

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation TI-Messenger-Dienst

Version:	1.0-01.1
Revision:	68057872746
Stand:	01.1031.07.20213
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_TI-Messenger-Dienst

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	01.10.2021		Erstversion des Dokumentes	gematik
1.1.0	29.07.2022		<u>Überarbeitung folgender Features:</u> - Erreichbarkeit einzelner Organisationseinheiten mittels Funktionsaccounts - Öffnung des TI-Messengers für Drittsysteme durch clientseitige Schnittstellen zur Integration z.B. ins Praxisverwaltungssystem - schnelles Finden von Kontaktdaten durch Zugriff auf FHIR-basiertes Adressbuch	gematik
	16.08.2022		<u>Möglichkeit einer Art Zugriffskontrolle für Org-Admin</u>	gematik
1.1.1	31.07.2023		<u>Einarbeitung TI-Messenger Maintenance 23.1 / VZD FHIR Maintenance_23.1</u>	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes	5
1.1 Zielsetzung	5
1.2 Zielgruppe	5
1.3 Geltungsbereich	5
1.4 Abgrenzungen	6
1.5 Methodik	6
2 Systemüberblick	8
3 Systemkontext	10
3.1 Akteure und Rollen	10
3.2 Nachbarsysteme	13
3.3 Ausprägungen des Messenger-Service	13
3.4 Nutzung von Personal Assertion Token (PASSport)	16
3.5 Verwendung der Token	17
4 Systemzerlegung	19
4.1 TI-Messenger-Fachdienst	19
4.1.1 Registrierungs-Dienst	20
4.1.2 Push-Gateway	20
4.1.3 Messenger-Service	20
4.1.3.1 Messenger-Proxy	21
4.1.3.2 PASSport-Service des Messenger-Service	21
4.1.3.3 Matrix-Homeserver	21
4.2 TI-Messenger-Client	22
4.3 VZD-FHIR-Directory	22
5 Übergreifende Festlegungen	24
5.1 Datenschutz und Sicherheit	24
5.2 Verwendete Standards	24
5.3 Authentifizierung und Autorisierung	25
5.3.1 Authentifizierung von Nutzern	25
5.3.2 Autorisierung am Messenger-Service	26
5.3.3 Autorisierung am FHIR-Proxy	26
5.4 Föderation	26
5.5 Rechtekonzept VZD-FHIR-Directory	27
5.5.1 Schreibzugriffe für TI-Messenger-Fachdienste	27
5.5.2 Schreibzugriff für TI-Messenger-Clients	27
5.5.3 Lesezugriff für TI-Messenger-Clients	27
5.6 Betrieb	28

6 Anwendungsfälle.....	29
6.1 AF – Anmeldung eines Nutzers an Messenger-Service.....	29
6.2 AF – Leistungserbringer als Practitioner hinzufügen.....	33
6.3 AF – Messenger-Service bereitstellen.....	36
6.4 AF – Organisationsressourcen im VZD-FHIR-Directory hinzufügen.....	39
6.5 AF – TI-Messenger Remote Invite.....	42
6.6 AF – Message senden (Remote).....	45
6.7 AF – Messenger-Service (Lokal).....	47
6.8 AF – Check remote Domain.....	49
7 Anhang A – Verzeichnisse.....	52
7.1 Abkürzungen.....	52
7.2 Glossar.....	53
7.3 Abbildungsverzeichnis.....	53
7.4 Tabellenverzeichnis.....	56
7.5 Referenzierte Dokumente.....	56
7.5.1 Dokumente der gematik.....	56
7.5.2 Weitere Dokumente.....	57
8 Anhang B – Abläufe.....	58
8.1 OIDC – Authorization Code Flow.....	58

1 Einordnung des Dokumentes.....	8
1.1 Zielsetzung.....	8
1.2 Zielgruppe.....	8
1.3 Geltungsbereich.....	8
1.4 Abgrenzungen.....	9
1.5 Methodik.....	9
2 Systemüberblick.....	11
3 Systemkontext.....	15
3.1 Akteure und Rollen.....	15
im Gesundheitswesen) oder ein technisches System.....	16
3.1.1 Rolle: "User".....	16
3.1.2 Rolle: "User-HBA".....	19
3.1.3 Rolle: "Org-Admin".....	19
3.2 Nachbarsysteme.....	22
3.3 Ausprägungen des Messenger-Services.....	23
3.3.1 Anwendungsbeispiel für Apotheken.....	26

3.3.2 and für HBA-Inhaber.....	28
3.4 TI-Messenger Föderation.....	28
ist der Betrieb eines Messenger-Proxies als Teil des Messenger-Services, der sicherstellen MUSS, dass nur zugelassene TI-Messenger-Fachdienste Zugang in die Föderation erhalten. Für die Aufnahme in die Föderation MÜSSen.....	
3.5 Berechtigungskonzept.....	30
3.5.1 Client-Server Kommunikation.....	31
3.5.1.1 Berechtigungskonzept - Stufe 1.....	31
3.5.2 Server-Server Kommunikation.....	31
3.5.2.1 Berechtigungskonzept - Stufe 1.....	31
3.5.2.2 Berechtigungskonzept - Stufe 2.....	32
3.5.2.3 Berechtigungskonzept - Stufe 3.....	32
3.6 Verwendung der Token.....	32
4 systemzerlegung.....	36
4.1 IDP-Dienst.....	37
4.2 VZD-FHIR-Directory.....	37
4.2.1 FHIR-Proxy.....	39
4.2.2 Auth-Service.....	40
4.2.3 OAuth.....	40
4.2.4 FHIR-Directory.....	41
4.3 TI-Messenger-Fachdienst.....	41
4.3.1 Registrierungs-Dienst.....	42
4.3.2 Push-Gateway.....	43
4.3.3 Messenger-Service.....	43
4.3.3.1 Messenger-Proxy.....	43
4.3.3.1.1 Client-Server Proxy.....	44
Matrix-Homeserver registriert sind. Ist dies.....	44
4.3.3.1.2 server-Server Proxy.....	45
keine der drei ST.....	45
4.3.3.2 Matrix-Homeserver.....	46
4.4 TI-Messenger-Client.....	47
5 Übergreifende Festlegungen.....	49
5.1 Datenschutz und Sicherheit.....	49
5.2 Verwendete Standards.....	49
5.2.1 OpenID-Connect.....	50
5.2.2 FHIR.....	50
5.3 Authentifizierung und Autorisierung.....	51
5.3.1 Authentifizierung von Akteuren am Messenger-Service.....	51
5.3.2 Authentifizierung am VZD-FHIR-Directory.....	51
5.3.2.1 Registrierungs-Dienst.....	51
5.3.2.2 TI-Messenger-Client.....	52
5.3.3 Autorisierung am Messenger-Service.....	52
Autorisierung am VZD-FHIR-.....	53
5.3.4 Directory.....	53
5.3.4.1 Registrierungs-Dienst.....	53
5.3.4.2 TI-Messenger-Client.....	53
5.4 Rechtekonzept VZD-FHIR-Directory.....	53

5.4.1 Lesezugriff.....	53
5.4.1.1 Registrierungs-Dienst.....	53
5.4.1.2 TI-Messenger-Clients.....	54
5.4.2 Schreibzugriff.....	54
5.4.2.1 Registrierungs-Dienst.....	54
5.4.2.2 TI-Messenger-Clients.....	54
5.5 User Management.....	55
des Matrix-Homeservers hinterlegt. Alle im User-.....	56
5.6 Funktionsaccounts.....	57
tungen im Gesundheitswesen sind sehr unterschiedlich strukturiert und wollen hinsichtlich ihrer Erreichbarkeit flexibel eigene Strukturen abbilden können. Daher sind beim TI-Messenger-Dien.....	57
5.6.1 Chatbot.....	58
5.7 Test.....	60
er-Anbieter MUSS eine Referenz-Instanz und mindestens eine Test-Instanz des TI- Messenger-Fachdienstes und TI-Messenger-Clients.....	60
5.8 Betrieb.....	62
6 Anwendungsfälle.....	65
verwendet. Die Authentisierung.....	70
6.1 AF - Bereitstellung eines Messenger-Service für eine Organisation.....	76
6.2 AF - Organisationsressourcen im Verzeichnisdienst hinzufügen.....	82
6.3 AF - Anmeldung eines Akteurs am Messenger-Service.....	87
Abbildung 13: LauFzeitsicht - Anmeldung eines Akteurs am Messenger.....	91
6.4 AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen.....	91
6.5 AF - Föderationszugehörigkeit eines Messenger-Service prüfen.....	96
6.6 AF - Einladung von Akteuren innerhalb einer Organisation.....	100
6.7 AF - Austausch von Events zwischen Akteuren innerhalb einer Organisation.....	106
6.8 AF - Einladung von Akteuren außerhalb einer Organisation.....	Error!
Bookmark not defined.	
6.9 AF - Austausch von Events zwischen Akteuren außerhalb einer Organisation.....	115
7 Anhang A - Verzeichnisse.....	118
7.1 Abkürzungen.....	118
7.2 Glossar.....	119
7.3 Abbildungsverzeichnis.....	119
7.4 Tabellenverzeichnis.....	125
7.5 Referenzierte Dokumente.....	126
7.5.1 Dokumente der gematik.....	126
7.5.2 Weitere Dokumente.....	126
8 Anhang B - Abläufe.....	128
8.1 Einträge im VZD-FHIR-Directory suchen.....	128

8.2 Aktualisierung der Föderationsliste.....130

8.3 Die folgende Abbildung beschreibt, wie der Messenger-Proxy seine lokal vorgehaltene Föderationsliste aktualisiert. Für die Aktualisierung der Föderationsliste MUSS der Messenger-Proxy diese beim Registrierungs-Dienst seines TI-Messenger-Fachdienstes anfragen. Die Häufigkeit der Anfrage einer neuen Liste wird durch den Anbieter festgelegt, Ziel sollte eine möglichst aktuelle Föderationsliste sein. Hierbei übergibt der Messenger-Proxy die durch ihn gespeicherte Version der Föderationsliste im Aufruf an den Registrierungs-Dienst. Bei Übereinstimmung der Version wird für den Messenger-Proxy keine neue Föderationsliste durch den Registrierungs-Dienst bereitgestellt. Ist die Version größer als die vom Messenger-Proxy übergebene, dann wird durch den Registrierungs-Dienst eine aktualisierte Föderationsliste zur Verfügung gestellt. Bei jeder Anfrage eines Messenger-Proxys beim Registrierungs-Dienst nach einer aktuellen Föderationsliste MUSS der Registrierungs-Dienst die Aktualität der durch ihn ausgelieferten Liste sicherstellen, indem er die von ihm gespeicherte Version der Föderationsliste im Bedarfsfall mit einer aktuelleren Version, die vom FHIR-Proxy bezogen wurde, überschreibt. Ein Download der Föderationsliste ist nur notwendig, wenn eine neuere Version auf dem FHIR-Proxy existiert. Die Struktur der Föderationsliste ist in [gemSpec_VZD_FHIR_Directory] beschrieben. Nach dem Abruf der Föderationsliste vom Registrierungs-Dienst, durch den Messenger Proxy, MUSS dieser die Signatur der Föderationsliste prüfen.....130

8.4 Stufen der Berechtigungsprüfung.....134

1 Einordnung des Dokumentes

1.1 Zielsetzung

Beim vorliegenden Dokument handelt es sich um die Festlegungen zur ersten Ausbaustufe des TI-Messengers. Diese Ausbaustufe ist definiert durch die Ad-hoc-Kommunikation zwischen Organisationen des Gesundheitswesens. Dabei wird insbesondere die Ad-hoc-Kommunikation zwischen Leistungserbringern bzw. zwischen Leistungserbringerinstitutionen betrachtet. Festlegungen zur Nutzergruppe der Versicherten und Anforderungen an Kassenrankenversicherungsorganisationen werden in der zweiten Ausbaustufe des TI-Messengers Berücksichtigung finden und daher im vorliegenden Dokument nicht weiter betrachtet.

Dieses Dokument beschreibt basierend auf den Anforderungen des Konzeptpapiers TI-Messenger [gemKPT_TI_Messenger] die systemspezifische Lösung des TI-Messengers des deutschen Gesundheitswesens. An dieser Stelle werden insbesondere die Anforderungen des Konzeptes in Form von definierten Anwendungsfällen zu Herstellung, Test und Betrieb des TI-Messenger-Dienstes beschrieben. Die jeweiligen Anwendungsfälle beschreiben den gesamten, für die Erfüllung notwendigen, Prozess und benennen alle für die Umsetzung notwendigen Teilkomponenten. Die weitere funktionale Spezifikation erfolgt in der jeweiligen dedizierten Spezifikation des Produkttyps.

Die vorliegende Spezifikation ist als funktionale Einheit mit der jeweils auf einen konkreten Produkttyp bezogenen Spezifikation zu betrachten.

1.2 Zielgruppe

Das Dokument richtet sich zum Zwecke der Realisierung an Hersteller von Produkttypen des TI-Messengers sowie an Anbieter, welche einen oder mehrere dieser die beschriebenen Produkttypen betreiben [gemKPT_Betr]. Alle Hersteller und Anbieter von TI-Anwendungen, deren Schnittstellen einen der Produkttypen des TI-Messengers nutzen, oder Daten mit den Produkttypen des TI-Messengers austauschen oder solche Daten verarbeiten, müssen dieses Dokument ebenso berücksichtigen.

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, Anbietertypsteckbrief, u.a.) oder Webplattformen (z. B. gitHub, u.a.) 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

In diesem Dokument werden die übergreifenden Anforderungen in Form von Anwendungsfällen spezifiziert. Die Funktionsmerkmale, die für die hier beschriebenen Anwendungsfälle genutzt werden, werden in den Spezifikationen der einzelnen Produkttypen des TI-Messenger-Dienstes weiter definiert.

Die vom TI-Messenger-Dienst bereitgestellten Schnittstellen werden in den Spezifikationen der einzelnen Komponenten des TI-Messenger-Dienstes definiert. Von anderen Produkttypen benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert.

Die vollständige Anforderungslage für den TI-Messenger-Dienst ergibt sich aus mehreren Spezifikationsdokumenten. Diese sind in den einzelnen Produkt- und Anbietertypsteckbriefen des TI-Messengers verzeichnet.

1.5 Methodik

Die Spezifikation ist im Stil einer RFC-Spezifikation verfasst. Dies bedeutet:

- **Der gesamte Text in der Spezifikation ist sowohl für den Hersteller des Produktes TI-Messenger-Dienst als auch für den betreibenden Anbieter entsprechend [gemKPT_Betr] verbindlich zu betrachten und gilt als Zulassungskriterium beim Produkt und Anbieter.**
- Die Verbindlichkeit SOLL durch die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet werden.
- 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 KÖNNEN außerdem um Pronomen in Großbuchstaben ergänzt werden, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

Anwendungsfälle und Akzeptanzkriterien als Ausdruck normativer Festlegungen werden als Grundlage für Erlangung der Zulassung durch Tests geprüft und nachgewiesen. Sie besitzen eine eindeutige, permanente ID, welche als Referenz verwendet werden SOLL. Die Tests werden gegen eine von der gematik gestellte Referenz-Implementierung durchgeführt.

Anwendungsfälle und Akzeptanzkriterien werden im Dokument wie folgt dargestellt:

<ID> - <Titel des Anwendungsfalles / Akzeptanzkriteriums>

Text / Beschreibung

[<=]

Die einzelnen Elemente beschreiben:

- **ID:** einen eindeutigen Identifier.
 - Bei einem Anwendungsfall besteht der Identifier aus der Zeichenfolge 'AF_' gefolgt von einer Zahl,
 - Der Identifier eines Akzeptanzkriterium wird von System vergeben, z.B. die Zeichenfolge 'ML_' gefolgt von einer Zahl
- **Titel des Anwendungsfalles / Akzeptanzkriteriums:** Ein Titel, welcher zusammenfassend den Inhalt beschreibt
- **Text / Beschreibung:** Ausführliche Beschreibung des Inhalts. Kann neben Text Tabellen, Abbildungen und Modelle enthalten

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

Der für die Erlangung einer Zulassung notwendige Nachweis der Erfüllung des Anwendungsfalles wird in den jeweiligen Steckbriefen festgelegt, in denen jeweils der Anwendungsfall gelistet ist. Akzeptanzkriterien werden in der Regel nicht im Steckbrief gelistet.

Hinweis auf offene Punkte

Offener Punkt: Das Kapitel wird in einer späteren Version des Dokumentes ergänzt.

2 Systemüberblick

Der TI-Messenger-Dienst sichere Nachrichtenaustausch zwischen beteiligten Akteuren des deutschen Gesundheitswesens wird durch erfolgt über die von TI-Messenger-Anbietern betrieben. Dabei werden von jedem Anbieter die benötigten Produkttypen bereitgestellt. Für den Nachrichtenaustausch wird verbreiteten TI-Messenger-Fachdienste und TI-Messenger-Clients. Die Ad-Hoc Kommunikation zwischen beteiligten Akteuren findet hierbei über zugelassene TI-Messenger-Client verwendet statt. Hierbei findet die sichere Ad-hoc-Kommunikation zwischen den Nutzern über die Produkttypen TI-Messenger-Fachdienst sowie TI-Messenger-Clients und die von werden durch von der gematik zugelassene TI-Messenger-Anbieter bereitgestellt.

Ein TI-Messenger-Fachdienst statt.

besteht aus einem oder mehreren Messenger-Services werden immer (basierend auf dem Matrix-Protokoll) die jeweils für eine Organisation (SMC-B-Inhaber) des Gesundheitswesens bereitgestellt und werden. Diese unterscheiden sich lediglich in der Art des verwendeten Authentifizierungsverfahrens. Akteure, Dies ermöglicht zugehörig zu eine nahtlose Integr Organisation agieren, KÖNNEN den durch diese Organisation in bereitgestellten Messenger-Service verwenden Alltag, da bestehende sichere und die innerhalb dieser Organisation bereits eingesetzten Authentifizierungsverfahren methoden nachgenutzt werden können. Nutzer. Dies ermöglicht eine nahtlose Integration in den Alltag. Akteure, die nicht zugehörig zu einer Organisation agieren, KÖNNEN Messenger-Services von Verbänden nutzen, falls diese durch einen Verband für ihre Mitglieder zur Verfügung gestellt werden. Hierbei kann das bestehende Authentifizierungsverfahren des Verbandes nachgenutzt verwendet werden. Nutzer die zugehörig zu einer Organisation agieren, Messenger-Services KÖNNEN den durch diese Organisation bereitgestellt mit unterschiedlichen TI-Messenger-Service nutzen und die innerhalb dieser Organisation Clients verwendeten Authentifizierungsmetho werden verwenden. Es, So ist für Nutzer möglich verschiedene TI-Messenger-Clients unterschiedlicher Organisationen zu nutzen (Beispiel: Ärzt beispielweise möglich, dass ein Arzt, der parallel in ist in einer Klinik und in einer niedergelassenen Praxis tätig und bekommt von ist, durch beiden Organisationen eijeweils einen TI-Messenger-Service zur Verfügung gestell); t bekommt.

Die Messenger-Services werden durch des TI-Messenger-Anbieter dezentral für Organis Dienstes werden in einer TI-Föderationen (SMC-B-Inhaber) bereitgestellt, die über das Matrix-Protokoll Nachrichten zusammengefasst, um nicht zugehörige Messenger- Dienste austauschen.

ließen. Um Teil der Föderation des TI-Messenger-Dienstes des deutschen Gesundheitswesens zu werden, MUSS die jeweilige Domain eines Messenger-Services vom TI-Messenger-Anbieter durch einen Registrierungs-Dienst in des TI-Messenger-Fachdienstes im VZD-FHIR-Directory hinterlegt werden. Ist dies erfolgt, erhalten dessen Nutzer Akteure Lesezugriff auf das VZD-FHIR-Directory und KÖNNEN je nach Berechtigung die Kommunikation mit Nutzer Akteuren in anderen Organisationen und/oder Leistungserbringern starten. Die Kommunikation findet dabei Ende-zu-Ende-verschlüsselt zwischen den jeweiligen TI-Messenger-Clients der beteiligten Messenger-Services und TI statt. Die Adressierung der Akteure innerhalb eines Messenger-Clients statt. Services erfolgt über die Matrix-User-ID und wird im Kontext des TI-Messenger-Dienstes als MXID bezeichnet. Um die beteiligten Akteure über den Eingang neuer Nachrichten zu informieren, MÜSSEN die USS der TI-Messenger-Fachdienst-Anbieter ein Push-Gateway betreiben. über ein Push-Gateway verfügen.

Hinweis: Im Sinne des Matrix-Protokolls sind Enden Endgeräte - in der Matrix-Spezifikation als "devices" bezeichnet -, welche die Fähigkeit haben, die an sie gesendeten Daten erstmalig nach der vollständigen Übertragung zu entschlüsseln. Dabei ist zu beachten, dass mit "Endgeräten" dedizierte Client-Instanzen und nicht zwangsläufig physische Geräte gemeint sind, die eindeutig über ihre device ID identifizierbar sind und von einem Client in dem Moment erzeugt werden, in dem dieser zur Anmeldung an einem Nutzerkonto verwendet wird. Damit sind ein oder mehrere Endgeräte einem Nutzerkonto, das selbst durch eine kryptographische Identität gekennzeichnet ist, untergeordnet und befähigen den Nutzer überhaupt erst zum Empfang und Versand Ende-zu-Ende-verschlüsselter Daten. Erst nach der Entschlüsselung der Daten können diese von einem Nutzer gelesen und von den von ihm eingesetzten Systemen wie beispielsweise einem Krankenhausinformationssystem dem Zweck entsprechend verarbeitet werden.

In der folgenden Abbildung sind alle beteiligten Komponenten der TI-Messenger-Architektur dargestellt:

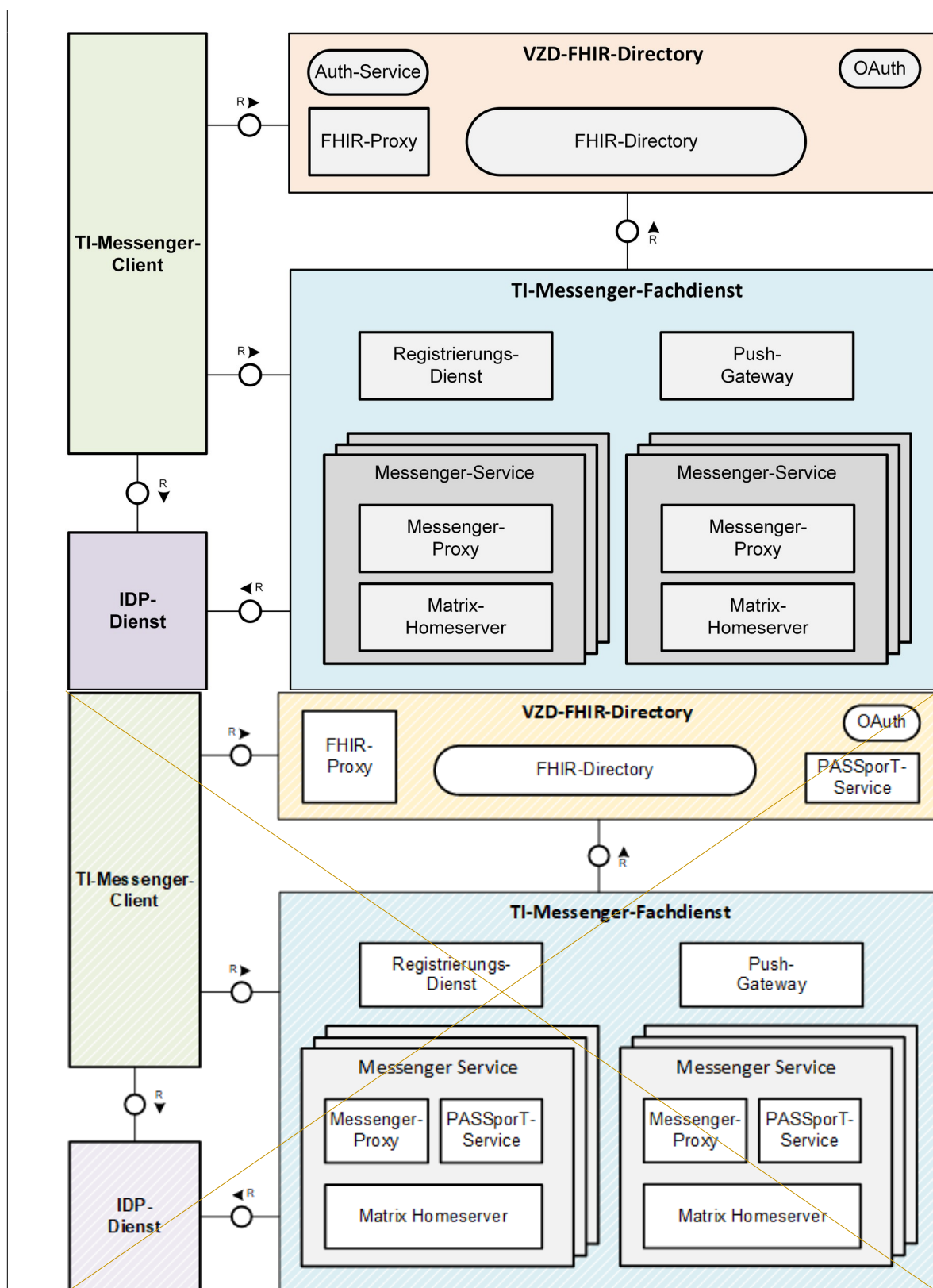


Abbildung 1: Komponenten der TI-Messenger-Architektur (vereinfachte Darstellung)

Der TI-Messenger-Dienst basiert auf dem offenen Kommunikationsprotokoll Matrix, das

| bereits von der Matrix Foundation gemäß [Matrix ~~Found~~Specification] spezifiziert ist. In
| den von der Matrix Foundation erstellten Spezifikationen ist sowohl die Client-Server-, die
| Server-Server-Kommunikation ~~und als~~ auch die API des Matrix-Push-Gateways
| beschrieben. Für die Sicherstellung der föderalen und dezentralen Struktur des TI-
| Messenger-Dienstes ~~und im deutschen Gesundheitswesen und~~ zur
| ~~Kontrolle~~Einschränkung des Nutzerkreises werden weitere Komponenten benötigt, welche
| in der jeweiligen durch die gematik veröffentlichten Spezifikation ~~dieser Komponenten~~
| beschrieben werden. ~~Die Komponenten si~~

3 Systemkontext

3.1 Akteure und so ausgelegt, dass Rollen

Im Kontext des TI-Messenger-diese der Matrix Spezifikation entsprechen und somit die Funktionen des TI-Messenstes werden verschiedene Akteure und Rollen definiert. Ein Akteur ist eine natürliche Person (Leistungserbringers / mit-darbeiter Funktionalität-deiner Matrix-SpezifikOrganisation weiterentwickelt werden können.

4-Sim Gesundheitswesen) oder ein technisches Systemkontext

4.1 Akteure und Rollen

Im Kontext des (Chatbot) die mit einem TI-Messenger-FachDienstes werden verschiedene Akteure und Rollen betrachtet interagieren. Abhängig von dem verwendeten Authentifizierungsverfahren ergeam Messenger-Service eines TI-Messenger-Fachdienstes ergeben sich unterschiedliche Rollen, die ein Akteur einnehmen kann. Diese sind in der Tabelle "Akteure undIm Folgenden werden diese Rollen" weiter beschrieben.

4.1.1 TabeRolle 1: Akteure und "User"

Die Rollen

Akteur	Rolle	Beschreibung und Berechtigungen
Leistungserbringer im Besitz eines HBAs (z. B. Zahnärzte, Apotheker, psychologische Psychotherapeuten)	User-HBA	<p>Ein LE im Besitz eines HBAs kann</p> <ul style="list-style-type: none"> • sich am Smartcard-IDP authentisieren • sich am Messenger-Service anmelden • seine MXID auf dem VZD-FHIR-Server hinterlegen und sich damit sektorübergreifend erreichbar machen • den TI-Messenger-Dienst nutzen <ul style="list-style-type: none"> • Kommunikationen innerhalb seiner Organisation aufbauen und entgegennehmen • Kommunikationen mit anderen Organisationen aufbauen • Kommunikationen mit LEs aufbauen und entgegennehmen, die ebenfalls mit HBA authentisiert und somit für ihn auf dem VZD-FHIR-Server auffindbar sind • *Direct Messaging [Direct Messaging] mit allen Teilnehmern der TI-Messenger-Dienste • **Group Messaging [Group Messaging] mit allen Teilnehmern der TI-Messenger-Dienste • im Namen der Organisation

		Kommunikation empfangen
	Org-Admin	<p>Ein LE im Besitz eines HBAs und einer SMC-B kann</p> <ul style="list-style-type: none"> • sich am Smartcard-IDP authentisieren • einen Messenger-Service für seine Organisation (korrespondierend zu seiner SMC-B) anlegen • seine Organisation auf dem VZD-FHIR-Server administrieren und damit sektorübergreifend erreichbar machen • die User dieses Messenger-Services administrieren • Homeserver-Konfigurationen vornehmen
Mitarbeiter einer Organisation im Gesundheitswesen (z. B. Pflegepersonal, Hebammen, Arzt im Krankenhaus, Mitarbeiter einer Kasse)	User	<p>Ein Mitarbeiter einer Organisation im Gesundheitswesen kann</p> <ul style="list-style-type: none"> • sich gegenüber dem Messenger-Service authentisieren • sich am Messenger-Service anmelden • den TI-Messenger-Dienst nutzen <ul style="list-style-type: none"> • Kommunikationen innerhalb seiner Organisation aufbauen und entgegennehmen • Kommunikationen mit anderen Organisationen aufbauen • Direct Messaging [Direct Messaging] mit allen Teilnehmern der TI-Messenger-Dienste • Group Messaging [Group Messaging] mit allen Teilnehmern der TI-Messenger-Dienste • im Namen der Organisation Kommunikation empfangen
	Org-Admin	<p>Ein Mitarbeiter einer Organisation im Gesundheitswesen mit Zugriff auf eine SMC-B</p> <ul style="list-style-type: none"> • sich am Smartcard-IDP authentisieren • einen Messenger-Service für seine Organisation (korrespondierend zu seiner SMC-B) anlegen • seine Organisation auf dem VZD-FHIR-Server administrieren und damit sektorübergreifend erreichbar machen

		<ul style="list-style-type: none"> • die User dieses Messenger-Services administrieren • Homeserver-Konfigurationen vornehmen
TI-Messenger-Anbieter	Org-Admin	<p>Ein TI-Messenger-Anbieter kann, auf Wunsch des LEs im Besitz einer SMC-B</p> <ul style="list-style-type: none"> • einen Messenger-Service für die Organisation (korrespondierend zur SMC-B des LEs) anlegen • diese Organisation auf dem VZD-FHIR-Server administrieren und damit sektorübergreifend erreichbar machen • die User dieses Messenger-Services administrieren • Homeserver-Konfigurationen für LEs vornehmen

*) Unter dem Begriff "Direct Message" kann von einem Leistungserbringer verstanden werden, dass im Kontext der Matrix-Spezifikation eine Kommunikation zwischen sowie von einem Mitarbeiter im Gesundheitswesen zwei Teilnehmern [gemSpec_TI-Messenger-Client].

**) Untereingenommen werden. Die Authentifizierung dem Begriff Group-Messaging versteht Akteurs erfolgt hierbei nicht man im Kontext über eine SMC-B oder Matrix-Spezifikation eine Kommunikation zwischen mehr als zwei Teilnehmern [gemSpec_TI-Messenger-Client].

Es besteht kein notwendiger Rollenausschluss zwischen den Service bereitgestellten Authentifizierungsverfahren. Für einzelnen Rollen Akteur in der Rollen, auch wenn sich U- "User und User-HBA rein logisch ausschließen.

Für KANN dessen MXID im Org-Admins besteht die Notwendigkeit einen Administriaansisationsverzeichnis auf dem VZD-FHIR-Director einzusetzen, hinterlegt welcher rden, um für Themen der Inform Akteure außerhalb seiner Organisationssicherheit geschult und sensi auffindbar zu werden. Chatbots zur Abbilisiert wurde. Sofern eine Organisation nicht über solches Personal verfügt, kann hierzu auf Org-Admins vom Anbietung von Funktionsaccounts nehmen ebenfalls die Rolle "User" ein und werden im Kapitel 5.6- Funktionsaccounts näher zurückgegriffen werden.

beschrieben.

In dieser Rolle kann Ein Akteur ist e:

- sich gegenüber eine Person oder eine Organisation, die mit dem Messenger-Service authentisieren und
- sich an einem TI-Messenger-Fachdienst interagiert. Diese InteraktiService anmelden.

4.1.2 Rolle: "User-HBA"

Die Rolle "User-HBA" kann ausschließlich von wird durch einem Leistungserbringer einen Anwendungsfall ausgelöst.

Leistungserbringer im Besitz eines ~~genommen~~ werden. Die Authentifizierung des Akteurs erfolgt hierbei über seinen HBA. Ein Akteur in der Rolle "User-HBAs KÖNNEN ihr" KANN seine MXID im ~~VZ~~Personenverzeichnis im VZD-FHIR-Directory hinterlegen, ~~um für~~ damit andere LeistungserbringerAkteure in der Rolle "User-HBA", die ebenfalls die eigene MXID auf dem VZD-FHIR-Directory hinterlegt haben, ~~auffindbar zu sein~~ kontaktieren können.

in ~~(dieser Rolle: User-HBA)~~. Hinterlegt ein Leistungserbringer im Besitz eines HBAs ~~kann ein Akteur:~~

- ~~sich am zuständigen IDP-Dienst authentisieren,~~
- ~~sich am Messenger-Service anmelden und~~
- ~~seine MXID nicht auf dem VZD-FHIR-Directory, so kann er ledigl hinterlegen, um sich als Mitarbeiter einer damit persönlich, sektorübergreifend erreichbar zu machen.~~

4.1.3 Rolle: "Organisation gefunden werden o-Admin"

Die Rolle "Org-Admin" stellt eine besonder-Chatnachrichtene Rolle im Namen seinTI-Messenger Organisation empfaKontext dar. Leistungserbringen (Rolle: User).

r oder Mitarbeiter einer Organisation im Gesundheitswkönnen diesen in der R_Rolle User-KÖeiNNEN zunächst nur Akteuren schreiben, die ihnen, nachdem sie ihrer Organisation zugeordnet sind. Um mit Mitarbeiter vor erfolgreich am Registrierungs-Dienst unter Verwendung ihrer SMC-B oder durch das KIM-Verfahren außerhalb diesthentifiziert haben (siehe AnwendungsfallAF_10103 - Authentisieren einer Organisation am TI-Messenger-Dienst). Nach der Organisation kommenerfolgreichen Authentifizieren zu können, MUSS zwischen den Teilnehmern ein gültiges PASSporT ausgetauscht werung wird ein Admin-Account am Registrierungs-Dienst vom TI-Messenger-Fachdienst angelegt. Mit der Anmeldung am Registrierungs-Dienst über den-Dieses Token wird je nach Anwendungsfall entweder vom PASSporT-Service des Admin-Account nimmt ein Akteur die Rolle "Org-Admin" ein. Dieser KANN Messenger-Services für seine Organisation registrieren und Einträge im VZD-FHIR-Directory oder des jeweilig verwalten. Für die Rolle "Org-Admin" besteht die Notwendigkeit, Administratoren Messenger-Service-bereinzusetzen, welche für Themen der Informationssicherheit gestellt. Nchult und sensibilisiert wurden. eben-derfalls ist es möglich, dass direkte Organisation den Kommunikation zwischen Personen, haben Mitarbeiter TI-Messenger-Anbieter beauftragt, die Rolle "Org-Admin" zu übernehmen.

In dieser Rolle kann ein Akteur:

- ~~Messenger-Services für seiner Organisation zusätzlich registrieren,~~
- ~~die Möglichkeit Kontaktpunkte seine anderer Organisation anzuschreibuf dem VZD-FHIR-Server administrieren (z. B. Kardiologie eines Krankenhauses). Dabei KANN hinund damit sektorübergreifend erreichbar machen,~~
- ~~die Mitarbeiter der eigenen Organisation eine Person oder eine Gruppe von Personen stehen. Hiermit wird vor allem der Kommunikals Akteure dieses Messenger-Services im Matrix-Homeserver administrieren (Benutzerverwaltung) sowie für seine Organisation Funktionsaccounts einrichten und~~
- ~~Matrix-Homeserver-Konfiguration zwischenen für seine Organisationen Sorge-getragen vornehmen.~~

Die folgende Tabelle "Akteure" und weitergehende Prozesse vorbereitet:

"Leistungserbringer" gibt einen Überblick über die im Kontext des TI-Messenger-Dienstes definierten Rollen, abhängig vom verwendeten Authentifizierungsverfahren im Besitz eines HBAs, die ein Akteur einnehmen kann. Die Tabelle stellt alle möglichen Nutzerszenarien nach der erfolgreichen Authentifizierung einer Organisation im Gesundheitswesen am Registrierungs-Dienst dar.

Tabelle 2 mit Zugriff auf eAkteure und Rollen

<u>Welcher Akteur bin ich</u>	<u>Wie authentisiere ich mich</u>	<u>Welcher Dienst authentifiziert mich</u>	<u>Welche Rolle nehme ich ein</u>
<u>Leistungserbringer (z. B. Ärzte, Zahnärzte, Apotheker, psychologische Psychotherapeuten, Pflegepersonal, Hebammen, Mitarbeiter einer Kasse) im Sinne SGB V</u>	<u>HBA</u>	<u>VZD-FHIR-Directory über den zentralen IDP-Dienst</u>	<u>User-HBA</u>
	<u>Authentifizierungsverfahren der Organisation + 2. Faktor</u>	<u>Messenger-Service</u>	<u>User</u>
	<u>Admin-Account Credentials + 2. Faktor</u>	<u>Registrierungs-Dienst</u>	<u>Org-Admin</u>
<u>Mitarbeiter einer Organisation im Gesundheitswesen, die keine Leistungserbringer im Sinne SGB V sind.</u>	<u>Authentifizierungsverfahren der Organisation + 2. Faktor</u>	<u>Messenger-Service</u>	<u>User</u>
	<u>Admin-Account Credentials + 2. Faktor</u>	<u>Registrierungs-Dienst</u>	<u>Org-Admin</u>
<u>Beauftragter Administrator eines TI-Messenger-Anbieters</u>	<u>Admin-Account Credentials + 2. Faktor</u>	<u>Registrierungs-Dienst</u>	<u>Org-Admin</u>
<u>Chatbot</u>	<u>Authentifizierungsverfahren der Organisation</u>	<u>Messenger-Service</u>	<u>User</u>

Hine-SMC-B der Organisation, bekommen:

Bei den in der RoTabelle Org-Admin die Möglichkeit auf dem VZD-FHIR-Directory Einträge zu genannten Nutzerszenarien mit der 2-Faktor-Authentifizierung MUSS der TI-Messenger Anbieter sicherstellen und zu administrieren. Ein TI-Messenger Anbieter, dass die Sicherheitsempfehlungen des Bundesamt für Sicherheit in der Informationstechnik (BSI) gemäß [BSI 2-Faktor] berücksichtigt werden. Hierbei MUSS zur Resilienz gegen Angriffe aus der Ferne ein Verfahren gewählt werden, das mindestens mit "mittel" bewertet ist.

- Versicherte DÜRFEN aktuell NICHT als NutzerAkteure auf einem Messenger-Service eingetragen werden. Für die Nutzung eines Messenger-Service sind nur NutzerAkteure zugelassen, die durch ein bestehendes Vertragsverhältnis mit der jeweiligen Organisation zugeordnet werden können. Ein Nutzer-Account MUSS einer juristischen

Person oder im Besitz eines HBAs sind.

Im Folgenden wird die Kommunikation für eindeutig zugeordnet sein. Das Teilen von
Passwörtern eingehende und ausgehende Nachrichten aus der Zugangsdaten für die
gleichzeitige Nutzung Sicht eines Akteurs in den verschiedenen Rollen in eines Accounts
ist in Kommunikationsmatrix verdeutlicht.

Tabelle 3: Kommunikationsmatrix

<u>Org-Admin</u>	<u>User</u>	<u>User-HBA</u>	<u>Kommunikationsart</u>
<u>Ausgehende Kommunikation an:</u>			
<u>x</u>	<u>x</u>	<u>x</u>	<u>Akteure in der Rolle "User" innerhalb seiner Organisation</u>
<u>=</u>	<u>x</u>	<u>x</u>	<u>Akteure in der Rolle "User" außerhalb seiner Organisation</u>
<u>=</u>	<u>=</u>	<u>x</u>	<u>Akteure in der Rolle "User-HBA" außerhalb seiner Organisation</u>
<u>=</u>	<u>x</u>	<u>x</u>	<u>Akteure in der Rolle "User" und "User-HBA" durch Scan eines QR-Codes</u>
<u>Eingehende Kommunikation von:</u>			
<u>x</u>	<u>x</u>	<u>x</u>	<u>Akteuren in der Rolle "User" innerhalb seiner Organisation</u>
<u>=</u>	<u>x</u>	<u>=</u>	<u>Akteuren in der Rolle "User" außerhalb seiner Organisation</u>
<u>=</u>	<u>=</u>	<u>x</u>	<u>Akteure in der Rolle "User-HBA" außerhalb seiner Organisation</u>
<u>=</u>	<u>x</u>	<u>x</u>	<u>Akteuren in der Rolle "User" und "User-HBA" durch Scan eines QR-Codes</u>

4.2 Nachbarsysteme

Die folgende Abbildung zeigt die benachbarten Produkttypen des TI-Messenger-Dienstes:

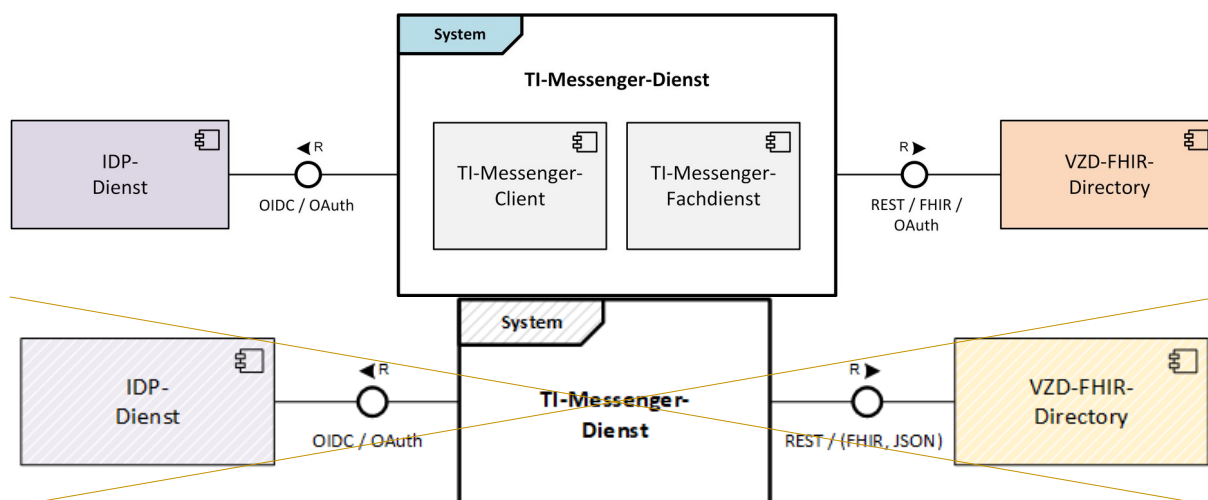


Abbildung 2: Benachbarten Produkttypen des TI-Messenger-Dienstes

Der TI-Messenger-Dienst nutzt als System besteht aus den Komponenten TI-Messenger-Fachdienst und TI-Messenger-Client.

Der Registrierungs-Dienst des TI-Messenger-Fachdienstes nutzt die OAuth- und REST-Schnittstellen von des VZD-FHIR-Directory, um Smartcard-IDPich mittels OAuth Client Credential Flow zu authentisieren um somit Zugriff auf das FHIR-Dienst der gematikrectory zu erhalten. Der TI-Messenger-Client nutzt die Schnittstellen eines zuständigen IDP-Dienstes zur Authentifizierung von eines Akteurs sowie Schnittstellen des gesondert spezifizierten VZD-FHIR-Directory, um z. B. Nutzer und der FHIR-Ressourcen zu finden MXIDs oder zu ändern.

4.3 Ausprägungen des Messenger-Services

Der Messenger-Service ist eine Teilkomponente des TI-Messenger-Fachdienstes und wird dezentral durch den jeweiligen Anbieter für Organisationen bereitgestellt. Der Messenger-Service besteht aus einem Matrix-Homeserver (basierend auf dem Matrix-Protokoll) und Komponenten die einem Messenger-Proxy der sicherstellen, dass eine FöderKommunikation mit anderen Messenger-Services, als Teil des TI-Messenger-Dienstes erfolgt. Bei diesen zusätzlichen Komponenten handelt es sich jeweils um, nur innerhalb der gemeinsamen Messenger-Proxy und einen PASSport-Service TI-Föderation erfolgt. Die Messenger-Services KÖNNEN den Nutzern aufgrund der Vielzahl an verschiedenen Akteuren unterschiedliche Authentifizierungsverfahren anbieten, bei denen der Besitz einer SMC-B oder eines HBAs nicht vorausgesetzt werden kann. Messenger-Services MÜSSEN immer Organisation en bzw. Verbänden zugeordnet werde sein, die über die Kontrolle der rs verbuwendenten Authentifizierungsverfahren verfügen.

Abhängig vom jeweiligen Messenger-Service gibt es verschiedene Abläufe bei der Anmeldung an einem TI-Messenger-Fachdienst. Dabei können diverse Authentifizierungsmechanismen durch eine Organisation für Ihre NutzerAkteure bereitgestellt werden. Die Organisation und der von ihr gewählte TI-Messenger-Anbieter vereinbaren den-as zur Anwendung kommende Authentifizierungsmechanismusverfahren bilateral und stimmen sich über die technische Realisierung der Authentifizierdafür notwendigen Anbindung ab. Möglich ist beispielsweise die Nachnutzung eines in der

Organisation betriebenen Active Directory ~~Servers~~ (AD/LDAP) oder eines geeigneten Single-Sign-On-Verfahrens (SSO). Der Anbieter MUSS sicherstellen, dass die Organisation die Kontrolle über die jeweiligen Authentifizierungsmechanismen besitzt, ~~um ein und die mögliche Nutzerkeit erhält eine notwendige~~ Löschung oder Sperrung ~~seines Nutzer-~~ Accounts sicherzustellen.

Zum besseren Verständnis werden im Folgenden ~~vier Aerschiedene, beispielhafte Anwendungsbeispiele dargestellt~~ Szenarien für den TI-Messenger skizziert und mögliche Ausprägungen eines Messenger-Service erläutert. Es besteht hierbei kein Anspruch auf Vollständigkeit :

Anwendungsbeispiel für eine Arztpraxis

Eine ArztDie folgenden User Stories sollen die Bedarfe von niedergelassenen Leistungserbringern an asynchrone Ad-hoc-Kommunikation beispielhaft verdeutlichen:

User Story 1 - Nutzung des TI-Messengers unabhängig von der HBA-Verfügbarkeit
Als niedergelassener Arzt in einer praxis registriert sich mittels SMC-B bei e stehe ich den Großteil meines Tages in direktem Patientenkontakt. Einen großen Teil der Organisation in der Praxis und der Kommunikation mit externen Stakeholdern übernimmt daher das Praxisteam. Als niedergelassener Arzt möchte ich meinem ganzen Praxisteam unabhängig von der Verfügbarkeit eines HBAs die Nutzung des TI-Messengers ermöglichen.

User Story 2 - Persönliche Erreichbarkeit als Arzt
Als niedergelassener Arzt in einem Registrierungs-Dienst eines Messenger-Anbieters. r Praxis möchte ich persönlich nicht immer für alle anderen TI-Messenger-Nutzer erreichbar sein. Vor allem für medizinische Anfragen von ärztlichen Kollegen möchte ich in der Nutzersuche intersektoral gefunden werden können.

User Story 3 - Erreichbarkeit der eigenen Praxis für externe Leistungserbringer
Als niedergelassener Arzt in einer Praxis möchte ich, dass meine Praxis als Einrichtung im Gesundheitswesen für andere TI-Messenger-Nutzer erreichbar ist und adressiert werden kann. Dabei möchte ich selbst entscheiden, wie ich die individuelle Struktur meiner Praxis bei Der AnbietKontaktsuche abbilde und ob ich selbst oder mein Praxistellt daraufhin am initial in die Kommunikation eingebunden wird.

User Story 4 - Erreichbarkeit anderer Einrichtungen im Gesundheitswesen
Als niedergelassener Arzt in einer praxis ein bekomme ich Patienten aus anderen Einrichtungen Messenger-Serviceim Gesundheitswesen überwiesen und habe Rückfragen zu Befunden oder Verschreibungen. Besonders bei Einrichtungen, mit einem sdenen ich nicht regelmäßig im Kontakt stehe, möchte icheren Authentifizierungsverfahr auch ohne bekannte Kontaktdaten eine Kommunikation aufbauen können und dabei sowohl die richtige Unterstruktur der Einrichtung (z. B. bestimmte Station in einem Krankenhaus) als auch den richtigen bereit. Durch die Dezentralität KANN dieser Ansprechpartner in dieser Unterstruktur (z. B. diensthabender Entscheider) erreichen können.

User Story 5 - Herstellung des Fallbezugs bei Kommunikationen
Als niedergelassener Arzt in einer Praxis findet ein großer Teil meiner Kommunikation mit anderen Leistungserbringern unter Bezugnahme zu einem Patienten oder Fall statt. Meine Nachrichten möchte ich unter diesem Aspekt verwalten können.

UService sowohl on-premise, als auch in einem Rechenzentrum in **Story 6** - Archivieren von Kommunikationen

Als niedergelassener Arzt in einer Praxis möchte ich fallbezogene Kommunikation in meinem Praxisverwaltungssystem in der jeweiligen Akte dokumentieren und somit nachvollziehbar speichern können.

User Story 7 - Geräte unabhängige Nutzung des TI-Messengers
Als Arzt in einer niedergelassenen Praxis arbeite ich vorrangig in meinem

Praxisverwaltungssystem an meinem staltiert werden. tionären Arbeitsplatz und möchte den TI-Messenger in diesem System integriert nutzen können. Wenn ich Hausbesuche mache, möchte ich Zusätzlich wird einen Account für ein die Möglichkeit haben, auch mobil auf alle meine Kommunikationen zuzugreifen und den TI-Messenger so überall nutzen können.

User Story 8 - Archivierbarkeit von Kommunikationen

Als Arzt in einer Praxis möchte ich fallbezogene Kommunikation in meinem Praxisverwaltungssystem in der jeweiligen lokalen Akteur in der Rolle Org- des Patienten dokumentieren und somit nachvollziehbar speichern können.

Aus den aufgezeigten User Stories ergibt sich der nachfolgende Ablauf für die Einrichtung und die Admin-durch den-istration eines TI-Messenger-Services:

Ein Akteur in einer Arztpraxis authentisiert seine Organisation unter Verwendung der SMC-B bei einem Registrierungs-Dienst eines TI-Messenger-Anbieter-erstellt. Der-s. Nach erfolgreicher Authentifizierung durch den Registrierungs-Dienst wird für die Organisation ein Administrator-Account angelegt. Nach erfolgreicher Anmeldung am Registrierungs-Dienst nimmt der Akteur die Rolle "Org-Admin-meldet sich am" ein und registriert einen Messenger-Service, der in einem Rechenzentrum bereitgestellt wird. Der Anbieter stellt daraufhin der Arztpraxis einen Messenger-Service an und hinterlegt sämtmit einem sicheren Authentifizierungsverfahren bereit. Zusätzliche-Nutzer- kann der Akteur in der Rolle "Org-Admin"Akteure für seiner-Arztpraxis- Organisation auf den Matrix-Homeserver einrichten (z. B. MFA, Ärzte). Die angelegten NutzerAkteure melden sich am Messenger-Service an und können den TI-Messenger in der Roller- "User" direkt nutzen.

Die Arztpraxis wird als Ein Akteur in der Rolle "Org-Admin" richtet für seine Organisation Funktionsaccounts im Organisation-für-Nutzersverzeichnis auf dem VZD-FHIR-Directory ein, um diese für Akteure anderer Organisationen des TI-Messenger-Dienstes erreichbar. Dazu KANN zu machen. Einem Funktionsaccount wird ein Akteur in der Rolle Org-Admin Kontaktpunkte auf dem VZD-FHIR-Directory einrichten. NutzerEinrichtung (z. B. MFA) zugeordnet, der weitere Akteure in den Chatraum einladen kann. Akteure der Arztpraxis im Besitz eines HBAs (Rolle "User-HBA") KÖNNEN sich zusätzlich im TI-Messenger-Client mittels HBA authentisieren und so die eigene MXID als Practitioner-Eintrag im Personenverzeichnis auf dem VZD-FHIR-Directory hinterlegen. -DaSomit könnhaben dsie Nutzer-zusätzlich die Möglichkeit andere hi, auf dem VZD-FHIR-Directory hinterlegte, HBA-Inhaber per Direct/Group-Messaging erreichen, (Rolle "User-HBA") in einen Chatraum einzuladen oder für diese erreichbar zu werden.

Anwendungsbeispiel für ein Krankenhaus

Ein-Die folgenden User Stories sollen die Bedarfe innerhalb eines Krankenhaus-registriert-sich-mitteses an asynchrone Ad-hoc-Kommunikation beispielhaft verdeutlichen:

User Story 1 - Einfache Administration der Nutzer

Als SMC-B-IT-Administrator der Klinik möchte ich die Administration der Nutzer meiner Organisation beim TI-Messenger möglichst automatisiert abbilden können, um Arbei-einem-Registriertsaufwand bei der regelmäßigen Pflege der Nutzereinträgen zu minimieren.

User Story 2 - Einfache Bereitstellungs-Dienst eines Messenger-Anbieters. Der Anbieter prüft die- und Anmeldung am Dienst

Als Arzt in einer Klinik möchte ich die bereits vorhandenen Mittel zur Anmeldung an den IT-Systemen für den TI-Messenger nachnutzen können. Die Anmeldung am Dienst sollte

für mich analog zu den Anmeldungen an anderen IT-Systemen ablaufen, die ich in der Klinik nutze.

User Story 3 - Abbildbarkeit der unterschiedlichen Funktionsbereiche in einer Klinik
Als Arzt in einer Klinik habe ich Rückfragen an einen anderen Fachbereich gestellt. SMC-B
und stelle dem Krankenhaus und möchte die entsprechende Abteilung oder Station
erreichen können, ohne dass ich bei der Kontaktsuche weiß, welche anderen Kollegen
dort beschäftigt sind oder Dienst haben.

User Story 4 - Interdisziplinäre Teams
Als Arzt in einer Klinik bin ich in einem interdisziplinären Team mit Kollegen anderer
Fachrichtungen tätig und möchte dabei zu einem Messenger-Service in Fall neue
Laborbefunde oder neu verfügbare Bilddaten mit den Kollegen austauschen können.

User Story 5 - Fallbasierte Kommunikation
Als Pflegefachkraft auf einer Station möchte ich die Kollegen auf meiner Station überrei-
te. Die Neuigkeiten zu einem Patienten informieren und relevante Informationen (z. B.
anstehende To-Dos bei einem Schichtwechsel) teilen.

Aus den aufgezeigten User Stories ergibt sich der nachfolgende Ablauf für die
Dezentralität KANN dieser Service sowohl on-premise, als auch in Einrichtung und die
Administration eines TI-Messenger-Services innerhalb eines Krankenhauses:

Ein Akteur eines Krankenhauses authentisiert sich mittels SMC-B bei dem Registrierungs-
Dienst eines TI-Messenger-Anbieters. Der Registrierungs-Dienst verifiziert die verwendete
SMC-B der Organisation. Bei Erfolg stellt der Registrierungs-Dienst der Organisation
einem Rechenzentrum in Administrator-Account bereit. Nach erfolgreicher Anmeldung am
Registrierungs-Dienst stellt werden nimmt der Akteur die Rolle "Org-Admin" ein und
registriert einen Messenger-Service für das Krankenhaus. Dieser Service wird on-
premise im Krankenhaus bereitgestellt. Der Messenger-Service KANN das verwendet bei
der Registrierung der Akteure am Matrix-Homeserver das bestehende
Authentifizierungsverfahren des Krankenhauses (z. B. Active Directory) nutzen. Die
NutzerAkteure des Krankenhauses können anschließend mit den bestehenden
Anmeldedaten den TI-Messenger-Dienst nahtlos verwenden, auch ohne im Besitz eines
HBA's (Pflege, Therapeuten, Ärzte ohne HBA =) zu sein.

Ein Akteur in der Rolle: User zu "Org-Admin" richtet für die Abteilungen in sein:

Das Krankenhaus wird als Organisation Funktionsaccounts im VZD-FHIR-Directory ein,
um diese für andere Akteure Nutzeraußerhalb des TI-Messenger-DienstKrankenhauses
erreichbar. Da zu KANN machen. ein Akteur ein Funktionsaccount wird in der Rolle Org-
Admin Kontaktpunkte auf dem VZD-FHIR-Directory Chatbot zugeordnet, der automatisiert
den diensthabenden Arzt ermittelt und in den Chatraum einrichten. Nutzlädt.

4.3.1 Anwendungsbeispiel für Apotheken

Die folgenden User dStories Krankenhauses im Besitz sollen die Bedarfe von
Apotheken an asynchrone Ad-hoc-Kommunikation beispielhaft verdeutlichen:

User Story 1 - Versand von Fotos
Als Apotheker bin ich mit eines HBAs KÖNNEN zusätzlich fehlerhaften Rezept
konfrontiert und möchte den Sachverhalt mittels des TI-Messe dem verschreibenden
Leistungserbringer Clients die eigene MXID als Practi klären. Dazu mache ich ein Foto von
betreffenden Rezept und stelle meine Rückfrage per Chat an die Organisationer-Eintrag
des auf dem VZD-FHIR-Direcsstellenden Leistungserbringers.

User Story hinterlegt - Gruppenchats zur regelmäßigen (Rolle = User-HBA). Damit können die Nutzereinfach weitergegeben werden.

Als Apotheker möchte ich die Leistungserbringer in räumlicher Nähe zu meiner anderen hinterlegten HBA-Inhaber-Apotheke in einer gemeinsamen Gruppe über Direct/Group-Messaging erreichen, oder die Wiederverfügbarkeit eines vergriffenen Präparates informieren.

Aus den aufgezeigten User Stories ergibt sich der nachfolgende Ablauf für diese Einrichtung:

Anwendungsbeispiel - Nutzung und die Administration eines TI-Messenger-Services innerhalb einer Apotheke

Der Anbieter stellt:

Ein Akteur einer Apotheke authentisiert sich mittels SMC-B bei dem Registrierungs-Dienst eines TI-Messenger-Service-Anbieters. Der Registrierungs-Dienst verifiziert die verwendete SMC-B der Organisation. Bei Erfolg stellt der Registrierungs-Dienst Dezentralität-KANN-Organisation einen Administrator-Account bereit. Nach erfolgreicher Anmeldung am Registrierungs-Dienst nimmt der Service sowohl on-premise, als auch der Akteur die Rolle "Org-Admin" ein und registriert einen Messenger-Service für die Apotheke, der in einem Rechenzentrum installiert werden bereitgestellt wird. Für die Authentifizierung der Akteure am Messenger-Service wird mit dem bestehenden zuständigen IDP-Dienst der Apotheken verwendet, so dass die dort hinterlegten NutzerAkteure der Apotheke sich am TI-Messenger mittels OpenID-Connect verwenden auch ohne im Besitz eines HBA zu sein (z. B. PTA, angestellte Apotheker ohne HBA) anmelden können.

Die Apotheke wird als Organisation für andere NutzerAkteure des TI-Messengers erreichbar, indem ein Akteur in der Rolle "Org-Admin-Kont" MXIDs von Akteuren seiner Apotheke im Organisationsverzeichnis auf dem VZD-FHIR-Directory einrichtet. NutzerAkteure der Apotheke im Besitz eines HBAs KÖNNEN (Rolle "User-HBA") hinterlegen zusätzlich mittels des TI-Messenger-Clients die eigene MXID als Practitioner-Eintrag im Personenverzeichnis auf dem VZD-FHIR-Directory hinterlegen. Somit haben Sie zusätzlich die Möglichkeit andere hier, auf dem VZD-FHIR-Directory hinterlegte HBA-Inhaber per Direct-Messaging zu erreichen (Rolle "User-HBA") in einen Chatraum einzuladen oder für diese erreichbar zu werden.

Anwendungsbeispiel für einen Verband

4.3.2 Der Anbieter eines TI-Messenger-Dienstes stellt ein für HBA-Inhaber

Die folgenden User Stories sollen die Bedarfe von Verbänden an asynchrone Ad-hoc-Kommunikation beispielhaft verdeutlichen:

User Story 1 - Diskussion von Fällen

Als Verbänden möchte ich meinen Messenger-Service-Mitgliedern eine Plattform geben, um schwierige Fälle gemeinschaftlich diskutieren zur Verfügung. Durch die Dezentralität können.

User Story 2 - Sichere Kommunikation unabhängig von der Einrichtung in der das Mitglied tätig ist - KANN dieser Service sowohl on-premise, als auch igt ist

Als Verband möchte ich meinen Mitgliedern die Möglichkeit geben, persönlich im TI-

Messenger erreichbar zu werden und so unabhängig von der Einrichtung, in einem Rechenzentrum installiert werden. Der der das jeweilige Mitglied tätig ist, den Dienst nutzen zu können.

Aus den aufgezeigten User Stories ergibt sich der nachfolgende Ablauf für die Einrichtung und die Administration eines TI-Messenger-Service KANN mit dem bestes innerhalb eines Verbandes:

Der Verband hat eine SMC-B ORG beantragt, die für die Authentifizierung am Registrierungs-Dienst eines TI-Messenger-Anbieters verwendet wurde. Der Registrierungs-Dienst verifiziert die verwendete SMC-B des Verbandes verbunden werden. Die dort hinterlegten Mitgli. Bei Erfolg stellt der Registrierungs-Dienst dem Verband einen Administrator-Account bereit. Nach erfolgreicher Anmeldung am Registrierungs-Dienst nimmt der Akteur die Möglichkeit ihre bestehende Rolle "Org-Admin" ein und registriert einen Messenger-Service für den Authentifizierungsdaten des TI-Messenger-Verband, der in einem Rechenzentrum bereitgestellt wird. Dieser Service wird für Mitarbeiter im Gesundheitswesen verfügbar gemacht, Dienstes nicht einer Organisation mit Zugriff auf eine SMC-B zu verwendend zugehörig sind.

Nutzer/Akteure des Verbandes im Besitz eines HBAs (Rolle "User-HBA") KÖNNEN zusätzlich mittelst des TI-Messenger-Clients die eigene MXID als Practitioner-Eintrag im Personenverzeichnis auf dem VZD-FHIR-Directory hinterlegen. Damit können sie Nutzer/andere, auf dem VZD-FHIR-Directory hinterlegte, HBA-Inhaber per Direct-Messaging erreichen, (Rolle "User-HBA") in einen Chatraum einladen oder für diese erreichbar werden.

4.4 Im Folgenden wird noch einmal die TI-Messenger Föderation

Da der TI-Messenger-Dienst auf dem offenen und dezentralen Kommunikation für eingehende und ausgehende Nachrichtenprotokoll Matrix basiert, MUSS gewährleistet werden, dass nur berechnete Matrix-Homeserver eines Messenger-Services teilnehmen.

Um allen berechtigten aus der Nutzersicht in der Rolle U Akteuren des deutschen Gesundheitswesens den Zugang zum TI-Messenger-Dienst zu gewähren, MUSS ein Anbieter eines TI-Messengers für Leistungserbringerinstitutionen und/oder Organisationen eigene Messenger-Services bereitstellen. Um nicht zum TI-Messenger-HBA in einer Kommunikationsdienst gehörende Matrix-Homeserver ausschließen zu können, werden die Domainnamen (im Weiteren auch als Matrix-Domain bezeichnet) der matrix-verdeutlicht.

Tab-Homeserver der Messenger-Services in einer Föderationsliste zusammengefasst. Diese wird durch das VZD-FHIR-Directory bereitgestellt. Voraussetzung für die Kommunikation in die Föderationsmatrix

Rolle	Ausgehende Kommunikation	Eingehende Kommunikation
User	<ul style="list-style-type: none"> Start der Kommunikation mit anderen Organisationen Start der Kommunikation mit Nutzern in der Rolle User und User-HBA innerhalb einer Organisation 	<ul style="list-style-type: none"> Kommunikationsanfragen durch Nutzer in der Rolle User und User-HBA innerhalb einer Organisation Kommunikationsanfragen durch Nutzer in der Rolle User und User-HBA anderer Messenger-Services durch

	<ul style="list-style-type: none"> Start der Kommunikation mit Nutzern in der Rolle <i>User</i> und <i>User-HBA</i> anderer Messenger-Services durch Scan eines QR-Codes 	<p>Scan eines QR-Codes</p> <ul style="list-style-type: none"> Kommunikationsanfragen durch Nutzer in der Rolle <i>User</i> und <i>User-HBA</i> anderer Messenger-Services als Ansprechpartner der Organisation. Die MXID wurde durch einen Nutzer in der Rolle <i>Org-Admin</i> bei entsprechender Ressource der Organisation auf das VZD-FHIR-Directory hinterlegt
User-HBA	<ul style="list-style-type: none"> Start der Kommunikation mit anderen Organisationen Start der Kommunikation mit Nutzern in der Rolle <i>User</i> und <i>User-HBA</i> innerhalb einer Organisation Start der Kommunikation mit Nutzern in der Rolle <i>User</i> und <i>User-HBA</i> anderer Messenger-Services durch Scan eines QR-Codes Start der Kommunikation mit Nutzern in der Rolle <i>User-HBA</i> anderer Messenger-Services durch Nutzersuche auf VZD-FHIR-Directory 	<ul style="list-style-type: none"> Kommunikationsanfragen durch Nutzer in der Rolle <i>User</i> und <i>User-HBA</i> innerhalb einer Organisation Kommunikationsanfragen durch Nutzer in der Rolle <i>User</i> und <i>User-HBA</i> anderer Messenger-Services durch Scan eines QR-Codes Kommunikationsanfragen durch Nutzer in der Rolle <i>User-HBA</i> anderer Messenger-Services durch Auffindbarkeit auf VZD-FHIR-Directory Kommunikationsanfragen durch Nutzer in der Rolle <i>User</i> und <i>User-HBA</i> anderer Messenger-Services als Ansprechpartner der Organisation. Die MXID wurde durch einen Nutzer in der Rolle <i>Org-Admin</i> bei entsprechender Ressource der Organisation auf das VZD-FHIR-Directory hinterlegt

4.5- ist der Betrieb eines Messenger-Proxies als Teil des Messenger-Services, der sicherstelle Nutz MUSS, dass nur zugelassene TI-Messenger-Fachdienste Zugang von Personal-Asserin die Föderation erhalten. Für die Aufnahme in die Föderation TokMÜSSen (PASSporT)

ausschließlich Matrix-Homeserver verwendet werden. Es MUSS Für die EtablierungAufnahme in die Föderation eines Rechtekonzeptes innerhalb des T. erfolgreiche Zulassung des TI-Messenger-Anbieters mit ebenfalls erfolgreichen Zulassungen für die Produkttypen TI-Messenger-FachDienstes ist es notwendig ein geeignetes Verfahren vorzuseh und TI-Messenger-Client durch die gematik erfolgt sein. Nach einer erfolgreichen Zulassung erhält der Registrierungs-Dienst des jeweiligen Fachdienstes die Möglichkeit die Matrix-Domains der jeweiligen Messenger-Services einer entsprechenden Organisation auf dem VZD-FHIR-Directory zuzuordnen. Es wird ein Personal-Assertion Tok Ein serverseitiges Bridging zu anderen Messaging-Protokollen DARF NICHT stattfinden. Um eine Integration eines TI-Messenger-Clients in bestehende Systemumgebungen (PASSporT) gemäß [RFC 8225#PASSporT: Persrimärsysteme oder alternative Messenger-Clients) zu ermöglichen, ist der clientseitige bidirektional-Assertion Töke Austausch mit Drittsystemen erlaubt.

4.6 Berechtigungskonzept

Wie im Kapitel 3.4- TI-Messenger Föderation beschrieben] in Anfragen an den, dient die TI-Messenger-Föderation dazu, nicht zugelassene Matrix-Homeserver hinzugefügt. Bestandteil des Paus dem TI-Messenger-Dienst auszuschließen. Ebenfalls MUSS es möglich sein, dass nur die im Kapitel 3.1- Akteure und Rollen genannten berT ist- sowohl die MXID des einladenden Nutzers, als auch berechtigten Akteure miteinander kommunizieren dürfen. Hierfür ist die Etablierung eines Rechtekonzeptes innerhalb des TI-Messenger-Dienstes notwendig.

Das Rechtekonzept basiert auch die MXID des f einer mehrstufigen Prüfung. Mit Hilfe des Berechtigungskonzeptes wird nachgewiesen, ob eingeladenen Nutzers. Aufgrund des Domain Parts- Akteur berechtigt ist, innerhalb der TI-Messenger-Föderation mit einem anderen Akteur zu interagieren. Die Art der Prüfung ist abhängig davon, ob es sich um eine Client-Server oder MXID und der Rolle eines Nutzers entscheidet das VZD-FHIR-DirectoryServer-Server Kommunikation handelt. Das Berechtigungskonzept wird im Folgenden näher beschrieben.

4.6.1 Client-Server Kommunikation

4.6.1.1 Berechtigungskonzept - Stufe 1

In dieser Stufe MUSS bei der Client-Server Kommunikation geprüft werden, ob die in PASSport ausgestellte Anfrage enthaltenen Matrix-Domains zugehörig zur TI-Föderation sind. Das PASSport, das hierbei MUSS der Messenger-Proxy bei jedem Invite-Event prüfen, ob die in der Anfrage an einen vom TI-Messenger-Client enthaltenen Matrix-Homeserver Domains der Einzuladenden in der Föderationsliste enthalten ist, wird sind. Ist dies der Fall, MUSS die Anfrage durch den Messenger-Proxy bei den Matrix-Homeserver der Einladung einenden weitergeleitet werden. Ist dies Nutzers in einen Chatraum (eicht der Fall, MUSS die beabsichtigte Anfrage des Akteurs vom Messengergehend/ausgehend) überprüft. Ein PASSport wird zentral durch dr-Proxy des Einladenden abgelehnt werden. Nach der Weiterleitung an den Matrix-Homeserver des Einladenden prüft dieser, ob der eingeladene Akteur der gleichen PASSport-Organisation angehört. Stellt der Matrix-HomeService im Rahmen des VZD-FHIR-Directory, aber obigen Prüfung fest, dass der auch, abhängig von der beabsichtigten eingeladene Akteur nicht zu seiner Domain gehört, wird das Invite-Event an den Messenger-Proxy des Matrix-Homeservers des einzuladenden Akteurs gerichtet, wobei die Regeln der Server-Server Kommunikation, lokal bei den PASSport durchzuführen sind.

4.6.2 Server-Server Kommunikation

4.6.2.1 Berechtigungskonzept - Stufe 1

In der 1. Stufe der Server-Service Kommunikation MUSS der Messenger-Services-ausgeProxy für alle Events eine Prüfung durchführen, die feststellt, ob Die Nutz im Event enthaltenen Matrix-Domains zur TI-Föderation gehören. Zur Prüfung des lokalen PASSport-Service ermöglicht es Nutzern einer Föderationszugehörigkeit MUSS der Messenger-Proxy im Authorization-Header die im Attribut "origin" enthaltene Domain (bei eingehender Kommunikation) und die im Attribut "destination" enthaltene Domain

(bei ausgehender Kommunikation ohne eine vor) gegen die Domains in der Föderationsliste prüfen. Bei erfolgreicher Abfrage am VZD-FHIR-Directory aufzubauen, wenn beide Gesprächspartner aktiv in Prüfung erfolgt dann die Weiterverarbeitung gemäß der Stufe 2.

4.6.2.2 Berechtigungskonzept - Stufe 2

In dieser Stufe prüft der Messenger-Proxy des Einzuladenden auf eine vorliegende Freigabe. Hierbei handelt es sich um eine Lookup-Table, in der alle erlaubten Akteure hinterlegt sind, von denen man eine eine Kommunikationladung in einen Chatraum akzeptiert. Ist ein Eintrag vom einladenden Akteur vorhanden, dann MUSS die beabsichtigte einwilligladung des Akteurs zugelassen werden. Ist Die Bereitstells nicht der Fall, MUSS die weitere Überprüfung gemäß der 3. Stufe erfolgen.

4.6.2.3 Berechtigungskonzept - Stufe 3

In des PASSporT durch den Mer letzten Stufe erfolgt die Prüfung ausgehend von den Einträgen der beteiligten Akteure im VZD-FHIR-Directory. Die Einladung MUSS zugelassenger-Ser werden, wenn:

- die MXID des einzuladenden Akteurs im Organisationsver-erfolgezeichenis hinterlegt analog zu und seine Sichtbarkeit in diesem Verzeichnis nicht eingeschränkt ist oder
- der einladende sowie der einzuladende Akteur im PASSporT-Service des VZD-FHIR-Directorypersonenverzeichnis hinterlegt sind und der einzuladende Akteur seine Sichtbarkeit in diesem Verzeichnis nicht eingeschränkt hat

Ist die Prüfung nicht erfolgreich, dann MUSS die beabsichtigte Einladung des Akteurs vom Messenger-Proxy abgelehnt werden.

4.7 Verwendung der Token

Für die Nutzung des TI-Messenger-Dienstes kommen unterschiedliche Arten von Token zum Einsatz Authentisierung und werden in Autorisierung an weiteren Diensten zum Einsatz die in verschiedenen Anwendungsfällen verwendet. Es existier werden. Aus diesem Grund werden die in der folgenden für eine Tabelle die verschiedenen Token näher beschrieben.

Tabelle 5: Authentirten von Token

Token	ausgestellt vom	Beschreibung
ID_TOKEN	zentralen IDP-Dienst	<p>Dieses Token wird auf Basis von SmartCard-Identitäten vom zentralen IDP-Dienst ausgestellt und beinhaltet die zugehörigen Identitätsdaten (TelematikID, ProfessionOID etc.).</p> <p>Der Registrierungs-Dienst nutzt dieses Token, um die enthaltene ProfessionOID auf einen gültigen Institutionstypen für eine SMC-B zu prüfen und im</p>

		<p><u>Rahmen einer Messenger-Service Bestellung die enthaltene TelematikID in die Föderationsliste einzutragen.</u></p> <p><u>Das VZD-FHIR-Directory nutzt dieses Token, um zu ermitteln für welche Ressource (identifiziert durch die TelematikID) ein owner-accesstoken ausgestellt wird.</u></p>
<u>Matrix-ACCESS_TOKEN</u>	<u>Matrix-Homeserver</u>	<p><u>Nach der erfolgreichen Anmeldung eines Akteurs am Matrix-Homeserver wird ein Access-Token vom Matrix-Homeserver ausgestellt. Im Kontext des TI-Messenger-Dienstes wird das vom Matrix-Homeserver ausgestellte Access-Token als Matrix-ACCESS_TOKEN bezeichnet.</u></p> <p><u>Dieses Token MUSS im lokalen Speicher des TI-Messenger-Clients sicher abgespeichert werden. Dieses Token wird bei jeder weiteren Interaktion mit dem ausstellenden Matrix-Homeserver verwendet, um den TI-Messenger-Client zu berechtigen bestimmte Dienste des Servers zu nutzen. Es ist an die Session des jeweiligen TI-Messenger-Clients gebunden.</u></p>
<u>Matrix-OpenID-Token</u>	<u>Matrix-Homeserver</u>	<p><u>Bei dem Matrix-OpenID-Token handelt es sich um ein 3rd-Party-Token, welches von einem Matrix-Homeserver gemäß [Client-Server API#OpenID] bei Bedarf für einen Akteur ausgestellt wird. Im Kontext des TI-Messenger-Dienstes wird das 3rd-Party-Token als Matrix-OpenID-Token bezeichnet.</u></p> <p><u>Das Matrix-OpenID-Token wird für die Verifizierung eines Messenger-Services sowie für das Suchen von FHIR-Ressourcen im VZD-FHIR-Directory benötigt. Hierfür wird das Matrix-OpenID-Token im Auth-Service des Verzeichnisdienstes gegen ein search-accesstoken ersetzt, welches am FHIR-Proxy für die weitere Verarbeitung benötigt wird. Das ursprünglich ausgestellte Matrix-OpenID-Token wird dann nicht mehr benötigt. Zur Überprüfung der Gültigkeit des Matrix-OpenID-Token ruft der Auth-Service den Userinfo-Endpoint am jeweiligen Matrix-Homeserver auf.</u></p>
<u>RegService-OpenID-Token</u>	<u>Registrierungs-Dienst</u>	<p><u>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.</u></p> <p><u>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</u></p>

		<u>ersetzt, welches am FHIR-Proxy für die weitere Verarbeitung benötigt wird.</u>
<u>ti-provider-accesstoken / provider-accesstoken</u>	<u>OAuth / Auth-Service des VZD-FHIR-Directory</u>	<p><u>Das ti-provider-accesstoken wird dem Registrierungs-Dienst durch den OAuth-Service und das provider-accesstoken durch den Auth-Service des VZD-FHIR-Directory bereitgestellt.</u></p> <p><u>Ein provider-accesstoken wird z. B. benötigt, wenn der Registrierungs-Dienst eines TI-Messenger-Fachdienstes, nach der Bereitstellung eines neuen Messenger-Service für eine Organisation, einen neuen Förderationslisteneintrag für diese Organisation anlegt oder der Registrierungs-Dienst eine Förderationsliste vom FHIR-Proxy abfragen möchte. Hierfür übergibt der Registrierungs-Dienst im ersten Schritt vereinbarte Client-Credentials an den OAuth-Service des VZD-FHIR-Directory und erhält nach der erfolgreichen Prüfung dieser Credentials das ti-provider-accesstoken. Das ti-provider-accesstoken wird anschließend an den Auth-Service des VZD-FHIR-Directory übergeben und bei erfolgreicher Prüfung durch das VZD-FHIR-Directory wird ein provider-accesstoken ausgestellt.</u></p>
<u>search-accesstoken</u>	<u>Auth-Service des VZD-FHIR-Directory</u>	<p><u>Das search-accesstoken wird einem berechtigten Akteur durch den Auth-Service des VZD-FHIR-Directory bereitgestellt.</u></p> <p><u>Dieses wird für die Suche im VZD-FHIR-Directory benötigt und stellt sicher, dass nur berechnigte Akteure im VZD-FHIR-Directory eine Suche auslösen können. Dazu wird das vom Matrix-Homeserver ausgestellte Matrix-OpenID-Token an den Auth-Service des VZD-FHIR-Directory übergeben. Dieses dient in diesem Fall als Nachweis, dass ein Akteur bei einem der TI-Föderation angehörenden Messenger-Service registriert ist. Nur dann wird durch den Auth-Service des VZD-FHIR-Directory ein search-accesstoken bereitgestellt. Es muss bei der dann folgenden Suche im VZD-FHIR-Directory im Aufruf enthalten sein. Die Prüfung erfolgt durch den FHIR-Proxy.</u></p>
<u>owner-accesstoken</u>	<u>Auth-Service des VZD-FHIR-Directory</u>	<p><u>Das owner-accesstoken wird einem berechtigten Akteur durch den Auth-Service des VZD-FHIR-Directory bereitgestellt.</u></p> <p><u>Dieses wird von einem Akteur in der Rolle "User-HBA" zur Verwaltung seiner FHIR-Ressource im Personenverzeichnis sowie von einem Akteur in der Rolle "Org-Admin" zum Hinzufügen der</u></p>

		<p><u>Organisations-Ressourcen im VZD-FHIR-Directory benötigt. Es dient zum Nachweis das die beabsichtigten Änderungen durch einen Akteur durchgeführt werden dürfen. Für die Authentifizierung MUSS der jeweilige Akteur den zentralen IDP-Dienst benutzen. Das durch den IDP ausgestellte ID_TOKEN wird durch den Auth-Service des VZD-FHIR-Directory geprüft. Bei erfolgreicher Prüfung wird das owner-accesstoken vom Auth-Service ausgestellt.</u></p>
--	--	---

5 Systemzerlegung

Wie bereits im Kapitel 2- Systemüberblick dargestellt:

ID_TOKEN gestellt sind bei der Umsetzung der Funktionalitäten des TI-Messenger-Dienstes mehrere Komponenten und ACCESS_TOKEN ausgestellt vom Smartcard-IDP-Dienst beteiligt, die durch verschiedene Anbieter bereitgestellt werden. Im Folgenden werden die jeweiligen beteiligten Komponenten des TI-Messenger-Dienstes weiter beschrieben.

Die folgende Abbildung zeigt alle an der TI-Messenger-Architektur beteiligten Komponenten mit deren Schnittstellen.

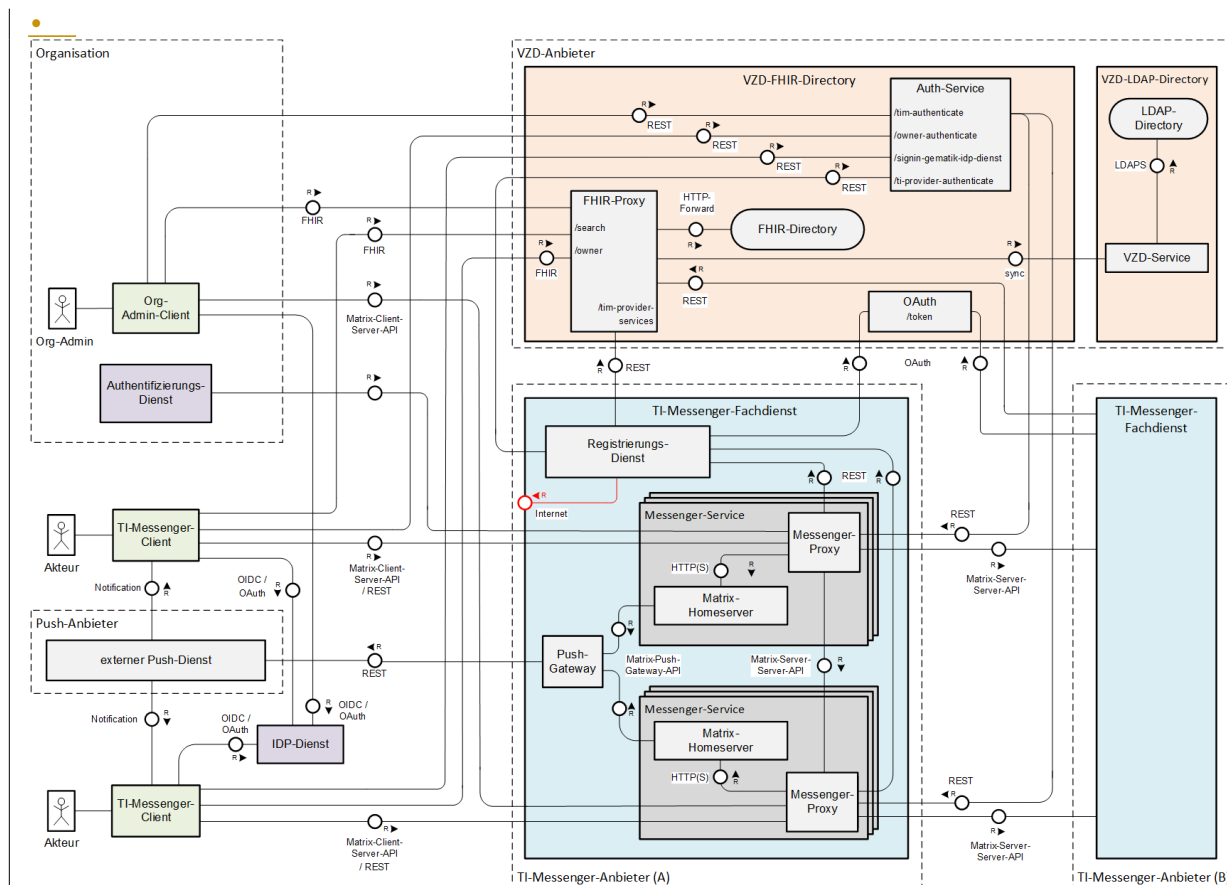


Abbildung 3: KoMatrix-ACCESS_TOKEN aus Komponenten der TI-Messenger-Architektur und deren Schnittstellen

Die in der Abbildung rot dargestellt von den Matrix-Homeservern

Maße Schnittstelle am Registrierungs-Dienst wird nicht durch die gematik normativ vorgegeben. Sie bietet einem Akteur in der Rolle "Org-Admin" die Möglichkeit, Messenger-Services für seine Organisation zu administrieren. Bei dieser Schnittstelle bleibt es dem TI-Messenger-Fachdienst Hersteller überlassen diese in geeigneter Form umzusetzen. Die gematik gibt lediglich grundlegende bereitzustellende Funktionen vor.

- Hinweis: Weitere Informationen über das Zusammenspiel der Komponenten sind im Kapitel 6- Anwendungsfälle zu finden.

5.1 ID-P-Dienst

Ein IDP-Dienst stellt **JSON Web TOKEN (Smartcard-IDP-DJWT)** für attestierte Identitäten aus. Er übernimmt die Aufgabe der Identifikation der Akteure für den Fachdienst. Das bedeutet, Fachdienst}

Das vom Smartcard-IDe MÜSSEN keine Überprüfung der Akteure selbst implementieren, sondern KÖNNEN davon ausgehen, dass der Besitzer des bei ihnen vorgetragenen "ID_TOKEN" bereits identifiziert und authentifiziert wurde. Anwendungsfrontends können über die Authentifizierung des Akteurs am IDP-Dienst aZugriff (gegen Vorlage des ausgestellten ID_TOKEN, wird) zu den vom Registrierung den Fachdiensten angebotenen Daten erhalten.

In der ersten Ausbaustufe des TI-Messengers-Dienst verwendet, um eine Organisation zu verifizieren.

ACCESS_TOKEN (es MUSS der von der gematik spezifizierte, zentrale IDP-Dienst verwendet werden. Weitere mögliche Formulierungen sind "zuständiger IDP", "zuständiger IDP-Dienst" oder "ein IDP-Dienst". Dieser ermöglicht die sichere Identifikation der Akteure anhand der ihnen bereitgestellten Identifikationsmittel (SMC-B / HBA). Die Identifikation des Akteurs wird anhand einer **Smartcard** und der Auswertung des vom Authenticator-Modul an den **IDP-Dienst** }

TI-Messenger-Clients verwenden das vom Smartcard- übergebenen Authentifizierungszertifikats (aus der Smartcard) sichergestellt. Der Authenticator wird auf dezentraler Hardware in Windows-Systemumgebungen zusammen mit dem Primärsystem betrieben. Das Authenticator-Modul für den zentralen IDP-Dienst aus wird von der gematik bereitgestellte ACCESS_TOK [gematik Authenticator]. Hersteller KÖNNEN ,um-schreibenden Zugriff auf das VZD-FHIR-eigene Authenticator Lösungen entwickeln.

Werden zukünftig weitere zugelassene IDP-Dienste verfügbar, KÖNNEN diese ebenfalls für die Authentifizierung von Akteuren genutzt werden. Im Folgenden wird der Begriff IDP-Directory zu erhaltenen verwendet, der in der ersten Ausbaustufe den zentralen IDP-Dienst meint.

5.2 Matrix-ACCESS_TOKEN (Matrix-HomeserVZD-FHIR-Directory

Beim VZD-FHIR-Directory handelt es sich um einen zentralen ver}

Nachzeichnisdienst der erfolgreich TI, der die deutschlandweite Suchen-initial von Organisationen Anmeldung einund Akteuren des TI-Messenger-Dienstes Nutzers am Matrix-Homeserermöglicht. Das VZD-FHIR-Directory basiert auf dem FHIR-Standard zum Austausch von definierten Informationsobjekten (FHIR-Ressourcen).

Der ver wird ein Matrix-ACCESS_TOKzeichnisdienst bietet zwei Arten von Verzeichnistypen an, die durchsucht werden können. Für die Suche von Organisationseinträgen vom Matrix-Hom wird das Organisationsverzeichnis (Healthcareserver-ausgestellte) und für die Suche von Akteuren das Personenverzeichnis (PractitionerRole) verwendet. Mit diesem TokIm Organisationsverzeichnis sind alle auf

eine Organisation bezogenen MUSS si Ressourcen hinterlegt die durch ein Nutzer, mit einem existierenden Matrix-Accounten Akteur in der Rolle "Org-Admin" der Organisation gepflegt werden. Das Personenverzeichnis bietet Akteuren in der Rolle "User-HBA" die Möglichkeit, anle zu seinem Matrix-Homeserver erneut authentisr *PractitionerRole* gehörenden FHIR-Einträge zu konfigurieren. Für Dieses Tok Suche nach FHIR-Einträgen wird im-lokalerden Speicher-desdurch die TI-Messenger-Clients sicher abgespeichert und FHIR-Schnittstellen am VZD-FHIR-Directory aufgerufen. Bei der Verwendung der Schnittstellen MUSS bei-jesich der weiteren Interaktion mit TI-Messenger-Client gegenüber dem VZD-FHIR-Directory authentifizieren. Für die Authentifizierung werden die im Kapitel 3.6- Verwendung der Token beseinem Matrix-Homeserchriebenen accesstoken (search-accesstoken und owner-accesstoken) ver-verwwendet. In der folgende~~en~~ Tabelle werden und ist an die Sessiondie beiden Verzeichnistypen in Abhängigkeit desr jeweiligen Clid~~ents~~-ität und den sich daraus ergebunden, enden Berechtigungen gezeigt.

MatTabelle 6: Verix-OzeichnistypenID-Tok - Rechtekonzept

Verzeichnistyp	FHIR-Ressource	Identität	Rolle	Berechtigungen
Organisationsverzeichnis	HealthcareService	SMC-B	Org-Admin	Lese- und Schreibzugriff
		=	User	Lesezugriff
		=	User-HBA	Lesezugriff
Personenverzeichnis	PractitionerRole	HBA	User-HBA	Lese- und Schreibzugriff
		=	User	Lesezugriff

Zusätzlich zur Bereitsten (Matrix-Homeserver)

Bei Bedarf MUSS siellung der Verzeichnistypen ermöglicht das VZD-FHIR-Directory ebenfalls die sektorenübergreifende Kommunikation. Hierfür wird die Matrix-Domain eines Messenger-Services durch ein Nutzer een Eintrag in Matrix-OpenID-Token gemäß [Nutzer Token] von seinemdas VZD-FHIR-Dircetory durch den Registrierungs-Dienst in die TI-Föderation aufgenommen. Für die Registrierung der Matrix-HomeserverDomain wird durch den Registrierungs-Dienst eine REST-Schnittstelle am VZD-FHIR-Directory aussfgerufen, die mittellen lassens OAuth2 Client Credentials Flow gesichert ist. Dieses-Token-MUSS für ermöglicht es TI-Messenger-Anbietern ihre betriebenen Messenger-Services in die AutorisierungTI-Messenger-Föderation aufzunehmen und zu verwalten.

Allgemein bei einem-Tsteht das VZD-FHIR-Directory aus mehreren Teilkomponenten (Fhird-Party-Proxy, Auth-Service, OAuth-Service und FHIR-Dienst-verwendereactory) die benötigt werden, um Als Beispiel wird auf die Anmeldung-am-le Funktionsmerkmale abbilden zu können. Im Folgenden werden die Teilkomponenten weiter beschrieben. Weiterführende Informationen zum VZD-FHIR-Directory sind in [api-vzd] zu finden.

5.2.1 FHIR-Proxy

Der FHIR-Proxy ist eine Teilkomponente des VZD-FHIR-Directory verwiesen. Mit dem Matrix-OpenID-Token, ausge. Alle Anfragen an das FHIR-Directory werden über den FHIR-Proxy verarbeitet. Der FHIR-Proxy stellt die folgenden drei Schnittstellen zur Verfügung, die durch seinen Mädie TI-Messenger-Clients sowie durch den Registrix-Homeserver, authentisiert sich ein Nutzer am FHIR-erungs-Dienst aufgerufen werden:

- /search (FHIR-Schnittstelle zur Suche)
- /owner (FHIR-Schnittstelle zur Pflege eigener Einträge)
- /tim-provider-services (REST-Schnittstelle zur Pflege eigener TIM Proxy und erhält lesenvider Einträge)

Bei Aufruf der Schnittstellen MUSS ein entsprechendes access-token mit übergeben werden Zugriff auf. Bei erfolgreicher Authentifizierung leitet der FHIR-Proxy die Anfragen an das VZD-FHIR-Directory weiter.

6 Systemzerlegung

6.1.1 Bei der Umsetzung der Funktionalitäten dAuth-Service

Die Teilkomponente Auth-Service stellt den TI-Messenger-Clients sowie dem Registrierungs-Dienst eines TI-Messenger- FachDienstes des deute für den Aufruf der FHIR-schnittstellen Gesundheitswesens sind mehrere Komponenten beteiligt, die durch am FHIR-Proxy benötigten access-token aus. Hierbei werden die folgenden REST-Schnittstellen:

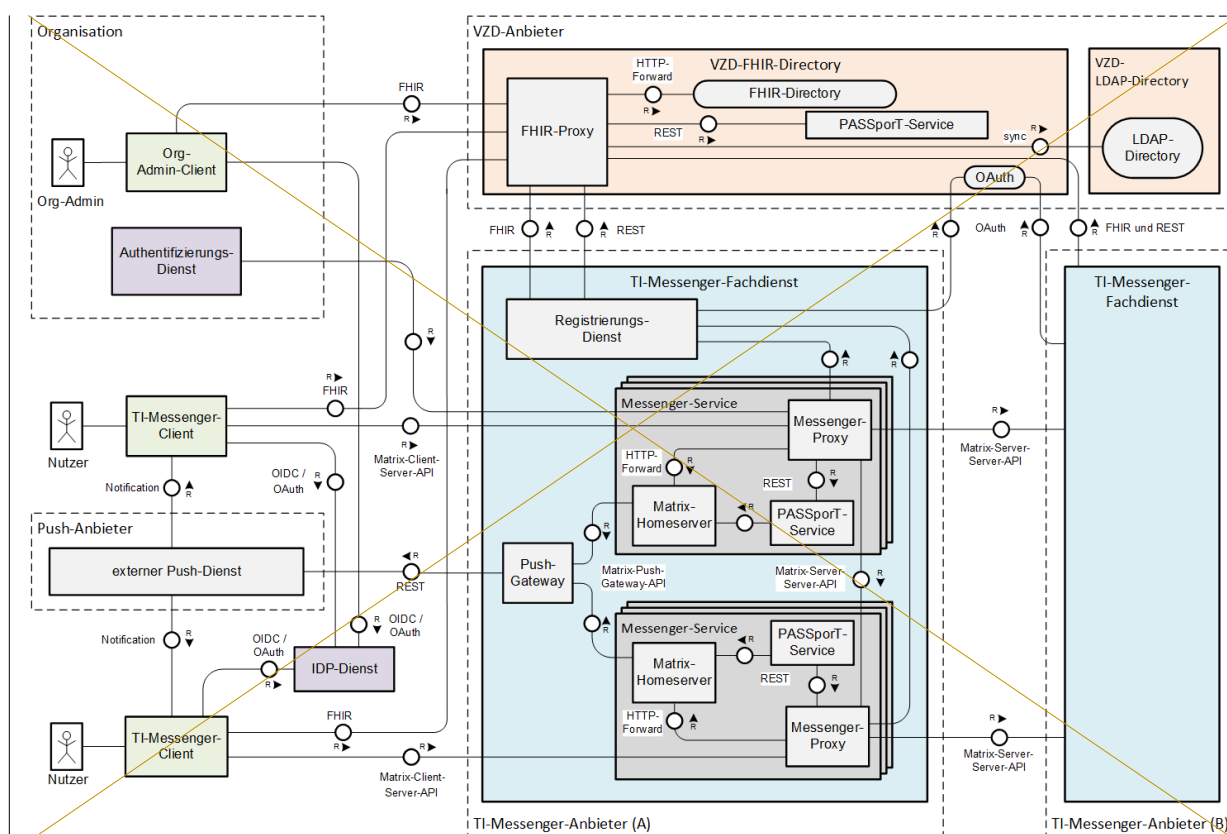
- /tim-authenticate,
- /owner-authenticate,
- /signin-gematik-idp-dienst und
- /ti-provider-authenticate

verwendet. Die schiedene Anbieter bereitgestnittstelle /tim-authenticate erwartet ein Matrix-OpenID-Token, wohingegen bei der Schnittstell werden können. Im Folgende /owner-authenticate das von einem Registrierungs-Dienst ausgestellte RegService-OpenID-Token übergeben werden die jeweiligen beteiligten Komponenten muss. Alternativ KANN eine Authentisierung mittels Smartcard am zentralen IDP-Dienst der gematik durchgeführt werden und der erhalten des TI-Messengere AuthorizationCode an die Schnittstelle /signin-gematik-idp-Dienstes beschri übergeben-

werden. Die folgende Abbildung zeigt alle an Schnittstelle /ti-provider-authenticate erwartet ein ti-provider-TI-M-accessenger Architektur beteiligten token, welches zuvor vom OAuth-Service des VZD-FHIR-Directorys ausgestellt wurde.

6.1.2 OAuth

Die TeilKomponenten mit der OAuth stellt dem Registrierungs-Dienst über den /token-Endpunkt ein für den Schnittstellen:



OAuth2 Client Credentials Flow temporäres ti-provider-accesstoken Abbildung. Bevor der Registrierung 4:s-Dienst den Komponenten/token-Endpoint am OAuth-Service aufrufen kann MUSS sich der TI-Messenger-Architektur und dem Anbieter zuvor beim VZD-Anbieter Client-Credentials beantragen, die bei Aufruf des Endpunktes mit übergeben werden MÜSSEN.

6.1.3 FHIR-Directory

Die Teilkomponente FHIR-Directory stellt das zentrale Verzeichnis der FHIR-Ressourcen bereit.

6.2 TI-Messenger-Fachdienst

Der TI-Messenger-Fachdienst ist die zentrale Komponente des TI-Messenger-Dienstes zur Ad-hoc-Kommunikation zwischen mehreren Akteuren. Für die Kommunikation mit den TI-Messenger-Clients stellt der Fachdienst alle notwendigen Schnittstellen bereit. Für eine fachdienstübergreifende Kommunikation werden alle Nachrichten an weitere Fachdienste übermittelt, die in der TI-Föderation aufgelisteten TI-Messenger-Fachdienst ist durch unterschiedliche Authentifizierungsverfahren abgesichert und ist abhängig vom Messenger-Service, der verwendet wurde übermittelt. Es MUSS sichergestellt werden, dass die Organisation die NutzerAkteure jederzeit identifizieren kann und dass die Organisationen NutzerAkteure jederzeit aus dem TI-Messenger-Dienst ausschließen können. Daher MUSS die Kontrolle über die Identitäten bei der Organisation liegen. Hierbei ist eine Delegation, z. B. an einen Dienstleister zulässig. Jeder Anbieter, der

einen TI-Messenger-Fachdienst bereitstellt, MUSS einen Registrierungs-Dienst, ein Push-Gateway sowie einen oder mehrere Messenger-Services betreiben. Im Folgenden werden die einzelnen Komponenten weiter beschrieben.

Hinweis: Die Komponenten sind als logische Dienste zu verstehen, welche letztendlich die in der Spezifikation beschriebenen Funktionalitäten umsetzen MÜSSEN. Die tatsächliche Realisierung bzw. Trennung dieser Dienste darf variabel durch die Produkthersteller erfolgen, solange alle Anforderungen an die Funktionalität, Sicherheit und Interoperabilität stets erfüllt sind und eingehalten werden.

6.2.1 Registrierungs-Dienst

Der Registrierungs-Dienst ist eine Komponente, die vom Anbieter/Hersteller des TI-Messenger-Fachdienstes bereitgestellt werden MUSS. Durch diesen KÖNN MÜSSEN im VZD-FHIR-Directory die Matrix-Domains der TI-Messenger-Fachdienste, die an der Föderation des TI-Messengers teilnehmen, eingetragen werden. Die Eintragung der Matrix-Domain SOLLTE automatisch erfolgen. Ebenfalls KANN über den Registrierungs-Dienst das Accounting durchgeführt werden. Dies wird von der gematik nicht normativ festgelegt.

Um einen interoperablen/benutzerfreundlichen Onboarding-Prozess zu gewährleisten, MUSS der Registrierungs-Dienst die Bereitstellung eines Messenger-Service über ein Frontend ermöglichen. So MUSS der (im Folgenden auch als Frontend des Registrierungs-Dienstes bei einer neuen bezeichnet). Hierfür MUSS sich die Organisation gegenüber dem Registrierungsanfrage den durch den Smartcard-ID-Dienst authentifizieren. Die Authentifizierung KANN hierbei entweder über OpenID Connect oder über eine bestehende KIM-Adresse der Organisation erfolgen. Bei der Authentifizierung via OpenID Connect wird ein durch den zentralen IDP-Dienst ausgestelltes ID_TOKEN ACCm Registrierungs-Dienst validiert. Bei der Authentifizierung mittels bestehender KIM-Adresse der Organisation wird durch den ID-TOKEN valid Registrierungs-Dienst eine KIM-Nachricht an die Organisation gesendet und durch Bestätigung einer in der KIM-Nachricht enthaltenen URL, die Organisation verifiziert. Nach der erfolgreichen Authentifizierung und einem dezentralen Meing einer Organisation wird für einen Akteur in der Rolle "Org-Admin" ein Administrations-Account im Registrierungs-Dienst angelegt. Das ermöglicht es einem Akteur in der Rolle "Org-Admin" einen oder mehrere Messenger-Service-startes für seine Organisation zu registrieren. Dazu MUSS das Frontend des Registrierungs-Dienstes am Smartcardbeim zentralen IDP-Dienst registriert sein. Vor dem Anlegen eines neuen Messenger-Service MUSS der Registrierungs-Dienst prüfen, ob der beantragte Domain-Name verfügbar ist und diesen in die TI- zur TI-Messenger Föderation eintrahinzufügen.

Neben der Registrierung neuer Messenger-Services, dient der Registrierungs-Dienst ebenfalls als Middleware zwischen TI-Messenger-ClientServices und dem VZD-FHIR-Directory und speichert eine aktuelle Liste aller verifizierten Domains (Föderationsliste), damit diese von dem Messenger-Proxy-aies des TI-Messenger-Fachdienstes abgerufen werden können. Für die Prüfung der (siehe Kapitel 3.5- Berechtigungskonzept Signatur der durch den PASSporT-Service im VZD-FHIR-Directory ausgestellten PASSporT wird das öffentliche Zertifikat des PASSporT-Servic- Stufe 1). Eine weitere Funktion des Registrierungs-Dienstes ist die Überprüfung auf Einträge im Registrierungs-VZD-FHIR-Directory. Diese Dienst abgelegt. Diet ebenfalls dem Messenger-Proxies aller Messey zur Prüfung von Berechtigung-Serviceen bei des TI-Messenger-Fachdienst-Anbieters MÜSSEN die Kontaktaufnahme von anderen Akteuren (siehe Kapitel 3.5- Berechtigungskonzept - ses Zertifikat amtufo 3). Zusätzlich stellt der Registrierungs-

Dienst ID_TOKEN (RegService-OpenID-Token) aus, die für die PrüfBerechtigung zur Änderung vom PASSporT-Servicen Organisations-Einträgen im VZD-FHIR-Directory ausgestellten PASSporT-nutz verwendet werden.

6.2.2 Push-Gateway

Jeder Anbieter eines TI-Messenger-Fachdienstes MUSS ein Push-Gateway bereitstellen, um seinen registrierten NutzerAkteuren den Eingang neuer Nachrichten zu signalisieren. Das Push-Gateway ist gemäß der Matrix-Foundation-Spezifikation [Matrix-PushGW Gateway API] zu implementieren. Dieses leitet die Benachrichtigung an Push-Dienste im Internet weiter.

6.2.3 Messenger-Service

Ein Messenger-Service besteht aus einem Messenger-Proxy, einem PASSporT-Service und einem Matrix-Homeserver der gemäß der Spezifikation der Matrix Foundation implementiert ist. Messenger-Services unterscheiden sich lediglich durch die jeweils unterstützten Authentifizierungsverfahren. Es ist notwendig, dass sich die Messenger-Services mit steigender Last skalieren lassen. Ein Messenger-Service wird immer einer e Organisation des Gesundheitswesens wird logisch einem Messenger-Service zugeordnet. Näheres zur Absicherung der Komponenten der Messenger-Services findet sich in der Spezifikation des TI-Messenger-Fachdienstes [gemSpec_TI-Messenger-FD]. Im Folgenden werden die Komponenten beschrieben.

6.2.3.1 Messenger-Proxy

Der Messenger-Proxy schließt nicht zur TI-Messenger-Föderation als Prüfinstanz aller eingehenden sowie ausgehende Matrix-Hon Anfragen zum meserver aus senger-Service ist Für die PrüfRegelung der Berechtigung hat der Messenggemäß Matrix Client-Server-Proxy Zugriff auf den Registrierungs-Dienst des API und Matrix-Server-Server-API geltenden Aufrufe zugehörigen TI-Messenger-Anbieters. Durch eine Anfrage bei jedem Transaction-Event an ständig. Die hierbei jeweils umzusetzenden Prüfrege unterscheiden sich und werden im Folgenden Registnäher beschrieben. Dienst erfolgende Abbildung zeigt die durchzuführenden Prüfung auf Zugehören in Abhängigkeit zur TI-Messengder Föderation. Diebeabsichtigten Komponemunikation.

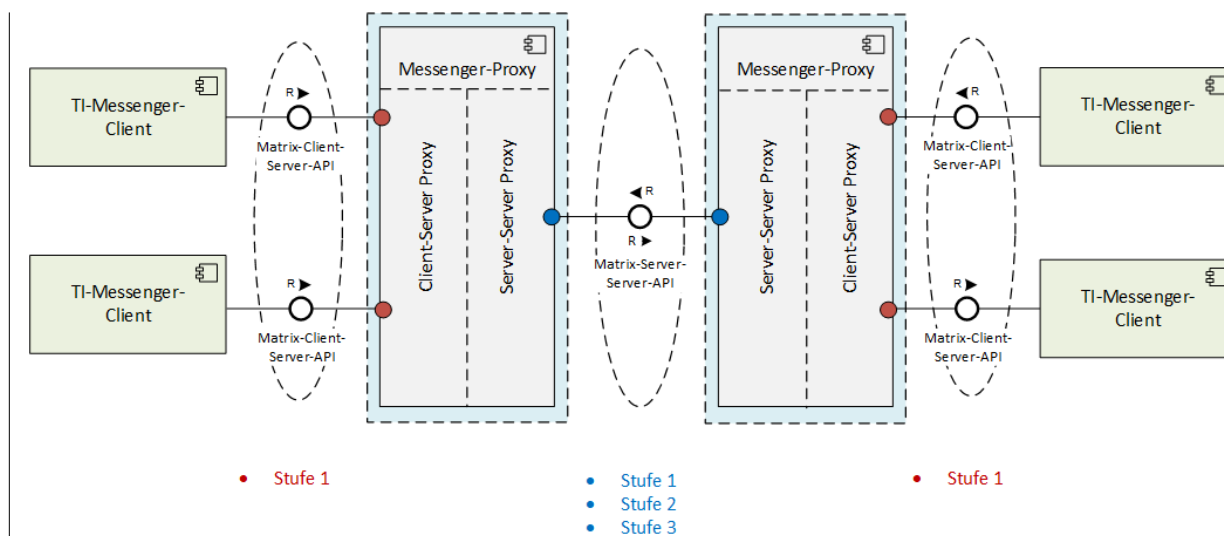


Abbildung 5: Darstellung der Messenger-Proxy-MUS für jede Darstellung der Berechtigungsprüfung am Messenger-Service separat bereitgestellt werden.

NebenProxy

6.2.3.1.1 Client-Server Proxy

In der stetigen Überprüfung bei Transactions-Requests,ktion als Client-Server proxy prüft der Messenger-Proxy zudem, ob ein Nutzer berechtigt ist eine Kommunikation mit anderen Nutzern aufzubauen (Invite-Request). Dazu benötigen Leistungserbringer und Mitarbeiter von Organisationen PASSport, die vom VZD-FHIR-Directory, oder dem Messenger-Service eingehende Invite- und createRoom-Events der TI-Messenger-Clients (in der Abbildung rot dargestellt) und fungiert so als Reverse-Proxy (siehe die im Kapitel 2- Systemüberblick ausdargestellt werden. Diese PASSport zeigen die e Abbildung als ÜBerechtigung zum Kommunikatblick bzw. Kapitel 4- Systemzerlegung für eionsaufbau an.

ne Detailansicht). Bei einer Nutzungjedem Invite-Event MUSS desr Messenger-Services für eine OrganisationProxy prüfen, ob dient in der Messenger-Proxy zusätzlich als Interface für den Anschluss des AuthentifizierAnfrage enthaltenen Matrix-Domains zur TI-Föderation gehören (siehe Kapitel 3.5.1- Client-Server Kommunikation - Stungs-Dienstesfe 1 sowie Kapitel 8.3- Stufen der Berechtigungsprüfung). der Organisation mit dem ZielNach erfolgreicher Prüfung wird das Event an den Matrix-Homeserver.

Der Messenger-Proxy MUSS des eine Funktionalität bereitstellen, die das Ändern des Displaynamens durch den Nutzer ladenden weitergeleitet. Der Matrix-Homeserververhindert. Änderungen des Displaynamens SOLL nur durch ein prüft daraufhin, ob die beteiligten Akteure auf demselben Akteur in der Rolle Org-Admin möglich sein.

6.2.3.2 PASSport-Service dMatrix-Homeserver registriert sind. Ist dies Messenger-Service

nicht Der PASSport-Service des TI-Fall, wird das Invite-Event an den zuständigen Messenger-Fachdienstes wird verwProxy des Einzuladendet, wenn Akteure, die nen gericht im VZD-FHIR-Directory gefunden werden, eineet, wobei die Regeln der Server-Server Kommunikation aufbauen möchten. In diesem durchzuführen sind.

Ebenfalls kann kein PASSporT durch den VZD-FHIR-Directory PASSporT-Service ausgestellt werden. MUSS der Messenger-Proxy jedes createRoom-Event prüfen. Dies hierbei MUSS dann durch den PASSporT-Service des TI-Messenger-Fachdienstes gemäß [gemSpec_TI-Messenger-FD#5.2.3] bereitgestellt werden.

6.2.3.3 Matrix-Homeserver

Für den Proxy prüfen, ob das im Event enthaltene Attribut "invite" mit maximal einem Element Betrieb des TI-Messenger-Dienstes erfüllt ist. Ist dies nicht der Fall, dann MUSS der TI-Messenger-Anbieter mProxy die Verbindungs-ung mit einem Matrix-Homeserver Fehlnachricht ablehnen.

6.2.3.3.1 server-gemäß der Server Matrix-Foundation Spezifikation Proxy

In der Funktion in der sektorübergreifenden Föderation betreiben. Es muss als Server-Server Proxy prüft der Messenger-Proxy alle Matrix-Homeserver die in der Föderation veranwendet werden den Anforderungen Events. Damit fungiert der Matrix-Foundation Spezifikation Server-Server Proxy sowohl als Forward als auch als Reverse-Proxy. Im Gegensatz zum Clientsprechen. Üblicherweise prüft der Matrix-Homeserver-server finde Proxy bei jedem Event die Ad-hoc-Kommunikation der Nutzer sowie Domainzugehörigkeit. Somit kann ausgeschlossen weitere Nutzerinteraktionen (Starten neuer Räume etc.) statt. Der TI-Messenger, dass mit einem nicht mehr zur Föderation gehörenden Messenger-Anbieter MUSS sicherstellen, dass folgende Matrix-Spec-Changes (MSCs) [MatrixSpec-Service kommuniziert werden kann. In der Funktion als Server-Server Proposal] zum Thema Proxy MÜSSEN alle Stufen gemäß Kapitel 3.5.2- Server-Server Kommunikation des Benachrichtigungskonzeptes von dem Matrix-Homeserver unterstützt werden. Messenger-Proxy geprüft wird:

- Encrypted Push — <https://github.com/matrix-org/matrix-doc/pull/3013>
- erden (in Delayed Push — <https://github.com/matrix-org/matrix-doc/pull/3359>
- Opfer Abbildung blau dargestellt). ist die Direct Push — <https://github.com/matrix-org/matrix-doc/pull/3361>

6.3 keine der drei STI-Messenger-Client

Beim TI-Messenger-Client handelt es sich um eine Anwendung erfolgreich geprüft worden, dann MUSS der Messenger-Proxy die Verbindung auf einem mobilen Gerät ablehnen. Darüber hinaus MUSS Desktop. Der TI-Messenger-Client ermöglicht die Server-Server Proxy auch weitere legitime Ad-hoc-Kommunikation im TI-Messenger-Dienst. Die Akteure KÖNNEN über entsprechende Such über das Berechtigungskonzept hinausgehen. Beispielweise anfragen vom VZD-FHIR-Directory durch den einen TI-Matrix-Homeserver-Client gesucht werden. Der TI-Messenger-Client basiert auf der von der Server, damit dieser ein zu prüfendes Matrix-Foundation definiertes OpenID-Token verifizieren kann.

Weiterführende Vorgaben

Der TI-Messenger-AnbieterProxy MUSS mindeeeine Freigabelisten einen mobi bereitstellen und einen desktopfähigen TI-Messenger-Client anbieten. Welche Art des Clients angeboten. Diese dient zur Prüfung von Berechtigungen bei der Kontaktaufnahme von anderen Akteuren wird, ist dem (siehe Kapitel 3.5 - Berechtigungskonzept Anbieter überlassen.

- Stufe 2). Ebenfalls MUSS Der TI-Messenger-Client MUSS am Smartcard-IDP-Dienst registriert seiProxy eine Schnittstelle bereitstellen, damit mittels SMC-B oder HBA Änderungen am VZD-FHIR-Directory durch einer TI-Messenger-Clients Berechtigungen Akteur in der Rolle Org-Admin vorgenommen werdenFreigabeliste hinterlegen können.

6.4 VZD-FHIR-Directory

Beim VZD-FHIR-Directory hande

Der Messenger-Proxy MUSS nach dem Erhalt es sich um eininer neuen zentralen VerzeichnisFöderationsliste vom Registrierungs-dienst, dest die Signatur die deutschlandweite Nutzersuche des TI-Messenger-Diensteser erhaltenen Datei prüfen und diese nur nach ermöglicht. Das VZD-FHIR-Directory basiert auf dem FHIR-Standard zum Austausch von definierten Informationsobjekten. Das VZD-FHIR-Directory bietet eine FHIR-Schnittstelle zur Suche nach Leistung Prüfung verwenden.

Die Komponente Messenger-Proxy MUSS für jeden Messenger-Service separat bereitgestellt werden. Es ist nicht zwingend notwendig, diese auf die Matrix-Server-Server-API und Matrix-Client-serbringern (Practitioner) und Organisation-API bezogenen Prüfungen durch getrennte Komponenten an. Somit wird eine einfache Suche nach Akteuren, die an ten zu realisieren. Die Art der Umsetzung bleibt dem TI-Messenger teilnehmen, gewährleistet. D-Fachdienst-Hersteller überlassen.

Bei einer Zugriff auf das VZD-FHIR-Directory ist mittels OAuth2-ClNutzung des Messenger-Services für eine Organisation dient Credentials-Flow-gesder Messenger-Proxy zusätzlichert. Ebenfal als ermöglicht das VZD-FHIR-Directory die sektorenübergreifende KommunikSchnittstelle für den Anschluss des Authentifizierungs-Dienstes der Organisation. Hierzu wird die Domain der an den Ziel Matrix-Homeserver.

6.4.1.1 Matrix-Homeserver durch einen Eintrag im VZD-FHIR-Directory registriert. Für

Für den Betrieb des TI-Messenger-die Nutzungstes MUSS desr TI-Messenger-DienAnbieter mindestens bietet das zentrale VZD-FHIR-Direens einen Matrix-Homeserver gemäß der Matrix-Foundation Spezifikation in der sektory einübergreifenden FHIR-Proxy sowie einen PASSporT-TI-Föderation betreiben. Es MÜSSEN alle Matrix-HomeService an, er die im Folgenden weiter beschrieben der Föderation verwendet werden.

FHIR-Proxy

den AnforDer FHIR-Proxy ist das zungen der Matrix Foundation Spezifikation entrale Interfacesprechen. Über der TI-Messenger-Fachdienste zum VZD-FHIR-Directory.n Matrix-Homeserver findet die Ad-hoc-Kommunikation Der FHIR-Proxy (Akteure sowie weitet autorisierte Anfrage Nutzerinteraktionen (z. B. Starten und Kommandos vom neuer Räume etc.) statt.

6.5 TI-Messenger-Client an das VZD-FHIR-Directory weiter. Die Komponente Registrier

Ein TI-Messenger-Client ist eine mobile oder stationäre Anwendungs-. Dienst benutztse basiert auf den FHIR-Proxy ebenfalls für dr von der Matrix-Foundation definierten Zugriff auf das VZD-FHIR-Directory. Der Spezifikation und ermöglicht die Ad-hoc-Kommunikationsablauf für den Zugriff auf das VZD-FHIR-Directory durch von Akteuren über den TI-Messenger-Client ist in [gemSpec_VZD_FHIR_Directory#6.2] best. Im Kontext des TI-Messenger-Dienstes wird zwischrieben.

PASSporT-Serviceen zwei Ausprägungen des VZD-FHIR-Directory

Im TITI-Messenger-Kontext werClients unterschieden für, die Prüfungen von-Berechtigungse ergeben sich aus den jeweiligen Rollen PASSporT-verwder Akteure, die im Folgendet. Berechtigte-Akteure erhaltenn weiter beschrieben werden.

Für die Realisierung vom PASSporT-Service des VZD-FHIR-Direeen Anwendungsfällen, die ausschließlich ein Administrator ein PASSporT. Das PASSporT wir der Organisation ausführt (siehe Kapitel 6- Anwendungsfälle, d durch die Messenger-Proxies für das Invite-Event geprüft. Dem Akteur "Org-Admin" zugeordneten Anwendungsfälle), MUSS ein TI-Messenger-Anbieter PASSporT-Service stellt automeinen TI-Messenger-Client mit Administratisiert PASSporT aus, sollteonsfunktionen anbieten (auch als Org-Admin-Client bezeichnet). die gesuchte Ressource vom VZD-FHIR-Directory erfolgreich zurückgegeben werdeese erweiterte Funktionalität KANN auch in den TI-Messenger-Client für Akteure integriert sein. Das PASSporT wird als Query-ParameterTI-Messenger-Clients für Akteure (Akteure in der MatrixRolle User URI angehängt-/ User-HBA) unterstützen Dies wird i von der [gemMatrix-Spec_VZD_FHIR_Directory]zifikation festgelegt.

OAuth

Der Registrierungs-Dienst des TI-Messenger-Fachdienst MUSS sich beien Funktionalitäten sowie die Abfragen im VZD-FHIR-Directory mit OAuth2-Client-Credentials-Flow-authentisieren. Der geforderte mindestens bereitzustellende Funktionsumfang wird in der [gemSpec_TI-Messenger-Client] beschrieben.

7 Übergreifende Festlegungen

7.1 Datenschutz und Sicherheit

Der TI-Messenger-Dienst baut auf flächendeckender Verwendung von Transportverschlüsselung mittels TLS (gemäß den Vorgaben aus [gemSpec_Krypt]), zusätzlicher moderner Ende-zu-Ende-Verschlüsselung von Chatinhalten mittels OLM/MEGOLM und einer dezentralen Gesprächsarchitektur mittels föderierten Matrix-Homeservern auf.

Die Vorgaben für die Absicherung des TI-Messengers bestehen aus komponentenbezogenen Akzeptanzkriterienforderungen, die in den jeweiligen Dokumenten in eigenen Kapiteln untergebracht sind, funktionsbezogenen Akzeptanzkriterienforderungen, die im Rahmen der jeweiligen Funktionsbeschreibungen zu finden sind, und ergänzenden übergreifenden Anforderungen, die aus anderen Spezifikationen stammen und den Steckbriefen zugeordnet werden.

7.2 Verwendete Standards

Matrix

Für den TI-Messenger-Dienst wird das offene Kommunikationsprotokoll der Matrix-Foundation gemäß [Matrix-Foundation] verwendet. Im Rahmen der Spezifikation wird daher das Server-Server- (gemäß [Server-Server-API]) und das Client-Server-Protokoll (gemäß [Matrix-Foundation]Client-Server API]) nachgenutzt. Für die Kommunikation der Matrix-Homeserver in der Föderation wird somit die API gemäß Matrix-[Server-Server-Protokoll-API] verwendet. Der TI-Messenger-Client setzt bei der Kommunikation mit den TI-Messenger-Matrix-Homeservern die API des Matrix-Client-Server-Protokolls um. Bei der Benachrichtigung der Akteure über eingehende Nachrichten wird ein Push-Gateway verwendet, welches gemäß [Push Gateway API] nachgenutzt wird. Bei der Kommunikation werden REST-Webservices über HTTPS (JSON-Objekte) aufgerufen.

OpenID-Connect

Das VZD-FHIR-Directory nutzt als Authentifizierungsserver. Das Matrix-Protokoll erlaubt während der Erstellung eines Chatraumes einen eigenen Raumtyp (*Custom Room Type*) für diesen mit Hilfe einer Typeninitialisierung im `/createRoom` Endpunkt zu definieren, um spezielle Raumeigenschaften (*Room State*) für den Smartcard-IDP-Dienst der TI. Hierfür stellt der IDP diesen *Custom Room Type* zu verwenden. Außerdem erlaubt das Matrix-Protokoll die Eigenschaften eines Chatraumes mit *State Events* zu erweitern bzw. zu ändern. Typische *State Events*, die ein *Room State* definieren und Dienst ein ID- und ACCESS- durch das Matrix-Protokoll definiert sind, sind zum Beispiel `m.room.name` oder `m.room.topic`. Das Matrix-Protokoll erlaubt auch ein Token für Nutzer in Form eines JSON-Web-Token (JWT) gemäß [OpenID] aus-

FHIR

Der TI-Messenger-Client nutzt definierte *State Events (Custom State Events)* zu verwenden. In der vorliegenden Spezifikation werden bereits erste *Custom Room Types* sowie *Custom State Events* mit von der gematik definierten *Event Types* und *Event Content* die Schnittstellen des VZD-FHIR-Directories gemäß dem FHIR definiert. Dies ermöglicht im Kontext des TI-Messengers, eine spezifischere und damit strukturiertere und gerichteter Kommunikation durchzuführen, als es mit Standard [FHIR] mit einer RESTful API.

PASSport

Matrix-Chaträumen möglich wäre. Konkret werden Definitionen Für die Prüfen Fallbezug (Referenzierung von RechtBehandlungsfällen der beteiligten Nutzer innerhalb im medizinischen Versorgungskontext) von Chats sowie für die interne und intersektorale Kommunikation einer beabsichtigten Kogeführt. Für die fallbezogene sowie die föderierte und intersektoraler Kommunikation verwendet der TI-Messenger-Dienst PASSport gemäß [RFC 8225]. Die Verist es vorgesehen im *Event Content* eines *Custom State Events* definierte FHIR-Objekte als Payload zu hinterlegen.

Hinweis: In der vorliegenden Spezifikation wird die produktive Verwendung der Custom Room Types und Custom State Events aktuell nicht gefordert, da die notwendigen Vorbedingung des PASSPorts im Kontexten für den produktiven Einsatz seitens des Matrix-Protokolls noch nicht vollständig erfüllt sind.

7.2.1 OpenID-Connect

Das VZD-FHIR-Directory, des-r Registrierungs-Dienst sowie die TI-Messenger-DClients wird im Kapitel "Nutzts nutzen im Rahmen der Authentifizierung von Personal AID_TOKEN in Form eines JSON-Web-Token (JWT) gemäß [OpenID].

7.2.2 FHIR

Die TI-Messertion-Token" weiter beschriebennger-Clients nutzen die FHIR-Schnittstellen der Teilkomponente FHIR-Proxy des VZD-FHIR-Directories gemäß dem FHIR-Standard [FHIR] mit einer RESTful API.

7.3 Authentifizierung und Autorisierung

7.3.1 Authentifizierung von NutzernAkteuren am Messenger-Service

Für die Authentifizierung von Nutzern, also z. B. Mitarbeiter in einer Organisation, oder Leistungserbringer Akteuren werden die durch den jeweiligen Matrix-Homeserver bereitgestellten Authentifizierungsverfahren genutzt. Dies ermöglicht es z. B. Krankenhäusern ihre eigene Benutzerverwaltung (z. B. Active Directory) zu nutzen, oder Verbänden eihre eigenen Identitätsserver (IDP-Dienst) zu verwenden. Die Abstimmung,

welches Authentifizierungsverfahren verwendet wird, trifft die Organisation mit dem jeweiligen TI-Messenger-Fachdienst-Anbieter. Die Benutzerverwaltung erfolgt durch autorisierte Mitarbeiter in der jeweiligen Organisation (Akteur In der Rolle "Org-Admin"). Die Administration der verwendeten Authentifizierungsmethoden MÜSSEN unter der Kontrolle der jeweiligen Organisation sein.

Bezüglich der Einschränkung der Authentisierungsmittel, welche von einer Organisation verwendet werden dürfen, befindet sich die gematik derzeit noch in Abstimmung mit dem BSI, weswegen mit einer verbindlichen Regelung erst im geplanten Hotfix 1 zu rechnen ist. Bis dahin MUSS zusätzlich zur Prüfung der SMC-B als erstem Faktor noch ein zweiter Faktor nach [BSI-TR-03107] Kap. 4 geprüft werden, bis die übliche Kombination aus Gerätebindung und Homeserver-Access-Token erreicht sind.

7.3.2 Authentifizierung am VZD-FHIR-Directory

Die Authentifizierung für Sden Lese- und Schreibzugriff der Nutzer gegen auf das FHIR-Directory erfolgt mit Hilfe von Identitätstoken. Die jeweilige Überprüfung dem r Identitätstoken erfolgt am FHIR-Proxy des VZD-FHIR-Directory erfolgt für Le. Die Authentifizierung der Komponenten Registrierungserbri-Dienst und TI-Messenger und Organisationen des Gesundheitswes-Client wird im Folgenden weiter beschrieben.

7.3.2.1 Registrierungs-Dienst

Die Authentifizierung des Registrierungs-Diens mittels SMC-B/HBA:tes für Die BestätigungNutzung der AuthentizitätSchnittstelle I VZD TIM Provider Services am VZD-FHIR-Directory erfolgt am Smartcard-IDP-Dienst. Mitarbeitmittels OAuth am OAuth/Auth-Service des VZD-FHIR-Directory. Nach erfolgreicher einer Organisation (in-Authentifizierung mit vereinbarten Client-Creden-Rollen User, User-HBA und Org-Admin)-verwendtials wird dem Registrierungs-Dienst ein provider-accesstoken ausgestellt.

die durch die Organisation festgelegten AuthClient Credentials erhält der TI-Messenger Anbieter, indem er einen Service des TI-ITSM-Systems zur Beantragung der Credentifizierals nutzt. Die Beantragungsmethoden und der Credentials dient auch dazu, ein Vertrauensverhältnis zwischen Lesezugriff auf das dem Registrierungs-Dienst und dem VZD-FHIR-Directory für Organisations-Ressourcen.

Für dieherzustellen, da der Registrierungs-Dienst RegService-OpenID-Token Authentifizisstellt, die für die Berechtigung zur Änderung von Leistungserbringern und OrganisationOrganisations-Einträgen im FHIR-Directory verwendet werden. Das Vertrauen zwischen des Gesm VZD-FHIR-Directory undheitswes den Registrierungs-Diens, die im Besitz-einten der TI-Messenger SMC-B/HBA-sind, wirdAnbieter wird hergestellt, indem der durch die gematik-spezifizierte-IDP-DiTI-Messenger Anbieter das Signatur-Zertifikats, das für die Signatur des RegService-OpenID-Tokenst verwendet {gemSpec_IDP_Dienst}. Dazu MUSS der verwendete wird, bei der Beantragung der Client Credentials übergibt und somit bei der Token-Prüfung vom VZD-FHIR-Directory berücksichtigt werden kann. Das Signatur-Zertifikat erhält der TI-Messenger-Client beim Smartcard-IDP-Dienst registriert sein. Anbieter mittels eines TI-ITSM-Service Requests zur Beantragung von TI-Komponenten-PKI-Zertifikaten (C.FD.Sig mit Anwendungskennzeichen oid_tim). Ein RegService-OpenID-Token mit Der Leistungserbringer oderTelematikID der Organisation wird nach erfolgreichem Login eines Akteurs in der Rolle "Org-Admin KANN mittels des ACCESS" der Organisation ausgestellt.

7.3.2.2 TI-Messenger-Client

TI-Messenger-Clients MÜSSEN sich gegenüber dem Auth-Service des VZD-FHIR-Directory mit Hilfe eines ID_TOKEN die MXID als Teil eines Eintrags der Practitioner-Ressource oder des Matrix-OpenID-Token authentifizieren. Dem Matrix-OpenID-Token des Matrix-Homeservers wird vertraut, wenn der ausstellende Matrix-Homeserver als Matrix-Domain einer verifizierten Organisations-Ressource zuordnen im VZD-FHIR-Directory eingetragen wurde. Diese Zuordnung verifiziert die MXID des Leistungserbringers, der Auth-Service des VZD-FHIR-Directory stellt nach erfolgreicher Prüfung des jeweiligen Matrix-OpenID-Token ein search-access-token aus. Dem ID_TOKEN wird vertraut, wenn der ausstellende IDP die jeweilige Organisationsressource beim VZD-FHIR-Directory registriert ist und somit das Token durch den Auth-Service validiert werden kann. Nach erfolgreicher Prüfung des ID_TOKEN durch den Auth-Service des VZD-FHIR-Directory wird ein owner-access-token ausgestellt.

7.3.3 Autorisierung am Messenger-Service

TI-Messenger-Clients erhalten Zugriff auf den Messenger-Service einer, in der Föderation registrierten Organisation durch Übergabe eines Matrix-ACCESS_TOKENS. Dieses wird durch den Matrix-Homeserver ausgestellt nachdem ein Nutzer erfolgreich authentifiziert wurde. Das Matrix-ACCESS_TOKEN MUSS sicher auf dem Endgerät gespeichert werden.

7.3.4 Autorisierung am VZD-FHIR-Proxy

7.3.5 TI-Messenger-Client

7.3.5.1 Registrierungs-Dienst

Für den Schreibzugriff des Registrierungs-Dienstes autorisiert dieser sich gegenüber dem FHIR-Proxy des VZD-FHIR-Directory für den Lesezugriff mittels Matrix-OpenID mit einem provider-access-Token, welches vom Matrix-HomeAuth-Service des VZD FHIR-Directory ausgestellt wird. Für den Schreibzugriff.

7.3.5.2 TI-Messenger-Client

Für den Lesezugriff autorisieren sich TI-Messenger-Clients gegenüber dem FHIR-Proxy des VZD-FHIR-Directory mit einem search-ACCESS_TOKEN, welches durch den Auth-Service des VZD FHIR-Directory ausgestellt wird. Der Ablauf der Autorisierung am FHIR-Proxy wird in der [gemSpec-urde. Für den Schreibzugriff nutzen TI-Messenger-Clients das owner-access-token, welches vom Auth-Service des VZD-FHIR-Directory im Anwendungsfall "Nutzer su" ausgestellt wurde.

7.4 Recht ~~TI~~Organization- und ~~TI~~Practitioner-Einträge im ~~ekonzept~~ VZD-FHIR-Directory"

Im folgenden Kapitel wird beschrieben. Eine Erläuterung zu dem Rechtekonzept des VZD-FHIR-Directory findet sich in dieser Spezifikation im Kapitel "Rechtekonzept, wie der Lese- und Schreibzugriff durch die TI-Messenger-Clients und dem Registrierungs-Dienst auf dem VZD-FHIR-Directory" erfolgt.

7.5 Föderation

7.5.1 ~~Da der~~Lesezugriff

7.5.1.1 Registrierungs-Dienst

Die TI-Messenger-FachDienst auf dem offenen und dezentralen Kommunikationse erhalten die Möglichkeit, mittels ihres Registrierungs-Dienstes die Föderationsliste vom FHIR-protokoll-Matrix-basxy des VZD-FHIR-Directory abzurufen. Hierfür MUSS gewährleide Schnittstet werden, dass nur die im Kapitel "Akteure und Rollen" genannten berechtigltle /tim-provider-services am FHIR-Proxy des VZD-FHIR-Directory unter Vorlage des provider-accesstoken aufgerufen werden.

7.5.1.2 TI-Messenger-Clients

Durch den Akteure teilnehmen können.

Um allen berechtigten Akteurufruf der Schnittstelle /search am FHIR-Proxy des VZD-FHIR-Directory KANN ein TI-Messenger-Client unter Vorlage des search-accesstoken Suchanfragen des deutschen Gesundheitswesens an das FHIR-Directory stellen. Die Suchergebnisse sind abhängig von den Zugang zum TI-Meingetragenen FHIR-Ressenger zu gewähourcen und deren, MUSS ein Anbieter eines Sichtbarkeit.

7.5.2 Schreibzugriff

7.5.2.1 Registrierungs-Dienst

Die TI-Messenger-Fachdienstes für Leistungserbringerinstitutionen und/oder einer Organisation-entsprechende erhalten die Möglichkeit, mittels ihres Registrierungs-Dienstes Messenger-Services bereitstellin die TI-Föderation aufzunehmen.

Um nicht zum TI-Messenger gehörende Matrix-Server ausschließ Hierfür MUSS die Schnittstelle /tim-provider-services am FHIR-Proxy des VZD-FHIR-Directory unter Vorlage des provider-accesstoken zu können, aufgerufen werden die.

7.5.2.2 TI-Messenger-Fachdienste in einer Föderation zusammengefasst. Voraussetzung für diClients

Durch den Aufruf der Schnittstelle /owner am FHIR-Proxy des VZD-FHIR-Directory erhält ein Akteur unter Vorlage des owner-accesstoken Schreibzugriffe Aufnahme das FHIR-Directory. in die Föderation ist er folgenden Tabelle wird die zu verändernde FHIR-Ressource in Abhängigkeit zu der Betriebverwendeten Identität eines Messenger-Proxies als Teil des Messenger-Akteurs beschrieben (siehe dazu auch die Tabelle "Verzeichnistypen - Rechtekonzept").

Tabelle 7: Servicechreibzugriff - VZD-FHIR-Ressourcen

Rolle	Identität	FHIR-Ressource	Beschreibung
Org-Admin	SMC-B (stellvertretend durch einen RegService-OpenID-Token)	HealthcareService	Ein Akteur in der Rolle "Org-Admin" kann mit Hilfe eines TI-Messenger-Clients mit Administrationsfunktion 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 HealthcareService 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 I requestToken.
User-HBA	HBA	PractitionerRole	Die Nutzung eines HBAs ermöglicht es einem Akteur in der Rolle "User-HBA" mit Hilfe eines TI-Messenger-Clients seine bereits bestehende FHIR-Ressource PractitionerRole um einen Endpunkt im Personenverzeichnis zu erweitern, um für andere Leistungserbringer anschreibbar zu werden oder um andere Leistungserbringer anzuschreiben.

7.6 User Management

Aufgrund der sicherstellen MUSS, dass nur zugelassene Vielzahl an Teilnehmern wird eine komfortable Benutzerverwaltung innerhalb des TI-Messenger-Fachdienste Zugangs benötigt. in die Föderation erhalten. Voraussetzungem Kapitel werden die für die-

Aufnahme in die Föderation ist eine erfolgreiche Zulassung durch das User Management notwendigen Rollen und die gematik. Nach einer erfolgrä dafür verwendeten Nutzer-Verzeichnis Zulassung erhält der Registrierte die Beschreibung des Benutzers.

Voraussetzung für Dienst Nutzung des jeweiligen Fach TI-Messenger Dienstes die Möglichkeit die Domains des jeweiligen Messenger Services sind zunächst, dass sich ein Akteur über ein Authentifizierungsverfahren am Matrix-Homeserver entsprechend seiner Organisation auf dem VZD-FHIR-Directory zuzuordnen.

Für die Aufnahme in die Föderation kann und ein Nutzer-Account auf dem Matrix-Homeserver angelegt wurde. deration MÜSSEN ausschließlich Nutzer-Account auf dem Matrix-Homeserver verwendet werden. wird entweder vom Akteur in der Rolle "Org-Admin" oder ein Bridging einer Organisation bereitgestellt oder Messaging-Protokolle DARF NICHT stattfinden.

7.7 Rechtekonzept VZD-FHIR-Directory

Im Folgenden Kapitel wird beschrieben, vom Akteur selbst am Matrix-Homeserver registriert. Bei der Erstellung des Nutzer-Accounts wird die MXID des Akteurs erzeugt sowie der Schreib- und Lesezugriff durch die Displayname des Akteurs festgelegt (siehe gemSpec TI-Messenger-Clients des TI-Messenger Fachdienstes auf dem VZD-FHIR-Directory weitere Funktionen). Nach der Erstellung des Nutzer-Accounts am Matrix-Homeserver wird die MXID des Akteurs im User-Directory erfolgt.

7.7.1 Schreibzugriffe für TI-Messenger des Matrix-Homeservers hinterlegt. Alle im User-Fachdienste

Die TI-Directory des Matrix-Homeservers hinterlegen die Möglichkeit, mittels ihres Registrierungs-Dienstes die bereits bestehende MXIDs sind anschließend durch andere Akteure seiner Organisation auffindbar und erreichbar. Soll der Akteur auch von außerhalb der Organisation auffindbar werden, so MUSS die Services zu erweitern. Die Autorisierung mit seiner MXID in das Organisationsverzeichnis im VZD-FHIR-Directory des Registrierungs-Dienstes erfolgt mittels OAuth und ermöglicht werden. Das Hinterlegen der MXID eines Akteurs in das Organisationsverzeichnis Fachdienstes MUSS durch den Akteur in der Rolle "Org-Admin" erfolgen. Voraussetzung ist das Vorhandensein einer HealthcareService-Ressource um Endpoints der Organisation. Die MXIDs werden in der HealthcareService-Ressourcen zu erweitern. Eine zugeordnete Endpoint-Ressource stellt dabei hinterlegt. Die einen Messenger-Richtung einer HealthcareService da, welcher Ressource einer Organisation erfolgt durch die Matrix-Domain auf den Akteur in der Rolle "Org-Admin". Möchte einen Host verweist und auf Akteur ohne Zugehörigkeit zu einer Organisation referenziert wird. Der Registrierungs-Dienst MUSS durch die Überprüfung gefunden werden, so MUSS seine MXID in das Personenverzeichnis des VZD-FHIR-Directory hinterlegt werden. Voraussetzung hierfür ist der Besitz eines HBAs.

Die folgende Tabelle zeigt einen zusammenfassenden Überblick der Benutzerverwaltung.

Tabelle 8: Überblick der SMC-Benutzerverwaltung in Abhängigkeit der Rolle

Rolle	Client	Administration	Wo

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

7.8 Funktionsaccounts

Einrichtung einer zugelassenen Organisation handelt.

7.8.1 Schreibzugriff für Organisationen im Gesundheitswesen sind sehr unterschiedlich strukturiert und wollen hinsichtlich ihrer Erreichbarkeit flexibel eigene Strukturen abbilden können. Daher sind beim TI-Messenger-Client

Nutzer MÜSSEN Accounts notwendig, die es ermöglichen als Leistungserbringer, einen Akteure unterhalb der Struktur erreichbar zu machen. der Organisation mittels OpenID-Connect authentifizierender Akteur muss dann nicht die genaue interne Struktur der Organisation kennen. Diese Authentifizierung gewährt Schreibaccounts werden im folgenden Zugriff auf die jeweils Funktionsaccounts bezeichnet. Ein Funktionsaccount ist als eigene, für eine Endpoint-Ressource (mit dem Leistungserbringer, oder "payloadTyp: TI-Messenger_chat") eines HealthcareService einer Organisation angelegt. Der HealthcareService bildet im FHIR-Ressource- (Practitioner, Directory eine Struktur (z. B. Station in einem Krankenhaus) der Organisation).

Schreibzugriff für Nutzer in der Rolle Org-Admin

Um die FHIR-Ressource-chbarkeit dieser Struktur wird die MXID im URI Format eines Chatbots oder eines Akteurs (der jeweiligen stellvertretend für die Organisation bearbeiten zu können MUSS eintritt) in das "address" Attribut der Endpoint Ressource hinterlegt. Somit kann die Identität angelegte Struktur der Organisation bestätigt werden. Dies erfolgt aktuell durch eine SMC-B. Die Nutzung über den Funktionsaccount und dessen hinterlegten Namen (*Endpoint.name*) im VZD-FHIR-Directory von einer SMC-B ermöglicht es einem Akteur gefunden werden.

7.8.2 Chatbot

Chatbots sind spezielle Akteur-ine (siehe Kapitel 3.1- Akteure und Rollen), der Rolle ie stellvertretend für eine Struktur einer *Org-Admin* mit Hilfe eines TI-Messenger-Clients FHIR-Ressourcen im Nameanisation von einem die Kommunikation initiierenden Akteur eingeladen werden können. Chatbots KÖNNEN die Kommunikation vollständig automatisiert abschließen (z. B. Terminvergabe) oder in der Organisation anzuhinterlegen. Die FHIR-Ressource natürliche Personen werden als *part of* dem Chat hinzuziehen (z. B. Ausstellen eines Rezeptes). Beispiele für Chatbots sind unter [Matrix Bots] zu der entsprechenden Stamm-Organisfinden. Treten Chatbots als Kommunikationsressource referenziert.

Schreibzugriff für Nutzer in der Rolle User-HBA

teilnehmer des TI-Messengers auf, so MÜSSEN diese im jeweiligen Chat als Chatbot gekennzeichnet werden.

Im Folgenden wird ein Beispiel für Ein-Leistungserbringer KANN die eigene, bereits bee mögliche Zuordnung für die Abbildung von Funktionsaccounts mit Hilfe von Chatbots und eines Akteurs der stehlvertretende FHIR-Ressource *Practitioner* erweitern, um für die Organisation auftritt.

Der Chatbot KANN automatisiert Anfragen von Akteuren (z. B. für andere LeistTerminanfragen, Medikationsentscheidungserbringer aus-) bearbeiten oder Ferneanschreibbar bei Bedarf die zu werden, oder um andere Leistungserbringer anzuschreibgeordneten und zu diesem Zeitpunkt verfügbaren Akteure in den Chatraum einladen. Dafür MUSS sich Die dem Chatbot zur Verfügung stehenden Akteure (in der Leistungserbringer entsprechend miSpalte Akteur blau hinterlegt) sind in der Konfiguration des Chatbots zu definieren. Im abschließenden Beispiel ist einem TI-Messenger-Client am Smartcard-IDP-Dienst authentifizieren. Di Akteur (natürliche Person) als Endpoint hinterlegt und tritt stellvertretend für die Organisation in den Chat ein.

Tabelle 9: Beser Vorganispiel für Funktionsaccounts

Abteilu ng	Funktionsacco unt	Endpoint.address	Akteur (MXID)	Displayname
Kardiolog ie	Labor_Kardiolog ie	@MXID_Bot01:<do main>.de	@MXID_01:<do main>.de @MXID_02:<do main>.de	Empfang_Kardio logie (Chatbot) Dennert, Maltilde Fritsche, Sarah
Neurolog	Ambulanz_Neur	@MXID_Bot02:<do	@MXID_03:<do	Ambulanz_Neur

ie	ologie	main>.de	main>.de	ologie (Chatbot) Gotsch, Gerd
Radiologi e	Empfang_Radiol ogie	@MXID_04:<domai n>.de	-	Fruechtl, Wilfried

Im Folg-verifiziert den Nutzer als Leistungsenden wird die Interaktion eines externen Akteurs mit einem Funktionsaccount gezeigt.

Prozess:

1. Vorbedingung:

- Organisation verfügt über einen TI-Messenger-Client mit Administrationsfunktion und einen Messenger-Service
- Chatbots stehen zur Verfügung und können vom Akteur in der Rolle "Org-Admin" verwaltet werden

2. Konfiguration von Funktionsaccounts:

- Der Akteur in der Rolle "Org-Admin" legt einen Funktionsaccount (organisationsbezogene MXID) als einenEndpoint des gewünschten HealthcareService der Organisation an und ordnet dieser MXID einen Chatbot zu
- Der Akteur in der Rolle "Org-Admin" weist zuständige Akteure der Organisation (personenbezogene MXIDs) dem Chatbot zu
- Die Zuordnung von Akteuren zu einzelnen Anfragen innerhalb eines Funktionsaccounts (z. B. Terminanfragen, Medikationsentscheidung) erfolgt durch die Konfiguration im Chatbot

Alternative: Der Akteur in der Rolle "Org-Admin" legt einen Funktionsaccount (organisationsbezogene MXID) als einenEndpoint des gewünschten HealthcareService der Organisation an und hinterlegt in diesem Endpoint die MXID von einem Akteur.

3. Beispielhafter Ablauf (siehe Abbildung "Interaktion mit einem Chatbot"):

1. Ein Akteur sucht nach einer Organisation und/oder Unterstruktur dieser Organisation (z. B. in einem Krankenhaus die Abteilung Kardiologie)
2. Der Akteur öffnet einen Chatraum mit dem Funktionsaccount der Abteilung Kardiologie
3. —
 - a. Der Chatbot des Funktionsaccounts der Abteilung Kardiologie betritt den Raum
 - b. Der Chatbot KANN automatisiert das Anliegen vom Akteur (z. B. Terminanfrage, Rückfrage an Arzt etc.) abfragen

4. Der Akteur antwortet dem Chatbot
5. Der Chatbot lädt je nach Anliegen die ihm zugeordneten und verfügbaren Akteure in den Chatraum ein
6.
 - a. Eingeladene Akteure betreten den Chatraum mit ihrem Displaynamen
 - b. Eingeladene Akteure kommunizieren mit dem Akteur

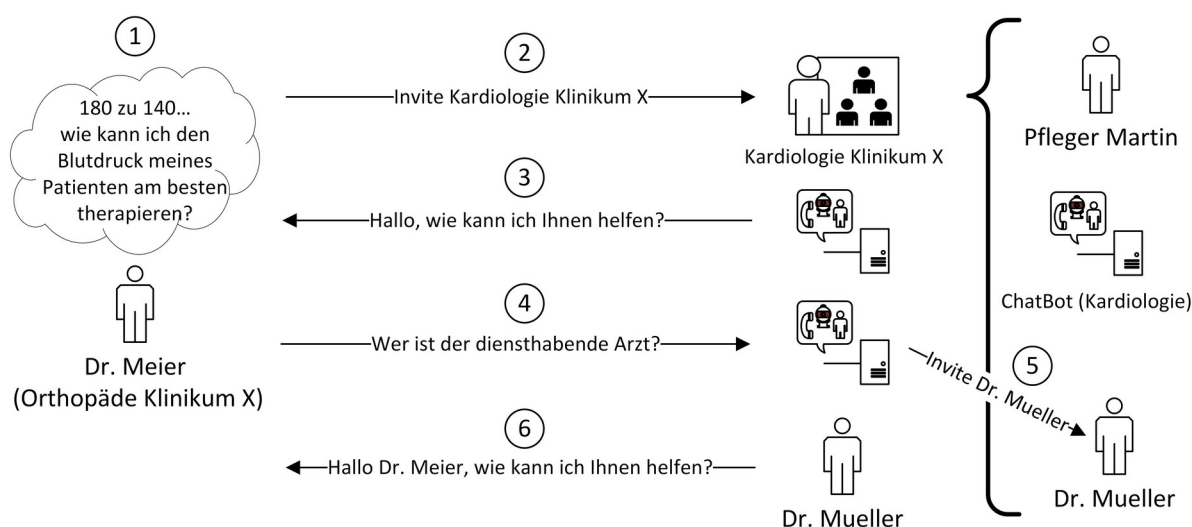


Abbildung 6: Beispiel einer innerhalb-desteration mit einem Chatbot

7.9 Test

Der TI-Messengers-

7.9.1 Lesezugriff fürer-Anbieter MUSS eine Referenz-Instanz und mindestens eine Test-Instanz des TI-Messenger-Fachdienstes und TI-Messenger-Clients

Für lesend bereitstellen Zugriff auf das VZD-FHIR-Directory und betreiben. Die Referenz-Instanz hat die gleiche Version wird das Matrix-OpenID-Token des jeweilige die Produktionsumgebung und kann von anderen Herstellern für Tests und Entwicklung gegen Matrix-Homeser die zugelassene vers verwendet. Ein Nutzion benutzt werden. Weiterhin wird die Referenz-Instanz für die Reproduktion aktueller Fehler/Probleme aus der Produktionsumgebung genutzt. Der KANN somit Suchanfragen an das VZD-FHIR-Directory senden. Dem Matrix-OpenID-Token des Matrix-Homeservers Zugriff auf die Referenz-Instanz MUSS für die gematik zur Fehleranalyse gewährleistet sein. Die Test-Instanz dient den Herstellern bei der Entwicklung neuer TI-Messenger-Clients

und TI-Messenger Fachdienste Versionen, den IOP-Tests zwischen den verschiedenen TI-Messenger-Anbietern und wird vertraut, wenn auch von der gematik für die Zulassung genutzt.

der Matrix-~~TI-messenger~~-Anbieter als Matrix-Domain ein MUSS die verschiedenen Benutzer verifizierten Organisations-Ressource im VZD-FHIR-Directory zugeordnet wurde und ihm somit der Referenz-Instanz und der Test-Instanz koordinieren (Verwaltung eines Test-/Nutzungsplans). Bei Bedarf (Entwicklung verschiedener Versionen, hoher Auslastung durch andere Hersteller oder durch die gematik) MUSS der TI-Messenger-Anbieter auch vertraut werden kann mehrere Test-Instanzen mit Der Lesezugriff wird mitgleichen oder mit verschiedene Versionen bereits als-Berechnen und betreiben.

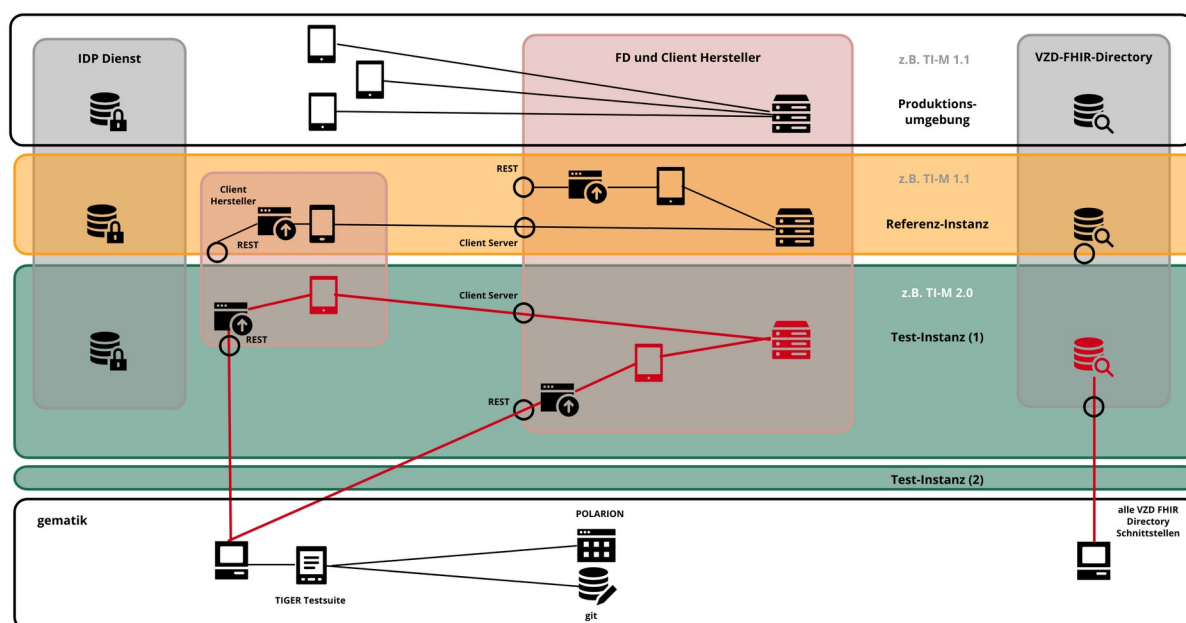


Abbildung 7: tigu-Messenger (Per-Dienst Instanzen)

Hinweis: Grundsätzliches) auf dem VZD-FHIR-Directory gh ist es möglich, eine CC-Zertifizierung für das Gesamtprodukt oder Produktbestandteile durchzuführen und damit anderegelt.

Es gilt:

Testtypen und -arten, die die Sichtbarkeit auf dstechnische Eignung prüfen sowie Organisations-RProduktgutachten zu ersetzen.

7.10 Betrieb

Der TI-Messenger-Anbieter verantwortet im Betrieb folgende Produkte:

- TI-Messourcen-KANNenger-Fachdienst(e),
- TI-Messenger-Client(s) für andere Orgakteure und
- TI-Messenger-Clients mit Administrationsfunktionen oder Practitioners-ei(Org-Admin-Client) inkl. Authenticator(-modul).
- Der TI-Messenger eingeschränkt werden und

die Sichtbarkeit auf Practitioner-Anbieter MUSS mindestens einen TI-Messenger-Fachdienst, mindestens einen TI-Messenger-Ressourcen ist nur möglich, wenn Client für Akteure und mindestens einen Org-Admin-Client (die Clients jeweils oder Nutzer selbst mit der Matrix-User URI (MXID) als Practitioner auf dem VZD hinterlegt ist in einen TI-Messenger-Client integriert) anbieten.

A_23658 - Produktnachweise im Rahmen der kontrollierten Inbetriebnahme

- Das Produkt MUSS die Vorgaben zur Funktionalität, Sicherheit und die Interoperabilität gemäß [Spec_VZD-FHIR_Directory] gesetzt wurde.

7.11 Betrieb

Der TI-Messenger-Anbieter entsprechend des jeweiligen Produkttypsteckbriefs in der Produktivumgebung erfüllen. Die Nachweise dafür MUSS der Anbieter verantworten, entsprechend und im Rahmen des Konzepts zur kontrollierten Inbetriebnahme erbracht werden.

[<=]

Hinweis: Die Anforderung [A_22658] ist eine Ergänzung für die Produkte: TI-Messenger-Fachumgebung und ersetzt nicht dienst und TI-Messenger-Client(s)- vorgelagerten Prüfverfahren der Produkte in der Referenzumgebung.

Der TI-Messenger-Anbieter KANN auch mehrere TI-Messenger-Clients an und mehrere TI-Messenger-Fachdienste anbieten. Der tatsächliche Betrieb kann gemäß [gemKPT_Betr#Anbieterkonstellationen] ausgelagert werden.

Der TI-Messenger-Anbieter MUSS seinen Nutzern und Organisationen einen Helpdesk entsprechend [gemKPT_Betr] anbieten, welcher auch Störungen zu allen verantworteten TI-Messenger-Clients an und TI-Messenger-Fachdiensten entgegen-nimmt.

Der TI-Messenger-Anbieter ist gemäß Betriebskonzept [gemKPT_Betr] ein Teilnehmer im TI-ITSM mit (IT-Service-Management der TI) mit allen damit verbundenen Rechten und Pflichten.

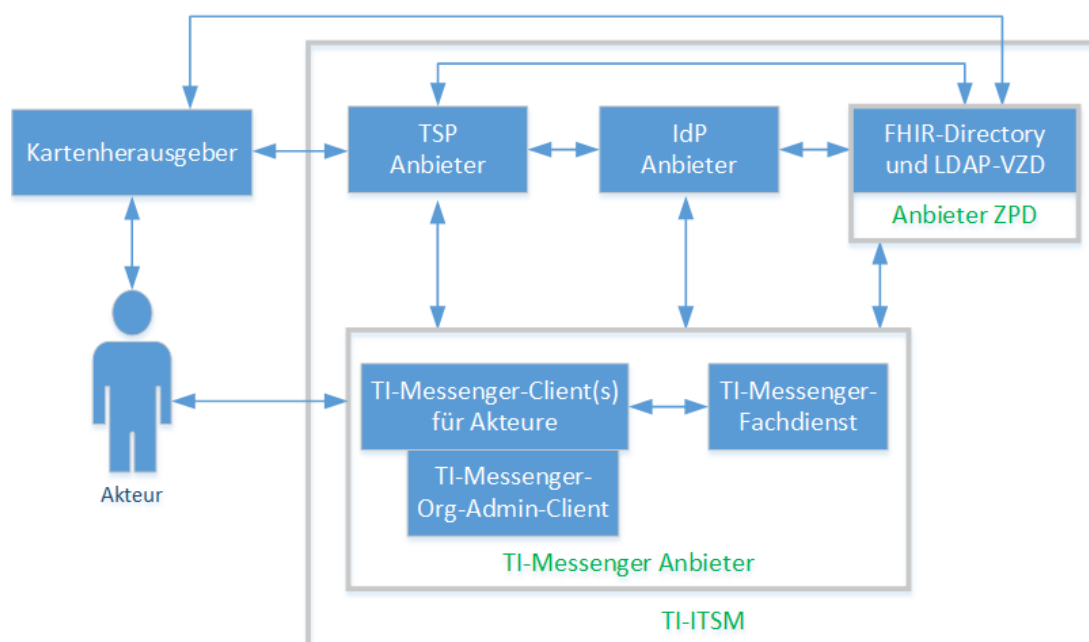


Abbildung 8: Ausschnitt - TI-Messenger-Anbieter MUSS Referenzinstanzen des TI-Messenger-Fachdienstes im TI-ITSM

Hinweis: dienstes bereitstellen und betreiben.

Dabei MUSS es eine Referenzinstanz geben, welche die organisatorische Hersteller bei der Entwicklung neuer TI-Messenger-Clients und im Vordergrund des TI-Messenger-Fachdienstes dient und eine Referenzinstanz, welche ausschließlich der gematik zur Verfügung gestellt wird, gegen welche das TI-ITSM-System zwischen den jeweiligen Entitäten ab. Die Produkte beim TI-Messenger Anbieter können einzeln zugelassen werden kann.

8 Anwendungsfälle

~~Alle Anwendungsfälle, die gemäß Matrix-Client-Server-Protokoll umgesetzt werden können, werden in dies, werden aber im Bundle im Sinne des Nutzers mit einem Konzept nicht aufgeführt. Stattdessen wird auf die Matrix-Client-SPOC für die jeweiligen Komponent-Server-API verwiesen vom jeweiligen ([Matrix-Foundation#Client-Server]). Anbieter angeboten.~~

9 Anwendungsfälle

Die nachfolgend beschriebenen Anwendungsfälle sind spezifisch für den TI-Messenger-Dienst und weichen daher teilweise von der Matrix-Client-Server-API ab. Das gleiche gilt für die auf dem Matrix-Server-Server-Protokoll ([Matrix-Foundation#Server-Server-API]) basierenden Anwendungsfälle.

Im Folgenden werden die Anwendungsfälle, die gemäß dem Konzeptpapier TI-Messenger [gemKPT-TI-Messenger] beschrieben.

9.1 AF – Anmeldung eines Nutzers an Messenger-Service

Mainline_OPB1/ML-123516AF_10057 – Anmeldung eines Nutzers am Matrix-Client-Server-Protokoll umgesetzt werden, an dieser Stelle nicht weiter aufgeführt sind. Statt Messenger-Service

Mit diesem Anwendungsfall meldet sich ein Nutzer als Person an einem Messenger-Service an. Die Anmeldung erfolgt durch den Nutzer mit einer API.

Im Kontext des TI-Messenger-Clients und einem Authentifizierungsverfahren, das vom Messenger-Service unterstützt wird. Entsprechend der TI-Messenger-Client präsentiert dem Nutzer eine Liste von Rollen eines Akteurs. Unterschiedliche Anwendungsfälle unterstützen Messenger-Service. Für die Rollen "Org-Admin und User/Services". Ebenfalls ist es möglich, dass der Nutzer "HBA" wird, dies in den folgenden Abbildungen dargestellt.

Rolle: Org-Admin

Ein Akteur in der Rolle "Org-Admin" kann einen Messenger-Service direkt eingeben, um sich an diesen zu authentifizieren. Nach erfolgreicher Anmeldung erhält der Administrator des TI-Messenger-Client-Anbieters ein Matrix-ACCESS_TOKEN (AuthZ) vom Matrix-Home-Server, das für die spätere Autorisierung des Akteurs genutzt wird. Das Matrix-ACCESS_TOKEN einer freigeschalteten SMC-B, im Kontext des TI-Messenger-Clients des Nutzers über die device_id verknüpft.

folgenden Anwendungsfälle aus.

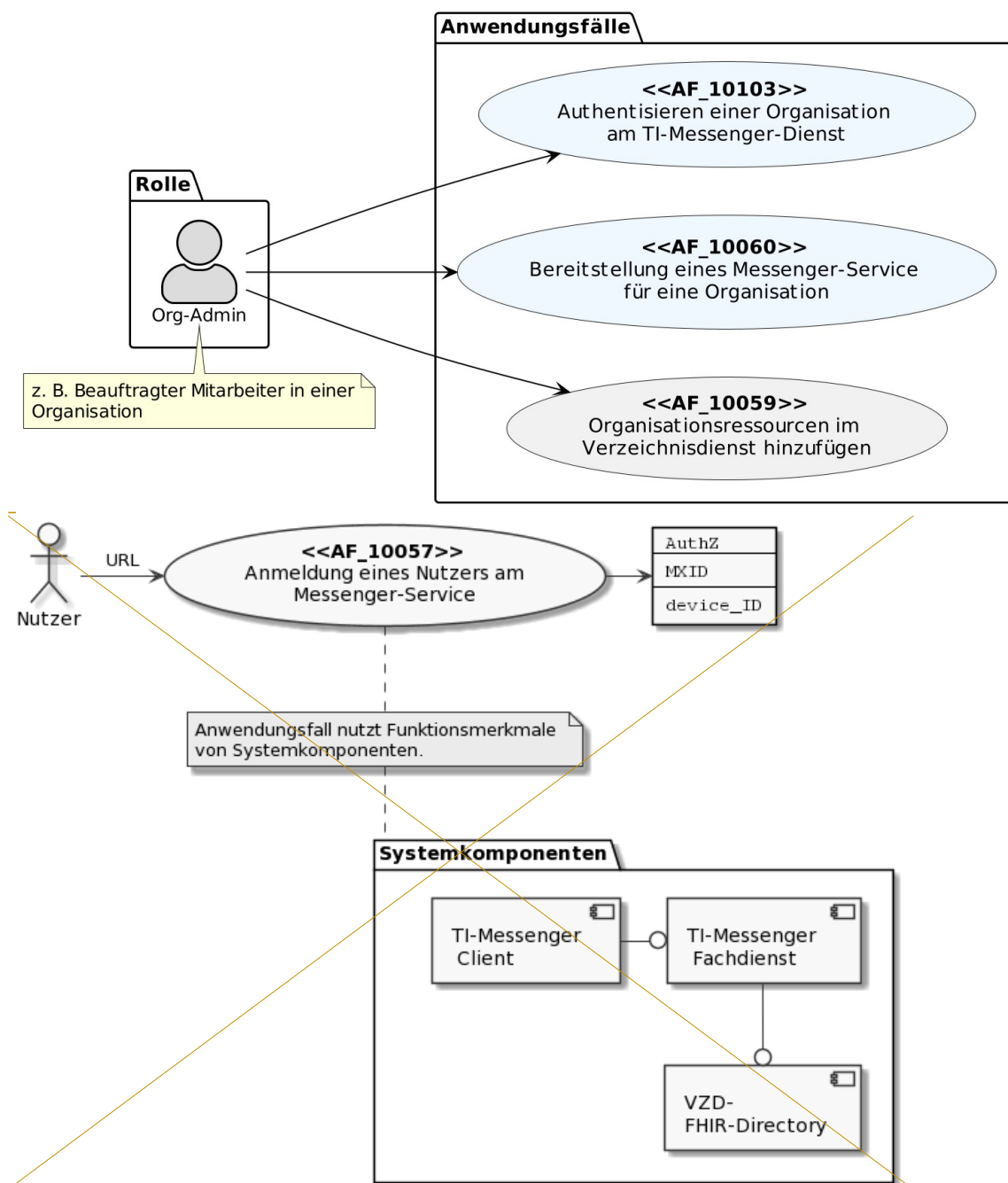


Abbildung 9: **Systemkomponenten**Org-Admin - Übersicht Anwendungsfälle

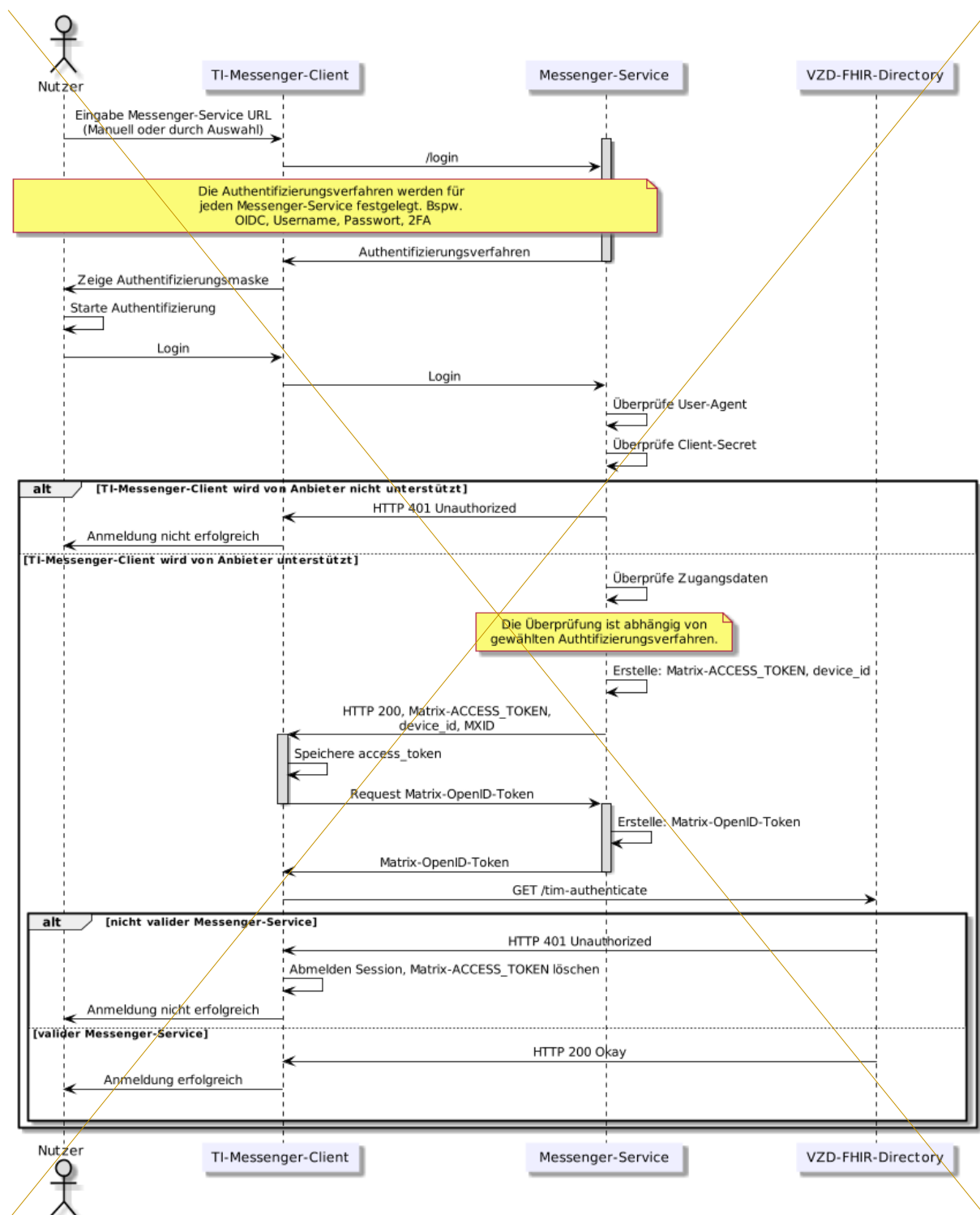
Der Anwendungsfall AF_10060 - Bereitstellung eines Messenger-Service für eine Organisation des AF--Anmeldesetzt die erfolgreiche Authentifizierung eines der Organisation durch den Anwendungsfall AF_10103 - Authentisieren einer Organisation am TI-Messenger-Dienst voraus. WerdeNutzers am durch eine Organisation mehrere Messenger-Service

Tabelle 10:s benötigt (z. AF--AnmB. im Krankenhausumfeldung eines Nutzers am) KANN der Anwendungsfall Messenger-Service

AF_10057	Anmeldung eines Nutzers am Messenger-Service
-----------------	---

Akteur	Nutzer
Auslöser	Nutzer möchte sich mit TI-Messenger-Client bei einem Messenger-Service anmelden
Komponenten	TI-Messenger-Client, Messenger-Service, VZD-FHIR-Directory
Vorbedingungen	<ol style="list-style-type: none"> Der Nutzer verfügt über einen TI-Messenger-Client Der Nutzer kennt die URL des Messenger-Services oder die URL ist bereits in seinem Client konfiguriert. Der Nutzer kann sich durch ein beim Matrix-Homeserver unterstütztes Authentisierungsverfahren identifizieren. Der verwendete Matrix-Homeserver unterstützt vereinbarte Authentisierungsverfahren. Der verwendete Matrix-Homeserver ist in die Föderation integriert.
Eingangsdaten	URL des Matrix-Homeservers
Ergebnis	TI-Messenger-Account erzeugt
Ausgangsdaten	Matrix-ACCESS_TOKEN, MXID, device_id
Akzeptanzkriterien	<ol style="list-style-type: none"> ML-123571 ML-123576 ML-123575

hinfach ausgeführt werden. Mit der Laufzeitsicht sind die Interfärbblichen Zuordnung soll auf eine funktionenale Beziehung zwischen den Komponenten, die durch deeinzeln Anwendungsfall genutztällen hingewiesen werden, dargestellt.



Eine weitere Aufgabe des Akteurs in der Rolle "Org-Admin", welche hier nicht weiter in einer Anwendung eines Nutzers am Messenger-Service

[<=]

falls gezeigt wird, ist die Einrichtung von Funktionsaccounts und die Benutzerverwaltung.

Akzeptanzkriterien für den Rolle: User / User-HBA

Ein Akteur in der Rolle "User / User-HBA" KANN die folgenden Anwendungsfälle auslösen.

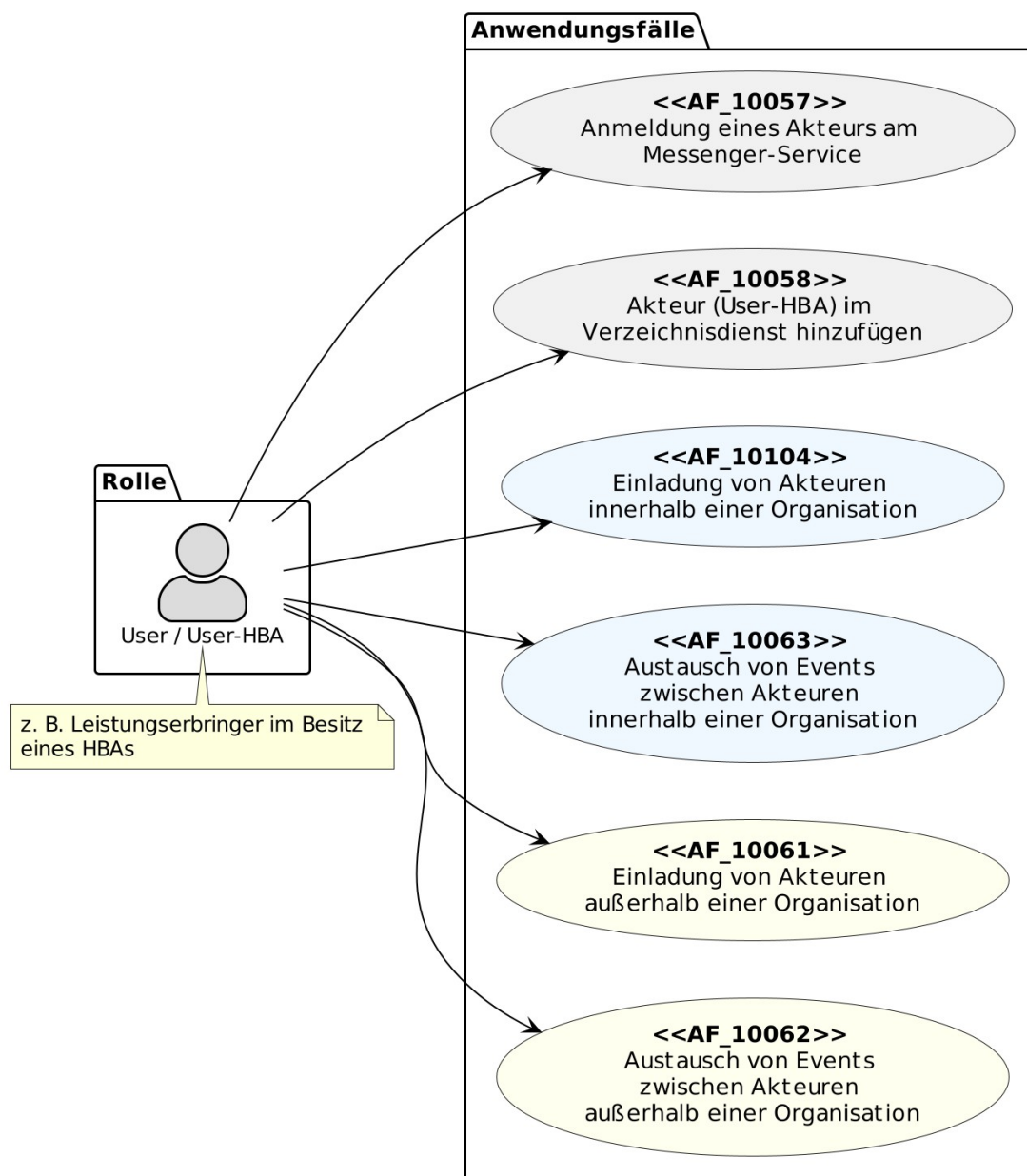


Abbildung 11: Use eines Nutzers am Messenger-Service (AF_10057)

r / User HBA - Übersicht Anwendungsfälle

Mainline_OPB1/ML-123571**ML-123571**-Der Anwendungsfall AF_10058 - Akteur (User-HBA) im Verzeichnisdienst hinzufügen **AF_10057 - Nutzer kann sich erfolgreich an einem gültig**KANN nur von einem Akteur in der Rolle "User-HBA" ausgeführt werden. Alle anderen gezeigten **Messenger**-Anwendungsfälle KÖNNEN von den Akteuren in der Rolle "U**Service anmel** / User-HBA" ausgeführt werden

Ein Nutz. Mit der kann sich erfolgreich a farblichen Zuordnung soll auf eine funktionale Beziehung zwischen den einem gültigen Meszelen Anwendungsfällen hingewiesenger-Service-anmel werden.

Hinweis: In den folgen den, An wenn er sich mit einem zugelassenen Authentisierungsverfahren erfolgreich authentisiert. Es MUSS sichedungsfällen wird auf Abläufe verwiesen, die im Anhang B zu finden sind. Ebenfalls können für eine bessere Lesbarkeit die in den jeweiligen Anwendungsfällen dargestellt werden, dass die Anmeldung an en Laufzeitsichten als PlantUML-Quelle in [api-Messenger-Services,] unter src/plantuml und in die nicht Teil der Föderation sind, nicht möglich ist. [<=]agrammform unter /images/diagrams abgerufen werden.

AF - Authentisieren einer Organisation am TI-Messenger-Dienst

23576ML-123576 -- AF_10057 -- Der Messenger-Service stellt de103-01 - Authentisieren einer Organisation am TI-Messenger-Client ein Access-Tokenst

Mit diesem Anwendungsfall aus

Bei der erfolgreichethentisiert ein Anmeldung stellt der Messenger-Service dekteur, in der Rolle "Org-Admin", seine Organisation bei einem TI-Messenger-Client ein Access-TokenAnbieter. Für die aus-

[<=]

Mainline_OPB1/ML-123575**ML-123575 -- AF_10057 -- Speichthentisierung Access-Token-durch**einer Organisation stellt der **TI-Messenger-Client**achdienst

Der TI-Messenger-Client eine Schnittstelle an seinem Registrierungs-Dienst speichert das ihmst bereit. Diese wird übergebene Access-Token zur Verwend das Frontend des Registrierung in den folgenden Anwends-Dienstes für die Authentisierungsfällen.[<=]

9.2 AF -- Leist verwendet. Die Authentisierungserbringer als Practitioner hinzufügen

Mainline_OPB1/ML-123517**AF_10058 -- Leist** der Organisation erfolgt individuell und nutz**ungserbringer als Practitioner hinzufügen**

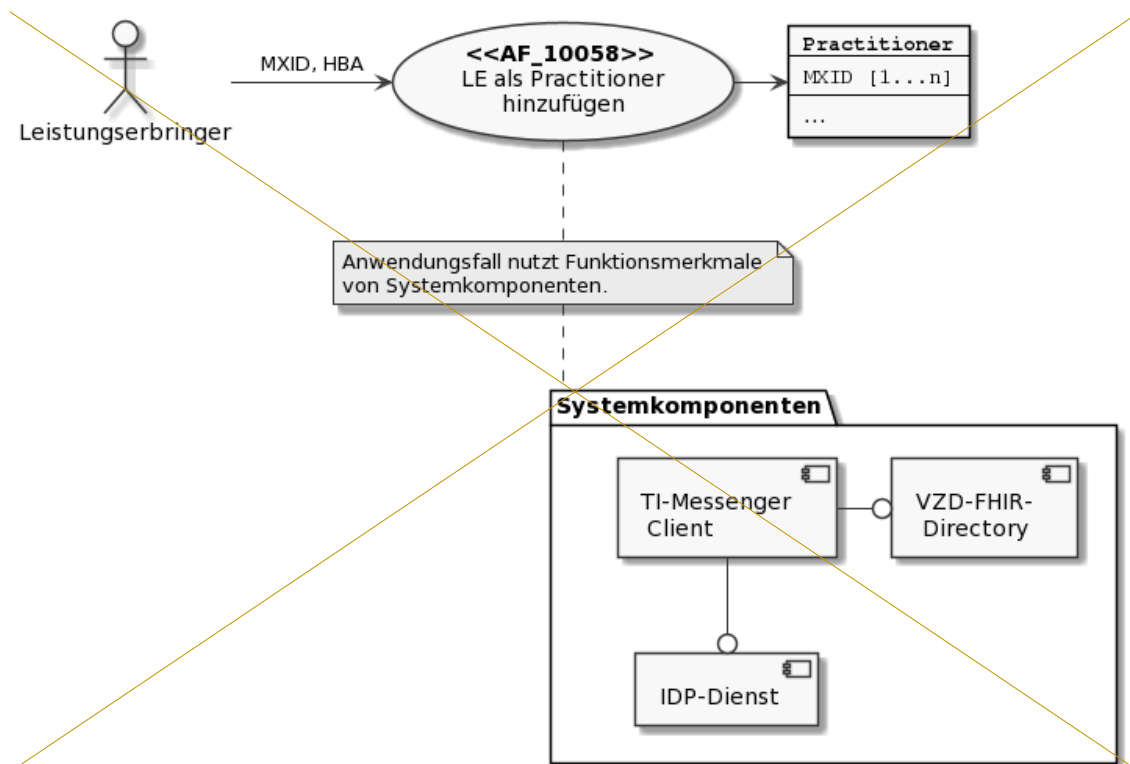
Mitabhängig durch einen Akteur in der Rolle "Org-Admin". Durch diesem Anwende Authentifizierungsfall trägt ein Leistungserbringer mit HBA seine MXID in seinen Practi MUSS der Besitz einer gültigen SMC-B nachgewiesen werden, da nur Organisationer-Datensatz auf dem VZD-FHIR-Directory ein. Danach hat der Leistungserbringer die Möglichkeit, mit ann des Gesundheitswesens berechtigt sind einen Messenger-Service zu erhalten. Als Nachweis MUSS eins deren folgenden verifiziertfahren LE in Kontakt zu treten und ist verwendet werden.

für anderedie verifizierte LE-übung der das VZD-FHIR-Directory erreichbar. Dieser Flow-SOLL direkt mit dem initiOrganisation MUSS

- Verfahren 1: bei der Authentisierung am zentralen Anmeldevorgang kombinierIDP-Dienst eine freigeschaltete SMC-B verwendet werden. Hi oder
- Verfür wird der LE während des Onboardings durch dahren 2: eine KIM-Nachricht an die Adresse der Organisation mit der freigeschalteten TI-Messenger-Client gefragt, ob es sich bei dem Nutzer um SMC-B gesendet werden.

Als Nachweis zur Prüfung auf einen Leistungserbringer mit Zugriff auf HBA handelt. gültige Organisation MUSS der Registrierungs-Dienst in beiden Verfahren prüfen, ob die











Profession0ID Zusätzlich KAN einer Organisation der LE angeben, ob er andere LE übs Gesundheitswesens gehört. Bei erfolgreicher das VZD-FHIR-Directory finden möchte und ob eine Sichtbarkeit gegenüber Verifizierung der Organisation wird ein Administrator-Account für die Organisation am Registrierungs-Dienst anderen LE gewünsgelegt. Dies ermöglicht ist.



es einem Abbildung 12: dminiSystemkomponenten dtrator Messenger-Services AF-Lezu registierungserbringieren und seiner als Practitioner hinzufügenOrganisation am TI-Messenger-Dienst teilzunehmen.

Tabelle 11: ATabelle : AF - LeistungserbringAuthentisieren einer als PractiOrganisationer hinzufügen am TI-Messenger-Dienst

AF_10058103	LeistungserbringAuthentisieren einer als Practitioner hinzufügenOrganisation am TI-Messenger-Dienst
Akteur-	<u>LeistungserbringerBeauftragter Mitarbeiter einer Organisation in der Rolle "Org-Admin"</u>
Auslöser	<u>Leistungserbringer möchte seinen PractitionEine Organisation des deutschen Gesundheitswesens möchte am TI-Messenger-Datensatz auf dem VZD-FHIR-Dit teilnehmen und benötigt die Berectory-aktualishtigung einen Messenger-Service zu registrieren-</u>
Komponenten	<ul style="list-style-type: none"> <u>TI-Messenger-Client, Frontend des Registrierungs-Dienstes,</u> <u>Authenticator (Optional bei Verfahren 2),</u>

	<ul style="list-style-type: none"> • <u>Konnektor,</u> • <u>eHealth Kartenterminal mit gesteckter SMC-B,</u> • <u>Registrierungs-Dienst,</u> • <u>zentraler IDP-Dienst,</u> <u>VZD-FHIR-Directory (Optional bei Verfahren 2)</u> <u>KIM-Clientmodul und Mailclient (Optional bei Verfahren 1)</u>
<u>Vorbedingungen</u>	<ol style="list-style-type: none"> <u>1. Der LE verfügt Akteur kann über einen TI-Messenger-Cl Frontend des Registrierungs-Dienst</u> <u>2. Der LE ist beim Smartcard IDPstes für die Kommunikation auf den Registrierungs-Dienst der TI registriert.</u> <ol style="list-style-type: none"> <u>1. zugreifen.</u> <u>2. Verifizierung der Organisation:</u> <u>3. Verfahren 1:</u> <u>Der LE ist als Nutzer im Messenger-Service angemelAkteur kann den Authenticator verwenden sowie das verwendet- (AF_10057):</u> <u>4. Das VZD-FHIRE Frontend des Registrierungs-Directory istenstes, welches beim Smartcardzentralen IDP-Dienst registriert:</u> <ul style="list-style-type: none"> • <u>Der ist.</u> <u>5. verwendete Matrix Hofahren 2:</u> <u>Der Anbieter des TI-mesersenger ver ist in dfügt über eine SMC-B Org und eine KIM-Adresse sowie Föderation integriert:</u> <ul style="list-style-type: none"> • <u>Dein eHealth Kartenterminal und einen Konnektor mit TI-Zugang. Der Akteur verfügt über LE kann sich am (Practitioner) Smartcard IDP eine SMC-B und eine KIM-Adresse sowie ein eHealth Kartenterminal und einen Konnektor mit TI-Zugang.</u> <u>6. Dienst auth im eHealth Kartentisierenerminal gesteckte SMC-B ist freigeschaltet.</u>
<u>Eingangsdaten</u>	<u>MXIDIdentität des Leistungserbringers, HBAr Organisation, SMC-B, Alternativ KIM-Adresse</u>
<u>Ergebnis</u>	<u>MXID im PractiDie Organisationer Datensatz des Nutzers auf dem FHIR-Server ei wurde am Registrierungs-Dienst des TI-Messengetragen, (gemäß [gemSpec_VZD_FHIR_Directory])r-Fachdienstes verifiziert</u>
<u>Ausgangsdaten</u>	<u>aktualisierter Practitioner Datensatzdmin-Account, Status</u>
<u>Akzeptanzkriterien-</u>	4  ML-123611  ML-128757 , 5  ML-123612  ML-128759 ,   ML-128758 ,   ML-129853 ,   ML-132446

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den

Anwendungsfall genutzt werden, dargestellt. Für das zu benutzende
Authentifizierungsverfahren gilt die Spezifikation gemäß OpenID-Connect.
~~Das Verfahren OIDC wird im Anhang B beschrieben. einer Organisation wird in der~~
~~Laufzeitsicht der zentrale IDP-Dienst der TI verwendet.~~

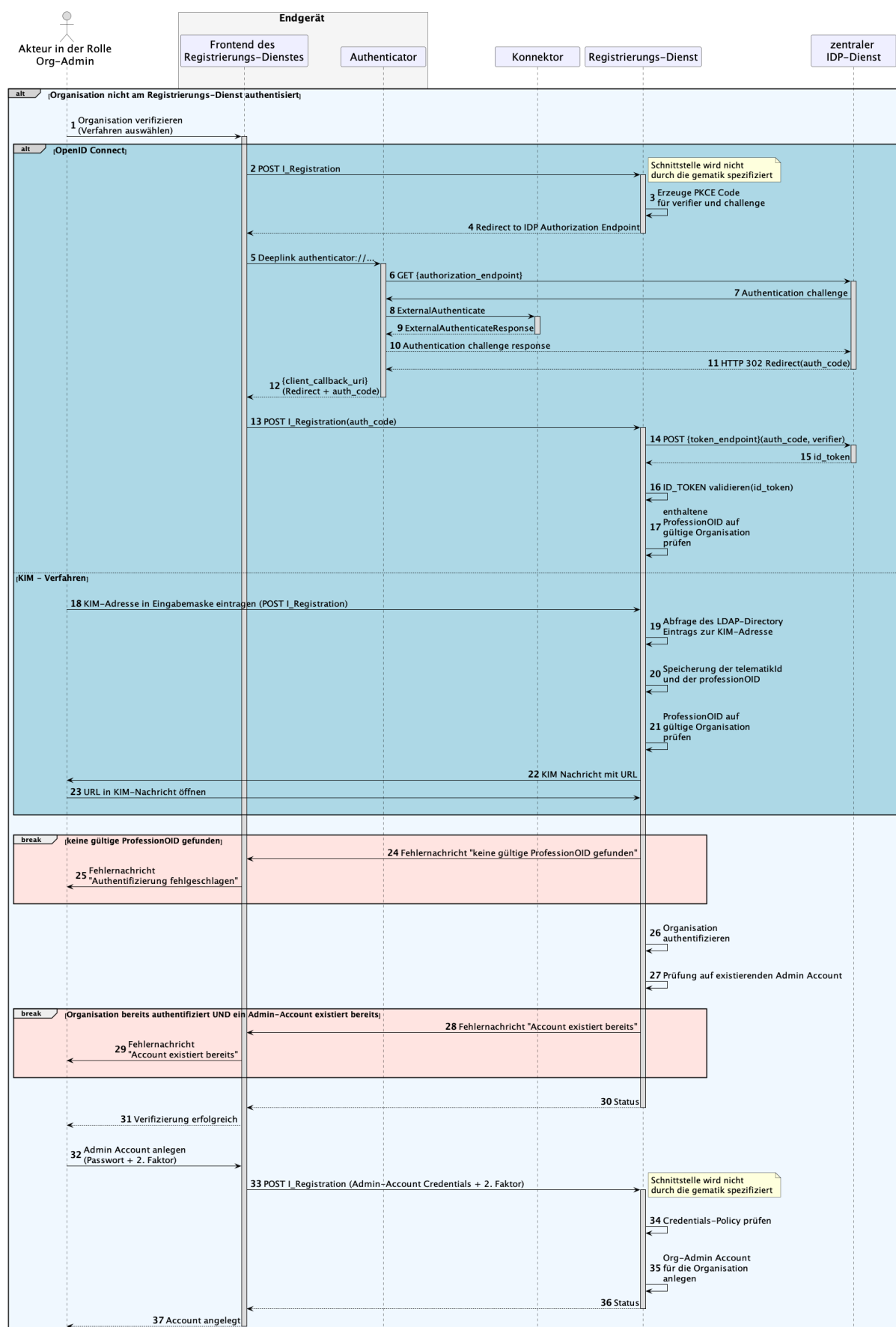


Abbildung 13: Laufzeitsicht - LE als Practitioner Authentisieren einer Organisationer hinzufügen am TI-Messenger-Dienst

[<=]

Akzeptanzkriterien für den Anwendungsfall: LE als Practitioner Authentisieren einer Organisationer hinzufügen am TI-Messenger-Dienst (AF_10058103)

3612ML-1236128757 - AF_10058103 - LE als Practitioner Verifizierung der Organisationer hinzüfuge als Akteur in der Rolle Org-Admin

Nach erfolgreicher nur ein Akteur in der Rolle "Org-Admin" darf seine Organisation gegenüber dem TI-Messenger-Fachdienst Authentisierung am IDP-Dienst wird in den Practitionerfizieren.

[<=]

ML-128759 - AF_10103 - Organisation wurde erfolgreich verifiziert

Die Organisation wurde beim TI-Messenger-FHIR-Datenachdienst erfolgreich mit einer Identität einer Organisatz-ion des authentGesundheitswesens verifizierten-Leistungserbringers—die Matrix-User-URI eingefügt

[<=]

ML-128758 - AF_10103 - ID-Token wurden ausgestellt und übergeben

Das vom IDP-Dienst ausgestellte ID_TOKEN ist gültig und der-Liegt dem Frontend des Registrierungsbrri-Dienstes vor.

[<=]

ML-129853 - AF_10103 - Administrator Account anger-übelegt

Ein Administrator Account für den-Eie Organisation wurde erfolg-informreich am Registriert-ungs-Dienst angelegt.

[<=]

23611ML-12361132446 - AF_10058103 - MXID-Eintrag nur für eigenTI-M Rohdatenerfassung und -lieferung

Die Rohdaten wurdenen Practitioner-FHIR-entsprechend der RohDatensatz Der Leistungserbringedefinition gemäß [gemSpec_TI-Messenger-FD#Betrieb] für darf nur-eigene FHIR-Ressourcen (AF_10037—gemSpec_VZD_FHIR_Directory) ändern-en TI-Messenger-Fachdienst erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet.[<=]

9.3 AF - Bereitstellung eines Messenger-Service bereitstellefür eine Organisation



23519AF_10060-01 - Bereitstellung eines Messenger-Service bereitstellefür eine Organisation

Messenger-Services werden-dezit diesem Anwendungsfall wird einer zuvor am Registrierungs-Dienst authentral-fürifizierten Organisationen-des-Gesundheitswesens ein Messenger-Service für diese Organisation durch einen Akteur in der Rolle "Org-Admin" bereitgestellt. Nutzer einer Organisation-melden-sich-anDie Beantragung zur Bereitstellung eines Messenger-Services-an, um wird durch den Akteur in der Rolle "Org-

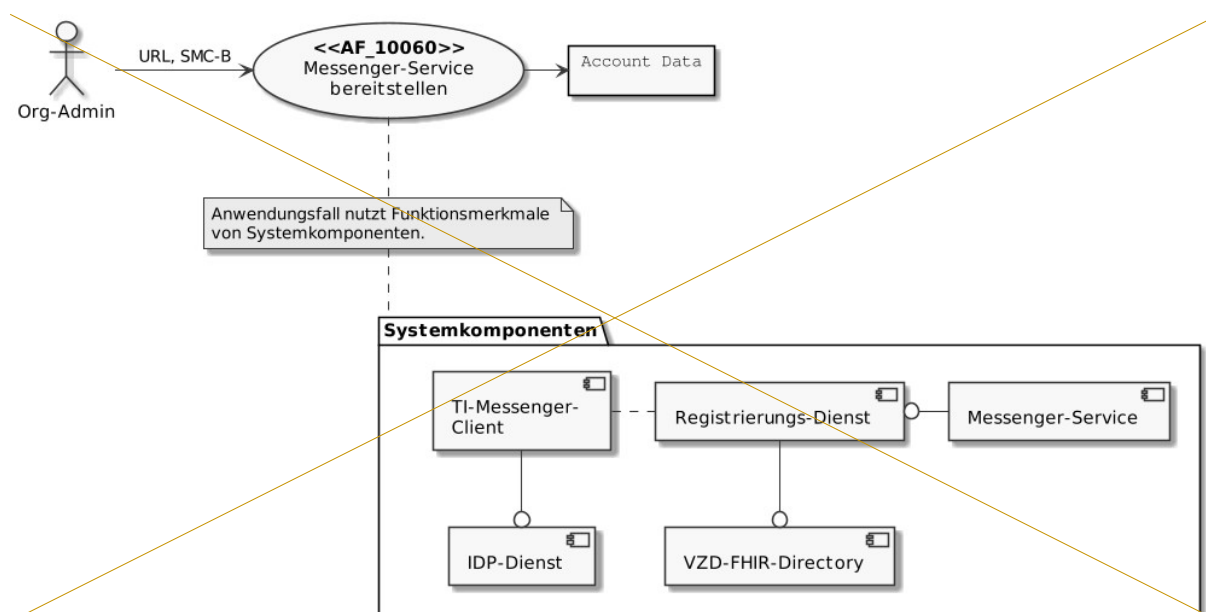
Admin" am TI-Messenger Frontend des Registrierungs-Dienst teilnehmen vorgenommen zu können. Dieser MUSS sich zuvor mit dem Admin-Account der Organisation am Registrierungs-Dienst anmelden. Für eine schnellzeitnahe Adaption des TI-Messenger-Dienstes MUSS eine schnelle Bereitstellung von Messenger-Services gewährleistet sein. TI-Messenger-Anbieter sind daher verpflichtet, Prozesse zu etablieren, damit Messenger-Services für Organisationen schnell und ggf. automatisiert bereitgestellt werden. Dazu MUSS d können. Nach erfolgreicher RegistrierBereitstellungs-Dienst mit einem Frontend- oder Schnittstellen, welche in eines Messenger-Service wird dieser in die Föderation des TI-Messenger-Client-Diensts oder anderen-stes aufgenommen. Werden mehrere Messenger-Services für eingebunden werden ie Organisation benötigt KANn dieser Lage sein eine SMC-B zu validieren und Anwendungsfall mehrfach ausgeführt werden.

Tabelle 12: anschließendF - Bereitstellung eines Messenger-Service für dieine Organisation

<u>AF_10060</u>	<u>Bereitstellung eines Messenger-Service für eine Organisation</u>
<u>Akteur</u>	<u>Beauftragter Mitarbeiter einer Organisation in der Rolle "Org-Admin"</u>
<u>Auslöser</u>	<u>Eine Organisation des deutschen Gesundheitswesen möchte am TI-Messenger-Dienst teilnehmen und benötigt die Bereitstellung eines oder mehrerer Messenger-Services</u>
<u>Komponenten</u>	<ul style="list-style-type: none"> <u>Frontend des Registrierungs-Dienstes,</u> <u>Registrierungs-Dienst,</u> <u>VZD-FHIR-Directory,</u> <u>Messenger-Service.</u>
<u>Vorbedingung</u>	<ol style="list-style-type: none"> <u>1. Es besteht ein Vertragsverhältnis mit einem TI-Messenger-Anbieter.</u> <u>2. Der Akteur verfügt über ein Frontend des Registrierungs-Dienstes für die Kommunikation mit dem Registrierungs-Dienst.</u> <u>3. Das verwendete Frontend des Registrierungs-Dienstes ist beim zentralen IDP-Dienst registriert.</u> <u>4. Die Organisation ist erfolgreich beim Registrierungs-Dienst authentifiziert und ein Admin-Account ist vorhanden.</u> <u>5. Der Registrierungs-Dienst kann sich beim VZD-FHIR-Directory Server für Schreibzugriffe mit OAuth2 authentisieren.</u>
<u>Eingangsdaten</u>	<u>Admin-Account, Identität der Organisation (SMC-B)</u>
<u>Ergebnis</u>	<ol style="list-style-type: none"> <u>6. Der Messenger-Service für die Organisation wurde erstellt.</u> <u>7. Die Matrix-Domain des neuen Messenger-Services</u>

	wurde als Endpunkt im VZD-FHIR-Directory eingetragen und in die Föderation aufgenommen.
Ausgangsdaten	Neuer Messenger-Service für die Organisation, Status
Akzeptanzkriterien	 ML-123648,  ML-123649,  ML-123650,  ML-132585

In berder Laufzeit zustellen.



sicht sind die Interaktionen zwischen Systemden Komponenten des AF-Messenger-Service bereit, die durch den Anwendungsfall genutzt werden, dargestellt

Tabelle 13: At. F – Messenger-Service bereitstellen

AF_10060	Messenger-Service bereitstellen
Akteur	Beauftragter Mitarbeiter der Organisation (z. B. <i>Org-Admin</i>)
Auslöser	Eine Organisation des deutschen Gesundheitswesens möchte am TI Messenger Dienst teilnehmen und benötigt die Bereitstellung eines Messenger-Service
Komponenten	TI-Messenger-Client IDP-Dienst Registrierungs-Dienst VZD-FHIR-Directory Messenger-Service

Vorbedingung	<ol style="list-style-type: none"> Der Nutzer verfügt über ein Frontend (innerhalb oder außerhalb eines TI-Messenger-Clients) für die Kommunikation mit dem Registrierungs-Dienst Das verwendete Frontend des Registrierungs-Dienst ist beim Smartcard-IDP-Dienst registriert. Der verwendete Registrierungs-Dienst kann sich beim VZD-FHIR-Directory-Server für Schreibzugriffe authentifizieren.
Eingangsdaten	Identität der Organisation, SMC-B
Ergebnis	<ol style="list-style-type: none"> Die Domain des neuen Messenger-Services wurde als Endpunkt im VZD-FHIR-Server eingetragen. Der Messenger-Service für die Organisation wurde erstellt. Für den beauftragten Mitarbeiter der Organisation (Org-Admin) wurde ein Account auf dem Messenger-Service mit Administrationsrechten erstellt.
Ausgangsdaten	Messenger-Service der Organisation, Account-Daten
Akzeptanzkriterien	6. ML-123648, 7. ML-123649, 8. ML-123650, 9. ML-123651

~~Für den Anwendungsfall wird die erfolgreiche Authentifizierung der Organisation mit Hilfe des Anwendungsfalles AF_10103 - Authentifizieren einer Organisation am TI-Messenger-Dienst von gemäß OpenID-Connect. Das Verfahren OIDC ausgesetzt. Die Komponente Messenger-Service für die Organisation wird im Anhang B beschrieben. Verlauf des Anwendungsfalles zu einem späteren Zeitpunkt erstellt.~~

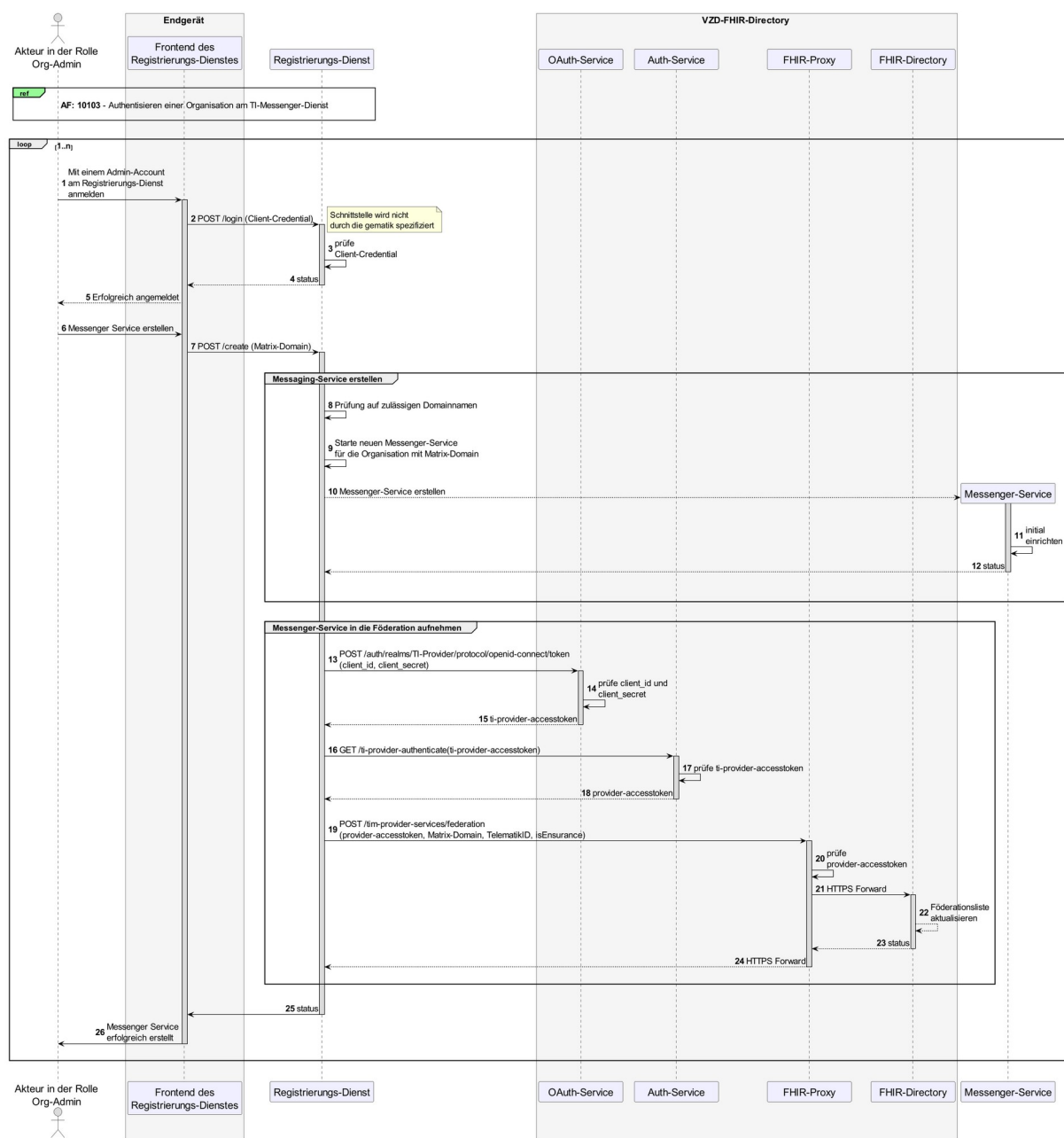


Abbildung 15: Laufzeitsicht - Bereitstellung eines Messenger-Service automatisch bereitstelle für eine Organisation

[<=]

Akzeptanzkriterien für den Anwendungsfall: Bereitstellung eines Messenger-Service –bereitstelle für eine Organisation (AF_10060)

ML-123648 - AF_10060 - Messenger-Service bereitstellen nur als NutzAkteur in der Rolle Org-Admin

Nur ein NutzeAkteur in der Rolle "Org-Admin" darf einen Messenger-Service automatisch bereitstellen. Es ist eine SMC-B-Karte für die Erstellung notwendig.

[<=]

ML-123649 - AF_10060 - Messenger-Service wurde erzeugt

Ein neuer Messenger-Service wurde mit dem gewählten Domainbezeichner erzeugt.

[<=]

ML-123650 - AF_10060 - Messenger-Service im VZD-FHIR-Directory existiert

Für den erzeugten Messenger-Service wurde ein neuer Eintrag im VZD-FHIR-Directory angelegt

[<=]

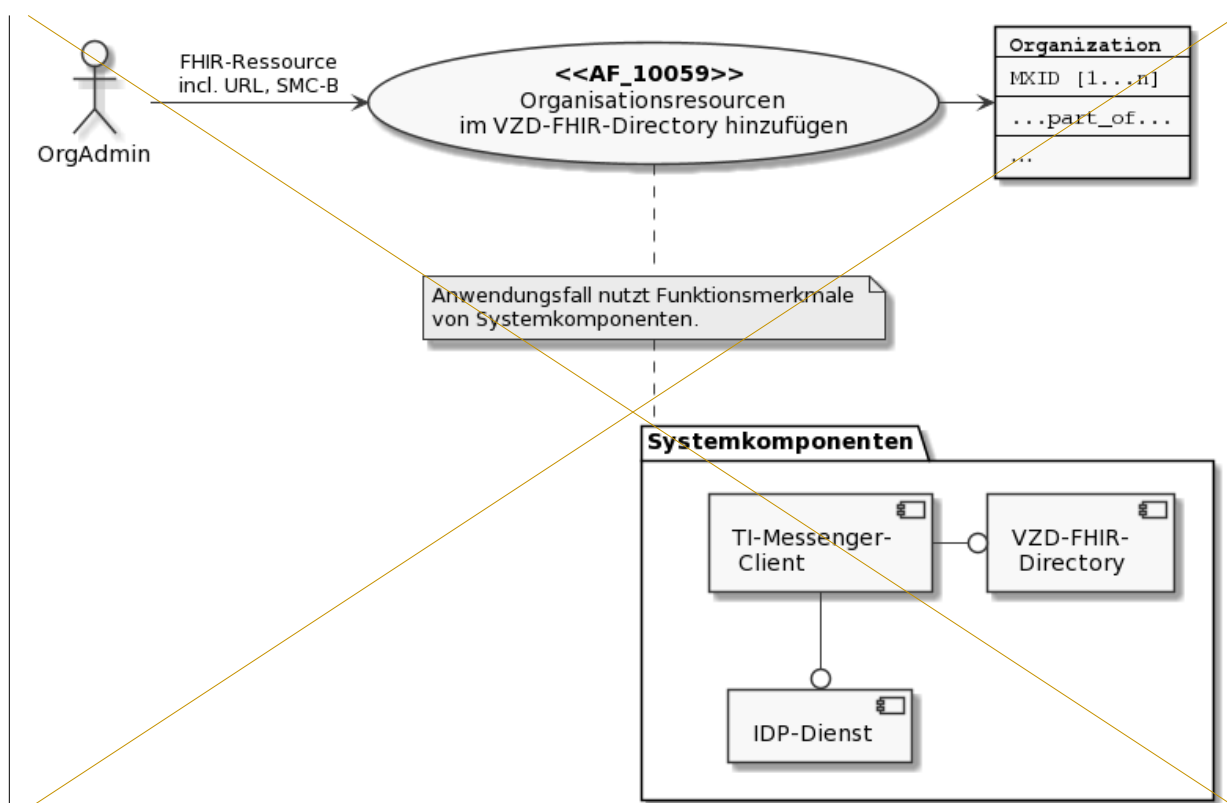
23651ML-12365132585 - AF_10060 - Org-Admin Administrator Account vorhanden

Der Nutzer in der Rolle Org-Admin TI-M Rohdatenerfassung und -lieferung Die Rohdaten wurden entsprechend der OrganisaRohdatendefinition hat einen Administrator Account aufgemäß [gemSpec_TI-Messenger-FD#Betrieb] für dem n TI- Messenger-Service seiner Organisation. Fachdienst erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet. [<=]

9.4 AF - Organisationsressourcen im VZD-FHIR-Directoryverzeichnisdienst hinzufügen

23518AF_10059-01 - Organisationsressourcen im VZD-FHIR-Directoryverzeichnisdienst hinzufügen

Mit diesem Anwendungsfall haben Organisationemacht ein Akteur in die Möglichkeit FHIR-Ressourcen mit MXIDs zu hinterlegen und damit für Nutzer dieser Rolle "Org-Admin" Akteure seiner Organisation im TI-Messenger-Dienstes kont für andere aktiereure auffindbar zu machen. Sound erreichbar. Dafür werden Endpoint-Ressourcen mit wird es- ermöglicht, dass Nutzer Anfragen an ihrer jeweiligen MXID im Organisationsverzeichnis (HealthcareService) des VZD-FHIR-Directory hinterlegt. Organisationen stellen können. Di mehrere FHIR-Ressourcen können orpro Organisation administrieren und somit eingehende Kommunikationsprozesse organisatorisch und thematisch strukturiert werden.



en (siehe [gemSpec_VZD_FHIR_Directory]).



Abbildungelle 1614: Systemkomponenten des AF - Organisationsressourcen im VZD-FHIR-Directoryverzeichnisdienst hinzufügen

<u>AF_10059</u>	<u>Organisationsressourcen im Verzeichnisdienst hinzufügen</u>
<u>Akteur</u>	<u>Beauftragter Mitarbeiter einer Organisation in der Rolle "Org-Admin"</u>
<u>Auslöser</u>	<u>Der Administrator der Organisation (Org-Admin) möchte seine Organisation erreichbar machen indem die MXIDs der Akteure der Organisation im VZD-FHIR-Directory hinterlegt werden.</u>
<u>Komponenten</u>	<ul style="list-style-type: none"> <u>TI-Messenger-Client (mit erweiterter Org-Admin Funktionalität).</u> <u>TI-Messenger Registrierungs-Dienst.</u> <u>Auth-Service.</u> <u>FHIR-Proxy.</u> <u>FHIR-Directory.</u>

<u>Vorbedingungen</u>	<p>7. <u>Für die Organisation wurde ein Messenger-Service bereitgestellt und es existiert ein Eintrag der Organisation im FHIR-Directory.</u></p> <p>8. <u>Der Administrator der Organisation verfügt über einen TI-Messenger-Client (mit erweiterter Org-Admin Funktionalität).</u></p> <p>9. <u>Es existiert eine Vertrauensbeziehung zwischen dem TI-Messenger Registrierungs-Dienst und dem VZD-FHIR-Directory (Übergabe des Zertifikates)</u></p> <p>10. <u>Der Administrator der Organisation wurde vom Registrierungs-Dienst authentifiziert.</u></p>
<u>Eingangsdaten</u>	<u>Org-Admin-Credentials, zweiter Faktor (*), FHIR-Organisations-Ressourcen</u>
<u>Ergebnis</u>	<u>FHIR-Organisations-Ressourcen aktualisiert, Status</u>
<u>Ausgangsdaten</u>	<u>Aktualisierte VZD-FHIR-Directory-Datensätze</u>
<u>Akzeptanzkriterien</u>	<u>  ML-123626,   ML-132586,   ML-138468</u>

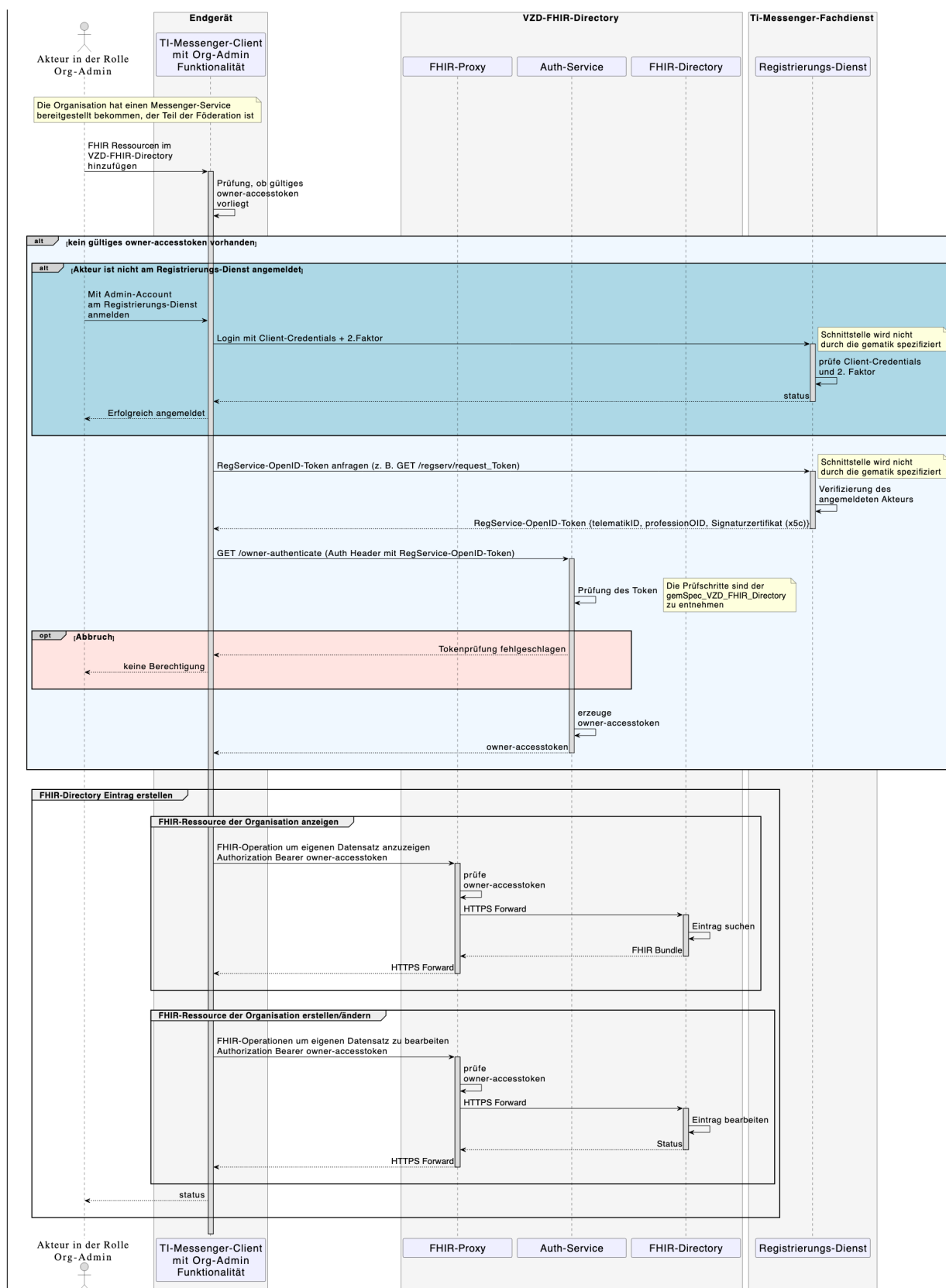
(*) Hinweis: Hinsichtlich des in der Tabelle 15 unter AF – Organisationsressourcen im VZD-FHIR-Directory hinzufügen

<u>AF_10059</u>	<u>Organisationsressourcen im VZD-FHIR-Directory hinzufügen</u>
<u>Akteur</u>	<u>Administrator der Organisation (In der Rolle Org-Admin)</u>
<u>Auslöser</u>	<u>Der Administrator der Organisation (Org-Admin) möchte seine Organisation erreichbar machen indem die Nutzer der Organisation als MXID im VZD-FHIR-Directory hinterlegt werden.</u>
<u>Komponenten</u>	<u>TI-Messenger-Client (mit erweiterter Org-Admin-Funktionalität), IDP-Dienst, VZD-FHIR-Directory</u>
<u>Vorbedingungen</u>	<p>1. <u>Der Administrator der Organisation verfügt über einen TI-Messenger-Client (mit erweiterter Org-Admin-Funktionalität).</u></p> <p>2. <u>Der VZD-FHIR-Directory-Server ist beim Smartcard-IDP-Dienst registriert.</u></p> <p>3. <u>Der Administrator der Organisation kann sich am Smartcard-IDP-Dienst authentisieren (Zugriff SMC-B).</u></p> <p>4. <u>Für die Organisation wurde ein Messenger-Service bereitgestellt und eine Ressource im VZD-FHIR-Directory angelegt.</u></p>

	5. Bei stationärer SMC-B erneute erfolgreiche PIN-Eingabe durch den Administrator der Organisation in der Rolle Org-Admin.
Eingangsdaten	FHIR-Organisations-Ressource mit Matrix-URL als Telecom, SMC-B
Ergebnis	Ressource-Organization (als "part_of" Beziehung) und MXID im FHIR-Server eingetragen
Ausgangsdaten	Aktualisierte VZD-FHIR-Directory-Datensätze
Akzeptanzkriterien	10  ML-123626, 11  ML-123627

"Eingangsdaten" genannten Zweitfaktors MÜSSEN die Sicherheitsempfehlungen des Bundesamt für Sicherheit in der Informationstechnik (BSI) gemäß [BSI 2-Faktor] berücksichtigt werden. Hierbei MUSS zur Resilienz gegen Angriffe aus der Ferne ein Verfahren gewählt werden, das mindestens mit "mittel" bewertet ist.

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Das Hierbei handelt es sich um eine Verfahren-ÖIDC wird im Anhang-B beschriebene einfache Laufzeitansicht in der zum Beispiel die TLS-Terminierung am FHIR-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde.



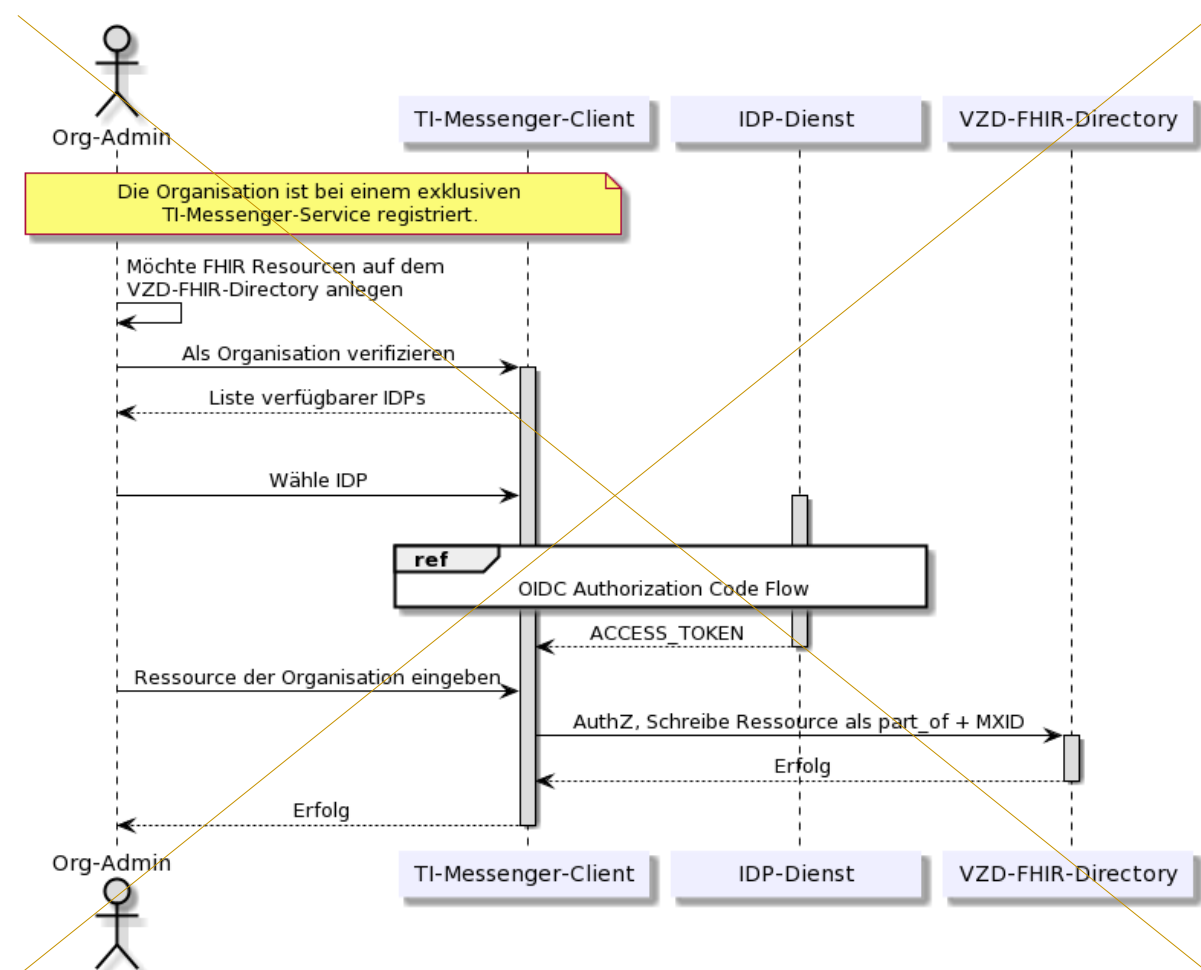


Abbildung 17: Laufzeitsicht - Organisations-Ressourcen im VZD-FHIR-Directoriesverzeichnisdienst hinzufügen

[<=]

Akzeptanzkriterien für den Anwendungsfall: Organisationsressourcen im VZD-Ferzeichnisdienst hinzufügen (AF_10059)

ML-123626 - AF_10059 - Änderungen nur für eigene Organization-FHIR-Directorieshinzu

Der Akteur in der "Rolle Org-Admin" darf nur FHIR-Ressourcen seiner eigenen Organisation (inklusive der Unterstrukturen) ändern. Ein Zugriff auf FHIR-Ressourcen, die nicht zu der eigenen Organisation gehören, MUSS unterbunden werden.

[<=]

ML-132586 - AF_10059}

- TI-M Rohdatenerfassung und -lieferung

Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet.

[<=]

23627ML-12362738468 - AF_10059 - Organisations-Ressourcen im VZD-FHIR-Directorieshinzu

Nach erfolgreicher Authentisierung an einem zugelassenen IDPm Registrierungs-Dienst als Administrator einer Organisation kann der NutzeAkteur in der Rolle "Org-Admin" sich einen RegService-OpenID-Token ausstellen lassen und die Matrix-User-URI (sen gegen einen owner-accesstoken beim VZD-FHIR-Directory eintauschen. Mit dem owner-accesstoken kann der Akteur die MXID in den FHIR eines Akteurs seiner Organisation-Datensatz unterhalb der HealthcareService-Ressourcen in einen Endpoint eintragen und Unterstruktur oder neue HealthcareService-Ressourcen für die Organisation anlegen. Der NutzeAkteur in der Rolle "Org-Admin" wird über den Erfolg der Operation informiert.

[<=]

Mai

9.5 AF - Anmeldung eines Akteurs am Messenger-Service

626ML-123626--AF_10059--7 - Anmeldung eines Akteurs am Messenger-Service

Mit diesem Anwendungsfall meldet sich ein Akteur an einem in der TI-Föderation zust ~~Änderungen~~ nigen Messenger-Service an und registriert seinen TI-Messenger-Client als Endgerät. Der Akteur für eigene Organization-FHIR-Datensätze Der Nutzer in MUSS die Matrix-Domain des gewünschten Messenger-Service direkt im TI-Messenger-Client eingeben können. Die Eingabe KANN dabei automatisiert oder durch andere Hilfsmittel wie beispielsweise durch ein QR-Code-Scan unterstützt werden. Die Authentifizierung erfolgt hierbei nach der Rollen Vorgaben der jeweiligen Org-Admin dar anisation. Nach der erfolgreichen Anmeldung eines Akteurs am Messenger-Service KÖNNEN die von ihm angebotenen Dienste verwendet werden.

Tabelle 16: Af-nu - Anmeldung eines Akteurs am Messenger-Service

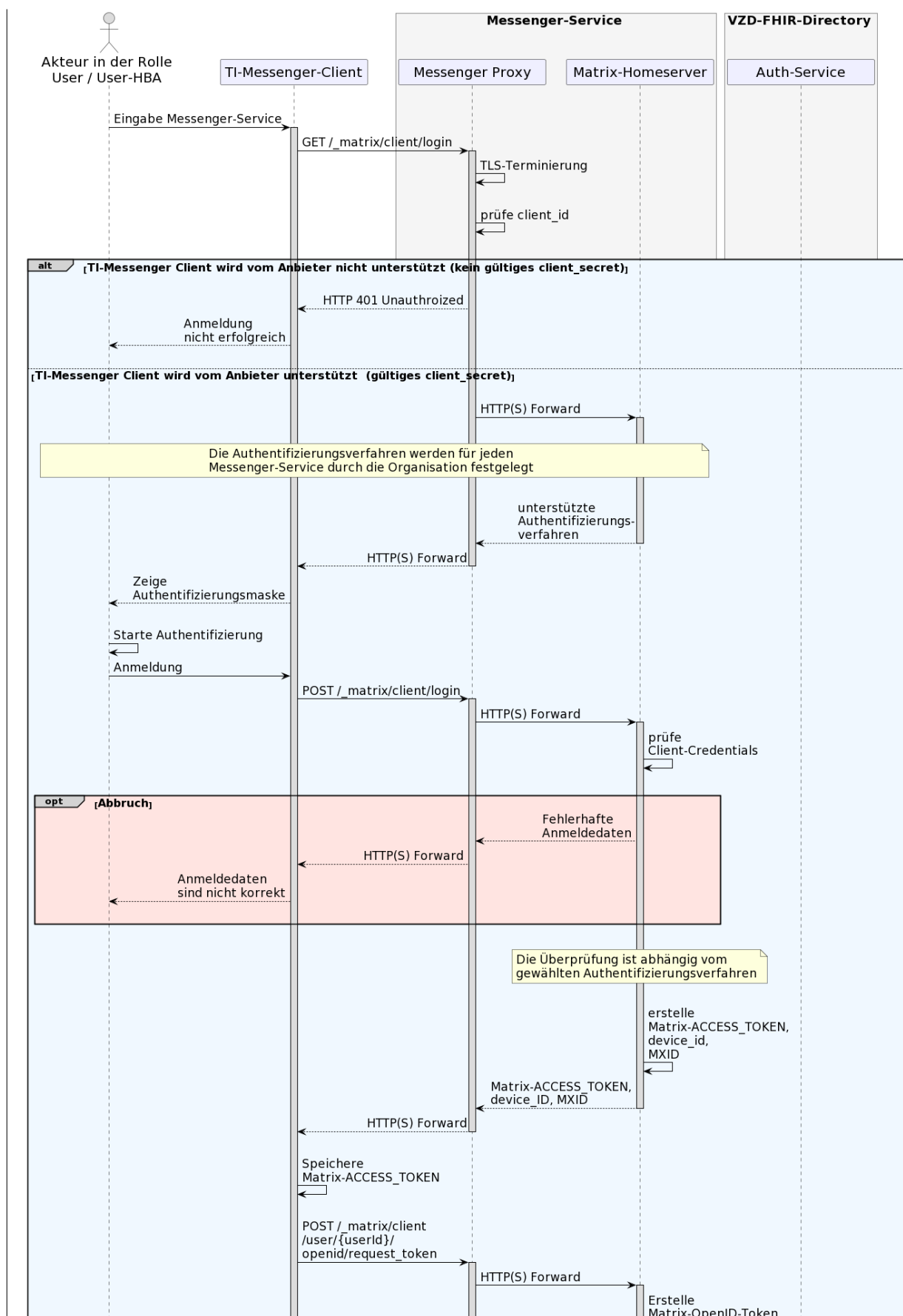
<u>AF_10057</u>	<u>Anmeldung eines Akteurs am Messenger-Service</u>
<u>Akteur</u>	<u>Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der "Rolle User / User-HBA"</u>
<u>Auslöser</u>	<u>Ein Akteur möchte sich mit seinem TI-Messenger-Client bei einem Messenger-Service anmelden.</u>
<u>Komponenten</u>	<ul style="list-style-type: none"> <u>TI-Messenger-Client.</u> <u>Messenger-Proxy.</u> <u>Messenger-Homeserver.</u> <u>FHIR-Proxy.</u> <u>FHIR-Directory.</u>
<u>Vorbedingungen</u>	<ol style="list-style-type: none"> <u>Der Akteur verfügt über einen vom Anbieter unterstützen TI-Messenger-Client.</u> <u>Der Akteur kennt die URL des Messenger-Services oder die URL ist bereits in seinem TI-Messenger-Client konfiguriert.</u> <u>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.</u>

	7. <u>Der verwendete Matrix-Homeserver ist in die Föderation integriert (valider Messenger-Service).</u>
<u>Eingangsdaten</u>	<u>URL des Matrix-Homeservers</u>
<u>Ergebnis</u>	<u>Es wurde ein TI-Messenger Account für einen Akteur in der Rolle "User / User-HBA" erzeugt.</u>
<u>Ausgangsdaten</u>	<u>Matrix-ACCESS_TOKEN, MXID, device_id Status</u>
<u>Akzeptanzkriterien</u>	<u>  ML-123571,   ML-123576,   ML-123575,   ML-129870,   ML-132587</u>

In der FHIR-Ressourcenlaufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den seiner eigenen Organisation (inklusive 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 Unterstrukturen) ändern.

[<=]Operation POST / matrix/client/register durchgeführt. Der Ablauf der Registrierung ist analog dem des Login-Verfahrens.

|



9.6 ~~Abbildung 18: Laufzeitsicht~~ - TI-Anmeldung eines Akteurs am Messenger-Remote-Invite

-Service

[<=]

Akzeptanzkriterien für den Anwendungsfall: Anmeldung eines Akteurs am Messenger-Service (AF_10057)

20ML-123571 - AF_10061 -- TI-57 - Akteur kann sich erfolgreich an einem gültigen Messenger-Remote-Invite

Nutzer haben die Mögl-Service anmelden

Ein Akteur hat sich erfolgreich an einem gültigen Messenger-Service angemeldet und mit einem zugelassenen Authentifizierungsverfahren erfolgreich authentisiert. Es MUSS sich innerhalbergestellt werden, dass die Anmeldung an Messenger-Services, die nicht Teil der Föderation des deutschen Gesundheitswesens zwischen sind, nicht möglich ist.

[<=]

ML-123576 - AF_10057 - Der Messenger-Service stellt dem TI-Messenger-Client ein Access-Token aus

Nach erfolgreicher Anmeldung hat der Messenger-Service dem TI-Messenger-Client ein Matrix-ACCESS_TOKEN ausgestellt.

[<=]

ML-123575 - AF_10057 - Speicherung Access-Token durch TI-Messenger-Client

Der TI-Messenger-Client speichert das ihm übergebene Matrix-ACCESS_TOKEN zur Verwendung in den folgenden Anwendungsfällen.

[<=]

ML-129870 - AF_10057 - Akteur kann sich an einen nicht validen Messenger-Services-Chatnachricht nicht anmelden

Ein Akteur kann sich nichten und andere durch bei einem öffentlichen Matrix-Homeserver anmelden, der nicht in die Matrix-SpezifikationTI-Föderation integriert ist.

[<=]

ML-132587 - AF_10057 - TI-M Rohdatenerfassung und -lieferung

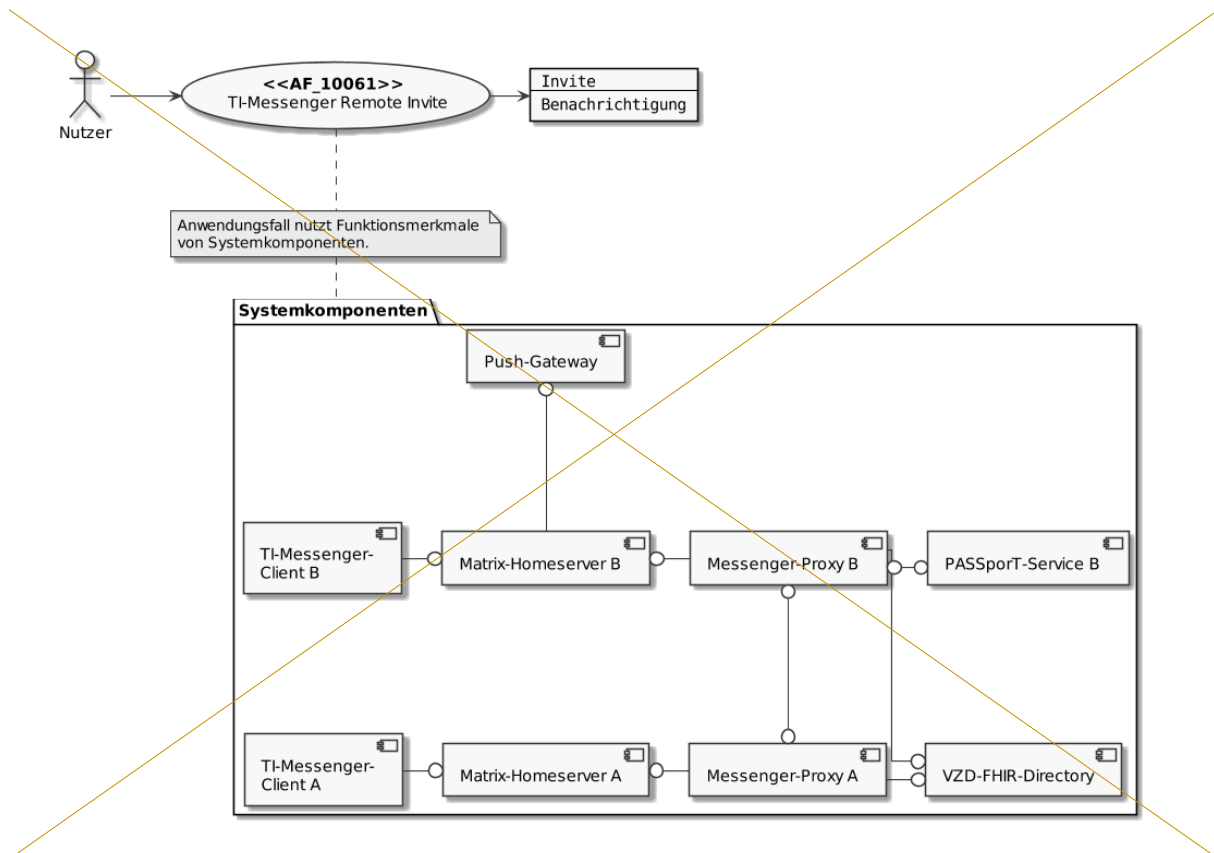
Die Rohdaten wurden entsprechend der Rohdatendefinition festgelegte Aktionen auszuführen. Dafür MUSS ein Chatraum zwischen den entsprechendgemäß [gemSpec_TI-Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet. [=<=]

9.7 AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen

AF_10058-01 - Akteur (User-HBA) im Verzeichnisdienst hinzufügen

Mit diesem Anwendungsfall wird ein Akteur in der Rolle "User-HBA" für andere Akteure anden-Parteier Messenger-Services auffindbar und erreichbar. Dafür werden entstehen. Dieser Ablauf zeigt, wie ein Chatraum zwifHIR-Ressourcen mit ihrer jeweiligen MXID im Personenverzeichnis (PractitionerRole) des VZD-FHIR-Directory hinterlegt. Zusätzlich

besteht die Möglichkeit die Sichtbarkeit für andere Akteure einzusuchen den Parteiränken. Dieser Anwendungsfall KANN direkt mit dem initialen entsteht.








Anmeldevorgang eines Akteurs am Messenger Service (siehe Anwendungsfall: 19AF_10057 - Anmeldung eines Akteurs am Messenger-Service-System) komponentebiniert werden. Hierfür wird der Akteur in des AF--r Rolle "User-HBA" während des Anmeldevorgangs durch den TI-Messenger Remote Invite-Client gefragt, ob dieser im Besitz eines HBAs ist.

Tabelle 17: AF - TI-MessengerAkteur (User-HBA) im Verzeichnisdienst hinzufügen

AF_10058	Akteur (User-HBA) im Verzeichnisdienst hinzufügen
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle "User-HBA"
Auslöser	Ein Akteur in der Rolle "User-HBA" möchte sich im Personenverzeichnis erreichbar machen, indem er seine MXID im seinen Practitioner-Datensatz im VZD-FHIR-Directory hinterlegt.
Komponenten	<ul style="list-style-type: none"> • TI-Messenger-Client, • Authenticator, • zentraler IDP-Dienst, • FHIR-Proxy,

	<ul style="list-style-type: none"> • <u>Auth-Service,</u> • <u>FHIR-Directory .</u>
<u>Vorbedingungen</u>	<p>6. <u>Der Akteur ist bei einem gültigen Messenger-Service angemeldet.</u></p> <p>7. <u>Der Akteur verfügt über einen zugelassenen TI-Messenger-Client.</u></p> <p>8. <u>Das VZD-FHIR-Directory ist beim zentralen IDP-Dienst registriert.</u></p> <p>9. <u>Der Akteur kann sich am zentralen IDP-Dienst authentisieren.</u></p>
<u>Eingangsdaten</u>	<u>HBA, FHIR-Practitioner-Ressourcen</u>
<u>Ergebnis</u>	<u>FHIR-Practitioner-Ressourcen aktualisiert, Status</u>
<u>Ausgangsdaten</u>	<u>aktualisierter Practitioner-Datensatz</u>
<u>Akzeptanzkriterien</u>	<u> ML-123612,  ML-123611,  ML-132588</u>

In der Remote-Laufzeitsicht sind die Invite

AF_10061	TI-Messenger Remote Invite
Akteur	Nutzer A, Nutzer B
Auslöser	Nutzer A möchte mit Nutzer B einen gemeinsamen Chatraum einrichten
Komponenten	TI-Messenger-Client Matrix-Homeserver VZD-FHIR-Directory PASSporT-Service Push-Gateway
Vorbedingungen	<ol style="list-style-type: none"> 1. Die Nutzer verfügen über einen TI-Messenger-Client 2. Die Nutzer kennen die URL ihres Matrix-Homeservers oder die URL ist bereits in ihren Clients konfiguriert. 3. Die Nutzer sind am Messenger-Services angemeldet (AF_10057) 4. Die verwendeten Matrix-Homeserver sind in die Föderation integriert.
Eingangsdaten	beabsichtigter Nachrichtenaustausch
Ergebnis	Nutzer A und Nutzer B sind beide in einem gemeinsamen Chatraum. Optional erfolgt eine Benachrichtigung von Nutzer B über die Einladung in den Chatraum.
Ausgangsdaten	keine
Akzeptanzkriterien	12  ML-123654, 13  ML-123659, 14  ML-123660, 15  ML-123661, 16  ML-123663

Interaktion: Es handelt sich um einen Prozess 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.

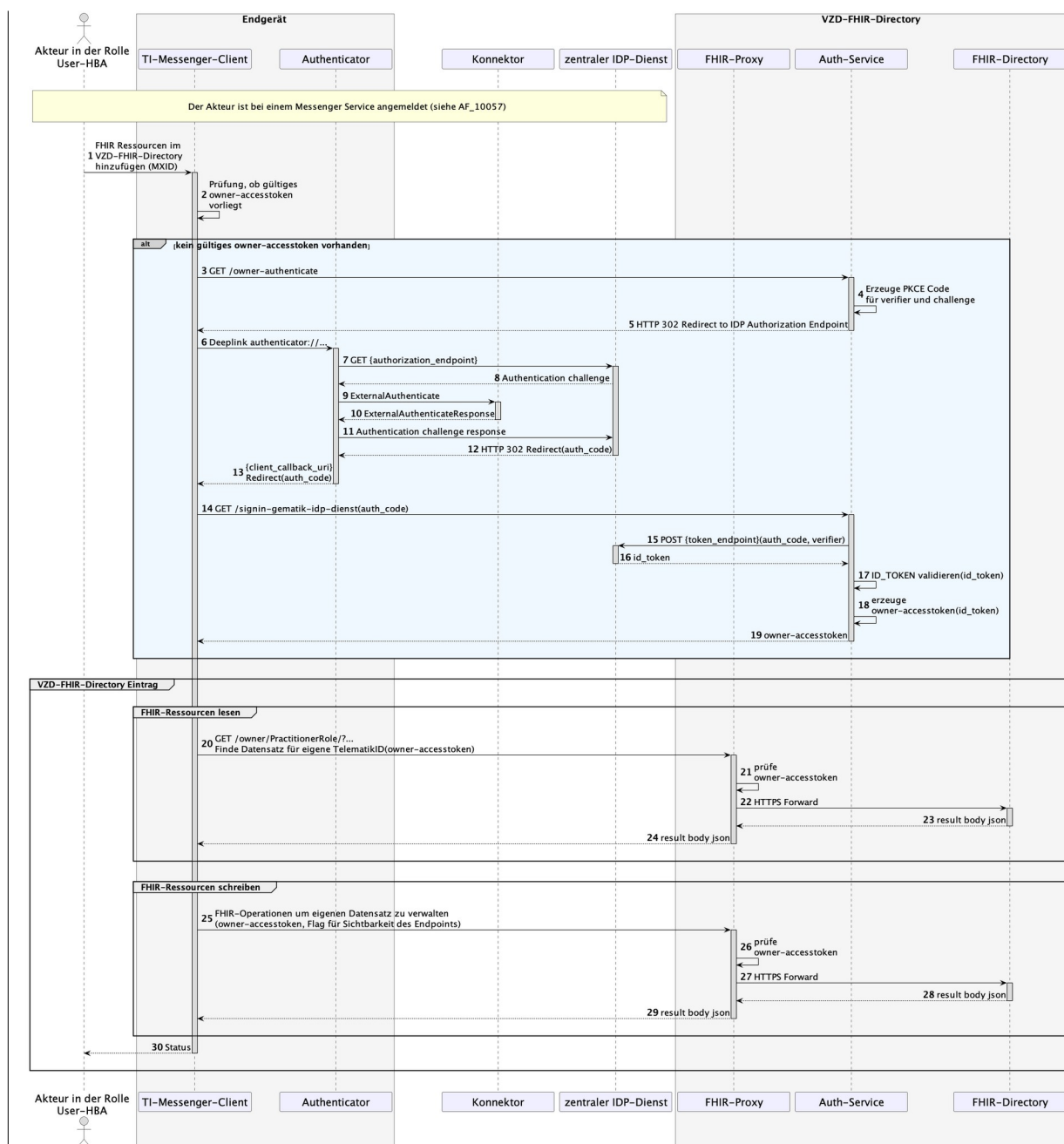


Abbildung 20: Laufzeitansicht wurde nicht betrachtet, dass dsicht - Akteur (User-HBA) im Verzeichnisdienst hinzufügen

[<=]

Akzeptanzkriterien für den Anwendungsfall: Akteur (User-HBA) im Verzeichnisdienst hinzufügen (AF_10058)

ML-123612 - AF_10058 - Akteur als Practitioner hinzufügen

Die MXID wurde in den Practitioner-FHIR-Datensatz eingefügt und der Akteur über den Erfolg informiert.

[<=]

ML-123611 - AF_10058 - MXID-Eintrag nur für eigenen Practitioner-FHIR-Datensatz

Der Akteur in der Rolle "User-HBA" darf nur ~~die Verbinde~~eigene FHIR-Ressourcen ändern. [\leq]

ML-132588 - AF_10058 - TI-M Rohdatenerfassung und -lieferung
~~Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-Messenger-FD#Betrieb] für den TI-Messenger-Client und Matrix-Homeserver über den Fachdienst erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet. [\leq]~~

9.8 AF - Föderationszugehörigkeit eines Messenger-Service prüfen

AF_10064-01 - Föderationszugehörigkeit eines Messenger-Proxy läuft. Ebenfalls Service prüfen

Dieser Anwendungsfall prüft gemäß der im Kapitel 3.5- Berechtigungskonzept festgelegten Kriterien für eine die Stufe 1 der Client-Server und Serververeinfachte Darstellung Server Kommunikation, ob ein Messenger-Service zugehörig zur TI-Messenger-Föderation ist und gilt für alle Anwendung ~~darauf verzichtet, dass es Fälle, welche die Matrix-Domain~~ eines Messenger-Services überprüfen müssen. Für die Prüfung der Zugehörigkeit der Matrix-Domain zur TI-Messenger-Föderation, verwendet der Messenger-Proxy ~~die eine Föderationsliste bei der, die vom Registrierungs-Dienst abrufen, welches~~ eines TI-Messenger-Fachdienstes bereitgestellt wird. Die Speicher ~~die~~ dauer der FöderationsListe ~~beim VZD-FHIR-Dire~~ des Messenger-Proxies ist limitiert. Die Aktualisierung der Föderationsliste erfolgt wie in Anhang 8.2- Aktualisierung der Föderationsliste beschrieben.

Tabelle 18: Föderationszugehörigkeit eines Messenger-Service prüfen

<u>AF_10064</u>	<u>Föderationszugehörigkeit eines Messenger-Service prüfen</u>
<u>Akteur</u>	=
<u>Auslöser</u>	<u>Der Messenger-Proxy empfängt oder sendet ein Matrix-Event und MUSS die im Request enthaltenen MXIDs auf Domain-Zugehörigkeit zur TI-Messenger-Föderation prüfen.</u>
<u>Komponenten</u>	<ul style="list-style-type: none"> • <u>Messenger-Proxy,</u> • <u>Matrix-Homeserver.</u>
<u>Vorbedingungen</u>	<u>keine</u>
<u>Eingangsdaten</u>	<u>Matrix-Event</u>
<u>Ergebnis</u>	<u>Der Messenger-Proxy ermittelt mittels der Föderationsliste, ob die Matrix-Domain des anderen Messenger-Service Teil der TI-Messenger-Föderation ist.</u>
<u>Ausgangsdaten</u>	<u>Status vom Matrix-Homeserver und Weiterleitung</u>
<u>Akzeptanzkriterien</u>	<u> ML-123672,  ML-123891,  ML-132589,  ML-137902</u>

In der Laufzeitsicht sind zur Verfügung die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Der Abruf des auslösenden Matrix-Event am Messenger-Proxy wird in der folgenden Abbildung nicht gezeigt. Die Aktualisierung der Föderationsliste ist in AF-6.8 – ~~Check remote domain~~ – hang 8.2- Aktualisierung der Föderationsliste hinreichend beschrieben.

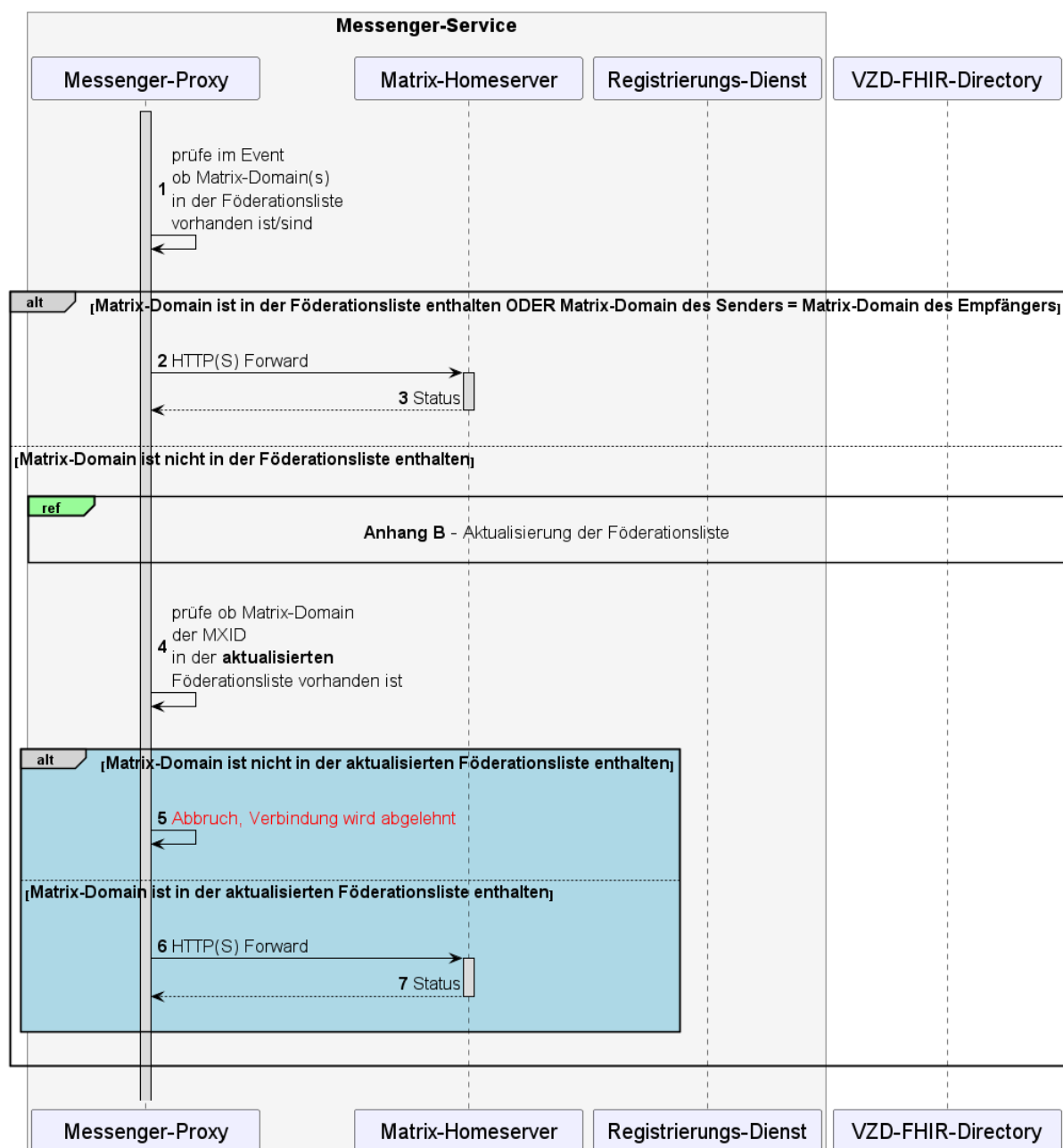


Abbildung 21: Laufzeitsicht - TI- Föderationszugehörigkeit eines Messenger-Remote Invite-Service prüfen

[<=]

Akzeptanzkriterien für den Anwendungsfall: TI- Föderationszugehörigkeit eines Messenger-Remote Inviter-Service prüfen (AF_10061)

4)

54ML-12365472 - AF_100614 - Suche iFöderationsliste vom VZD-FHIR-Directory Ein abrufen

Der Registrierungs-Dienst des TI-Messenger-GIFachdienst kannstes MUSS die Föderationsliste erfolgreich im vom FHIR-Proxy des VZD-FHIR-Directory nach einem Chatpartner suchabrufen.

[<=]

659ML-123659891 - AF_100614 - PASSporT-Übergabe

PASSporT-wuMatrix-Domain Teil der Föderationsliste & Aktualitätscheck
Es MUSS sichergestellt werde-erfolgreich ann, dass der Registrierungs-Dienst die Föderationsliste auf Aktualität überprüft, bevor eine aktualisierte Liste durch den Messenger-Proxy übergeabgerufen werden kann. Eben,enthäfalls MUSS sichergestellt alle benötigten Inforwerden, dass der Messenger-Proxy tatsächlich überprüft, ob die mationrix-Domain des anderen und ist auswertbarMessenger-Service Teil der Föderationsliste ist.

[<=]

23660ML-12366032589 - AF_100614 - Invite nur mit PTI-M RohdatenerfASSporT

Im Invite-Request steht das PASSporT anung und -lieferung
Die Rohdaten wurden entsprechend der richtigen Stelle und kann vom Meohdatendefinition gemäß [gemSpec_TI-Messenger-Proxy ausgewertet werden.

[<=]

Ein Beispiel FD#Betrieb] für einen Invite-Requeden TI-Messenger-Fachdienst ierfolgreich erfasst im Dokument [gemSpec_TI-Messenger-FD] im Kapitel "Messenger Proxy" zu fiund an die definierte Schnittstelle der Rohdatenerfassung versenden.

t.

[<=]

23661ML-12366137902 - AF_100614 - Aktualität - Föderationsliste Messenger-Proxy prüft P

Es MUSS sichergestellt werden, dASSporT-auf Gültigkeit
Der M die Föderationsliste vom Messenger-Proxy lehntaktuell ist, das Invite bei ungültigem PASSporT ab.

[<=]

Mainfür MUSS der Messenger-Proxy in e_OPB1/ML-123663ML-123663 - AF_10061 - Nutzer sind dem Chatraum beigetreten

Am festen Intervall von einmal pro Stunde eine aktuelle Chat-Parteien sind erfolgreich im Chatraum vorhandeListe beim Registrierungs-Dienst anfordern.

[<=]

9.9 AF - ~~Message senden (Remote)~~ Einladung von Akteuren innerhalb einer Organisation

~~23521 AF_10062104-01 - Message senden (Remote) Einladung von Akteuren innerhalb einer Organisation~~

~~In diesem Anwendungsfall setzt wird ein erfolgreicher Invite-Akteur der zu einer gemeinsamen oder mehrerer beteiligter Nutzer vorsamen Organisation gehört in einen Raum eingeladen um Aktionen aus und zu führt den eigentli. Für die Suchen-Nachrichtenaustausch durch. Die beteiligt von Akteuren innerhalb einer gemeinsamen Nutzer sind mit Organisation durchsucht ein TI-Messenger-Clients-Mitglied das Nutzerverzeichnis seiner Organisation auf des Chm Matraux-Homes und auf unterschiedlichenerver. In diesem Anwendungsfall prüft der Messenger-SProxy gemäß Kapitel 3.5- Berechtigungskonzept der services- Client-Serverteilt.~~

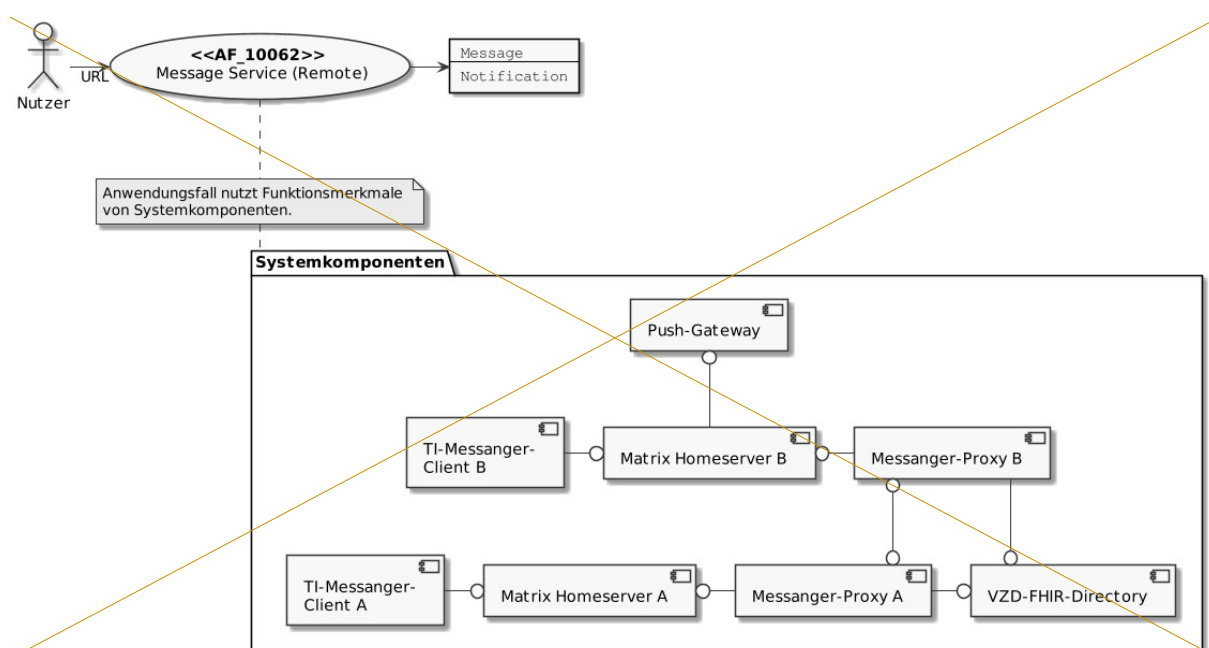







Abb Kommunikation 22: on, ob Systemkomponenten des AF -- Message senden (Remote)

Tabelle 19 die im Invite-Event enthaltenen Matrix-Domains Teil der TI-Föderation sind.
Ist dies der Fall erfolgt die Weiterleitung an den AF--Matrix-HomeMessage-senden
(Remote)

AF_10062	Message-senden (Remote)
Akteur	Nutzer A, Nutzer B
Auslöser	Nutzer A möchte eine Chatnachricht an Nutzer B (föderierter Matrix-Homeserver) versenden
Komponenten	TI-Messenger-Client A + B Matrix-Homeserver A + B Messenger-Proxy A + B Registrierungs-Dienst VZD-FHIR-Directory Push-Gateway
Vorbedingungen	6. Beide Nutzer sind Mitglied eines gemeinsamen Raumes. 7. Es liegt eine aktualisierte Föderationsliste vor. 8. Die Messenger-Proxys überprüfen die Remote-Domain (siehe AF 6.8)
Eingangsdaten	Chatnachricht
Ergebnis	Nutzer B erhält Chatnachricht von Nutzer A; optional erfolgt eine Benachrichtigung von Nutzer B über eine neue Nachricht
Ausgangsdaten	Chatnachricht erreicht Nutzer B
Akzeptanzkriterien	17.  ML-123665, 18.  ML-123666, 19.   ML-123667, 20.  ML-123668

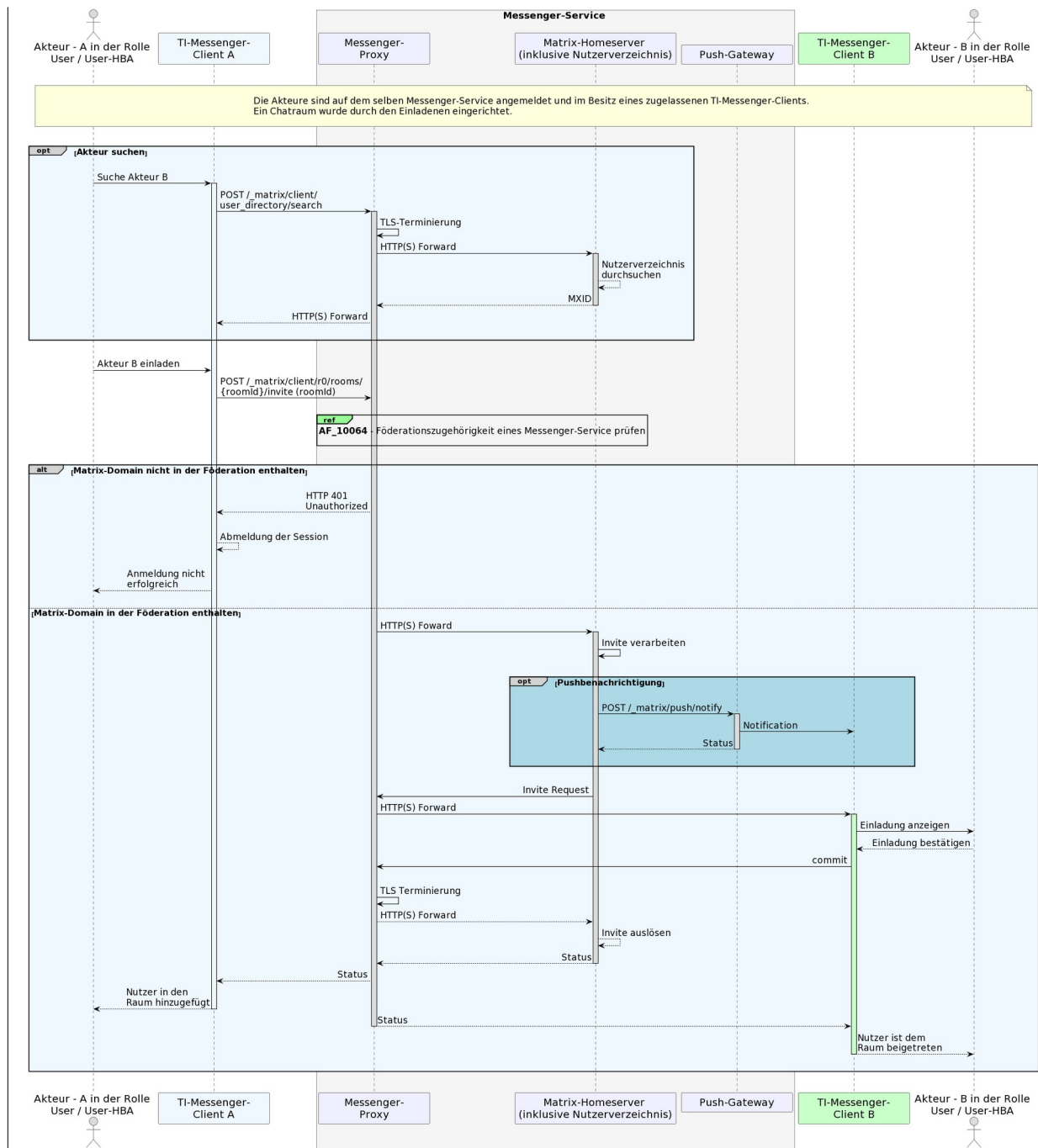
Hervor des Einladenden. Dieser prüft ob die beteiligten Akteure bei ihm registriert
sinweis: d. Ist dies nicht der Fall, handelt es sich hierbei um eine**verz**uladenden
Akteur nicht um **einfachte-Laufzeitansicht**. Bei einem Akteur innerhalb der Organisation
und das Invite-Event wird für die externe Zustellung weitergeleitet. der
LaufAnwendungsfall AF_10061 - Einladung von Akteuren außerhalb einer
Organisation **zeitangt** den **sicht-wurde** daraus ergebenden Verlauf.

Tabelle 20: Ein**nicht betrachtet,ladung von Akteuren innerhalb einer Organisation**

AF_10104	Einladung von Akteuren innerhalb einer Organisation
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle "User / User-HBA"

<u>Auslöser</u>	<u>Akteur A möchte Akteur B seiner Organisation in einen gemeinsamen Raum einladen.</u>
<u>Komponenten</u>	<ul style="list-style-type: none"> • <u>TI-Messenger Client A + B,</u> • <u>Messenger-Proxy,</u> • <u>Matrix-Homeserver,</u> • <u>Push-Gateway.</u>
<u>Vorbedingungen</u>	6. <u>Die Akteure sind am selben Messenger-Service angemeldet.</u> 7. <u>Jeder Akteur hat einen zugelassenen TI-Messenger-Client.</u> 8. <u>Ein Chatraum wurde durch den Einladenden eingerichtet.</u>
<u>Eingangsdaten</u>	<u>Invite-Event</u>
<u>Ergebnis</u>	<u>Akteur A und Akteur B sind beide in einem gemeinsamen Chatraum.</u> <u>Optional erfolgt eine Benachrichtigung an Akteur B über die Einladung in den Chatraum.</u>
<u>Ausgangsdaten</u>	<u>Status</u>
<u>Akzeptanzkriterien</u>	 <u>ML-123896,</u>  <u>ML-129415,</u>  <u>ML-129414,</u>  <u>ML-132590</u>

In der Laufzeitsicht sind die ~~Verbindung~~Interaktionen zwischen TI-Messenger-Client- und Matrix-Homeservden Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Der ~~über~~ für den Messenger-Proxy läuft. Ebenfallsie zukünftige Kommunikation genutzte Chatraum wurde für eine vereinfachte Darstellung den einladenden Akteur bereits erstellt. darauf verzichtet, dass der her wird in diesem Anwendungsbeispiel ein /_matrix/client/v3/rooms/{roomId}/invite Event am Messenger-Proxy geprüft. die Föderationsliste bei der Registrierung folgende Darstellung zeigt lediglich die Einladung zwischen zwei Akteuren. Weitere Akteure können unabhängig von Dienst abrufen, welcher die Liste beim VZD-FHIR-Directory abrufen und zur Verfügung stellt. In der Laufzeitsicht eingeladen werden (Hinweis: Group-Messaging). Für die vereinfachte Darstellung wird vorausgesetzt, dass die TI-Messenger-Clients der Abruf der Föderationsliste ist in AF 6.8 – Check remote domain hinreichend beschriebenen Akteure online sind. Ebenfalls wird davon ausgegangen, dass beide Akteure am selben Matrix-Homeserver registriert sind.



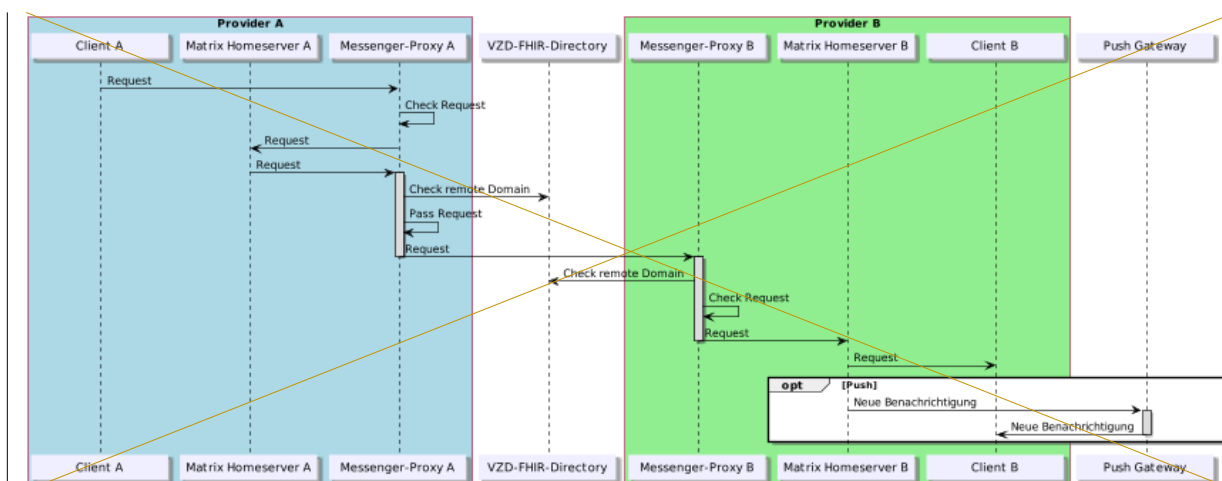


Abbildung 23: Laufzeitsicht – Message-senden (Remote) Einladung von Akteuren innerhalb einer Organisation

[<=]

Akzeptanzkriterien für den Anwendungsfall: Message-senden Einladung von Akteuren innerhalb einer Organisation (AF_10062)

104)

665ML-123665896 - AF_10062104 - Messenger-Proxy des Senders prüft Domainmatrix-Homeserver nach Akteuren des Empfängers

Der TI-Messenger-Proxy des Senders prüft die Domain des Empfängers auf Zugehörigkeit zur TI-Client zeigt eine Liste aller Akteuren eines Matrix-HoMessenger-Föderationservers an.

[<=]

3666ML-1236669415 - AF_10062104 - Messenger-Proxy des Empfängers prüft Domain des Senders TI-Föderationszugehörigkeit

Der Messenger-Proxy des Empfängers prüft die Domain des Senders auf Zugehörigkeiten Invite-Event ab, wenn die Matrix-Domain nicht zur TI-Messenger-Föderation gehört.

[<=]

3667ML-1236679414 - AF_10062104 - Auslösen einer Notifikation

Der Akteure sind dem Chatmatrix-Homeserver des Empfängers löst eine Benachrichtigung des Messenger-Clients über sein Push-Gateway aus. Alle Chat-Parteien sind erfolgreich im Chatraum vorhanden.

[<=]

23668ML-12366832590 - AF_10062 - Nachricht wird angezeigt

Die 104 - TI-M Rohdatenerfassung und -lieferung

Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich dem Empfänger im gemeinsamen Raum angezeigt.

erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet. [=>]

9.10 AF - ~~Messenger-Service (Lokal)~~Austausch von Events zwischen Akteuren innerhalb einer Organisation

AF_10063 - ~~Messenger-Service (Lokal)~~

~~Nutz~~**Austausch von Events zwischen Akteuren innerhalb einer Organisation**
~~Dieser haben die Anwendungsfall~~erMöglichkeit es Akteuren, welche sich inner einem gemeinsamen Raum innerhalb eines Messenger-Services-Chatn befinden, Nachrichten auszutauschen und ~~andeweitere~~ durch die Matrix-Spezifikation festgelegte Aktionen (Events) auszuführen. ~~Zum Starten eines Ch~~

Tabelle 21: ~~ats durchsuchen Nutzer mit Hilfe des TI-Messenger-Clients das Nutzerverzeichnis eines Matrix-Homeservers. Dabei liegt folge~~austausch von Events zwischen Akteuren innerhalb einer Organisation

<u>AF_10063</u>	<u>Austausch von Events zwischen Akteuren innerhalb einer Organisation</u>
<u>Akteur</u>	<u>Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle "User / User-HBA"</u>
<u>Auslöser</u>	<u>Alle Matrix-Events die innerhalb eines Messenger-Service einer Organisation ausgeführt werden</u>
<u>Komponenten</u>	<ul style="list-style-type: none"> <u>TI-Messenger Client A + B,</u> <u>Messenger-Proxy,</u> <u>Matrix-Homeserver,</u> <u>Push-Gateway.</u>
<u>Vorbedingungen</u>	5. <u>Die Akteure sind am selben Messenger-Service angemeldet.</u> 6. <u>Jeder Akteur hat einen zugelassenen TI-Messenger-Client.</u> 7. <u>Die Teilnehmer sind einem gemeinsamen Raum beigetreten.</u>
<u>Eingangsdaten</u>	<u>Matrix-Event</u>
<u>Ergebnis</u>	<u>Matrix-Event wurde erfolgreich verarbeitet</u>
<u>Ausgangsdaten</u>	<u>Abhängig vom Matrix-Event</u>
<u>Akzeptanzkriterien</u>	 <u>ML-123669</u> ,  <u>ML-123670</u> ,  <u>ML-132591</u>

In der Ablauf vor:

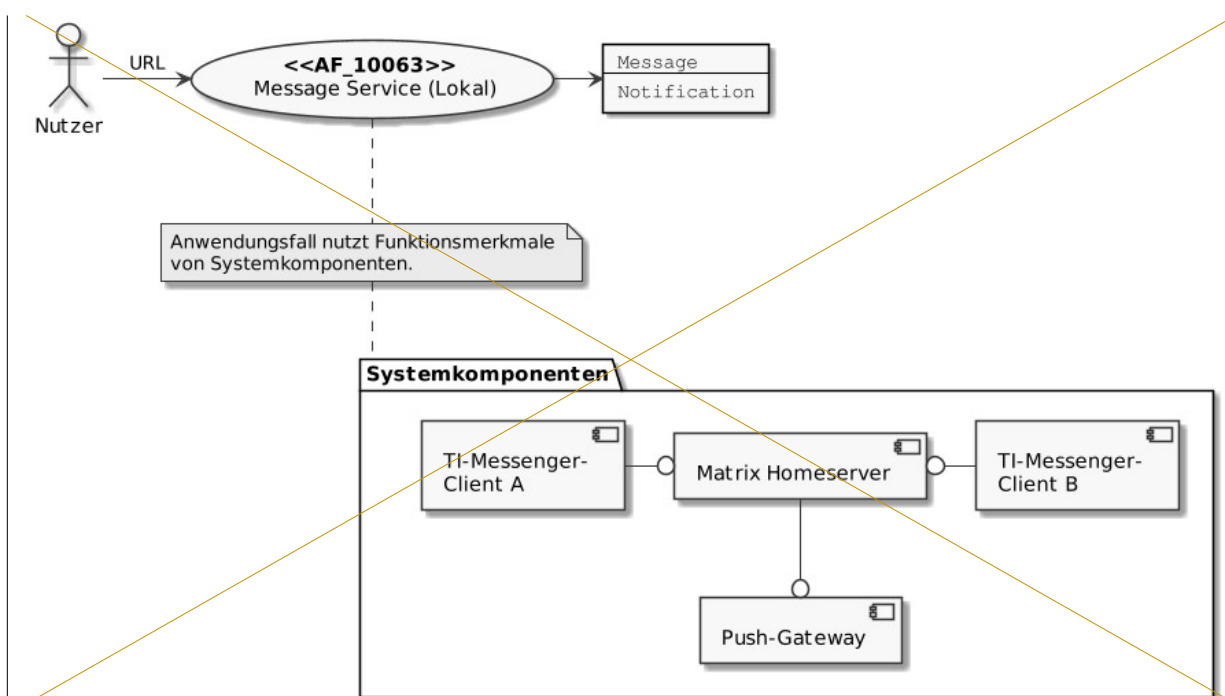




Abbildung 24: Aktionen zwischen Systemkomponenten des AF-Messenger-Service (Lokal)

Tabelle 22-M, die durch den Anwendungsfall genutzt wird: Messenger-Service (Lokal)

AF_10063	Messenger Service (Lokal)
Akteur-	Nutzer A, Nutzer B
Auslöser	Beispiel: Nutzer A versendet eine Chatnachricht an Nutzer B auf dem selben Matrix-Homeserver
Komponenten	TI-Messenger-Client A + B Matrix-Homeserver Push-Gateway
Vorbedingungen	Beispiel: Beide Nutzer sind Mitglied eines gemeinsamen Raumes
Eingangsdaten	Beispiel: Chatnachricht
Ergebnis	Beispiel: Client Nutzer B erhält Chatnachricht von Nutzer A; optional erfolgt eine Push-Benachrichtigung von Nutzer B über den Eingang einer neuen Nachricht
Ausgangsdaten	Beispiel: Chatnachricht erreicht Client Nutzer B
Akzeptanzkriterien	21  ML-123669, 22  ML-123670, 23 

~~ML-123896~~

reden, dargestellt. Hinweis: Es erbei handelt es sich hierbei um eine vereinfachte Laufzeitansicht – in der zum Bei der Lspiel die TLS-Terminierung am Messenger-Proxy aufzeiten Grund der Übersicht-wurdlichkeit nicht betrachtet, dassrücksichtigt wurde. die Verbinin der Abbildung zwischen TI-Messenger-Client und rot dargestellten Linien symbolisieren den Kommunikationsverlauf des auslösenden Matrix-HomeserRequest. Für die ver-über den-einfachte Darstellung wird vorausgesetzt, dass die TI-Messenger-Proxy-läuft Clients der beteiligten Akteure online sind.

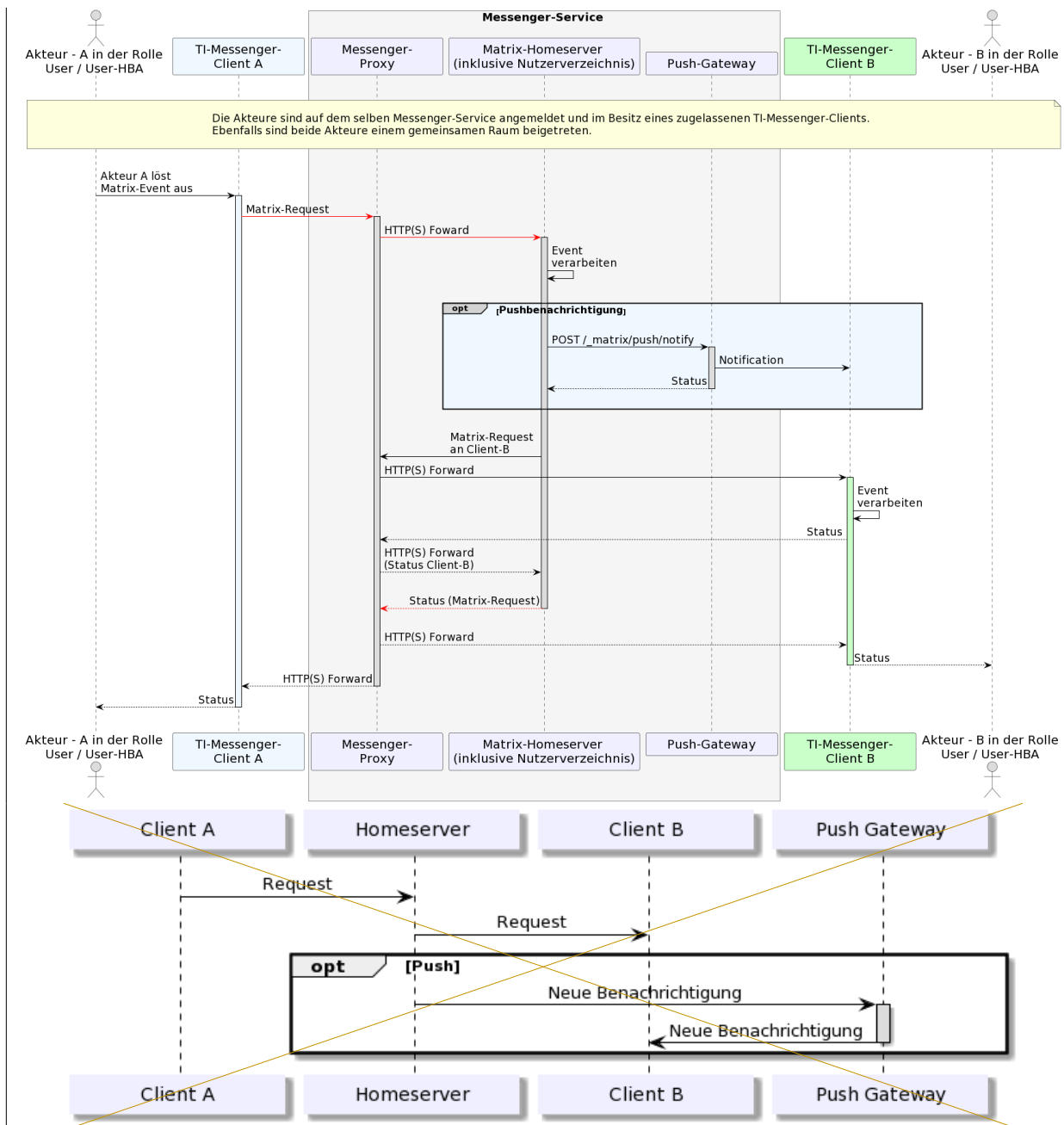


Abbildung 25: Laufzeitsicht - Messenger Service (Lokal) Austausch von Events zwischen Akteuren innerhalb einer Organisation

[<=]

Akzeptanzkriterien für den Anwendungsfall: Messenger-Service (Lokal) Austausch von Events zwischen Akteuren innerhalb einer Organisation (AF_10063)

ML-123670 - AF_10063

- Chatnachricht wird verarbeitet

Eine Chatnachricht vom TI-Messenger-Client A an TI-Messenger-Client B wurde vom Matrix-Homeserver erfolgreich verarbeitet.

[<=]

ML-123669 - AF_10063 - Auslösen einer Benachrichtigung

Der Matrix-Homeserver löst eine Benachrichtigung des TI-Messenger-Clients vom Empfänger über das mit dem TI-Messenger-Client verbundene Push-Gateway des TI-Messenger-Anbieters aus.

[<=]

23896ML-12389632591 - Matrix-Homeserver nach Nutzern durchsuchen

Der TI-Messenger-Client zeigt eine Liste aller AF_10063 - TI-M Rohdatenerfassung und -lieferung

Die Rohdaten wurden entsprechend der Nutzer eines Matrix-Homeservers an-

[<=]

Mainline_OPB1/ML-123670ML-123670 - AF_10063 - Chatnessenger-FD#Betrieb] für den TI-Messenger-Fachricht wird angezeigt

Die Chatnachricht wurde erfolgreich erfasst und an die dem TI-Messenger-Client zugeordnete Schnittstelle und wird im TI-Messenger-Client angezeigt der Rohdatenerfassung versendet.

[<=]

9.11 AF - Check remote DomainEinladung von Akteuren außerhalb einer Organisation

23523AF_100641-01 - Check remote Domain

FürEinladung von Akteuren außerhalb einer Organisation

In die Prüfung Anwendung der Zugehörigkeit dsfall wird ein Akteur außerhalb einer Domain zu der TI-Messenger-FöOrganisation eingeladen. Für die Suche von Akteuren außerhalb der Organisation wird durch den Registrierungs-DienKANN das VZD-FHIR-Directory verwendet werden. Ist die MXID des TI-Messenger-Fachdienstes gesucht Akteurs dort nicht vorhanden MUSS eine tas die Möglich-aktualisierte Föderationsliste vom VZD-FHIR-Directory geladkeit geben, die Kontaktaufnahme auch auf andere Wege zu ermöglichen. Der Messenger-Proxy eines Messenger-Services nutzt diese für die PrüfungEs MUSS mindestens die Kontaktaufnahme mit Hilfe eines QR-Code Scans angeboten werden. Weitere Optionen zur Eingabe der Remote-Domain. Die Speicherdauer der Födera MXID (z. B. manuelle Eingabe) sind zulässig. Im Gegensatz zu einer Einladung von Akteuren innerhalb einer Organisationss (siehe AF_10104 -

Einladung von Akteuren innerhalb einer Organisation), prüfte des in diesem Anwendungsfall der Messenger-Proxies ist limitiert. Die zusätzlich die im Kapitel 3.5-Berechtigungskonzept fe-Struktur-diestgelegten Kriterien der Server-ser-Föderver Kommunikationsliste wird in [gemSpec_VZD_ (Stufe 1 - 3).

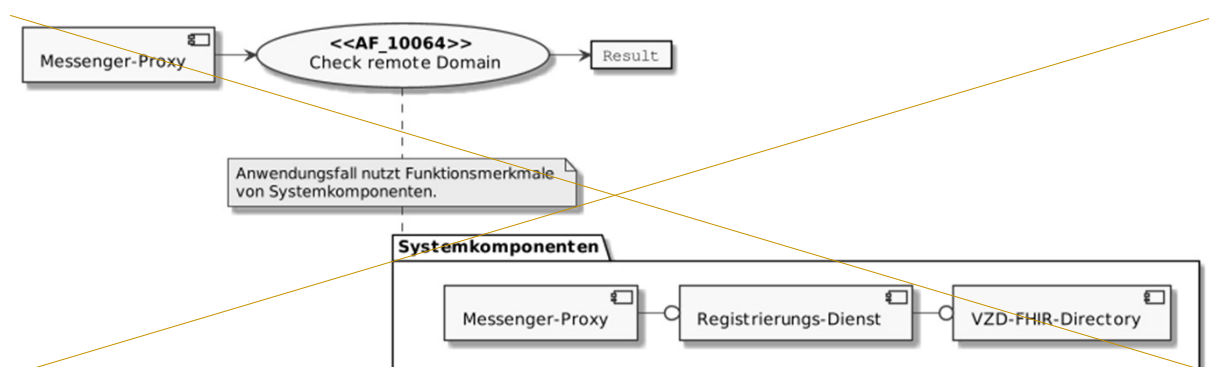
Tabelle 23 AFHIR_Directory] beschrieben. Für die Prüfu - Einladung von Akteuren außerhalb einer Organisation

<u>AF_10061</u>	<u>Einladung von Akteuren außerhalb einer Organisation</u>
<u>Akteur</u>	<u>Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der "Rolle User / User-HBA"</u>
<u>Auslöser</u>	<u>Akteur A möchte mit Akteur B außerhalb einer Organisation einen gemeinsamen Chatraum einrichten.</u>
<u>Komponenten</u>	<ul style="list-style-type: none"> <u>TI-Messenger Client A + B,</u> <u>Messenger-Proxy A + B,</u> <u>Matrix-Homeserver A + B,</u> <u>VZD-FHIR-Directory,</u> <u>Push-Gateway B.</u>
<u>Vorbedingungen</u>	<ol style="list-style-type: none"> <u>Die Akteure verfügen über einen zugelassenen TI-Messenger-Client.</u> <u>Die Akteure kennen die URL ihres Messenger-Service oder die URL ist bereits in ihren TI-Messenger-Clients konfiguriert.</u> <u>Die Akteure sind am Messenger-Services angemeldet</u> <u>Die verwendeten Messenger-Services sind Bestandteile der TI-Messenger-Föderation.</u>
<u>Eingangsdaten</u>	<u>Invite-Event</u>
<u>Ergebnis</u>	<u>Akteur A und Akteur B sind beide in einem gemeinsamen Chatraum.</u> <u>Optional erfolgt eine Benachrichtigung an Akteur B über die Einladung in den Chatraum.</u>
<u>Ausgangsdaten</u>	<u>Status</u>
<u>Akzeptanzkriterien</u>	<u> ML-123654,  ML-123663,  ML-132864,  ML-132592</u>

Ing durch den Messenger-Proxy gilt der Laufzeitsicht sind die Interaktionen zwischen der folgende Ablauf. Der Ablauf gilt für allen Komponenten, die durch den Anwendungsfälle,all genutzt welche die Remote-Domain überprüfen.

Ist die zu überprüfende Domain nrdn, dargestellt. Hierbei handelt es um eine vereinfachte Laufzeitsicht Teilin der Föderationsliste, MUSS derzum Beispiel die TLS-

Terminierung am Messenger-Proxy zunächst eine aktualisierte Version der Liste auf Grund der Übersichtlichkeit nicht berücksichtigt wurde. Ebenfalls wurde für eine vereinfachte vom Registrierungs-Dienst abfragen. Sollte der Messenger-Proxy ein darauf verzichtet eine eventuell notwendige Aktualisierung der Föderationsliste abfragen, MUSS der Registrierungs-Dienst überprüfen, ob die vorhandene zu zeigen. Der Abruf der Föderationsliste aktuell ist und im Anhang 8.2- Aktualisierung der Föderationsliste hier gegenreichend beschrieben falls aktualisieren, bevor. Die einzelnen Prüfschritte die der Messenger-Proxy für die neue Liste zurückgelegten Kriterien (Stufe 2 - 3) der Server-Server Kommunikation durchführt, sind im Anhang 8.3- Stufen der Berechtigungsprüfung zu finden wird.

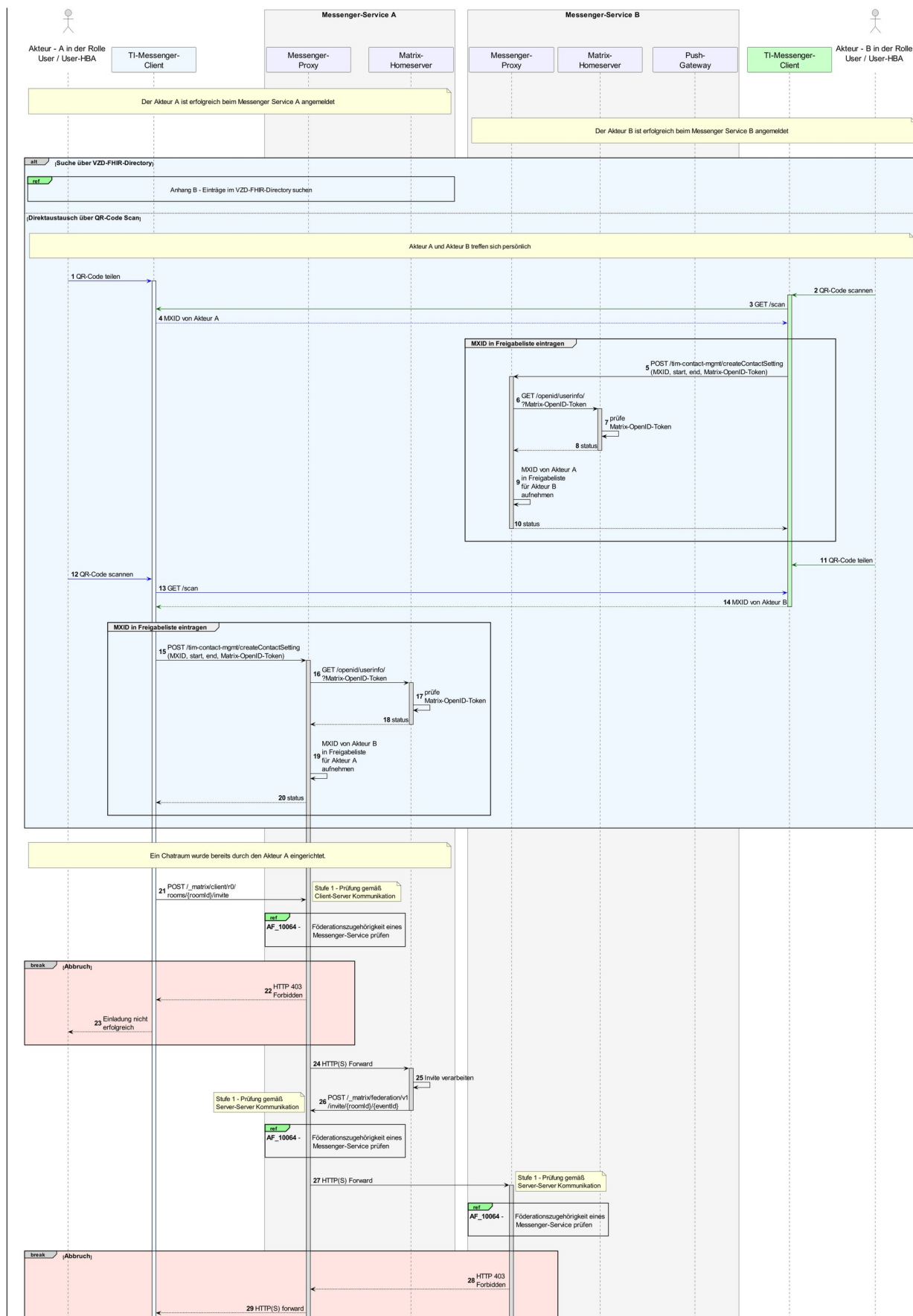


n. Für die vereinfachte Darstellung 26: wird Systemkomponenten des AF-- Check remote Domain

Tabelle 24 vorausgesetzt, dass die TI-Messenger-Clients der beteiligten Akteure online sind. In dieser Laufzeitansicht lädt der Akteur A den Akteur B unmittelbar in Check remote-Domain

AF_10064	Check-remote-Domain
Akteur-	Messenger-Proxy
Auslöser	Der Messenger-Proxy empfängt ein Matrix-Request und MUSS die Domain-Zugehörigkeit zur Föderation prüfen
Komponenten	Messenger-Proxy Registrierungs-Dienst VZD-FHIR-Directory
Vorbedingungen	keine
Eingangsdaten	Matrix-Request
Ergebnis	Der Messenger-Proxy ermittelt mittels der Föderationsliste, ob die Remote-Domain Teil der Föderation ist.
Ausgangsdaten	Result-
Akzeptanzkriterien	24  ML-123672, 25  ML-123891, 26  ML-123893

einem gemeinsamen Chatraum ein.



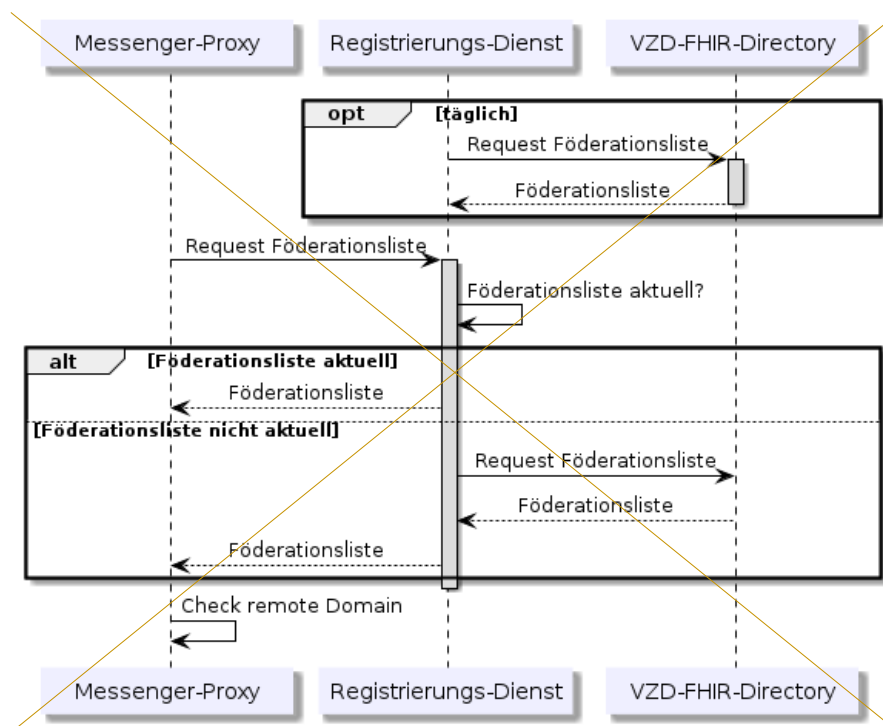


Abbildung 27: Laufzeitsicht - Ablauf Check remote Domain Einladung von Akteuren außerhalb einer Organisation

[<=]

Akzeptanzkriterien für den Anwendungsfall: Check remote Domain Einladung von Akteuren außerhalb einer Organisation (AF_100641)

72ML-12367254 - AF_100641 - Föderationsliste von Suche im VZD-FHIR-Directory
 Ein Messenger-Client kann erfolgreich im VZD-FHIR-Directory abrufen
 Der Registriernach einem Chatpartner suchen.
 [<=]

ML-123663 - AF_10061 - Akteure sind dem Chatraum beigetreten
 Alle Chat Parteien sind erfolgreich im Chatraum vorhanden.
 [<=]

ML-132864 - AF_10061 - Berechtigungsprüfung aller Stufen
 Dienst des Berechtigungsprüfung der Stufen 1-3 wurden berücksichtigt.
 [<=]

ML-132592 - AF_10061 - TI-Messenger-Fachdienstes MUSS die Föderationsliste Rohdatenerfassung und -lieferung
 Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich vom VZD-FHIR-Directory abrufen.
 erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet.
 [<=]

9.12 AF - Austausch von Events zwischen Akteuren außerhalb einer Organisation

23891ML-123891AF_10062-01 - Remote-Domain Teil Austausch von Events zwischen Akteuren außerhalb einer Organisation

In diesem Anwendungsfall können Akteure welche sich in einem gemeinsamen Raum befinden Nachrichten austauschen und an der Föderation durch die Matrix-Spezifikationsliste festgelegt & Aktualitätscheck

Es MUSS sichergestellt werden, dass derjenige ausführen. Dieser Anwendungsfall setzt ein erfolgreiches Invite-Event eines oder mehrerer beteiligter Akteure voraus. Die Prüfung auf Domainzugehörigkeit findet jedoch bei jedem Event der Server-Server Kommunikation statt. In diesem Anwendungsfall sind die beteiligten Akteure in einem gemeinsamen Chatraum und auf unterschiedlichen Messenger-Proxy-Servern verteilt.

Tabelle 25: tatsächlich über F - Austausch von Events zwischen Akteuren außerhalb einer Organisation

AF_10062	Austausch von Events zwischen Akteuren außerhalb einer Organisation
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle "User / User-HBA"
Auslöser	Alle Matrix-Events die zwischen Messenger-Services unterschiedlicher Organisationen ausgeführt werden.
Komponenten	<ul style="list-style-type: none"> • TI-Messenger-Client A + B, • Messenger-Proxy A + B, • Matrix-Homeserver A + B, • Push-Gateway B.
Vorbedingungen	<ol style="list-style-type: none"> 1. Beide Akteure sind Teilnehmer eines gemeinsamen Raumes. 2. Die Messenger Proxies verfügen über eine aktuelle Föderationsliste.
Eingangsdaten	Matrix-Event
Ergebnis	Matrix-Event wurde erfolgreich verarbeitet
Ausgangsdaten	Abhängig vom Matrix-Event, Status
Akzeptanzkriterien	 ML-123665,  ML-123666,  ML-123667,  ML-123668,  ML-132593

In der rüft, ob Laufzeitsicht sind die Remote-Domain Teil der Föderation Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es um eine vereinfachte Laufzeitsicht in der Föderationsliste ist zum Beispiel die TLS-Terminierung am Messenger-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde. Es MUSS wird in dem Anwendungsfall von lediglich hergestellt.

werden, dass der zwei beteiligten Akteuren ausgegangen. Auf die bei der Prüfung zur Föderationsliste, durch den Messenger-Proxy über, notwendigen Interaktionen wurde in dieser Laufzeitsicht verzichtet. Für eine ausführliche Beschreibung dieser prüft, ob die Lösung wird auf den Anwendungsfall AF_10064 - Föderationszugehörigkeit eines Messenger-Service prüfen verwirte aktuell ist. Es muss sichergeauslösenden Matrix-Request. Für die vereinfachte Darstellung wird vorausgesetzt, dass der Registrierungs-Dienst die TI-Messenger-Clients der beteiligten Akteure online sind.

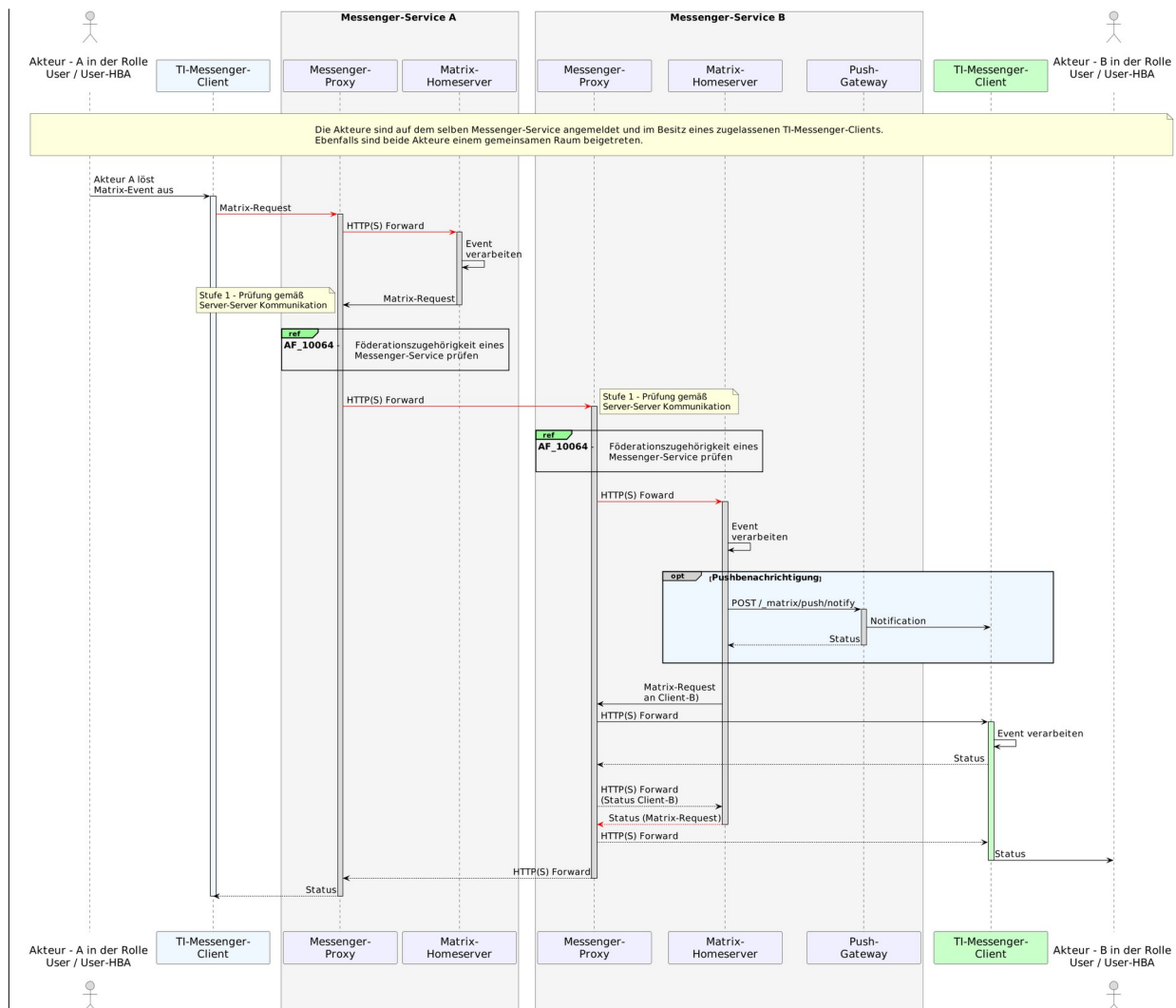


Abbildung 28: Listeraufzeitsicht - Austausch von Events zwischen Aktualität überprüft, bevor eineeuren außerhalb einer Organisation

[<=]

Akzeptanzkriterien für den Anwendungsfall: Austausch von Nachrichten zwischen aktualisierte Liste durch den euren außerhalb einer Organisation (AF_10062)

ML-123665 - AF_10062 - Messenger-Proxy des Senders prüft Domain des Empfängers

~~Der Messenger-Proxy ab des Senders prüft die Domain des Empfängerufen werden kans~~
auf Zugehörigkeit zur TI-Messenger-Föderation.

[<=]

893ML-123893666 - Aktualität FöderationslisteAF_10062 - Messenger-Proxy des Empfängers prüft Domain des Senders

~~Der Messenger-Proxy~~

~~Es MUSEmpfängers prüft die Domain deS sichergestellt werden, dass die Föenders auf~~
Zugehörigkeit zur TI-Messenger-Föderation.

[<=]

ML-123667 - AF_10062 - Auslösen einer Notifikation

~~derationsliste- Matrix-Homeserver des Empfängers löst eine Benachrichtigung des~~
Messenger-Proxy aktuell ist. Dafür MUSS der Messenger-ProxyClients über sein Push-
Gateway aus.

[<=]

ML-123668 - AF_10062 - Nachricht wird angezeigt

~~Die nach einricht wird dem Empfänger gewissim gemeinsamen Raum angeZeit eine-~~
aktuelle Liste beigt.

[<=]

ML-132593 - AF_10062 - TI-M Rohdatenerfassung und -lieferung

~~Die Rohdaten wurden entsprechend dem Registr Rohdatendefinition gemäß [gemSpec_TI-~~
Messenger-FD#Betrieungs-b] für den TI-Messenger-FachDienst anfordern.
erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet.

[<=]

10 Anhang A - Verzeichnisse

10.1 Abkürzungen

Kürzel	Erläuterung
AD	Active Directory
AF	Anwendungsfall
APN	Apple Push Notification Service
AuthZ	Authorization
BSIAZPD	Bundesamt für Sicherheit in der InAnbieter zentrale Plattformatiodientechnik
FCM	Firestore Cloud Messaging
FHIR	Fast Healthcare Interoperable Resources
HBA	Heilberufsausweis
HTTP	Hypertext Transfer Protocol
IDP-Dienst	Identity Provider
JSON	JavaScript Object Notation
JWT	JSON Web Token
KV	Kassenärztliche Vereinigung
LDAP	Lightweight Directory Access Protocol
LE	Leistungserbringer
MSCXID	Matrix-Spec-Change-User-ID

OAuth	Open Authorization
OIDC	OpenID-Connect
PASSportTA	Personalharmazeutisch-technischer Assertion Tokenistent
REST	Representational State Transfer
SMC-B	Institutionenkarte (Security Module Card Typ B)
SMC-B ORG	Security Module Card für Organisationen
SPOC	Single Point of Contact
SSO	Single Sign-on
TI	Telematikinfrastruktur
TI-ITSM	IT-Service-Management der TI
UIATI-M	User-Interactive Authorization Flow TI-Messenger
TSP	Trust Service Provider
VZD	Verzeichnisdienst

10.2 Glossar

Begriff	Erläuterung
MXID	eindeutige Identifikation eines TI-Messenger-Nutze Teilnehmers (Matrix-User-ID)
on-premise	das Produkt wird auf eigener oder gemieteter Hardware betrieben
Third-Party	Drittanbieter, der Zusatzleistungen oder Komponenten beisteuert

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

10.3 Abbildungsverzeichnis

Abbildung 1: Komponenten der TI-Messenger-Architektur (vereinfachte Darstellung).....	9
Abbildung 2: Benachbarten Produkttypen des TI-Messenger-Dienstes.....	13

Abbildung 3: Komponenten der TI-Messenger-Architektur und deren Schnittstellen.....19

Abbildung 4: Systemkomponenten des AF—Anmeldung eines Nutzers am Messenger-Service.....30

Abbildung 5: Laufzeitsicht—Anmeldung eines Nutzers am Messenger-Service.....32

Abbildung 6: Systemkomponenten des AF—Leistungserbringer als Practitioner hinzufügen.....34

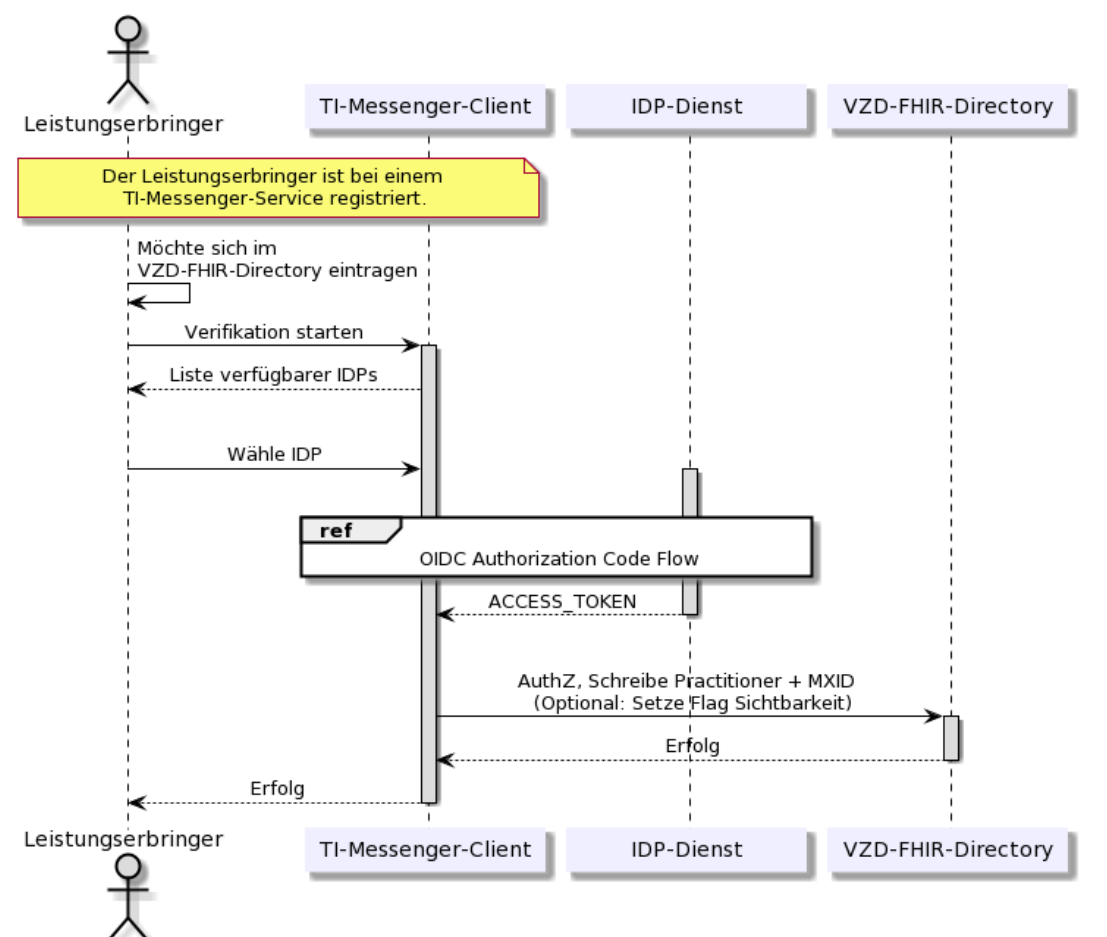


Abbildung 7: Laufzeitsicht—LE als Practitioner hinzufügen.....35

Abbildung 8: Systemkomponenten des AF—Messenger-Service bereitstellen.....36

Abbildung 9: Laufzeitsicht—Messenger-Service automatisch bereitstellen.....38

Abbildung 10: Systemkomponenten des AF—Organisationsressourcen im VZD-FHIR-Directory hinzufügen.....39

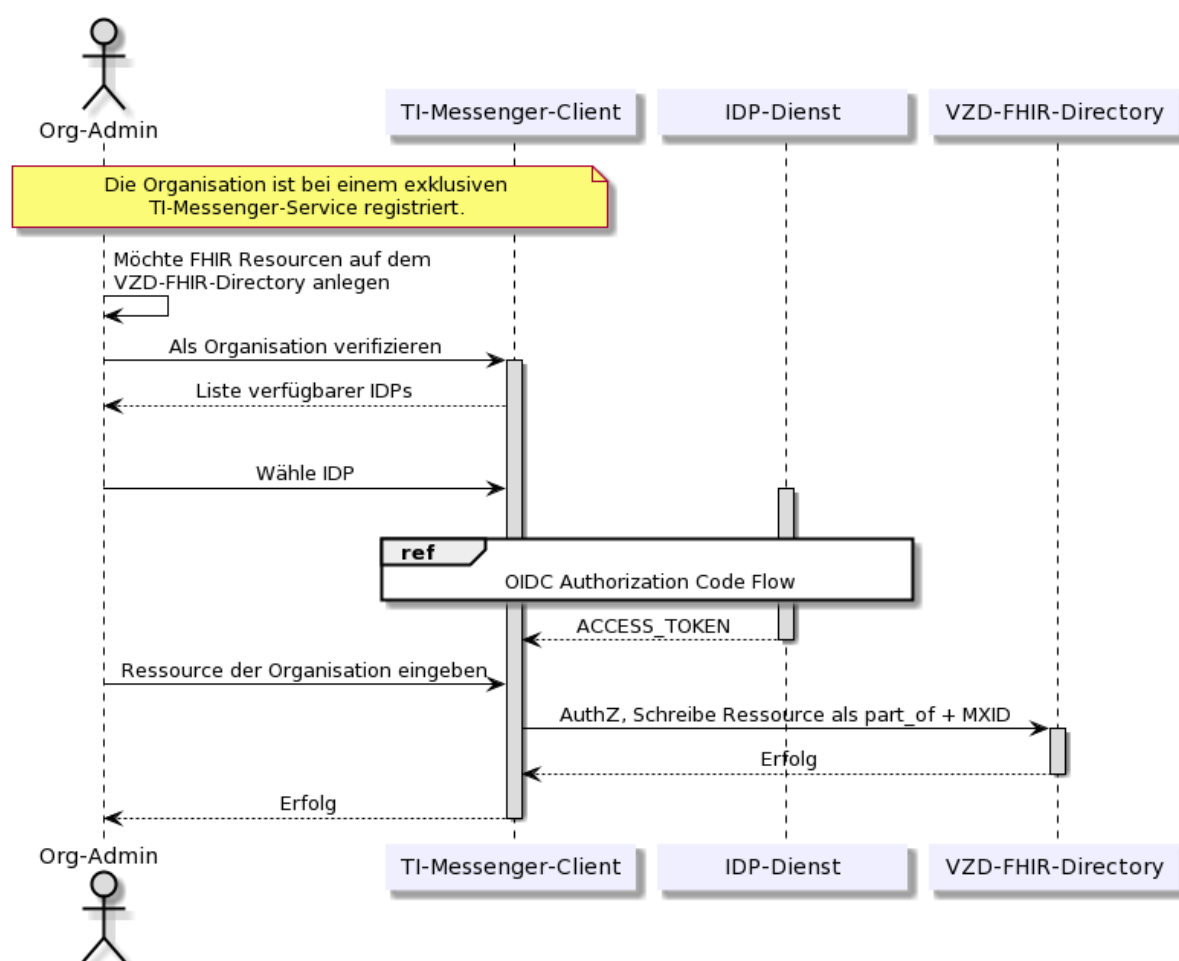


Abbildung 11: Laufzeitsicht—Organisations-Ressourcen im VZD-FHIR-Directory hinzufügen.....41

Abbildung 12: Systemkomponenten des AF—TI-Messenger Remote Invite.....42

Abbildung 13: Laufzeitsicht—TI-Messenger Remote Invite.....44

Abbildung 14: Systemkomponenten des AF—Message senden (Remote).....45

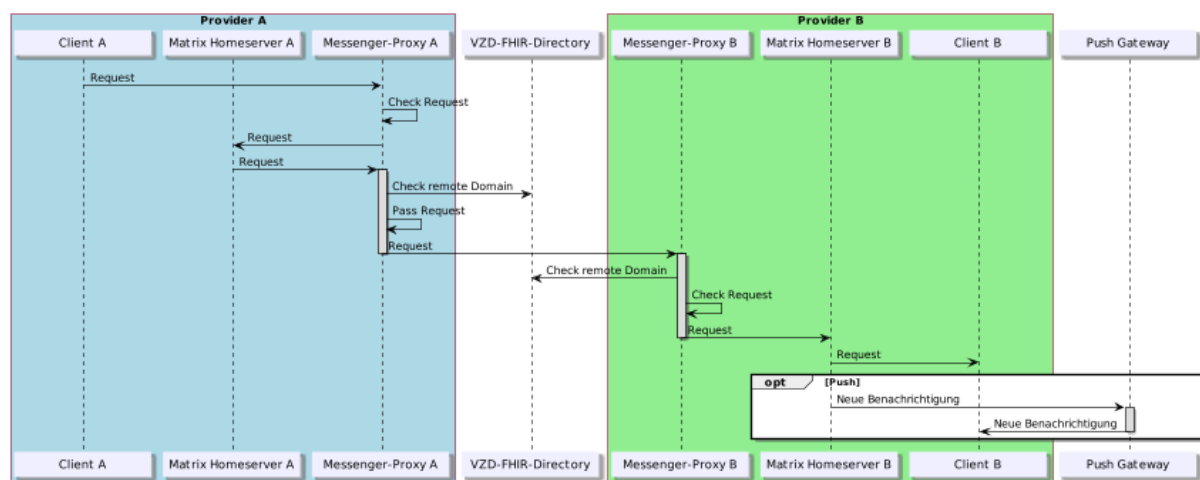
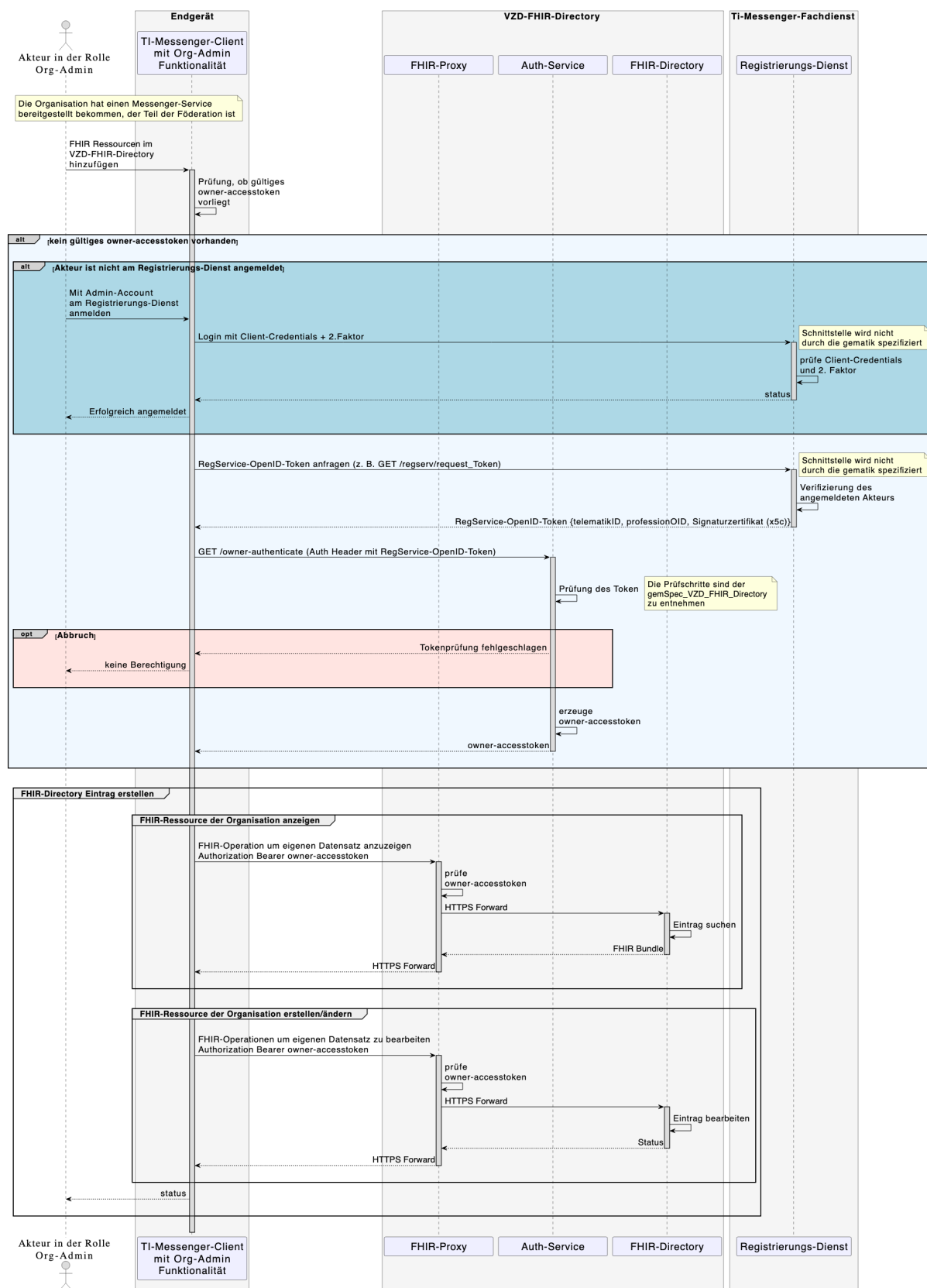


Abbildung 15: Laufzeitsicht—Message senden (Remote).....47

Abbildung 16: Systemkomponenten des AF—Messenger-Service (Lokal).....48

Abbildung 17: Laufzeitsicht – Messenger Service (Lokal).....	49
Abbildung 18: Systemkomponenten des AF – Check remote Domain.....	50
Abbildung 19: Laufzeitsicht – Ablauf Check remote Domain.....	51

Abbildung 1: Komponenten der TI-Messenger-Architektur (vereinfachte Darstellung).....	13
Abbildung 2: Benachbarten Produkttypen des TI-Messenger-Dienstes.....	22
Abbildung 3: KoMponenten der TI-Messenger-Architektur und deren Schnittstellen.....	36
Abbildung 4: Darstellung der Berechtigungsprüfung am Messenger-.....	44
Abbildung 5: Beispiel einer Interaktion mit einem Chatbot.....	60
Abbildung 6: ti-Messenger-Dienst Instanzen.....	61
Abbildung 7: Ausschnitt - TI-Messenger-Anbieter im TI-ITSM.....	63
Abbildung 8: Org-Admin - Übersicht Anwendungsfälle.....	66
Abbildung 9: Use.....	69
Abbildung 10: Laufzeitsicht - Authentisieren einer Organisation am TI-Messenger-Dienst	75
Abbildung 11: Laufzeitsicht - Bereitstellung eines Messenger-Service für eine Organisation	81



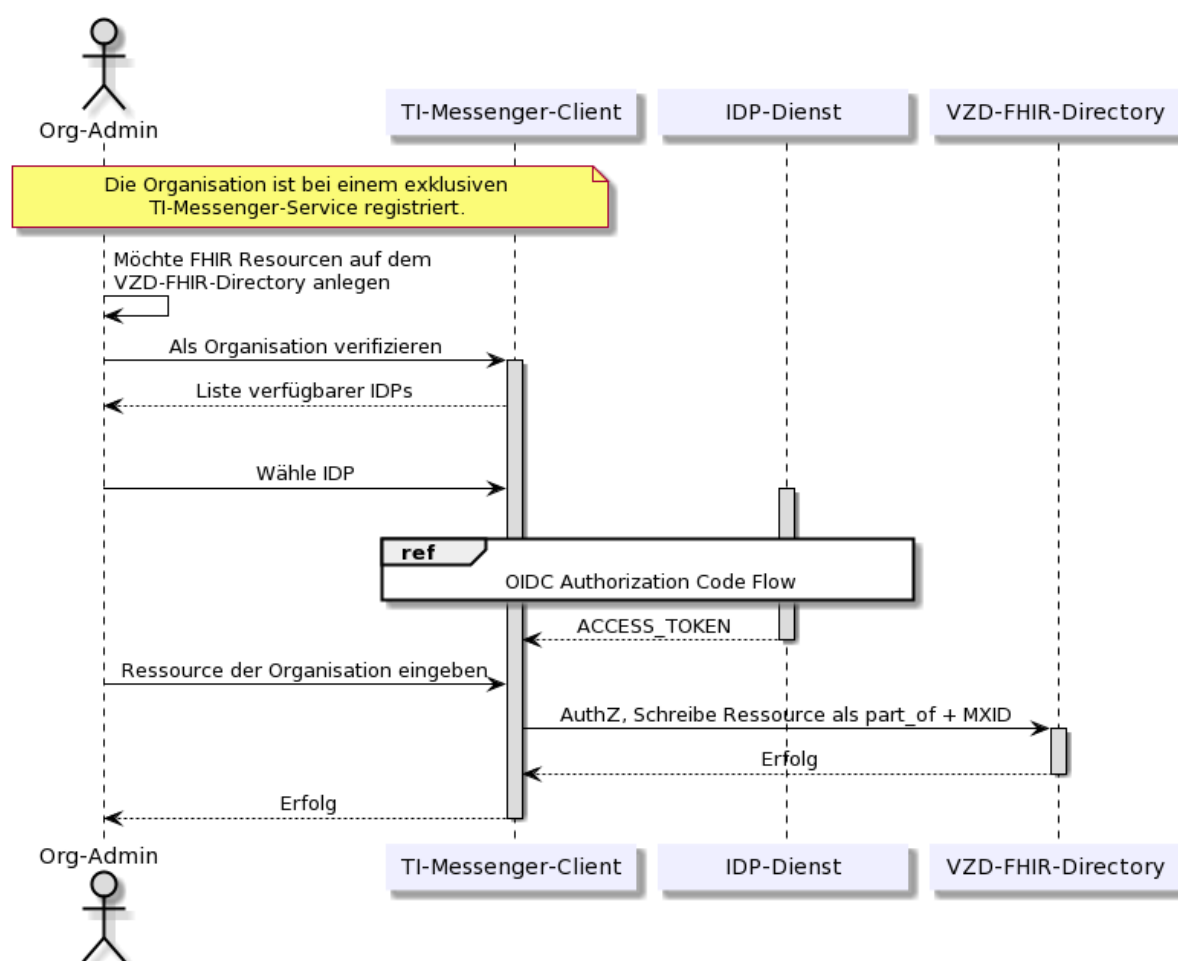


Abbildung 12: Laufzeitsicht - OrganisationsRessourcen im Verzeichnisdienst hinzufügen.....85

Abbildung 13: Laufzeitsicht - Anmeldung eines Akteurs am Messenger.....91

Abbildung 14: Laufzeitsicht - Akteur (User-HBA) im Verzeichnisdienst hinzufügen.....95

Abbildung 15: Laufzeitsicht - Föderationszugehörigkeit eines Messenger-Service prüfen 99

Abbildung 16: Einladung von Akteuren innerhalb einer Organisation.....105

Abbildung 17: Laufzeitsicht - Austausch von Events zwischen Akteuren innerhalb einer Organisation.....109

Abbildung 18: Laufzeitsicht - Einladung von Akteuren außerhalb einer Organisation.....114

Abbildung 19: Laufzeitsicht - austausch von Events zwischen Akteuren außerhalb einer Organisation.....116

Abbildung 20: Laufzeitansicht - Einträge im VZD-FHIR-Directory suchen.....129

Abbildung 21 Laufzeitansicht - Aktualisierung der Föderationsliste.....132

Abbildung 22 Provider authentifizieren und Föderationsliste abrufen.....133

Abbildung 23 Signatur der Föderationsliste prüfen.....134

Abbildung 24: Laufzeitansicht - Stufen der Berechtigungsprüfung.....135

10.4 Tabellenverzeichnis

Tabelle 1: Akteure und Rollen.....	10
Tabelle 2: Kommunikationsmatrix.....	15
Tabelle 3: AF – Anmeldung eines Nutzers am Messenger-Service.....	30
Tabelle 4: AF – Leistungserbringer als Practitioner hinzufügen.....	34
Tabelle 5: AF – Messenger-Service bereitstellen.....	37
Tabelle 6 AF – Organisationsressourcen im VZD-FHIR-Directory hinzufügen.....	39
Tabelle 7 AF – TI-Messenger Remote Invite.....	43
Tabelle 8 AF – Message senden (Remote).....	46
Tabelle 9 Messenger-Service (Lokal).....	48
Tabelle 10 Check remote Domain.....	50

Tabelle 1 Akteure und Rollen.....	20
Tabelle 2: Kommunika.....	21
Tabelle 3: Arten von Token.....	32
Tabelle 4: Verzeichnistypen - Rechtekonzept.....	38
Tabelle 5: Schreibzugriff - VZD-FHIR-Ressourcen.....	54
Tabelle 6: Überblick der Benutzerverwaltung in Abhängigkeit der Rolle.....	56
Tabelle 7: Beispiel für Funktionsaccounts.....	58
Tabelle 8: Tabelle : AF - Authentisieren einer Organisation am TI-Messenger-Dienst.....	71
Tabelle 9: aF - Bereitstellung eines Messenger-Service für eine Organisation.....	76
Tabelle 10: AF - Organisationsressourcen im Verzeichnisdienst hinzufügen.....	82
Tabelle 11: Af - Anmeldung eines Akteurs am Messenger-Service.....	87
Tabelle 12: AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen.....	92
Tabelle 13: Föderationszugehörigkeit eines Messenger-Service prüfen.....	97
Tabelle 14: Einladung von Akteuren innerhalb einer Organisation.....	102
Tabelle 15: austausch von Events zwischen Akteuren innerhalb einer Organisation.....	106
Tabelle 16 AF - Einladung von Akteuren außerhalb einer Organisation.....	110
Tabelle 17: aF - Austausch von Events zwischen Akteuren außerhalb einer Organisation	115

10.5 Referenzierte Dokumente

10.5.1 Dokumente der gematik

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

vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[api-messenger]	gematik: api-ti-messenger https://github.com/gematik/api-ti-messenger/
[gemKPT_TI_Messengerapi-vzd]	gematik: Konzeptpapier Verzeichnisdienst der TI-Messenger gematikinfrastruktur https://github.com/gematik/api-vzd
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktivbetrieb
[gemKPT_TI_Messenger]	gematik: Konzeptpapier TI-Messenger
[gemSpec_IDP_Dienst]	gematik: Spezifikation Identity Provider-Dienst
[gemSpec_TI-Messenger-FD]	gematik: Spezifikation TI-Messenger-Fachdienst
[gemSpec_VZD_FHIR_Directory]	gematik: Spezifikation Verzeichnisdienst FHIR-Directory

10.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[Direct-Messaging]	Matrix Foundation https://matrix.org/docs/spec/client_server/r0.6.1-
[Matrix Foundation]	Matrix Foundation https://matrix.org/docs/spec/
[Nutzer Token]	Matrix Foundation https://matrix.org/docs/spec/client_server/r0.6.1-
[Matrix-PushGWBSI 2-Faktor]	Matrix Foundation https://matrix.org/docs/spec/push_gateway/r0.1.1- www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/Bewertung-2FA-Verfahren/bewertung-2fa-verfahren_node.html

[MatrixSpecProposalClient-Server API]	Matrix Foundation: Matrix Specification - Client-Server API https://spec.matrix.org/unstable/proposalsv1.3/client-server-api/ _
[RFC 8225]	IETF https://datatracker.ietf.org/doc/html/rfc8225
[OpenID]	OpenID Foundation https://openid.net/developers/specs/
[FHIR]	HL7 FHIR Dokumentation https://www.hl7.org/fhir/documentation.html
[gematik Authenticator]	gematik Authenticator https://cloud.gematik.de/index.php/s/23ebxa75z3s7zGt?path=%2Fv2.1.0
[Matrix Bots]	Matrix Bot Implementierungen https://matrix.org/bots/
[Matrix Specification]	Matrix Foundation: Matrix Specification https://spec.matrix.org/v1.3/
[OpenID]	OpenID Foundation https://openid.net/developers/specs/
[Push Gateway API]	Matrix Foundation: Matrix Specification - Push Gateway API https://spec.matrix.org/v1.3/push-gateway-api/
[RFC 8225]	IETF https://datatracker.ietf.org/doc/html/rfc8225
[Server-Server API]	Matrix Foundation: Matrix Specification - Server-Server API https://spec.matrix.org/v1.3/server-server-api/

11 Anhang B - Abläufe

11.1 ~~OIDC – Authorization Code Flow~~ Einträge im VZD-FHIR-Directory suchen

Die folgende Abbildung beschreibt, wie ein Akteur im VZD-FHIR-Directory nach *HealthcareService*- und *PractitionerRole* Ressourcen sucht. Dies setzt eine erfolgreiche Anmeldung des Akteurs an einem Messenger-Service voraus. Der dargestellte Ablauf zeigt alle prinzipiell notwendigen Kommunikationsbeziehungen. Weitergehende Informationen zum Ablauf sind in der [gemSpec_VZD_FHIR_Directory] zu finden. Für die Prüfung des Matrix-OpenID-Tokens MUSS der Zugriff auf den Endpunkt `/_matrix/federation/v1/openid/userinfo` ermöglicht werden.

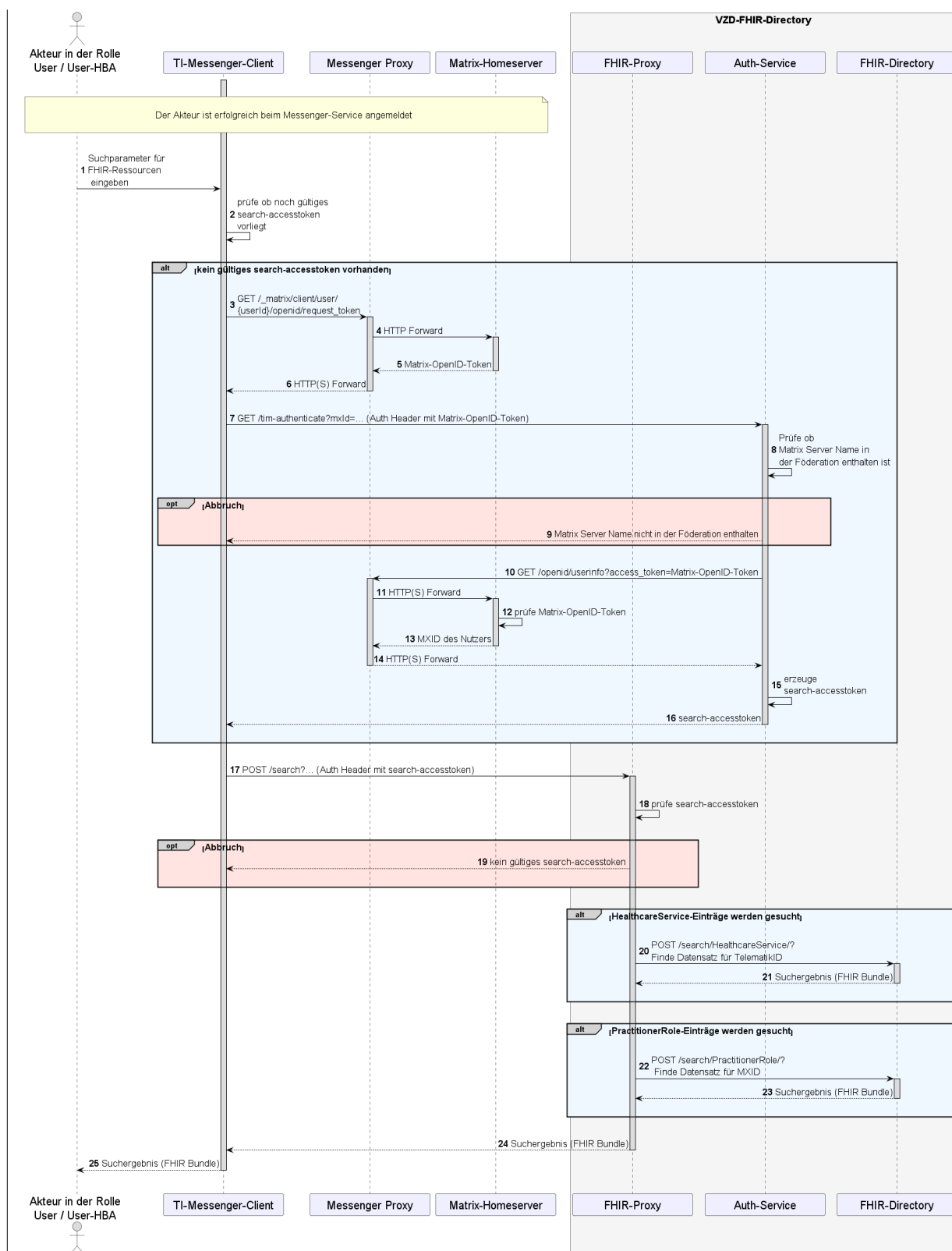
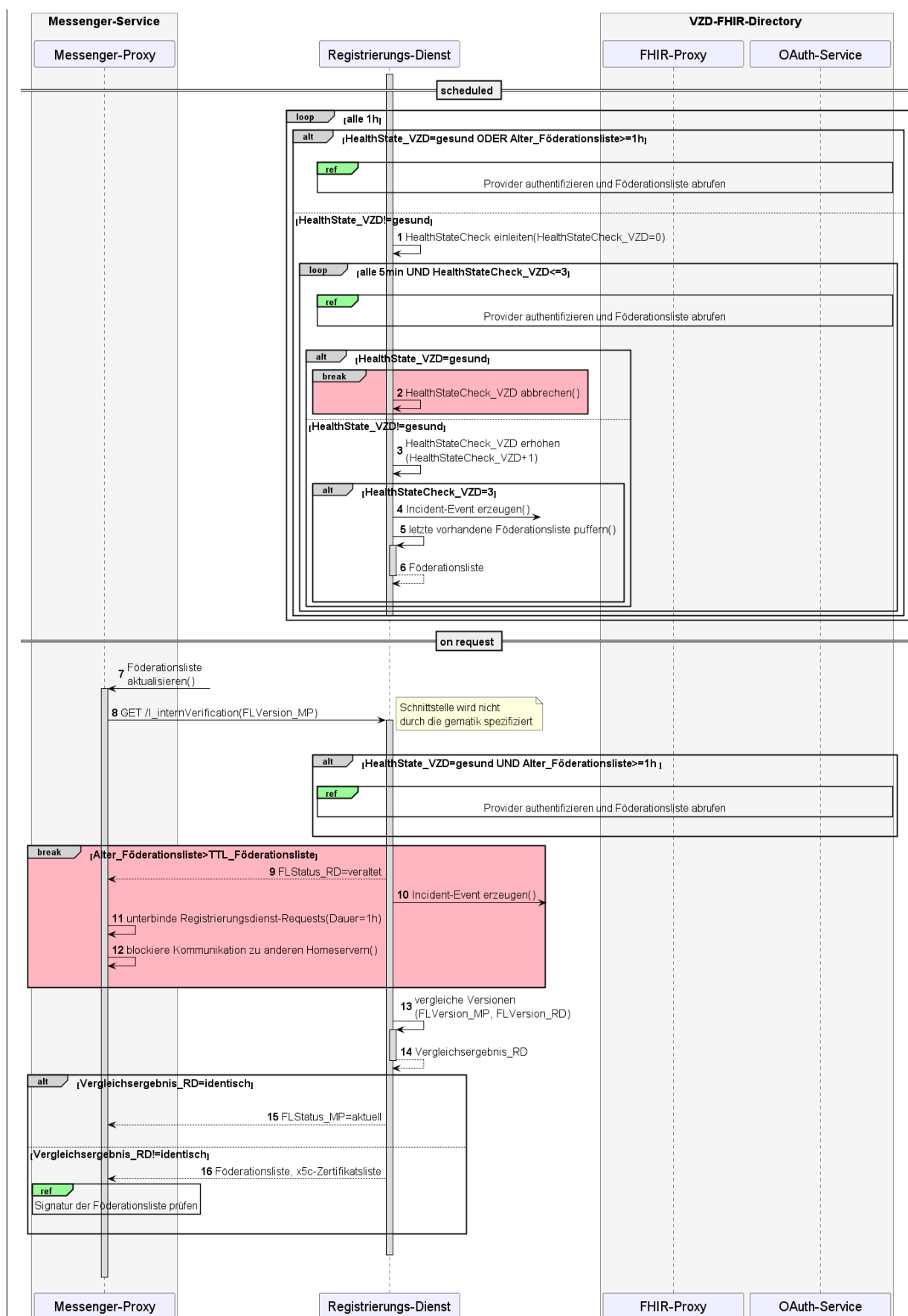


Abbildung 29: Laufzeitansicht - Einträge im VZD-FHIR-Directory suchen

11.2 Aktualisierung der Föderationsliste

11.3 Die folgende Abbildung beschreibt, wie der Messenger-Proxy seine lokal vorgehaltene Föderationsliste aktualisiert. Für die Aktualisierung der Föderationsliste MUSS der Messenger-Proxy diese beim Registrierungs-Dienst seines TI-Messenger-Fachdienstes anfragen. Die Häufigkeit der Anfrage einer neuen Liste wird durch den Anbieter festgelegt, Ziel sollte eine möglichst aktuelle Föderationsliste sein. Hierbei übergibt der Messenger-Proxy die durch ihn gespeicherte Version der Föderationsliste im Aufruf an den Registrierungs-Dienst. Bei Übereinstimmung der Version wird für den Messenger-Proxy keine neue Föderationsliste durch den Registrierungs-Dienst bereitgestellt. Ist die Version größer als die vom Messenger-Proxy übergebene, dann wird durch den Registrierungs-Dienst eine aktualisierte Föderationsliste zur Verfügung gestellt. Bei jeder Anfrage eines Messenger-Proxys beim Registrierungs-Dienst nach einer aktuellen Föderationsliste MUSS der Registrierungs-Dienst die Aktualität der durch ihn ausgelieferten Liste sicherstellen, indem er die von ihm gespeicherte Version der Föderationsliste im Bedarfsfall mit einer aktuelleren Version, die vom FHIR-Proxy bezogen wurde, überschreibt. Ein Download der Föderationsliste ist nur notwendig, wenn eine neuere Version auf dem FHIR-Proxy existiert. Die Struktur der Föderationsliste ist in [gemSpec_VZD_FHIR_Directory] beschrieben. Nach dem Abruf der Föderationsliste vom Registrierungs-Dienst, durch den Messenger Proxy, MUSS dieser die Signatur der Föderationsliste prüfen.



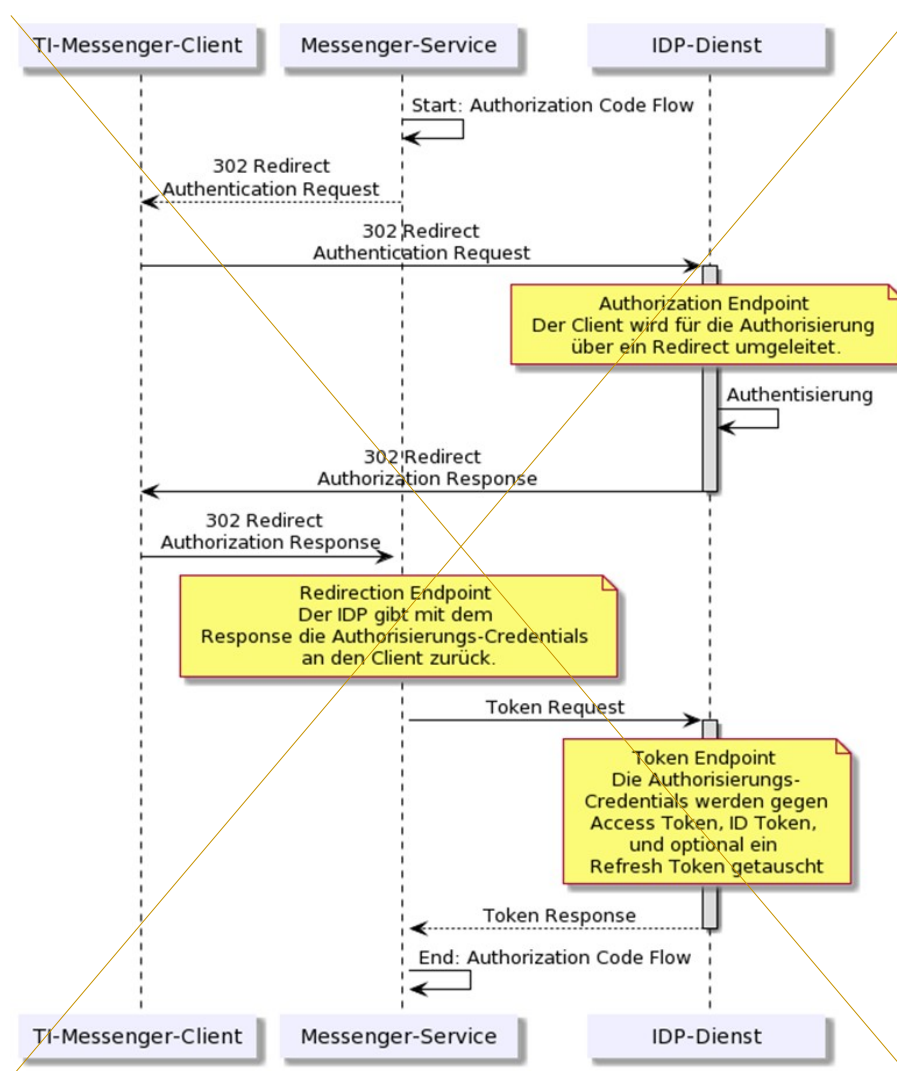


Abbildung 30 Laufzeitansicht - Aktualisierung der Föderationsliste

Das in der Abbildung "Laufzeitansicht - Aktualisierung der Föderationsliste" referenzierte Sequenzdiagramm "Provider authentifizieren und Föderationsliste abrufen":

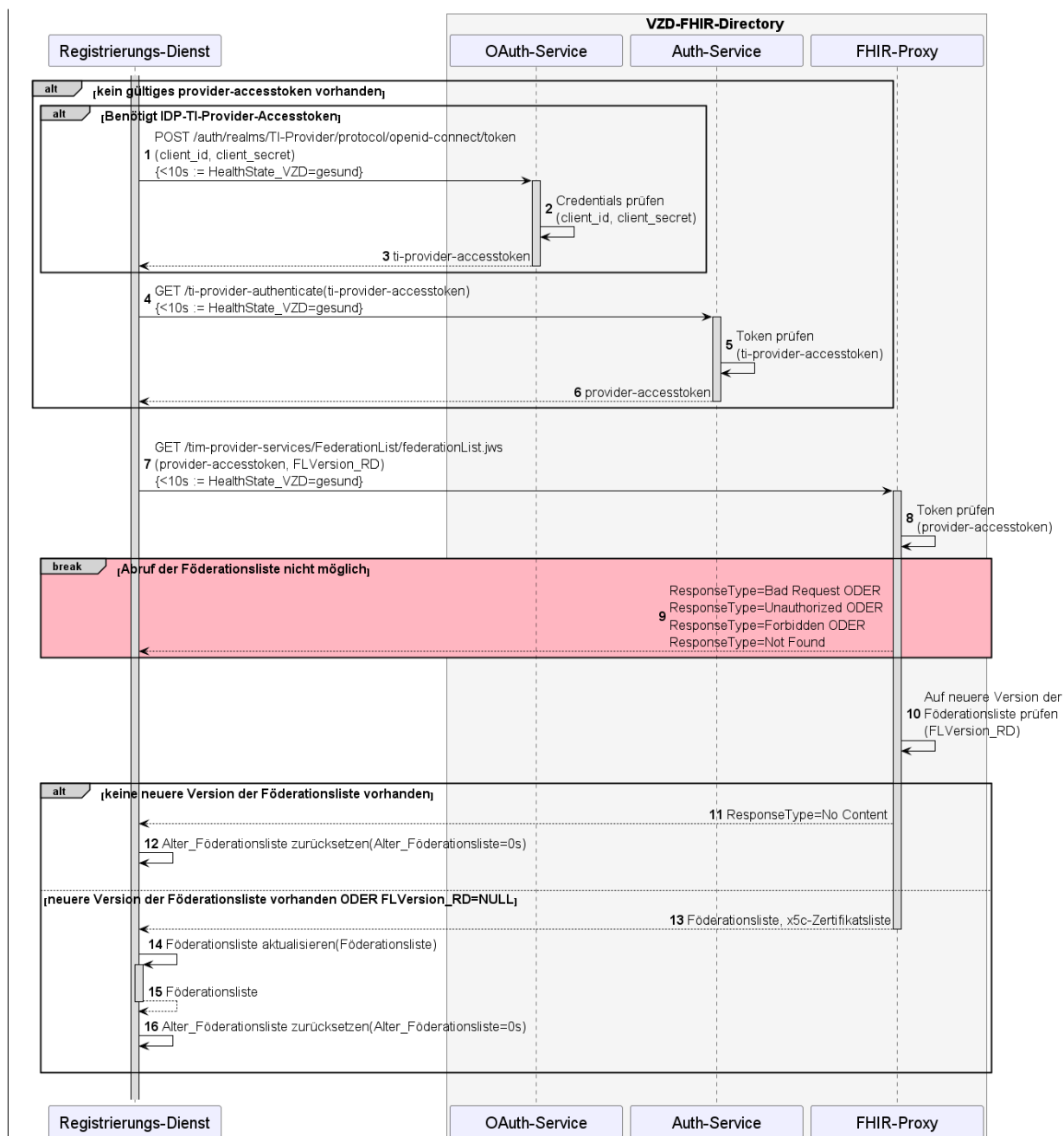


Abbildung 31 Provider authentifizieren und Föderationsliste abrufen

Das in der Abbildung "Laufzeitansicht - Aktualisierung der Föderationsliste" referenzierte Sequenzdiagramm "Signatur der Föderationsliste prüfen":

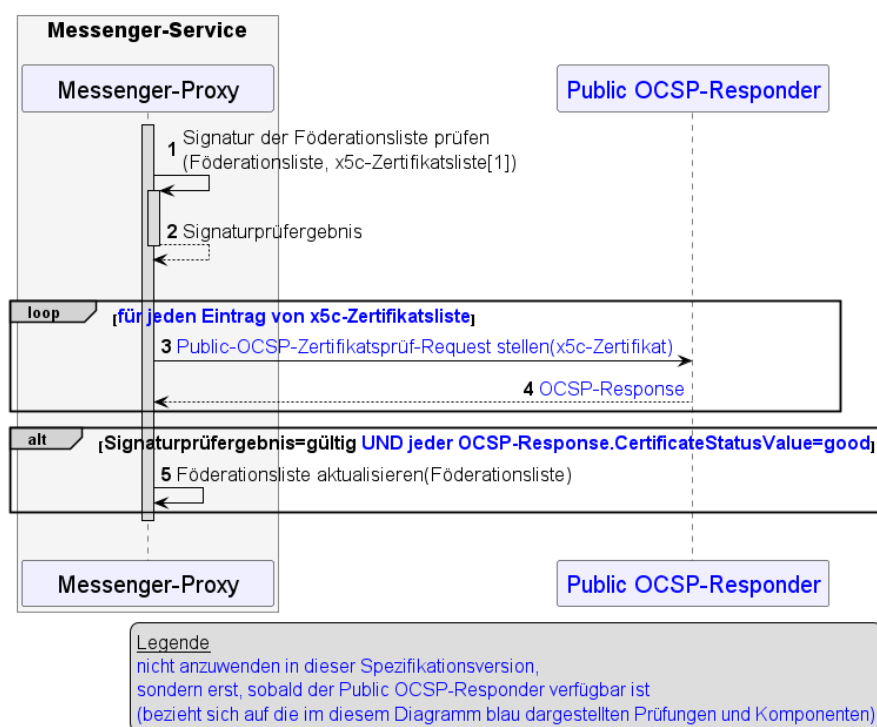


Abbildung 32 Signatur der Föderationsliste prüfen

11.4 Stufen der Berechtigungsprüfung

Die folgende Abbildung beschreibt, wie die Berechtigungsprüfung eingehender und ausgehender Matrix-Events am Messenger-Proxy erfolgen MUSS. Das Berechtigungskonzept basiert auf einer dreistufigen Prüfung, die in den Kapiteln 3.5.1- Client-Server Kommunikation und 3.5.2- Server-Server Kommunikation beschrieben sind. Es wird auf die Erwähnung notwendiger Authentifizierungen an dieser Stelle verzichtet.

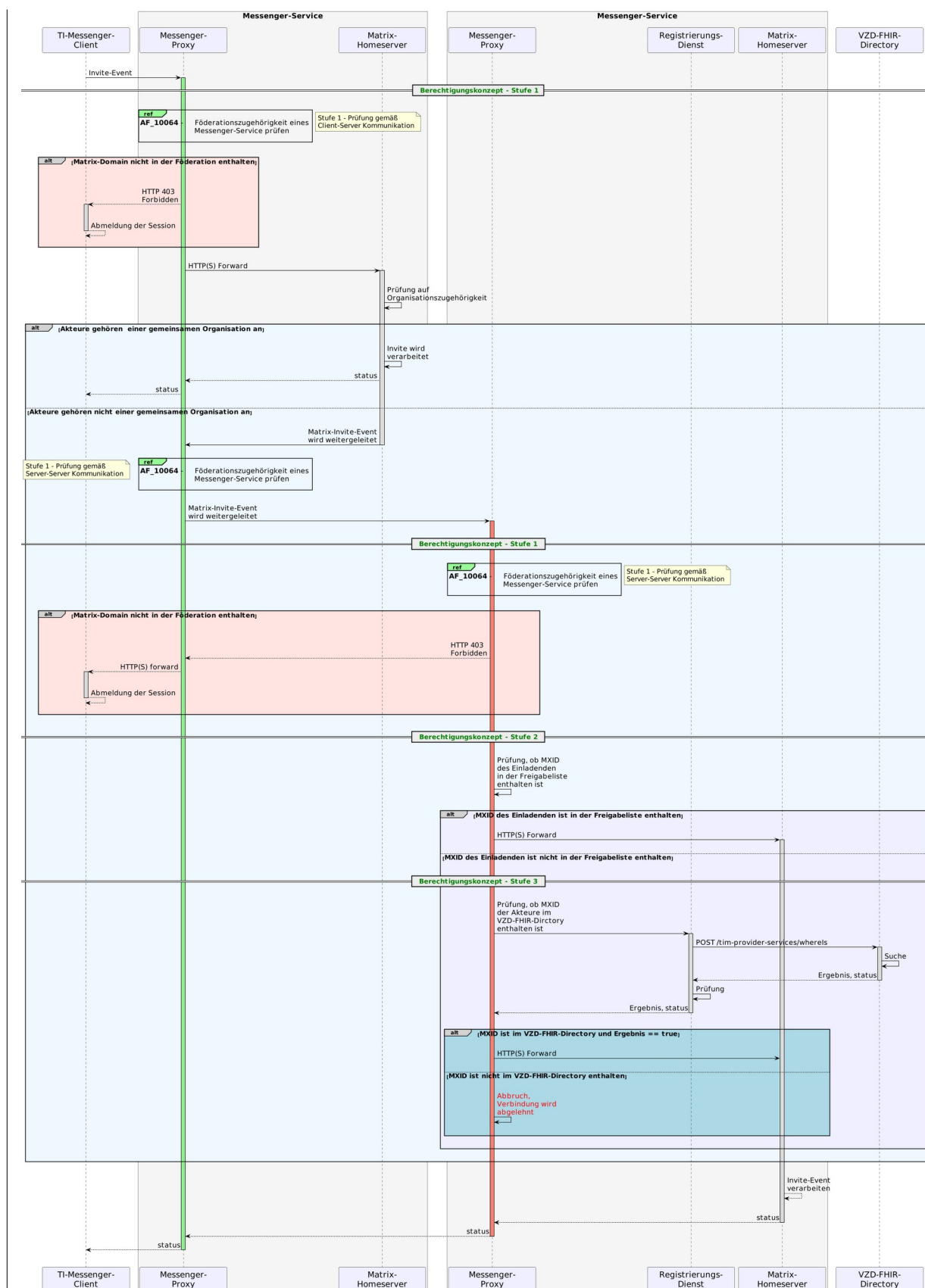


Abbildung 33: Laufzeitansicht - Stufen der Berechtigungsprüfung

