<=]

A_28684 -TI-M Pro Headless Client Selbstauskunft

Der TI-M Pro Headless Client MUSS Selbstauskunftsdaten inkl. Informationen zum integrierenden System senden.[<=]

3.4.4 Produkt und Anbieterkonstellationen

Dieses Kapitel beschreibt drei exemplarische Ansätze zur Entwicklung, Zulassung und Integration des TI-M Pro Headless Clients. Die Beispiele zeigen unterschiedliche Verantwortlichkeiten und Konstellationen zwischen Herstellern und Anbietern, die sich aus den spezifischen Anforderungen der Telematikinfrastruktur ergeben. Sie verdeutlichen, wie der Headless Client entweder als eigenständige Komponente in bestehende Primärsysteme integriert wird oder im Rahmen einer vollständig durch den Hersteller kontrollierten Lösung bereitgestellt werden kann.

Beispiel: Integration des Headless Clients in ein Primärsystem durch Dritte

1. Hersteller A entwickelt entsprechend dem Produkttypsteckbrief TI-M Pro Headless Client einen TI-M Pro Headless Client, reicht diesen zur Zulassung ein und erlangt eine Produktzulassung.
2. Hersteller A überreicht das zugelassene Produkt an einen PS-Hersteller B, und der PS-Hersteller integriert das Produkt in sein Primärsystem (z. B. PVS, KIS, AVS oder KTR-System).
3. Anbieter C möchte eine Anbieterzulassung für TI-M Pro erlangen und weist nach, dass er alle Anforderungen aus dem Anbietertypsteckbrief TI-M Pro erfüllt. Anbieter C verantwortet dabei im Produktivbetrieb das Produkt von Hersteller A und dessen betrieblichen Einsatz im Produkt von Hersteller B (wobei letzteres nicht der Anbietersteuerung der gematik unterliegt).

Dieses Szenario zeigt, wie ein spezialisierter Hersteller durch die Entwicklung und Zulassung eines TI-M Pro Headless Clients die Grundlage für die Integration in ein Primärsystem durch einen Dritten schafft. Der Anbieter übernimmt die Verantwortung für die Konformität und den Betrieb der Gesamtlösung innerhalb der Telematikinfrastruktur. Dieses Modell verdeutlicht die Flexibilität des Headless Clients, der sich nahtlos in unterschiedliche Systeme wie PVS, KIS, AVS oder KTR-Systeme einfügen lässt.

Beispiel: Einheitlicher Hersteller für Headless Client, TI-M Fachdienst und PS-System

1. Hersteller A entwickelt gemäß den Vorgaben der Produkttypsteckbriefe sowohl den TI-M Pro Headless Client als auch den TI-M Pro Fachdienst und reicht beide Produkte gemeinsam zur Zulassung ein. Nach erfolgreicher Prüfung erlangt er die Produktzulassungen für beide Komponenten.
2. Hersteller A integriert den zugelassenen TI-M Pro Headless Client in sein eigenes Praxisverwaltungssystem (PS-System).
3. Hersteller A, in der Rolle des Anbieters, weist nach, dass er alle Anforderungen aus dem Anbietertypsteckbrief TI-M Pro inkl. dem TI-M Headless Client erfüllt und erlangt die Zulassung für TI-M Pro. Er übernimmt die Verantwortung für den Betrieb seiner eigenen Produkte (TI-M Pro Headless Client, TI-M Pro Fachdienst und PS-System, wobei letzteres nicht der Anbietersteuerung der gematik unterliegt). Der Hersteller stellt das System den Nutzern im Gesundheitswesen in der Anbieterrolle bereit.

Dieses Szenario zeigt, wie ein Hersteller durch die vollständige Kontrolle über Entwicklung, Zulassung und Integration eine konsistente und aufeinander abgestimmte Lösung für seine Nutzer bereitstellen kann.

Beispiel: Zentrale Contact Center Integration bei einem Kostenträger

1. Hersteller A entwickelt entsprechend dem Produkttypsteckbrief TI-M Pro Headless Client einen TI-M Pro Headless Client, reicht diesen zur Zulassung ein und erlangt eine Produktzulassung.
2. Hersteller B entwickelt ein Contact Center System für Kostenträger und integriert den zugelassenen TI-M Pro Headless Client als Modul in eine zentrale Serverkomponente im Rechenzentrum des Kostenträgers.
3. Sachbearbeitende des Kostenträgers nutzen Arbeitsplatz- oder Web Clients, die über transportverschlüsselte Netzwerkschnittstellen mit der zentralen Serverkomponente kommunizieren.
4. Der TI-M Pro Headless Client wird ausschließlich lokal durch die Serverkomponente angesteuert. Nachrichteninhalte, Anhänge, Nutzerdaten und Metadaten zu Chats werden innerhalb der IT Landschaft des Kostenträgers verarbeitet und nur in Informationssystemen genutzt, die die Bedingungen aus A_28725 erfüllen.
5. Der Anbieter TI-Messenger Pro beschreibt diese Integration im Betriebshandbuch (inkl. Systembenennung, verantwortlichem Hersteller, Nutzungsformen und Maßnahmen) und stellt sicher, dass die Nutzung nur im Rahmen der von der gematik veröffentlichten Rahmenbedingungen erfolgt. Bei Verstößen unterstützt der Anbieter die von der gematik initiierten Sperrprozesse.

Dieses Szenario zeigt, wie der TI-M Pro Headless Client in einer zentralen Serverkomponente eines Kostenträgers eingesetzt werden kann, um TI-Messenger Funktionalitäten in ein bestehendes Contact Center System zu integrieren. Die fachliche Kommunikation mit Versicherten erfolgt dabei über die Arbeitsoberflächen der Sachbearbeitenden im Contact Center, während der TI-M Pro Headless Client im Hintergrund die Anbindung an den TI-M Pro Fachdienst übernimmt.

Durch die zentrale Integration des TI-M Pro Headless Clients in das Contact Center Backend können eingehende TI Chats anhand von Metadaten und Gesprächsinhalten im Rahmen der Gesundheitsversorgung automatisiert disponiert, geroutet und den jeweils zuständigen Sachbearbeitenden zugewiesen werden. Die Sachbearbeitenden arbeiten ausschließlich in der gewohnten Contact Center Oberfläche, ohne einen separaten TI-M Pro Client bedienen zu müssen.

Die Verantwortung für den sicheren und konformen Betrieb des TI-M Pro Headless Clients liegt beim Anbieter TI-Messenger Pro.

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 (Headless) 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. [<=]

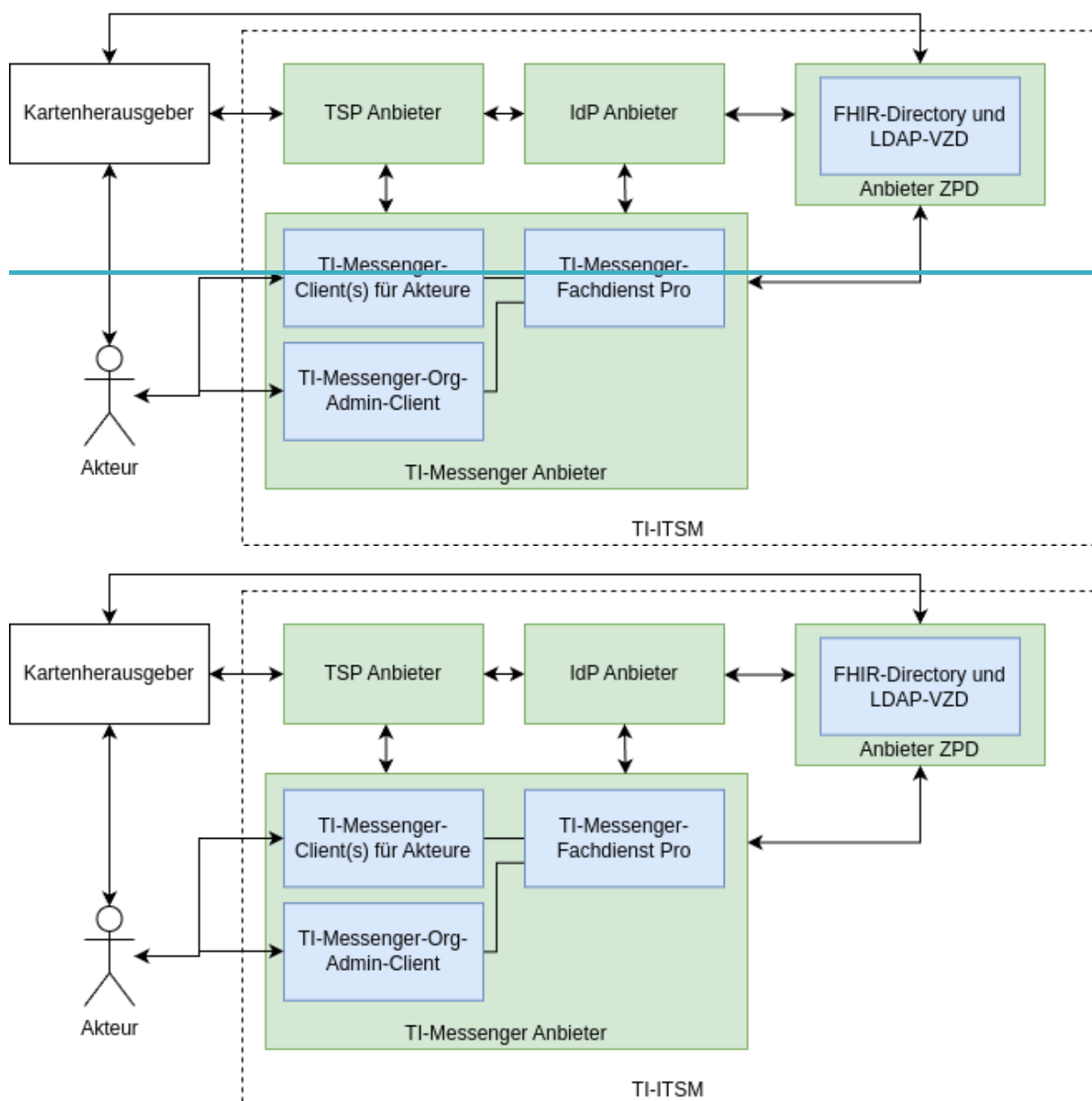


Abbildung 4: Betriebsmodell TI-M Pro

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 Institutionsidentitäten verwalten

AF_10438 -Institutionsidentitäten verwalten

Mit diesem Anwendungsfall kann ein Akteur in der Rolle "Org-Admin" weitere Institutionsidentitäten zu seinem Account verwalten, um stellvertretend für alle SM(C)-B, die zugehörigen Einträge im VZD-FHIR-Directory bearbeiten zu können.

Tabelle 4 : AF - Institutionsidentitäten verwalten

AF_10438	Institutionsidentitäten verwalten
Akteur	Nutzer mit der Rolle "Org-Admin"
Auslöser	Ein Akteur mit der Rolle "Org-Admin" möchte, die seinem Konto zugeordneten, Institutionsidentitäten verwalten.
Komponenten	• Org-Admin-Client • gematik Authenticator oder vergleichbare Software • zentraler IDP-Dienst
Vorbedingungen	1. Für die Organisation wurde bereits ein Org-Admin Konto angelegt 2. Der Administrator verfügt über einen Org-Admin-Client 3. Es existiert eine Vertrauensbeziehung zwischen dem Registrierungs-Dienst und dem VZD-FHIR-Directory 4. Auf dem Endgerät des Benutzers ist eine Authenticator Anwendung installiert, über die eine Challenge vom IDP-Dienst mit Hilfe einer SM(C)-B signiert wird. (optional nur beim Hinzufügen neuer Identitäten) 5. Die verwendete SM(C)-B ist freigeschaltet und besitzt ein gültiges Signaturzertifikat.(optional nur beim Hinzufügen neuer Identitäten)
Eingangsdaten	Identität des Org-Admin, SM(C)-B
Ergebnis	Am Konto des Org-Admin wurde eine weitere Institutsidentität hinzugefügt oder entfernt.
Ausgangsdaten	Status

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.

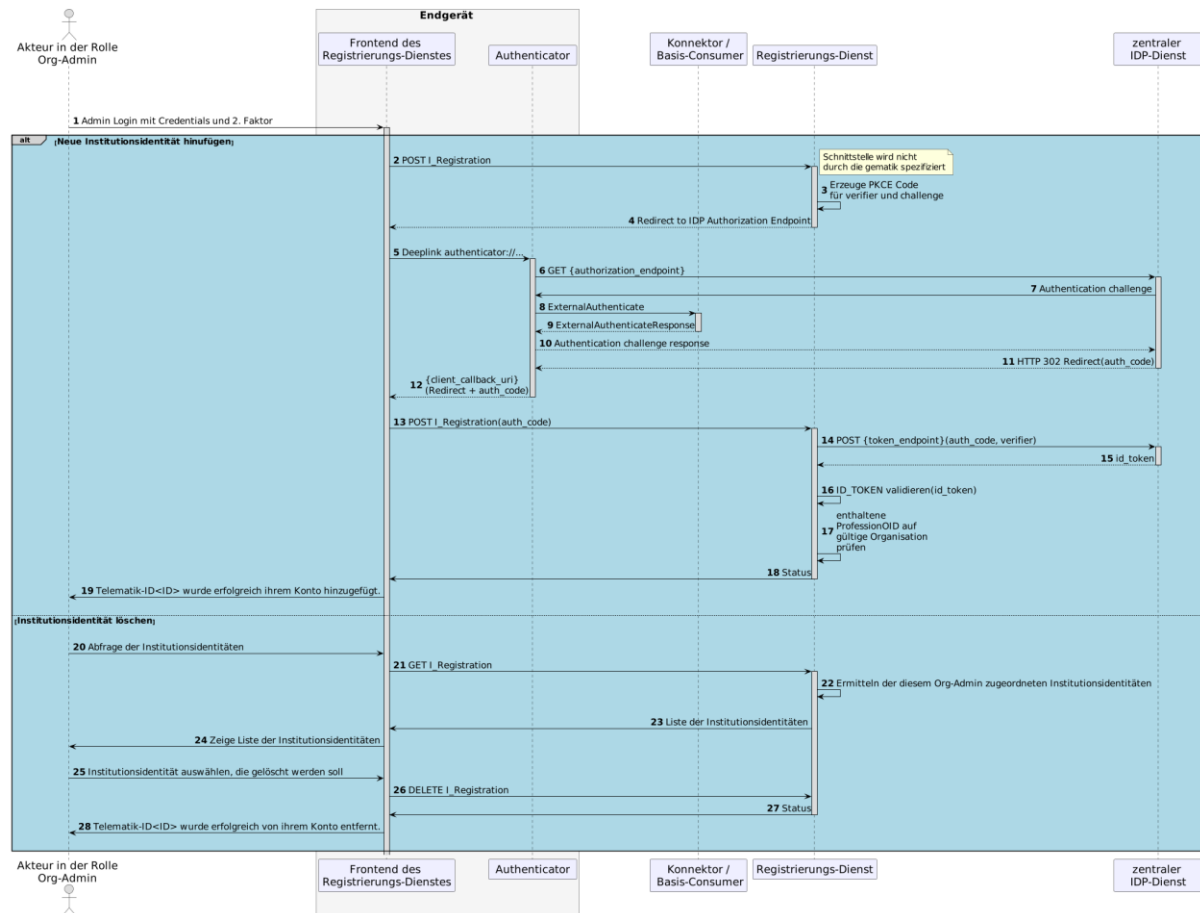


Abbildung 5 Laufzeitansicht Institutionsidentitäten verwalten

[<=]

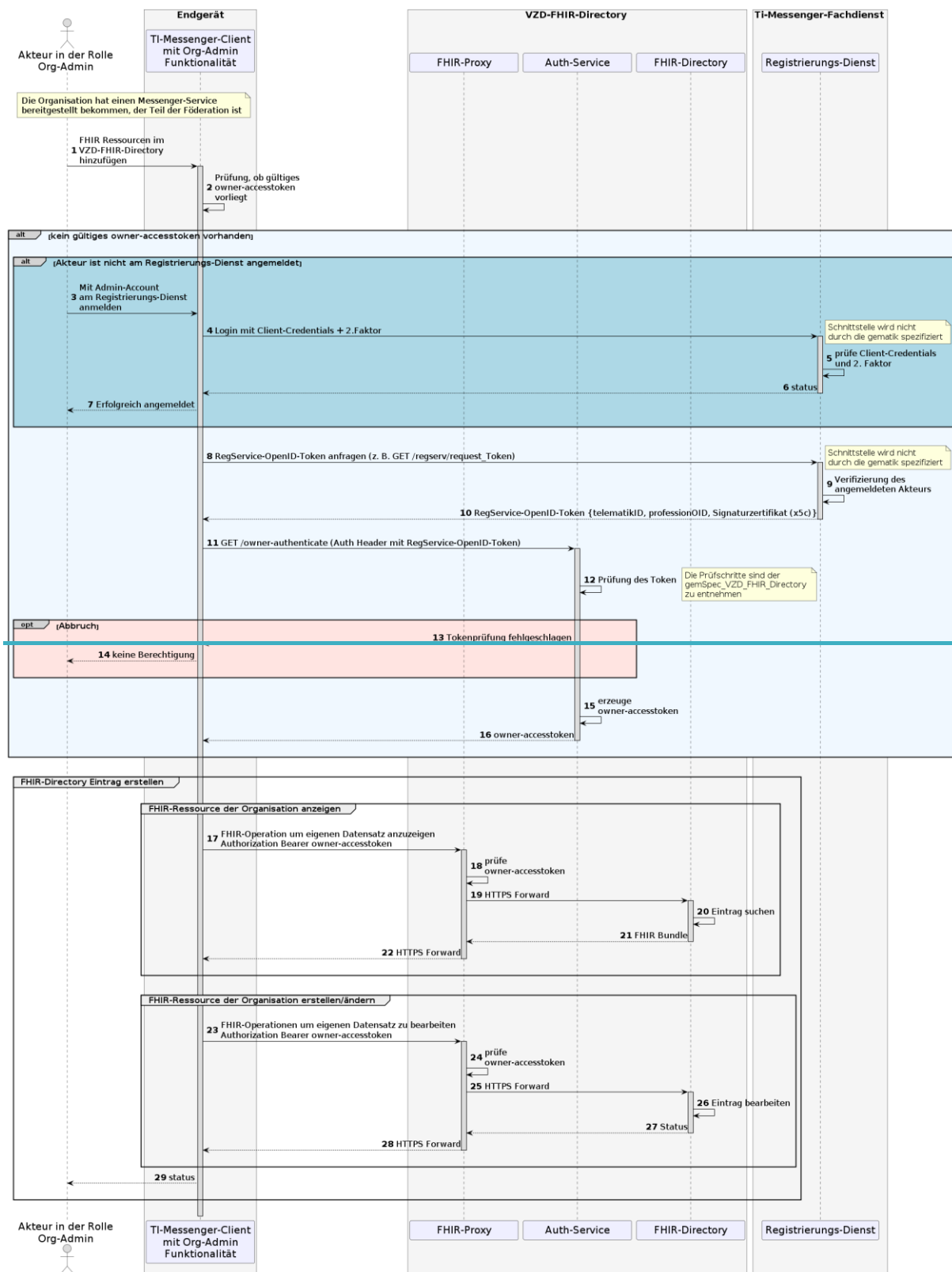
5.1.15.1.2 Organisationsressourcen im Verzeichnisdienst hinzufügen

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 5: 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	• Org-Admin-Client • TI-Messenger Registrierungs-Dienst • Auth-Service • FHIR-Proxy • FHIR-Directory
Vorbedingungen	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-Client 3. 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 Laufzeitsicht**, in der zum Beispiel die TLS-Terminierung am FHIR-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde.



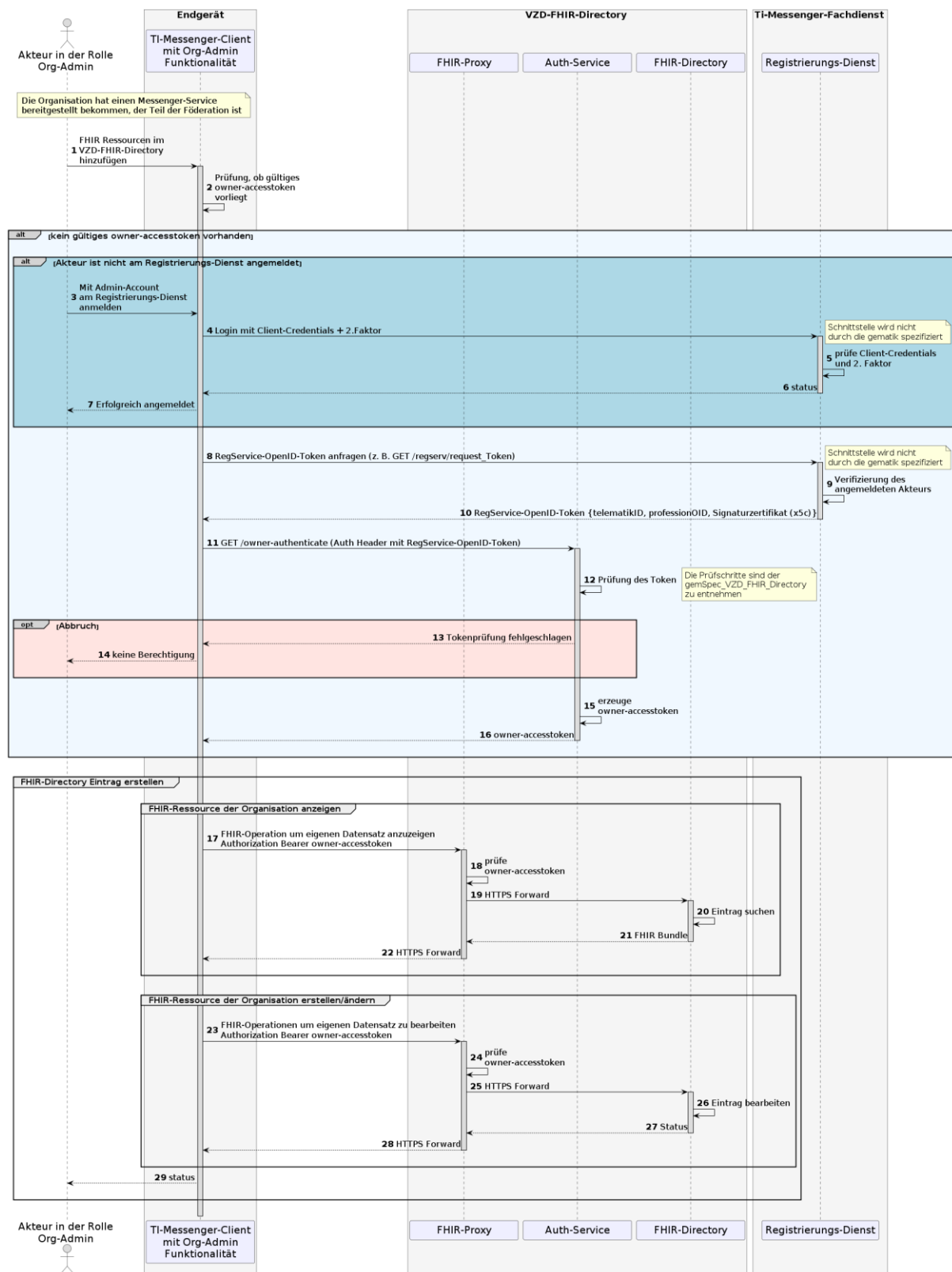


Abbildung 6: Laufzeitsicht - Organisationsressourcen im Verzeichnisdienst hinzufügen

[<=]

5.1.25.1.3 Akteur (User-HBA) im Verzeichnisdienst hinzufügen

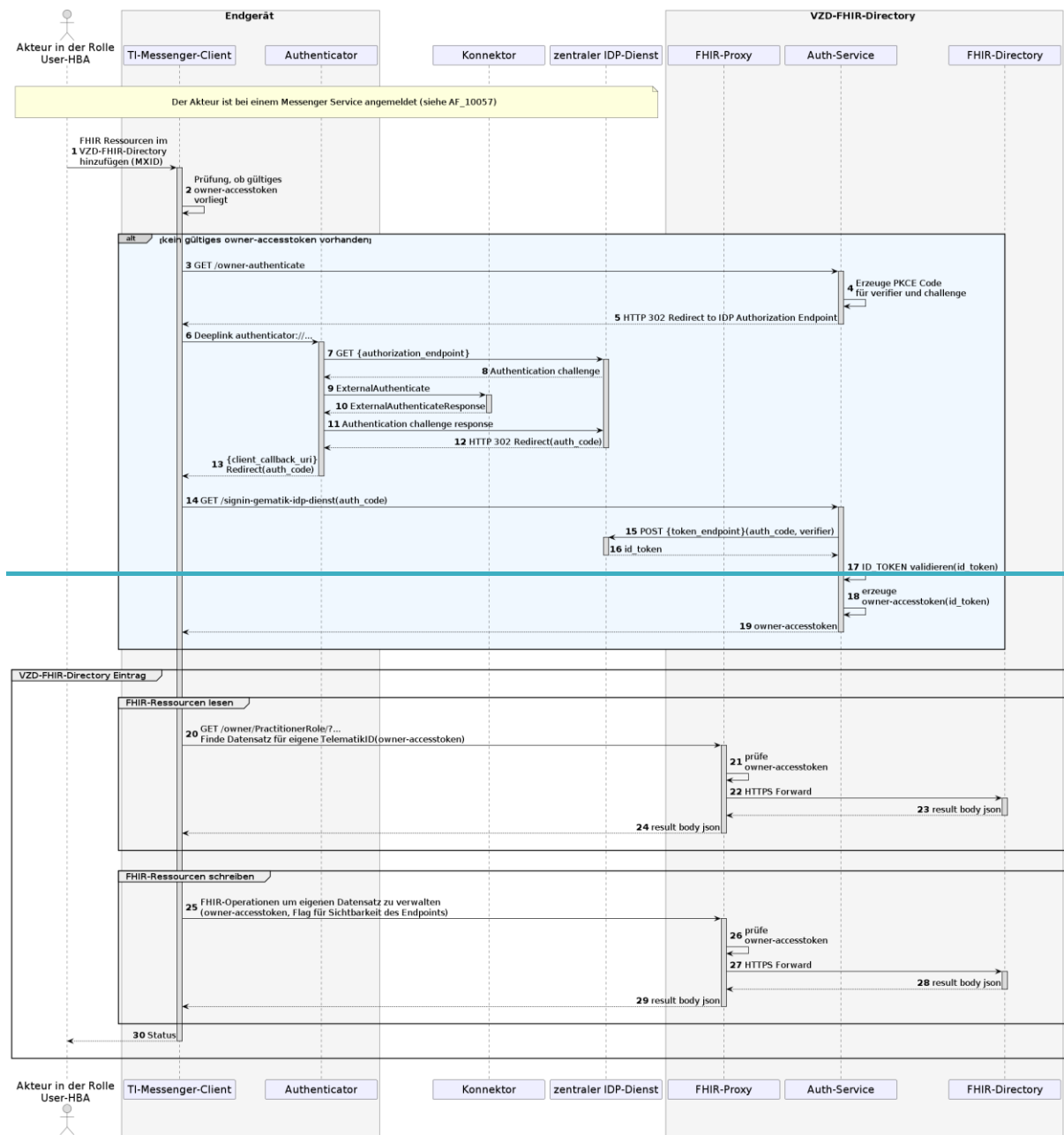
AF_10058-02 -Akteur (User-HBA) im Verzeichnisdienst hinzufügen

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 6: 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	• TI-Messenger-Client • Authenticator • zentraler IDP-Dienst • FHIR-Proxy • Auth-Service • FHIR-Directory
Vorbedingungen	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.



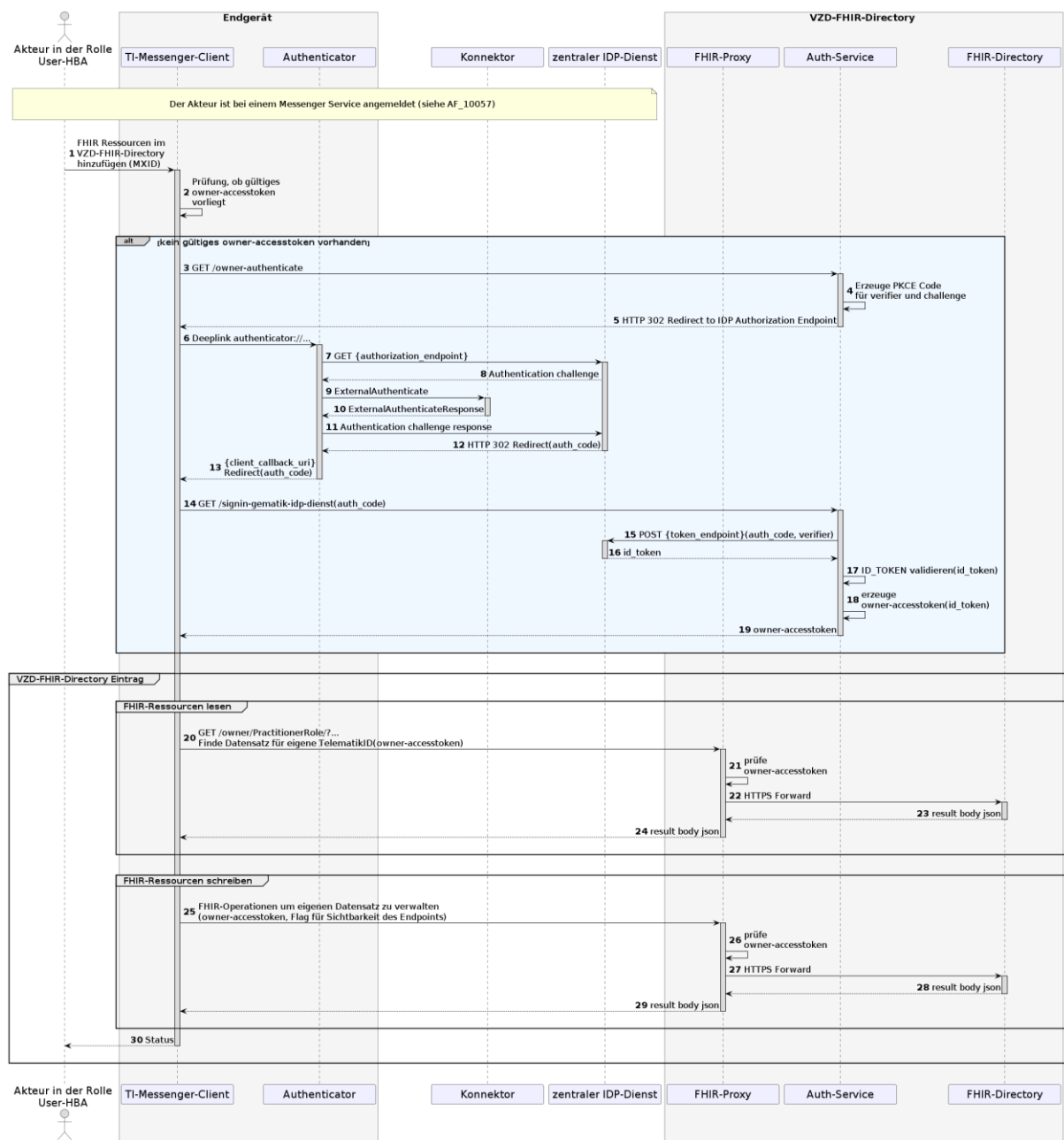


Abbildung 7: Laufzeitsicht - Akteur (User-HBA) im Verzeichnisdienst hinzufügen

[<=]

5.1.35.1.4 Anmeldung eines Akteurs am Messenger-Service

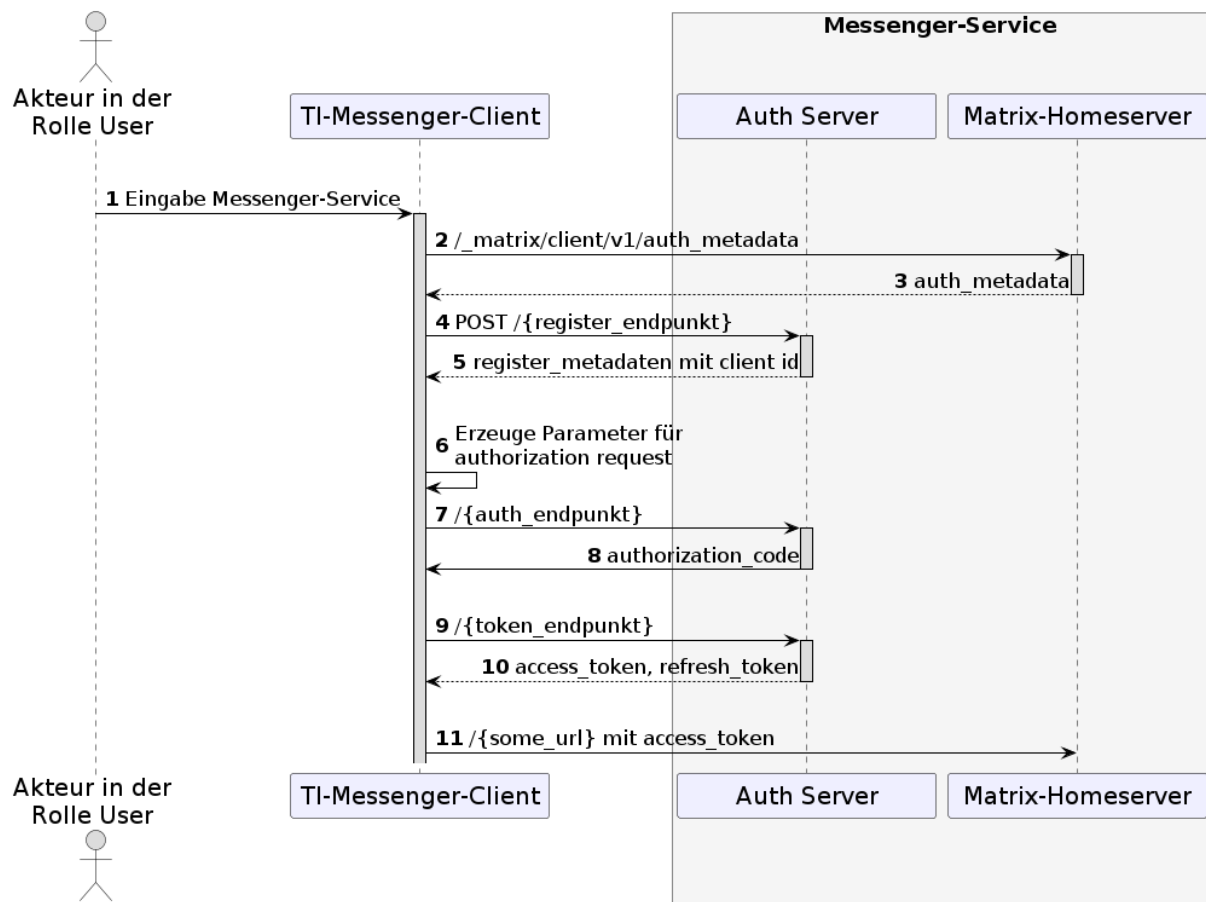
AF_10057-05 ~~AF_10057-04~~ -Anmeldung eines Akteurs am Messenger-Service

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 7: 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	• TI-M Client • Messenger-Proxy • Matrix-Homeserver
Vorbedingungen	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 Interaktion des Clients mit der Fachdienst-Seite, der Ablauf kann je nach eingesetzten Komponenten auf Client- oder Fachdienstseite weitere Komponenten umfassen.



~~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.~~

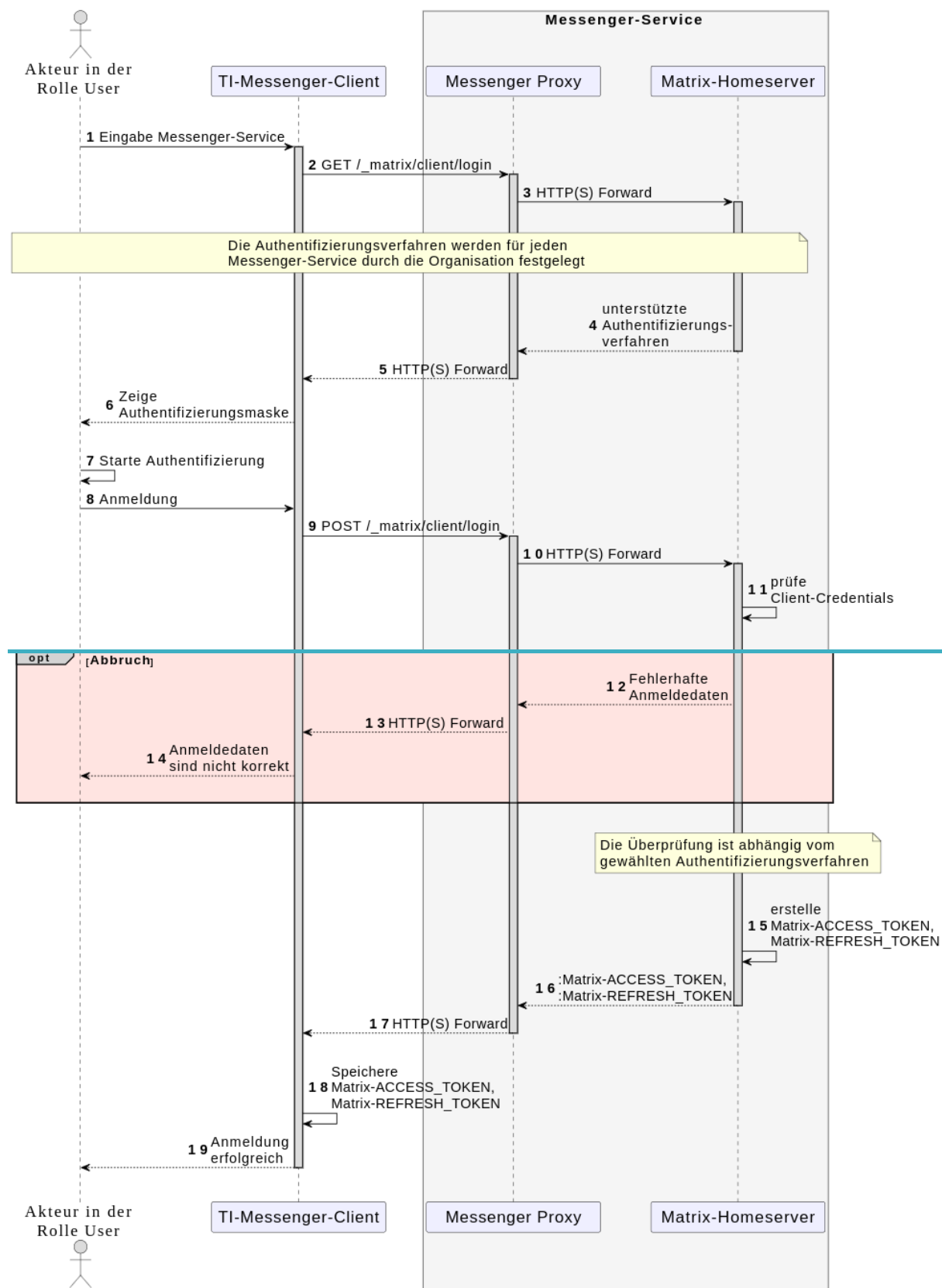


Abbildung 8: Laufzeitsicht - Anmeldung eines Akteurs am Messenger-Service

[<=]

A_30043 -Verbot der legacy Auth

Der TI-M Fachdienst DARF die Legacy API für die Client

Authentication(<https://spec.matrix.org/v1.17/client-server-api/#legacy-api>) NICHT anbieten. [=]

5.1.45.1.5 Einladung von Akteuren innerhalb einer Organisation

AF_10104-03 -Einladung von Akteuren innerhalb einer Organisation

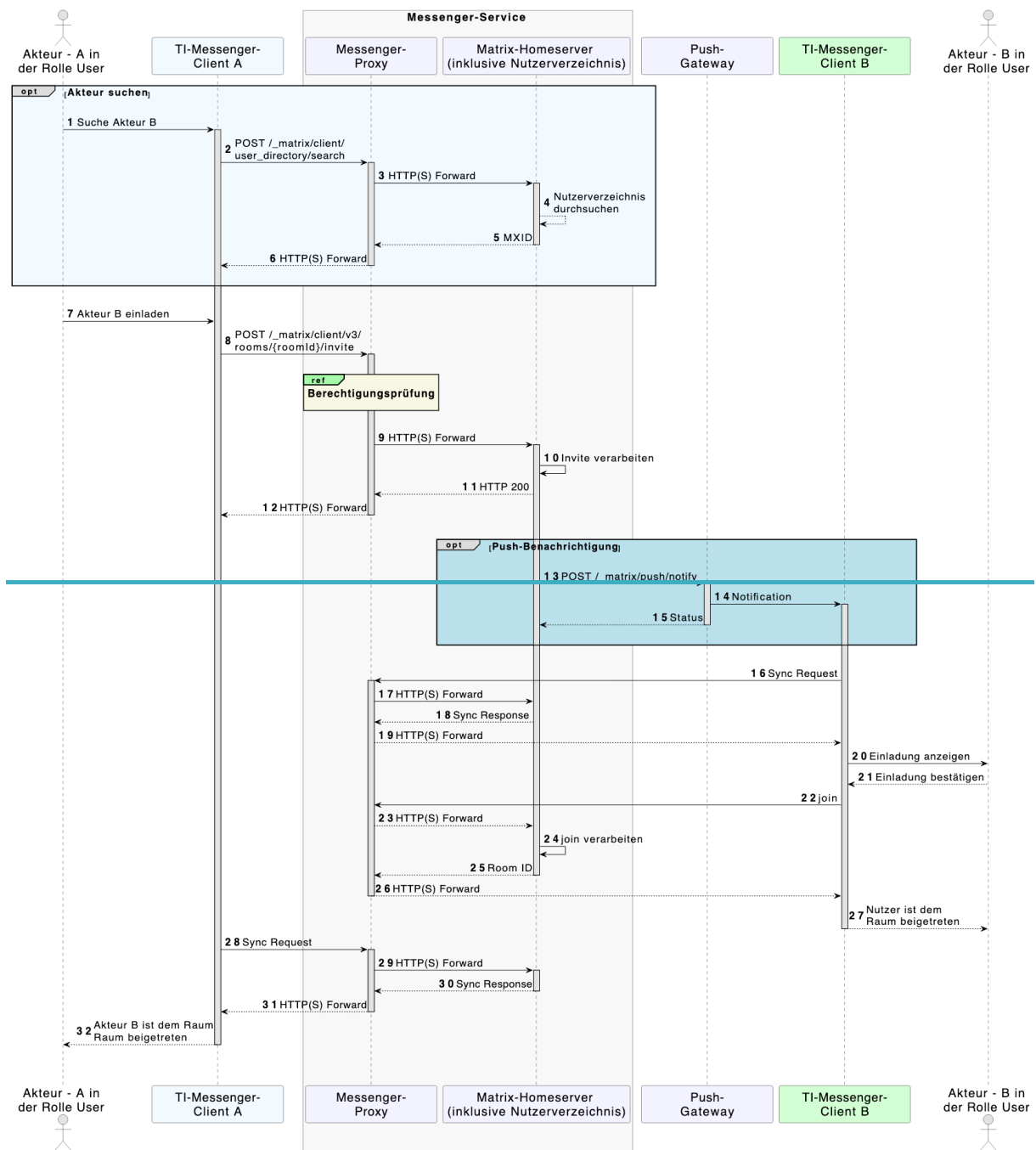
In diesem Anwendungsfall wird ein Akteur, der zu einer gemeinsamen Organisation gehört, in einen Raum eingeladen, um Aktionen auszuführen. Für die Suche nach Akteuren innerhalb einer gemeinsamen Organisation durchsucht ein TI-M Client das Nutzerverzeichnis seiner Organisation auf dem Matrix-Homeserver. 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 8: 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	• TI-Messenger Client A + B • Messenger-Proxy • Matrix-Homeserver • Push-Gateway
Vorbedingungen	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	Akteur A und Akteur B sind beide im Chatraum, zu dem die Einladung ausgesprochen wurde. 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.)

AF_10104	Einladung von Akteuren innerhalb einer Organisation
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).



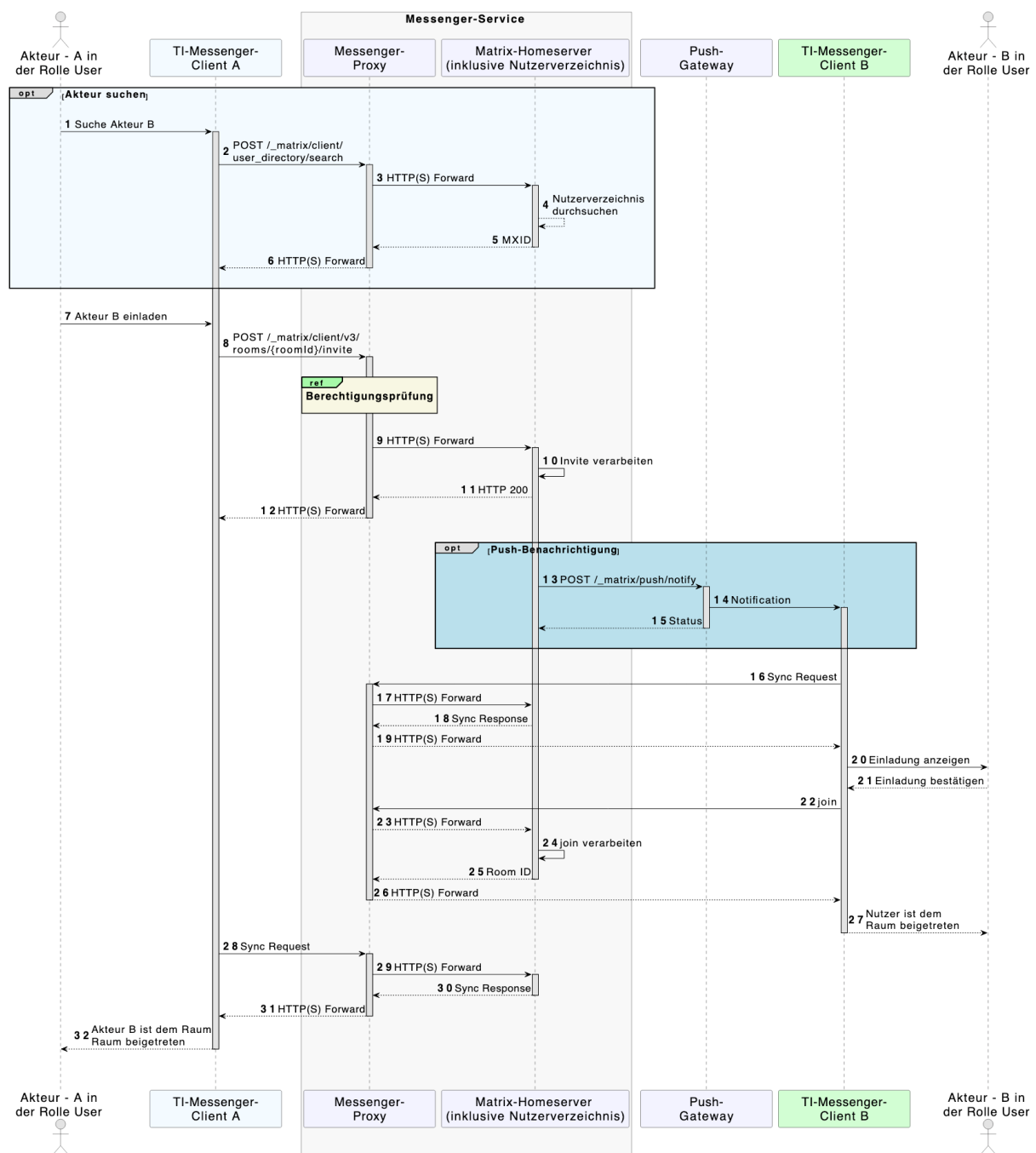


Abbildung 9: Einladung von Akteuren innerhalb einer Organisation

[<=]

5.2 Funktionsaccounts

5.2 Organisationsressourcen im Verzeichnisdienst

Einrichtungen im Gesundheitswesen sind sehr unterschiedlich strukturiert ~~und wollen hinsichtlich ihrer~~. Diese Unterschiede spiegeln sich in der Art der Erreichbarkeit ~~flexibel~~

eigene Strukturen abbilden können. Daher sind beim TI-M-Dienst Accounts notwendig, wider als auch in ihrer Flexibilität. Um dieser gerecht zu werden, bietet der FHIR-Verzeichnisdienst verschiedene Möglichkeiten an, Healthcare Services und entsprechende Endpunkte zur Kommunikation für Institutionen anzulegen. Im Folgenden werden diese Möglichkeiten erläutert und wie die es ermöglichen, Akteure unterhalb der Struktur erreichbar zu machen, entsprechenden TI-Messenger Komponenten diese umsetzen.

A_29022 -TI-M Org-Admin Benutzerhandbuch - Healthcare Services

Der anfragende Akteur muss dann nicht die genaue interne Struktur der Anbieter MUSS im Benutzerhandbuch für Org-Admins bzw. in der entsprechenden GUI darauf hinweisen und erklären, wie Healthcare Services zur Organisation eingesetzt werden können und welche Arten von Endpunkten wie zur Kommunikationsaufbau angelegt werden können. [<=]

kennen. Diese speziellen Accounts werden im folgenden als Funktionsaccounts bezeichnet.

Folgende Beispielszenarien

A_29023 -TI-M Info an Nutzer zur MXID

Der Anbieter MUSS seine Nutzer darüber informieren, dass die MXID keine Anonymisierung darstellt und auch nicht geheim bleibt, besonders nicht wenn der Echtnamen in der MXID enthalten ist. [<=]

Unter einem Healthcare Service können umgesetzt mit dem Org-Admin Client drei verschiedene Arten von Endpunkten angelegt werden:

5.2.1 Die Credentials Akteur

Der Endpunkt-Typ "Akteur" soll eine natürliche Person kennzeichnen welche ggf. auch mit dem echten Namen direkt als Kontaktpunkt hinterlegt wird.

A_29024 -ConnectionType Akteur

Der Org-Admin-Client MUSS für einen Akteur an der Endpoint-Ressource den Code des EndpointDirectoryConnectionType auf "tim" setzen. [<=]

5.2.15.2.2 Funktionsaccount werden an mehrere Mitarbeiter verteilt und somit können alle stellvertretend für die Organisation antworten.

- Hinter dem Endpunkt-Typ "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" soll einen Endpunkt analog zu einem Funktionspostfach einer E-Mail-Adresse abbilden.

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. [<=]

A_26524 -Funktionsaccount Address

Der Org-Admin-Client MUSS das `address` Attribut der `Endpoint`-Ressource mit der MXID des Funktionsaccounts im URI Format befüllen.[<=]

A_26525 -Funktionsaccount Name

Der Org-Admin-Client MUSS das `name` Attribut der `Endpoint`-Ressource mit dem Displaynamen des Funktionsaccounts befüllen.[<=]

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.[<=]

5.2.2 Chatbot

5.2.3 (Chat)bot

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/anwendungsfaelle/COM-chatbot.adoc]` hinterlegt.

A_25547 -ConnectionType Funktionsaccount Chatbot

Der Org-Admin-Client MUSS für einen [FunktionsaccountAccount](#), der von einem automatisierten System abgebildet wird, an der `Endpoint`-Ressource den Code des `EndpointDirectoryConnectionType` auf "tim-bot" setzen.[<=]

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)`. [<=]

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.

TI-Messenger

Wer darf mich kontaktieren?

☒ Jeder

☐ Niemand

Ausnahmen

Server: gematik.de 

MXID:@DrMeier:mypraxis.de 

Gruppe: Versicherte 

 Weitere Kategorie hinzufügen

TI-Messenger

Wer darf mich kontaktieren?

☒ Jeder

☐ Niemand

Ausnahmen

Server: gematik.de 

MXID:@DrMeier:mypraxis.de 

Gruppe: Versicherte 

 Weitere Kategorie hinzufügen

Abbildung 10: 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. [<=]

A_28740 -Funktionsumfang der Berechtigungskonfiguration im User Interface

Der TI-M Client Pro MUSS es in seinem UI für die Konfiguration der Berechtigungen ermöglichen, dass sowohl einzelne Nutzer als auch einzelne Server als auch einzelne Nutzergruppen auf der Block- bzw. Allow-List eingetragen werden können. [<=]

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 9: Überblick der Benutzerverwaltung in Abhängigkeit der Rolle

Rolle	Client	Administration	Wo
Org-Admin	TI-Messenger Client mit Administrationsfunktionen (Org-Admin-Client)	- Nutzer-Account anlegen - Nutzer-Account verwalten	Matrix-Homeserver (User Directory)
		- HealthcareService-Ressource anlegen - Endpoint einer HealthcareService-Ressource anlegen - Endpoint einer HealthcareService-Ressource verwalten	VZD-FHIR-Directory (Organisationsverzeichnis)
User	TI-Messenger Client	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.

5.4.1 Zusätzliche Attribute in den User Profilen

Um den Gesprächspartner schon bei der erhaltenen Einladung eindeutiger identifizieren zu können, sollen in den Profilen der Akteure auf dem Fachdienst vom Org-Admin weitere Informationen eingepflegt werden können.

A_30013 -Zusätzliche Informationen im User Profil

Der Org-Admin Client MUSS dem Akteur in der Rolle Org-Admin erlauben die folgenden zusätzlichen Felder ins Profil eines Akteurs in der Rolle User einzupflegen:

Tabelle 10 Zusätzliche Profilinformationen

Feld	Kategorie
de.gematik.user.orgname	MUSS hinterlegt werden
de.gematik.user.orgtype	OPTIONAL
de.gematik.user.orgfachrichtung	OPTIONAL
de.gematik.user.orgaddress	OPTIONAL
de.gematik.user.beruf	OPTIONAL

[<=]

Hinweis: Der TI M Fachdienst Anbieter kann die Inhalte der Profilfelder automatisiert bereitstellen. Dies gilt insbesondere für de.gematik.user.orgname, kann jedoch ebenso für die weiteren in dieser Anforderung beschriebenen Profilfelder erfolgen, beispielsweise auf Basis eines Verzeichnisdienstes oder einer vergleichbaren Benutzerverwaltung. Bei der Neuanlage eines Accounts können die Felder automatisch vorbelegt werden.

A_30014 -Unterstützung bei der Eingabe

Der Org-Admin Client MUSS den Akteur in der Rolle Org-Admin bei der Anlage der zusätzlichen Felder unterstützen, indem er die einzutragenden Werte aus dem FHIR-VZD extrahiert und dem Akteur zur Übernahme anbietet. [**<=**]

Hinweis: Die Daten sollten den FHIR-VZD

Feldern Organisation.name, Organisation.type.coding.display (bei "system": "https://gematik.de/fhir/directory/CodeSystem/OrganizationProfessionOID"), healthcareService.type.coding.display, Location.address.text und ggf. Practitioner.qualification.code.coding.display (bei "system": "https://gematik.de/fhir/directory/CodeSystem/PractitionerProfessionOID" entsprechen.

5.5 Löschen von Inhalten – Anpassungen

Dieses Kapitel ergänzt das gleichnamige Kapitel aus [gemSpec_TI-M_Basis] mit Regelungen für TI-M Pro Fachdienste und Clients.

5.5.1 Serverseitiges Löschen

5.5.1.1 Matrix-Events

Mitarbeiter des Gesundheitswesens sind ihren Organisationen und deren Regeln untergeordnet. Für diese Organisationen 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 Löschoperation selbst darf dabei allerdings nur server-lokal und ohne direkte Auswirkung auf die Föderation erfolgen damit Löschkonfigurationen auf unterschiedlichen Servern nicht interferieren. Eine serverlokale Löschung schließt z. B. die Verwendung von Redactions oder das Kicken der Nutzer anderer Homeserver aus.

Die konkrete Ausgestaltung einer automatischen serverseitigen Löschfunktion wird darüber hinaus durch die Spezifikation nicht näher vorgegeben. Hier gibt es verschiedene Möglichkeiten. So könnten z. B. Nutzer des eigenen Homeservers aus Räumen entfernt werden und diese Räume samt der zugehörigen Events dann aus der Datenbank des Servers gelöscht werden. Alternativ wäre auch ein fortlaufendes Löschen von veralteten Events aus der Datenbank des Servers möglich, wobei der Raum selbst bestehen bleibt. Homeserver wie Synapse bieten hierfür konfigurierbare Message Retention Policies an.

Damit Inhalte nicht unerwartet verloren gehen, müssen Nutzer über etwaige automatische Löschfunktionen informiert werden. Die konkrete Form dieser Information bleibt dabei dem Anbieter überlassen. So könnten einzelne Räumlöschungen z. B. über Server Notices angekündigt werden. Alternativ wäre es auch denkbar, dass nur einmalig über feste Löschintervalle informiert wird.

A_28340 -Lokale Beschränkung der automatischen serverseitigen Löschung von Events

Implementieren TI-M Pro Fachdienste Funktionen zum automatisch Löschen von Matrix-Events, so MUSS die Löschung serverlokal und ohne direkten Einfluss auf die Föderation erfolgen. [<=]

A_28341 -Information über automatische serverseitige Löschung von Events

Nutzen TI-M Pro Anbieter Funktionen zur automatischen serverseitigen Löschung von Matrix-Events, so MÜSSEN sie ihre Nutzer vorab darüber informieren. [<=]

5.6 Strukturierte Daten – Anpassungen

Dieses Kapitel ergänzt das gleichnamige Kapitel aus [gemSpec_TI-M_Basis] mit Regelungen für TI-M Pro Fachdienste und Clients.

5.6.1 Austausch von FHIR-Ressourcen

TI-M Clients können über den Event-Typ `de.gematik.fhir` beliebige FHIR-Ressourcen austauschen. Zusätzlich sind TI-M ePA Clients befähigt FHIR Questionnaires des Profils `ISiKFormularDefinition` darzustellen, auszufüllen und zu beantworten. Hieraus ergeben sich vielfältige Möglichkeiten für TI-M Pro Nutzer mittels Fragebögen Daten in strukturierter Form zu erheben. Exemplarisch ist im Folgenden ein fiktiver Fragebogen für die Einwilligungserklärung zum Datenschutz angeführt.

Tabelle 11: Beispiel für FHIR-Fragebogen zur Datenschutzeinwilligung als JSON-Serialisierung

```
{
  "resourceType": "Questionnaire",
  "meta": {
    "profile": [
      "https://gematik.de/fhir/isik/StructureDefinition/ISiKFormularDefinition"
    ]
  },
  "subjectType": [ "Patient" ],
  "name": "DSGVOConsent",
  "version": "1.2.3",
  "url": "https://waldklinik.de/fhir/DSGVOConsent",
  "status": "active",
  "title": "Einwilligungserklärung Datenschutz",
  "description": "Fragebogen zur Einholung der datenschutzrechtlichen
  Einwilligung",
  "item": [{
    "type": "group",
    "linkId": "1",
    "text": "Datenübermittlung an den weiterbehandelnden Arzt / Hausarzt /
    Konsiliarzt und dem UKW nach § 73 Abs. 1b SGB V:",
    "item": [{
      "type": "choice",
      "linkId": "1.1",
      "text": "Ich willige ein, dass die Waldklinik die mich betreffenden
      Behandlungsdaten und Befunde an meinen Arzt/Hausarzt/Konsiliarzt zum Zwecke
      der Dokumentation und Weiterbehandlung übermittelt. Die Übermittlung der
      Behandlungsdaten und Befunde dient der Erstellung und Vervollständigung
      einer zentralen Dokumentation bei meinem Arzt.",
      "answerOption": [{
        "valueCoding": {
          "display": "Ja"
        }
      }, {
        "valueCoding": {
          "display": "Nein"
        }
      }
    ]
  }, {
    "type": "display",
    "linkId": "1.2",
    "text": "Diese Einwilligung kann ganz oder teilweise jederzeit ohne
    Angaben von Gründen gegenüber der Waldklinik widerrufen werden."
  }
]}
}
```

Ein TI-M Pro Nutzer kann solch einen Fragebogen im Rahmen des Fachverfahrens `de.gematik.questionnaire.consent` in der Version `v1` aus `[gemSpec_TI-M_Basis]` an die TI-M ePA Clients eines Versicherten versenden und von diesem den ausgefüllten Fragebogen zurück erhalten.

5.7 Organisationsspezifische Raumnamen

Der Name eines Raumes wird gemäß [Matrix Specification] durch das State Event `m.room.name` gesetzt (bzw. bei Fehlen dieses Events über die in [Client-Server API/#calculating-the-display-name-for-a-room] definierte Vorschrift berechnet). Da das State Event global für alle Raumteilnehmer gilt, können sich Konflikte ergeben wenn eine Partei im Raum den Namen zum Zweck der Selbstorganisation ändern möchte. Für Versicherte wird dem entgegengewirkt, indem sie die Möglichkeit erhalten die Namen von Räumen über einen Datensatz vom Typ `de.gematik.room.name.private` im Account Data Bereich des Raumes zu überschreiben (siehe hierzu [gemSpec_TI-M_ePA]).

Für Mitarbeiter des Gesundheitswesens ist dies nicht hinreichend da hier der Bedarf bestehen kann, den Raumnamen nicht nur privat für einen Nutzer, sondern einheitlich für alle Akteure einer Organisation zu setzen ohne dabei den Namen für Akteure anderer Organisationen zu beeinflussen. Um dies zu ermöglichen wird für Nutzer des TI-Messenger Pro ein Verfahren basierend auf [MSC4432] umgesetzt.

Zentrales Instrument hierbei ist ein Datensatz vom Typ `de.gematik.room.name.server_wide`, der von Clients im Account Data Bereich von Räumen abgelegt wird. Das Schema dieses Datensatzes ist identisch zum Schema des Feldes `content` in `m.room.name` State Events.

Tabelle 12: Beispiel für den Abruf des Datensatzes zum serverweiten Überschreiben des Namen eines Raumes

```
GET
/_matrix/client/v3/user/${userId}/rooms/${roomId}/account_data/de.gematik.
room.name.server_wide

{
  "name": "Fallreferenz A38"
}
```

Die Synchronisation des Account Data Datensatzes über alle teilnehmenden Akteure des Fachdienstes wird vom Fachdienst selbst vermittelt. Die Berechtigung zum Setzen serverweiter Raumnamen kann dabei eingeschränkt werden. Ob eine Einschränkung vorliegt, wird Clients über eine dedizierte Capability `de.gematik.room.name.server_wide` angezeigt, die entweder eine Allow-Liste oder eine Block-Liste von Raum-IDs enthält.

Tabelle 13: Beispiel für den Abruf der Capability zum Schreiben serverweiter Raumnamen mit Allow-Liste von Räumen

```
GET /_matrix/client/v3/capabilities

{
  "capabilities": {
    "de.gematik.room.name.server_wide": {
      // Serverweite Raumnamen können *nur* in diesen beiden Räumen gesetzt
      werden
      "allowed": [
        "!nD4Jylhp0We0VmIM9ubjqWLBX_uV8YlTBbPa3a_v2uk",
        "!0KNSXYXB_2xtEUKQ9MGBRy5oNIOfAKoq2uIqPZCJbI8"
      ]
    }
  }
}
```

Tabelle 14: Beispiel für den Abruf der Capability zum Schreiben serverweiter Raumnamen mit Block-Liste von Räumen

```
GET /_matrix/client/v3/capabilities

{
  "capabilities": {
    "de.gematik.room.name.server_wide": {
      // Serverweite Raumnamen können in allen Räumen *außer* diesen beiden
      gesetzt werden
      "disallowed": [
        "!nD4Jylhp0We0VmIM9ubjqWLBX_uV8YlTBbPa3a_v2uk",
        "!0KNSXYXB_2xtEUKQ9MGBRy5oNIOfAKoq2uIqPZCJbI8"
      ]
    }
  }
}
```

A_28926 -Setzen des serverweiten Raumnamen

Der TI-M Client Pro MUSS, sofern nicht durch die Capability `de.gematik.room.name.server_wide` verhindert, dem Akteur ermöglichen den serverweiten Namen eines Raumes sowohl bei Raumerzeugung als auch danach zu setzen oder zu ändern. Hierzu ist ein Datensatz vom Typ `de.gematik.room.name.server_wide` im Account Data Bereich des Raumes zu schreiben.**[<=]**

Hinweis: Die Möglichkeit den globalen Raumnamen in Abhängigkeit der vorliegenden Power Level zu setzen bleibt sowohl bei Raumerzeugung als auch danach unberührt. Hierfür muss das Standard State Event `m.room.name` sowie das gematik-eigene State Event `de.gematik.tim.room.name` (gemäß `[gemSpec_TI-M_Basis]` in Abhängigkeit vom Raumtyp) geschrieben werden.

A_28927 -Entfernen des serverweiten Raumnamen nach Raumerzeugung

Der TI-M Client Pro MUSS es dem Akteur ermöglichen einen zuvor gesetzten serverweiten Namen eines bestehenden Raumes zu löschen, indem ein leeres Objekt `{}` in den Datensatz vom Typ `de.gematik.room.name.server_wide` im Account Data Bereich des Raumes geschrieben wird.**[<=]**

A_28928 -Anzeige des serverweiten Raumnamen

Existiert im Account Data Bereich eines Raumes ein Datensatzes vom Typ `de.gematik.room.name.server_wide` und entspricht der Datensatz nicht dem leeren Objekt {}, so MUSS der TI-M Client Pro den enthaltenen Namen bei der Anzeige des Raumes verwenden.[<=]

Hinweis: Es ist zulässig einen etwaigen globalen Raumnamen zusätzlich zum serverweiten Namen anzuzeigen.

Hinweis: Im Membership-Status `invite` werden Änderungen an Account Data Datensätzen nicht über `/sync` vermittelt. Zur Anzeige eines etwaigen serverweiten Namens bei eingeladenen Räumen ist es daher notwendig, dass der Client Account Data manuell abfragt. Des Weiteren ist eine manuelle Abfrage von Account Data auch notwendig, falls der Client Ergebnisse von Endpunkten anzeigt, die lediglich den globalen Raumnamen in ihrer Response beinhalten. Beispiele hierfür sind

`/_matrix/client/v3/publicRooms` und

`/_matrix/client/v1/room_summary/{roomIdOrAlias}`.

A_28929 -Synchronisation des serverweiten Raumnamens über alle teilnehmenden lokalen Nutzer

Schreibt ein Nutzer eines TI-M Fachdienstes Pro einen Datensatzes vom Typ `de.gematik.room.name.server_wide` im Account Data Bereich eines Raumes, so MUSS der TI-M Fachdienst Pro diesen Datensatz in den Account Data Bereich folgender anderer Nutzer duplizieren:

- wenn die Join Rule im Raum den Wert `public` hat, dann an alle lokalen Nutzer des Fachdienstes (unabhängig davon ob sie Mitglieder des Raums sind) oder
- wenn die Join Rule im Raum einen Wert ungleich `public` hat, dann an alle lokalen Nutzer des Fachdienstes mit Membership-Events im Raum (also nur an alle Raum-Mitglieder).

[<=]

A_28930 -Synchronisation des serverweiten Raumnamens bei neu eingeladenen lokalen Nutzern

Wird ein Nutzer eines TI-M Fachdienstes Pro in einen Raum eingeladen, in dem durch andere lokale Nutzerein Datensatz vom Typ `de.gematik.room.name.server_wide` im Account Data Bereich des Raumes geschrieben wurde, so MUSS der TI-M Fachdienst Pro diesen Datensatz in den Account Data Bereich des Raumes des neu eingeladenen Nutzer duplizieren.[<=]

A_28931 -Einschränkung der Berechtigung zum Setzen serverweiter Raumnamen

Der Org-Admin-Client MUSS es ermöglichen die Berechtigung zum Schreiben von Datensätzen des Typs `de.gematik.room.name.server_wide` im Account Data Bereich von Räumen auf bestimmte Nutzer und/oder Räume einzuschränken.[<=]

Hinweis: Bei fehlender Berechtigung ist fachdienstseitig eine HTTP 405 Response beim Versuch des Schreibens des Account Data Datensatzes auszugeben (siehe [Client-Server API/#put_matrixclientv3useruseridroomsroomidaccount_datatype]).

A_28932 -Anzeige der Einschränkung der Berechtigung zum Setzen serverweiter Raumnamen

Schränkt der TI-M Fachdienst Pro die Berechtigung zum Setzen serverweiter Raumnamen auf bestimmte Nutzer und/oder Räume ein, so MUSS er dies den betroffenen Clients anzeigen, indem am Endpunkt `/_matrix/client/v3/capabilities` eine Capability vom

Typde.gematik.room.name.server_wide ausgegeben wird. Der Inhalt dieser Capability ist entweder:

- ein Feld `allowed` mit einer Liste von Raum-IDs, in denen der Nutzer den serverweiten Namen setzen darf oder
- ein Feld `disallowed` mit einer Liste von Raum-IDs, in denen der Nutzer den serverweiten Namen *nicht* setzen darf.

Ein gleichzeitiges Befüllen von `allowed` und `disallowed` ist nicht zulässig.[<=]

Hinweis: Wird vom Fachdienst keine Capability ausgeliefert, so existiert auch keine Einschränkung der Berechtigung. Dieser Fall ist also äquivalent zu einer Capability mit `disallowed = []`.

6 Anhang A – Verzeichnisse

6.1 Abkürzungen

Tabelle 15: 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 16: 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	28
Abbildung 2: Laufzeitsicht – Organisationsressourcen im Verzeichnisdienst hinzufügen ..	34
Abbildung 3: Laufzeitsicht – Akteur (User-HBA) im Verzeichnisdienst hinzufügen	37
Abbildung 4: Laufzeitsicht – Anmeldung eines Akteurs am Messenger-Service	40
Abbildung 5: Einladung von Akteuren innerhalb einer Organisation	44
Abbildung 6: Beispielhaftes UI zum Setzen der Berechtigungen	47

Abbildung 1: Übersicht Headless Client Architektur. Farbig: von der gematik (teil-)regulierte Komponenten.....	18
Abbildung 2: Beispiel für Integration des Headless Client in eine Serverkomponente mit Netzwerkschnittstelle. Farbig: von der gematik (teil-)regulierte Komponenten.	18
Abbildung 3: Verantwortung im Betrieb für den Anbieter TI-Messenger Pro (farbig: neue/angepasste Anteile)	23
Abbildung 4: Betriebsmodell TI-M Pro	28
Abbildung 5 Laufzeitansicht Institutionsidentitäten verwalten	31
Abbildung 6: Laufzeitsicht - Organisationsressourcen im Verzeichnisdienst hinzufügen ..	34
Abbildung 7: Laufzeitsicht - Akteur (User-HBA) im Verzeichnisdienst hinzufügen	37
Abbildung 8: Laufzeitsicht - Anmeldung eines Akteurs am Messenger-Service	40
Abbildung 9: Einladung von Akteuren innerhalb einer Organisation	44
Abbildung 10: Beispielhaftes UI zum Setzen der Berechtigungen	47

6.4 Tabellenverzeichnis

Tabelle 1: Akteure und Rollen	9
Tabelle 2: Arten von Token	10
Tabelle 3: Schreibzugriff – VZD-FHIR-Ressourcen	14
Tabelle 4: AF – Organisationsressourcen im Verzeichnisdienst hinzufügen	32
Tabelle 5: AF – Akteur (User-HBA) im Verzeichnisdienst hinzufügen	35
Tabelle 6: AF – Anmeldung eines Akteurs am Messenger-Service	38
Tabelle 7: Einladung von Akteuren innerhalb einer Organisation	41
Tabelle 8: Überblick der Benutzerverwaltung in Abhängigkeit der Rolle	49
Tabelle 9: Im Dokument verwendete Abkürzungen	57
Tabelle 10: Im Dokument verwendete Begriffe	57
Tabelle 11: Referenzierte Dokumente der gematik	59
Tabelle 12: Weitere Dokumente	60
Tabelle 1: Akteure und Rollen	9
Tabelle 2: Arten von Token	10
Tabelle 3: Schreibzugriff - VZD-FHIR-Ressourcen	14
Tabelle 4 : AF - Institutionsidentitäten verwalten	30
Tabelle 5: AF - Organisationsressourcen im Verzeichnisdienst hinzufügen	32
Tabelle 6: AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen	35
Tabelle 7: AF - Anmeldung eines Akteurs am Messenger-Service	38
Tabelle 8: Einladung von Akteuren innerhalb einer Organisation	41
Tabelle 9: Überblick der Benutzerverwaltung in Abhängigkeit der Rolle	49

Tabelle 10 Zusätzliche Profilinformationen	49
Tabelle 11: Beispiel für FHIR-Fragebogen zur Datenschutzeinwilligung als JSON-Serialisierung	52
Tabelle 12: Beispiel für den Abruf des Datensatzes zum serverweiten Überschreiben des Namen eines Raumes	53
Tabelle 13: Beispiel für den Abruf der Capability zum Schreiben serverweiter Raumnamen mit Allow-Liste von Räumen.....	54
Tabelle 14: Beispiel für den Abruf der Capability zum Schreiben serverweiter Raumnamen mit Block-Liste von Räumen	54
Tabelle 15: Im Dokument verwendete Abkürzungen	57
Tabelle 16: Im Dokument verwendete Begriffe	57
Tabelle 17: Referenzierte Dokumente der gematik.....	59
Tabelle 18: Weitere Dokumente	60

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 17: 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 18: 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/
[Matrix Specification]	Matrix Foundation: Matrix Specification https://spec.matrix.org/v1.11
[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