

1
2
3
4
5
6
7
8
9
10
11 **Elektronische Gesundheitskarte und Telematikinfrastruktur**
12
13
14
15
16
17
18
19

20 Spezifikation 21 **TI-Messenger-Dienst**

22
23
24
25
26
27

Version:	1.1.0 CC
Revision:	469909
Stand:	13.06.2022
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_TI-Messenger-Dienst

28

29

Dokumentinformationen

30

Änderungen zur Vorversion

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

34

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	01.10.2021		Erstversion des Dokumentes	gematik
1.1.0 CC	13.06.2022		zur Abstimmung freigegeben	gematik

36

37	Inhaltsverzeichnis	
38	1 Einordnung des Dokumentes	5
39	1.1 Zielsetzung	5
40	1.2 Zielgruppe	5
41	1.3 Geltungsbereich	5
42	1.4 Abgrenzungen	6
43	1.5 Methodik	6
44	2 Systemüberblick	8
45	3 Systemkontext.....	10
46	3.1 Akteure und Rollen	10
47	3.2 Nachbarsysteme	13
48	3.3 Ausprägungen des Messenger-Services.....	14
49	3.4 TI-Messenger Föderation.....	17
50	3.5 Berechtigungskonzept	17
51	3.6 Verwendung der Token.....	18
52	4 Systemzerlegung	22
53	4.1 IDP-Dienst.....	23
54	4.2 VZD-FHIR-Directory.....	23
55	4.3 TI-Messenger-Fachdienst	25
56	4.3.1 Registrierungs-Dienst	25
57	4.3.2 Push-Gateway	26
58	4.3.3 Messenger-Service	26
59	4.3.3.1 Messenger-Proxy.....	26
60	4.3.3.2 Matrix-Homeserver.....	28
61	4.4 TI-Messenger-Client	28
62	5 Übergreifende Festlegungen	29
63	5.1 Datenschutz und Sicherheit	29
64	5.2 Verwendete Standards	29
65	5.3 Authentifizierung und Autorisierung	30
66	5.3.1 Authentifizierung von Akteuren am Messenger-Service	30
67	5.3.2 Authentifizierung am VZD-FHIR-Directory	30
68	5.3.3 Autorisierung am Messenger-Service	30
69	5.3.4 Autorisierung am VZD-FHIR-Directory	31
70	5.4 Rechtekonzept VZD-FHIR-Directory	31
71	5.4.1 Lesezugriff	31
72	5.4.2 Schreibzugriff	31

73	5.5 Funktionsaccounts	32
74	5.6 Test	35
75	5.7 Betrieb.....	36
76	6 Anwendungsfälle	38
77	 6.1 AF - Authentisieren einer Organisation am TI-Messenger-Dienst	40
78	 6.2 AF - Bereitstellung eines Messenger-Service für eine Organisation	43
79	 6.3 AF - Organisationsressourcen im Verzeichnisdienst hinzufügen	46
80	 6.4 AF - Anmeldung eines Akteurs am Messenger-Service	49
81	 6.5 AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen	52
82	 6.6 AF - Föderationszugehörigkeit eines Messenger-Service prüfen.....	55
83	 6.7 AF - Einladung von Akteuren innerhalb einer Organisation	58
84	 6.8 AF - Austausch von Events zwischen Akteuren innerhalb einer Organisation.....	61
85	 6.9 AF - Einladung von Akteuren außerhalb einer Organisation.....	64
86	 6.10 AF - Austausch von Events zwischen Akteuren außerhalb einer Organisation.....	67
89	7 Anhang A – Verzeichnisse.....	71
90	 7.1 Abkürzungen	71
91	 7.2 Glossar	72
92	 7.3 Abbildungsverzeichnis.....	72
93	 7.4 Tabellenverzeichnis	73
94	 7.5 Referenzierte Dokumente.....	73
95	7.5.1 Dokumente der gematik.....	73
96	7.5.2 Weitere Dokumente.....	74
97	8 Anhang B – Abläufe	76
98	 8.1 Einträge im VZD-FHIR-Directory suchen.....	76
99	 8.2 Aktualisierung der Föderationsliste	77
100	 8.3 Stufen der Berechtigungsprüfung	78
101		
102		
103		

104

1 Einordnung des Dokumentes

105

1.1 Zielsetzung

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

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

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

124

1.2 Zielgruppe

125 Das Dokument richtet sich zum Zwecke der Realisierung an Hersteller von Produkttypen
126 des TI-Messengers sowie an Anbieter, welche die beschriebenen Produkttypen betreiben.
127 Alle Hersteller und Anbieter von TI-Anwendungen, deren Schnittstellen einen der
128 Produkttypen des TI-Messengers nutzen, oder Daten mit den Produkttypen des TI-
129 Messengers austauschen oder solche Daten verarbeiten, müssen dieses Dokument
130 ebenso berücksichtigen.

131

1.3 Geltungsbereich

132 Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des
133 deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und
134 deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH
135 in gesonderten Dokumenten (z. B. gemPTV_ATV_Festlegungen, Produkttypsteckbrief,
136 Anbiertypsteckbrief, u.a.) oder Webplattformen (z. B. GitHub, u.a.) festgelegt und
137 bekanntgegeben.

138

Schutzrechts-/Patentrechtshinweis

140 *Die nachfolgende Spezifikation ist von der gematik allein unter technischen
141 Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass
142 die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist*

143 allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu
144 tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder
145 Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen
146 Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik
147 GmbH übernimmt insofern keinerlei Gewährleistungen.

148 1.4 Abgrenzungen

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

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

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

161 1.5 Methodik

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

- 163 • **Der gesamte Text in der Spezifikation ist sowohl für den Hersteller des
164 Produktes TI-Messenger-Dienst als auch für den betreibenden Anbieter
165 entsprechend [gemKPT_Betr] verbindlich zu betrachten und gilt als
166 Zulassungskriterium beim Produkt und Anbieter.**
- 167 • Die Verbindlichkeit SOLL durch die dem RFC 2119 [RFC2119] entsprechenden, in
168 Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT,
169 SOLL, SOLL NICHT, KANN gekennzeichnet werden.
- 170 • Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen.“ die
171 Phrase „DARF NICHT“ semantisch irreführend wäre (wenn nicht ein, dann
172 vielleicht zwei?), wird in diesem Dokument stattdessen „Eine leere Liste DARF
173 KEIN Element besitzen.“ verwendet.
- 174 • Die Schlüsselworte KÖNNEN außerdem um Pronomen in Großbuchstaben ergänzt
175 werden, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

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

181 Anwendungsfälle und Akzeptanzkriterien werden im Dokument wie folgt dargestellt:

182 **<ID> - <Titel des Anwendungsfalles / Akzeptanzkriteriums>**

183 Text / Beschreibung

184 [<=]

185 Die einzelnen Elemente beschreiben:

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

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

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

201 **Hinweis auf offene Punkte**

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

202

203

204

2 Systemüberblick

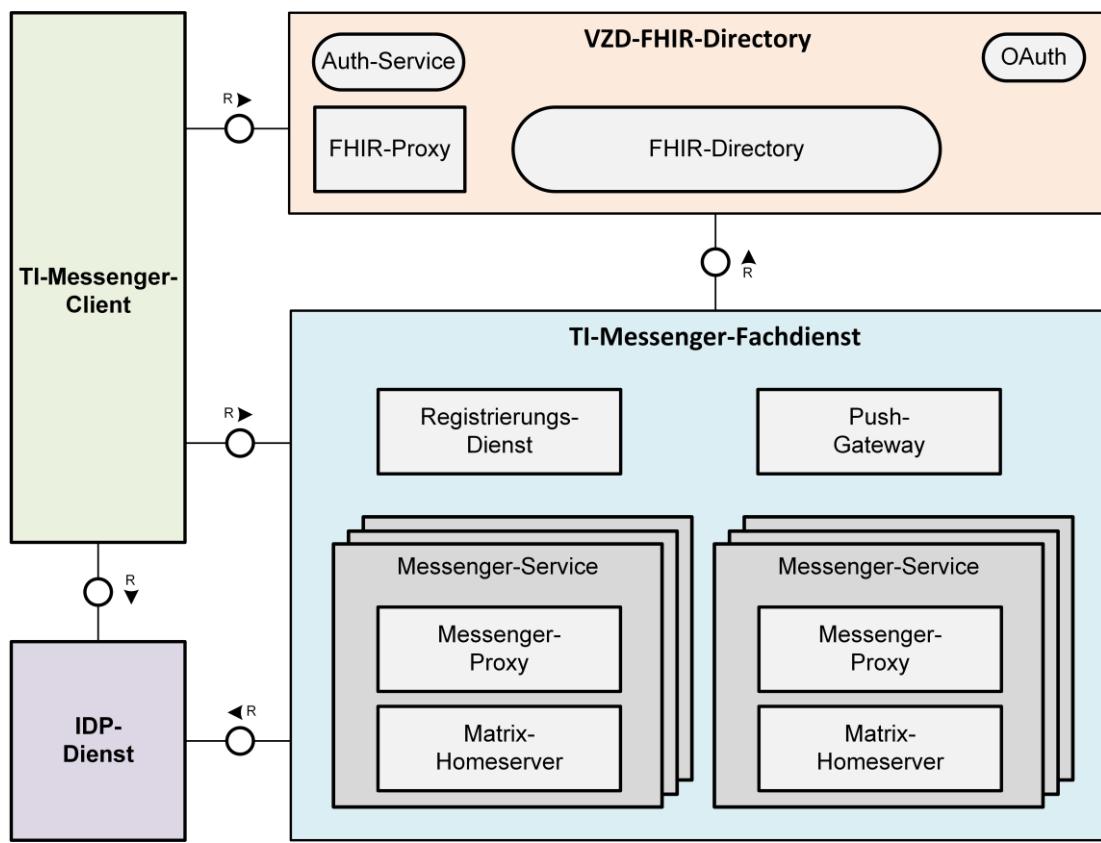
205 Der sichere Nachrichtenaustausch zwischen beteiligten Akteuren des deutschen
206 Gesundheitswesens erfolgt über die von TI-Messenger-Anbietern bereitgestellten TI-
207 Messenger-Fachdienste und TI-Messenger-Clients. Die Ad-Hoc Kommunikation zwischen
208 den Akteuren findet hierbei über zugelassene TI-Messenger-Clients statt. Die
209 Produkttypen TI-Messenger-Fachdienst sowie TI-Messenger-Client werden durch von der
210 gematik zugelassene TI-Messenger-Anbieter bereitgestellt.

211 Ein TI-Messenger-Fachdienst besteht aus einem oder mehreren Messenger-Services
212 (basierend auf dem Matrix-Protokoll) die jeweils für eine Organisation (SMC-B-Inhaber)
213 des Gesundheitswesens bereitgestellt werden. Diese unterscheiden sich lediglich in der
214 Art des verwendeten Authentifizierungsverfahrens. Akteure, die zugehörig zu einer
215 Organisation agieren, KÖNNEN den durch diese Organisation bereitgestellten Messenger-
216 Service verwenden und die innerhalb dieser Organisation bereits eingesetzten
217 Authentifizierungsmethoden nachnutzen. Dies ermöglicht eine nahtlose Integration in den
218 Alltag. Akteure, die nicht zugehörig zu einer Organisation agieren, KÖNNEN Messenger-
219 Services von Verbänden nutzen, falls diese durch einen Verband für ihre Mitglieder zur
220 Verfügung gestellt werden. Hierbei kann das bestehende Authentifizierungsverfahren des
221 Verbandes verwendet werden. Messenger-Services KÖNNEN mit unterschiedlichen TI-
222 Messenger-Clients verwendet werden. So ist es beispielweise möglich, dass ein Arzt, der
223 parallel in einer Klinik und in einer niedergelassenen Praxis tätig ist, durch beide
224 Organisationen jeweils einen Messenger-Service zur Verfügung gestellt bekommt.

225 Die Messenger-Services des TI-Messenger-Dienstes werden in einer TI-Föderation
226 zusammengefasst, um nicht zugehörige Messenger-Dienste auszuschließen. Um Teil der
227 Föderation des TI-Messenger-Dienstes zu werden, MUSS die jeweilige Domain eines
228 Messenger-Services vom TI-Messenger-Anbieter durch den Registrierungs-Dienst des TI-
229 Messenger-Fachdienstes im VZD-FHIR-Directory hinterlegt werden. Ist dies erfolgt,
230 erhalten dessen Akteure Lesezugriff auf das VZD-FHIR-Directory und KÖNNEN je nach
231 Berechtigung die Kommunikation mit Akteuren in anderen Organisationen starten. Die
232 Kommunikation findet dabei Ende-zu-Ende-verschlüsselt zwischen den jeweiligen
233 beteiligten Messenger-Services und TI-Messenger-Clients statt. Die Adressierung der
234 Akteure innerhalb eines Messenger-Services erfolgt über die Matrix-User-ID und wird im
235 Kontext des TI-Messenger-Dienstes als MXID bezeichnet. Um die beteiligten Akteure über
236 den Eingang neuer Nachrichten zu informieren, MUSS der TI-Messenger-Fachdienst ein
237 Push-Gateway verfügen.

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

240



241

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

243

244 Der TI-Messenger-Dienst basiert auf dem offenen Kommunikationsprotokoll Matrix, das
 245 bereits von der Matrix Foundation gemäß [Matrix Specification] spezifiziert ist. In den von
 246 der Matrix Foundation erstellten Spezifikationen ist sowohl die Client-Server-, die
 247 Server-Server-Kommunikation als auch die API des Matrix-Push-Gateways beschrieben.
 248 Für die Sicherstellung der föderalen und dezentralen Struktur des TI-Messenger-Dienstes
 249 im deutschen Gesundheitswesen und zur Einschränkung des Nutzerkreises werden
 250 weitere Komponenten benötigt, welche in der jeweiligen durch die gematik
 251 veröffentlichten Spezifikation beschrieben werden.

252

253

3 Systemkontext

254

3.1 Akteure und Rollen

255 Im Kontext des TI-Messenger-Dienstes werden verschiedene Akteure und Rollen
 256 definiert. Als Akteur wird in diesem Zusammenhang ein Nutzer des TI-Messenger-
 257 Dienstes betrachtet. Abhängig von dem verwendeten Authentifizierungsverfahren am
 258 Messenger-Service eines TI-Messenger-Fachdienstes ergeben sich unterschiedliche
 259 Rollen, die ein Akteur einnehmen KANN. Diese sind in der Tabelle "Akteure und Rollen"
 260 beschrieben.
 261

262

Tabelle 1: Akteure und Rollen

Akteur	Rolle	Beschreibung
Leistungserbringer im Besitz eines HBAs und einer SMC-B (z. B. Ärzte, Zahnärzte, Apotheker, psychologische Psychotherapeuten)	User-HBA	<p>Ein LE im Besitz eines HBAs kann:</p> <ul style="list-style-type: none"> • sich am zuständigen IDP-Dienst authentisieren, • sich am Messenger-Service anmelden, • seine MXID auf dem VZD-FHIR-Directory hinterlegen und sich damit persönlich, sektorübergreifend erreichbar machen, • den TI-Messenger-Dienst nutzen: <ul style="list-style-type: none"> • Kommunikationen mit Akteuren innerhalb seiner Organisation aufbauen und entgegennehmen, • Kommunikationen mit Akteuren in anderen Organisationen aufbauen und entgegennehmen, • Kommunikationen mit Akteuren in der Rolle "User-HBA" aufbauen und entgegennehmen, die ebenfalls mit HBA authentisiert und somit für ihn auf dem VZD-FHIR-Directory auffindbar sind.
	Org-Admin	<p>Ein LE im Besitz einer SMC-B kann:</p> <ul style="list-style-type: none"> • sich am zuständigen IDP-Dienst authentisieren,

Akteur	Rolle	Beschreibung
		<ul style="list-style-type: none"> • einen Messenger-Service für seine Organisation (korrespondierend zu seiner SMC-B) registrieren, • die Kontaktpunkte seiner Organisation auf dem VZD-FHIR-Server administrieren und damit sektorübergreifend erreichbar machen, • die Mitarbeiter der eigenen Organisation als Akteure dieses Messenger-Services im Matrix-Homeserver administrieren, • Matrix-Homeserver-Konfigurationen für seine Organisation vornehmen, • für seine Organisation Funktionsaccounts einrichten und Chatbots zuweisen.
Mitarbeiter einer Organisation im Gesundheitswesen (z. B. Leistungserbringer ohne HBA , Pflegepersonal, Hebammen, Mitarbeiter einer Kasse)	User	<p>Ein Mitarbeiter einer Organisation im Gesundheitswesen kann:</p> <ul style="list-style-type: none"> • sich gegenüber einem Messenger-Service authentisieren, • sich an einem Messenger-Service anmelden, • den TI-Messenger-Dienst nutzen: <ul style="list-style-type: none"> • Kommunikationen mit Akteuren innerhalb seiner Organisation aufbauen und entgegennehmen, • Kommunikationen mit Akteuren in anderen Organisationen aufbauen und entgegennehmen.
	Org-Admin	<p>Ein Mitarbeiter einer Organisation im Gesundheitswesen mit Zugriff auf eine SMC-B seiner Organisation kann:</p> <ul style="list-style-type: none"> • sich am zuständigen IDP-Dienst authentisieren, • einen Messenger-Service für seine Organisation (korrespondierend zu seiner SMC-B) anlegen, • die Kontaktpunkte seiner Organisation auf dem VZD-FHIR-

Akteur	Rolle	Beschreibung
		<p>Directory administrieren und damit sektorübergreifend erreichbar machen,</p> <ul style="list-style-type: none"> • die Mitarbeiter der eigenen Organisation als Akteure dieses Messenger-Services im Matrix-Homeserver administrieren, • Matrix-Homeserver-Konfigurationen für seine Organisation vornehmen, • für seine Organisation Funktionsaccounts einrichten und Chatbots zuweisen.
Beauftragter Administrator eines TI-Messenger-Anbieters	Org-Admin	<p>Ein TI-Messenger-Anbieter kann, auf Wunsch des LE im Besitz einer SMC-B:</p> <ul style="list-style-type: none"> • einen Messenger-Service für seine Organisation anlegen, • die Kontaktpunkte seiner Organisation auf dem VZD-FHIR-Server administrieren und damit sektorübergreifend erreichbar machen, • die Mitarbeiter der eigenen Organisation als Akteure dieses Messenger-Services im Matrix-Homeserver dieser Organisation administrieren, • Matrix-Homeserver-Konfigurationen an den beauftragten Matrix-Homeservern vornehmen, • an den beauftragten Matrix-Homeservern Funktionsaccounts einrichten und Chatbots zuweisen.
Chatbot	-	<p>Ein Chatbot wird durch einen Akteur in der Rolle "Org-Admin" einem Funktionsaccount zugewiesen und kann:</p> <ul style="list-style-type: none"> • die Kommunikation mit einem Akteur starten, wenn dieser über einen Funktionsaccount der Organisation die Kommunikation wünscht,

Akteur	Rolle	Beschreibung
		<ul style="list-style-type: none"> • zuständige und verfügbare Akteure einer Organisation in den Chatraum einladen.

263 Ein Akteur ist eine natürliche Person oder ein technisches System (Chatbot) das mit
 264 einem TI-Messenger-Fachdienst interagiert. Die Interaktionen mit dem TI-Messenger-
 265 Fachdienst werden im Kapitel "Anwendungsfälle" genauer dargestellt. Im Folgenden
 266 werden die Akteure mit ihren jeweiligen Rollen weiter beschrieben.
 267

268 **Rolle: "User-HBA"**

269 Ein Akteur in der Rolle "User-HBA" KANN seine MXID im Personenverzeichnis im VZD-
 270 FHIR-Directory hinterlegen, um für andere Akteure in der Rolle "User-HBA", die ebenfalls
 271 die eigene MXID auf dem VZD-FHIR-Directory hinterlegt haben, erreichbar zu sein.
 272

273 **Rolle: "User"**

274 Für einen Akteur in der Rolle "User" KANN dessen MXID im Organisationsverzeichnis auf
 275 dem VZD-FHIR-Directory hinterlegt werden. Somit kann der Akteur nur als Mitarbeiter
 276 seiner Organisation für Akteure außerhalb (Akteure die nicht Teil der Organisation sind)
 277 gefunden werden oder Chatnachrichten im Namen dieser mittels Funktionsaccounts
 278 empfangen. Chatbots zur Abbildung von Funktionsaccounts nehmen ebenfalls die Rolle
 279 "User" ein (siehe Kapitel [5.5- Funktionsaccounts](#)).
 280

281 **Rolle: "Org-Admin"**

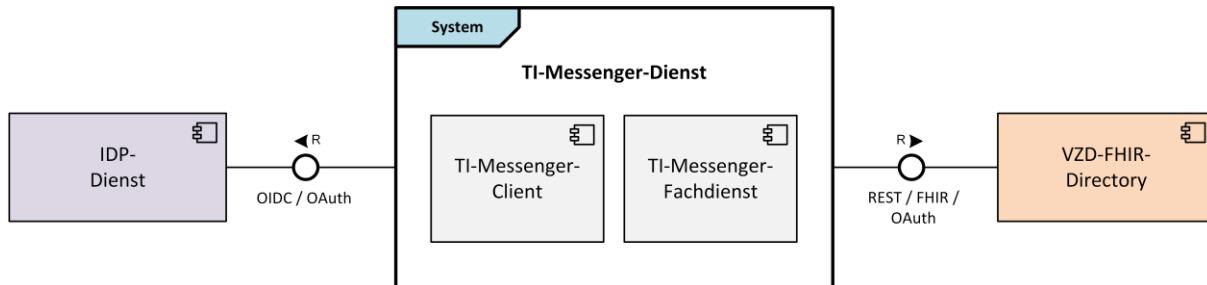
282 Ein Leistungserbringer oder ein Mitarbeiter einer Organisation im Gesundheitswesen mit
 283 Zugriff auf eine SMC-B der Organisation KANN die Rolle "Org-Admin" einnehmen, um
 284 Messenger-Services für seine Organisation zu registrieren und Einträge im VZD-FHIR-
 285 Directory zu verwalten. Für die Rolle "Org-Admin" besteht die Notwendigkeit, einen
 286 Administrator einzusetzen, welcher für Themen der Informationssicherheit geschult und
 287 sensibilisiert wurde. Ein TI-Messenger-Anbieter KANN im Auftrag einer Organisation
 288 einen Administrator mit der Rolle "Org-Admin" beauftragen und die in der Tabelle
 289 "Akteure und Rollen" beschriebenen Dienste anbieten.
 290

291 *Hinweis: Versicherte DÜRFEN aktuell NICHT als Akteure auf einem Messenger-Service
 292 eingetragen werden. Für die Nutzung eines Messenger-Service sind nur Akteure
 293 zugelassen die durch ein bestehendes Vertragsverhältnis der jeweiligen Organisation
 294 zugeordnet werden können oder im Besitz eines HBAs sind.*

295 **3.2 Nachbarsysteme**

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

297



298

Abbildung 2: Benachbarten Produkttypen des TI-Messenger-Dienstes

300

301 Der TI-Messenger-Dienst als System besteht aus den Komponenten TI-Messenger-Fachdienst und TI-Messenger-Client.
 302 Der Registrierungs-Dienst des TI-Messenger-Fachdienstes nutzt die OAuth- und REST-Schnittstellen des VZD-FHIR-Directory, um sich mittels OAuth Client Credential Flow zu authentisieren um somit Zugriff auf das FHIR-Directory zu erhalten. Der TI-Messenger-Client nutzt die Schnittstellen eines zuständigen IDP-Dienstes zur Authentifizierung eines Akteurs sowie Schnittstellen des VZD-FHIR-Directory, um z. B. FHIR-Ressourcen zu finden oder zu ändern.

309 **3.3 Ausprägungen des Messenger-Services**

310 Der Messenger-Service ist eine Teilkomponente des TI-Messenger-Fachdienstes und wird durch den jeweiligen Anbieter für eine Organisation bereitgestellt. Der Messenger-Service besteht aus einem Matrix-Homeserver (basierend auf dem Matrix-Protokoll) und einem Messenger-Proxy der sicherstellt, dass eine Kommunikation mit anderen Messenger-Services, als Teil des TI-Messenger-Dienstes, nur innerhalb der gemeinsamen TI-Föderation erfolgt. Die Messenger-Services KÖNNEN den Akteuren unterschiedliche Authentifizierungsverfahren anbieten, bei denen der Besitz einer SMC-B oder eines HBAs nicht vorausgesetzt werden kann. Messenger-Services MÜSSEN immer Organisationen bzw. Verbänden zugeordnet sein, die über die Kontrolle des verwendeten Authentifizierungsverfahren verfügen.

320 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 Akteure bereitgestellt werden. Die Organisation und der von ihr gewählte TI-Messenger-Anbieter vereinbaren das zur Anwendung kommende Authentifizierungsverfahren bilateral und stimmen sich über die technische Realisierung der dafür notwendigen Anbindung ab. Möglich ist beispielsweise die Nachnutzung eines in der Organisation betriebenen Active Directory (AD/LDAP) oder eines geeigneten Single-Sign-On-Verfahrens (SSO). Der Anbieter MUSS sicherstellen, dass die Organisation die Kontrolle über die jeweiligen Authentifizierungsmechanismen besitzt und die Möglichkeit erhält um eine notwendige Löschung oder Sperrung eines Nutzer-Accounts sicherzustellen.

331 Zum besseren Verständnis werden im Folgenden vier Anwendungsbeispiele erläutert:

332

333 **Anwendungsbeispiel für eine Arztpraxis**

334 Ein Akteur in der Rolle "Org-Admin" in einer Arztpraxis authentifiziert sich mittels der SMC-B der Organisation bei einem Registrierungs-Dienst eines TI-Messenger-Anbieters

336 und erstellt einen Messenger-Service der sowohl *on-premise*, als auch in einem
337 Rechenzentrum bereitgestellt werden kann. Der Anbieter stellt daraufhin der Arztpraxis
338 einen Messenger-Service mit einem sicheren Authentifizierungsverfahren bereit.
339 Zusätzlich KANN der TI-Messenger-Anbieter einen Admin-Account für den Akteur in der
340 Rolle "Org-Admin" auf diesem Messenger-Service erstellen, mit dem der Akteur für seine
341 Organisation weitere Akteure hinterlegt (z. B. MFA, Ärzte). Die angelegten Akteure
342 melden sich am Messenger-Service an und können den TI-Messenger in der Rolle "User"
343 direkt nutzen.

344 Ein Akteur in der Rolle "Org-Admin" KANN für seine Organisation MXIDs von Akteuren im
345 Organisationsverzeichnis auf dem VZD-FHIR-Directory einrichten, um diese für Akteure
346 anderer Organisationen des TI-Messenger-Dienstes erreichbar zu machen. Akteure der
347 Arztpraxis im Besitz eines HBAs (Rolle "User-HBA") KÖNNEN sich zusätzlich im TI-
348 Messenger-Client mittels HBA authentisieren und so die eigene MXID als Practitioner-
349 Eintrag im Personenverzeichnis auf dem VZD-FHIR-Directory hinterlegen. Somit haben
350 sie zusätzlich die Möglichkeit andere, auf dem VZD-FHIR-Directory hinterlegte, HBA-
351 Inhaber (Rolle "User-HBA") in einen Chatraum einzuladen oder für diese erreichbar
352 werden.

353

354 Anwendungsbeispiel für ein Krankenhaus

355 Ein Krankenhaus authentifiziert sich durch einen Akteur in der Rolle "Org-Admin" mittels
356 SMC-B bei dem Registrierungs-Dienst eines TI-Messenger-Anbieters. Der Anbieter prüft
357 die bereitgestellte SMC-B und stellt dem Krankenhaus einen Messenger-Service bereit.
358 Durch die Dezentralität KANN dieser Service sowohl *on-premise*, als auch in einem
359 Rechenzentrum bereitgestellt werden. Der Messenger-Service KANN das bestehende
360 Authentifizierungsverfahren des Krankenhauses (z. B. Active Directory) nachnutzen. Die
361 Akteure des Krankenhauses können mit den bestehenden Anmeldedaten den TI-
362 Messenger-Dienst nahtlos verwenden, auch ohne im Besitz eines HBAs (Pflege,
363 Therapeuten, Ärzte ohne HBA = Rolle: "User") zu sein.

364 Ein Akteur in der Rolle "Org-Admin" KANN für sein Krankenhaus MXIDs von Akteuren im
365 Organisationsverzeichnis auf dem VZD-FHIR-Directory einrichten, um diese für Akteure
366 anderer Organisationen (z. B. Krankenhaus, Arztpraxis) des TI-Messenger-
367 Dienstes erreichbar zu machen. Akteure des Krankenhauses im Besitz eines HBAs
368 KÖNNEN zusätzlich mittels des TI-Messenger-Clients die eigene MXID als Practitioner-
369 Eintrag im Personenverzeichnis auf dem VZD-FHIR-Directory hinterlegen (Rolle "User-
370 HBA"). Somit haben sie zusätzlich die Möglichkeit andere, auf dem VZD-FHIR-Directory
371 hinterlegte, HBA-Inhaber (Rolle "User-HBA") in einen Chatraum einzuladen oder für diese
372 erreichbar werden.

373

375 Anwendungsbeispiel für Apotheken

376 Ein TI-Messenger-Anbieter stellt der Apotheke einen Messenger-Service bereit. Durch die
377 Dezentralität KANN dieser Service sowohl *on-premise*, als auch in einem Rechenzentrum
378 bereitgestellt werden. Der Messenger-Service wird mit dem zuständigen IDP-Dienst der
379 Apotheken verwendet. Die dort hinterlegten Akteure der Apotheken KÖNNEN den TI-
380 Messenger mittels OpenID-Connect verwenden auch ohne im Besitz eines HBAs zu sein
381 (z. B. PTA, angestellte Apotheker ohne HBA).

382

383 Die Apotheke wird als Organisation für andere Akteure des TI-Messengers erreichbar,
384 indem ein Akteur in der Rolle "Org-Admin" MXIDs von Akteuren seiner Apotheke im
385 Organisationsverzeichnis auf dem VZD-FHIR-Directory einrichtet. Akteure der Apotheke

386 im Besitz eines HBAs (Rolle "User-HBA") KÖNNEN zusätzlich mittels des TI-Messenger-
387 Clients die eigene MXID als Practitioner-Eintrag im Personenverzeichnis auf dem VZD-
388 FHIR-Directory hinterlegen. Somit haben sie zusätzlich die Möglichkeit andere, auf dem
389 VZD-FHIR-Directory hinterlegte, HBA-Inhaber (Rolle "User-HBA") in einen Chatraum
390 einzuladen oder für diese erreichbar werden.

391

392 **Anwendungsbeispiel für Verbände**

393 Der Anbieter eines TI-Messengers stellt Verbänden einen Messenger-Service mit eigenem
394 Authentifizierungsverfahren (z. B LDAP) zur Verfügung. Durch die Dezentralität KANN
395 dieser Service sowohl *on-premise*, als auch in einem Rechenzentrum bereitgestellt
396 werden. Der Messenger-Service KANN mit dem bestehenden Authentifizierungsverfahren
397 des Verbandes genutzt werden. Die dort hinterlegten Mitglieder haben somit die
398 Möglichkeit ihre bestehenden Authentifizierungsdaten bei der Nutzung des TI-Messenger-
399 Dienstes zu verwenden.

400 Akteure des Verbandes im Besitz eines HBAs (Rolle "User-HBA") KÖNNEN zusätzlich
401 mittels des TI-Messenger-Clients die eigene MXID als Practitioner-Eintrag im
402 Personenverzeichnis auf dem VZD-FHIR-Directory hinterlegen. Damit können sie andere,
403 auf dem VZD-FHIR-Directory hinterlegte, HBA-Inhaber (Rolle "User-HBA") in einen
404 Chatraum einladen oder für diese erreichbar werden.

405 Im Folgenden wird die Kommunikation für eingehende und ausgehende Nachrichten aus
406 der Nutzersicht eines Akteurs in der Rolle "User" und "User-HBA" in einer
407 Kommunikationsmatrix noch einmal verdeutlicht.

408

409 **Tabelle 2: Kommunikationsmatrix**

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

Akteuren in der Rolle "User" als Ansprechpartner der Organisation (Die MXID wurde durch einen Akteur in der Rolle "Org-Admin" in das Organisationsverzeichnis auf dem VZD-FHIR-Directory hinterlegt)	-	x	-
Akteuren in der Rolle "User" und "User-HBA" durch Scan eines QR-Codes	-	x	x
Akteuren in der Rolle "User-HBA" anderer Messenger-Services	-	-	x

410

411 3.4 TI-Messenger Föderation

412 Da der TI-Messenger-Dienst auf dem offenen und dezentralen Kommunikationsprotokoll
 413 Matrix basiert, MUSS gewährleistet werden, dass nur berechtigte Matrix-Homeserver
 414 eines Messenger-Services teilnehmen.

415 Um allen berechtigten Akteuren des deutschen Gesundheitswesens den Zugang zum TI-
 416 Messenger-Dienst zu gewähren, MUSS ein Anbieter eines TI-Messengers für
 417 Leistungserbringerinstitutionen und/oder Organisationen eigene Messenger-Services
 418 bereitstellen. Um nicht zum TI-Messenger-Dienst gehörende Matrix-Homeserver
 419 ausschließen zu können, werden die Domännamen (im Weiteren auch als Matrix-Domain
 420 bezeichnet) der Matrix-Homeserver der Messenger-Services in einer Föderationsliste
 421 zusammengefasst. Diese wird durch das VZD-FHIR-Directory bereitgestellt.
 422 Voraussetzung für die Aufnahme in die Föderation ist der Betrieb eines Messenger-
 423 Proxies als Teil des Messenger-Services, der sicherstellen MUSS, dass nur zugelassene
 424 TI-Messenger-Fachdienste Zugang in die Föderation erhalten. Für die Aufnahme in die
 425 Föderation MÜSSEN ausschließlich Matrix-Homeserver verwendet werden. Ein Bridging
 426 anderer Messaging-Protokolle DARF NICHT stattfinden. Es MUSS für die Aufnahme in die
 427 Föderation eine erfolgreiche Zulassung des TI-Messenger-Anbieters mit ebenfalls
 428 erfolgreichen Zulassungen für die Produkttypen TI-Messenger-Fachdienst und TI-
 429 Messenger-Client durch die gematik erfolgt sein. Nach einer erfolgreichen
 430 Zulassung erhält der Registrierungs-Dienst des jeweiligen Fachdienstes die Möglichkeit
 431 die Matrix-Domains der jeweiligen Messenger-Services einer entsprechenden
 432 Organisation auf dem VZD-FHIR-Directory zuzuordnen.

433 3.5 Berechtigungskonzept

434 Wie im Kapitel "TI-Messenger Föderation" beschrieben, dient die TI-Messenger-
 435 Föderation dazu, nicht zugelassene Matrix-Homeserver aus dem TI-Messenger-Dienst
 436 auszuschließen. Ebenfalls MUSS es möglich sein, dass nur die im Kapitel 3.1- Akteure
und Rollen genannten berechtigten Akteure miteinander kommunizieren dürfen. Hierfür
 437 ist die Etablierung eines Rechtekonzeptes innerhalb des TI-Messenger-Dienstes
 438 notwendig.

439 Das Rechtekonzept basiert auf einer mehrstufigen Prüfung. Mit Hilfe des
 440 Berechtigungskonzeptes wird nachgewiesen, ob ein Akteur berechtigt ist, innerhalb der
 441 TI-Messenger-Föderation einen Akteur in einen Chatraum einzuladen.

443 Die einzelnen Stufen werden im Folgenden weiter beschrieben:

444

445 **Stufe 1**

446 In der 1. Stufe MUSS geprüft werden, ob die in der Anfrage enthaltenen Matrix-Domains
447 zugehörig zur TI-Föderation sind. Ist dies der Fall, SOLL die Anfrage an den Matrix-
448 Homeserver des Einladenden weitergeleitet werden. Ist dies nicht der Fall, MUSS
449 die beabsichtigte Anfrage des Akteurs vom Messenger-Proxy des Einladenden abgelehnt
450 werden. Nach der Weiterleitung an den Matrix-Homeserver prüft dieser, ob der
451 eingeladene Akteur der gleichen Organisation angehört. Stellt der Matrix-Homeserver
452 fest das der eingeladene Akteur nicht zu seiner Domain gehört wird das `Invite-Event` an
453 den Messenger-Proxy des einzuladenden Akteurs weitergeleitet. Dieser prüft erneut die
454 Zugehörigkeit zur TI-Föderation (Stufe 1). Bei erfolgreicher Prüfung erfolgt dann die
455 Weiterverarbeitung gemäß der Stufe 2.

456

457 **Stufe 2**

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

464

465 **Stufe 3**

466 In der letzten Stufe erfolgt die Prüfung ausgehend von den Einträgen der beteiligten
467 Akteure im VZD-FHIR-Directory. Die Einladung SOLL zugelassen werden, wenn:

- 468 • die MXID des einzuladenden Akteurs im Organisationsverzeichnis hinterlegt ist
469 oder
- 470 • der einladende sowie der einzuladende Akteur im Personenverzeichnis hinterlegt
471 sind.

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

474 **3.6 Verwendung der Token**

475 Für die Nutzung des TI-Messenger-Dienstes kommen unterschiedliche Arten von Token
476 zur Authentisierung an weiteren Diensten zum Einsatz die in verschiedenen
477 Anwendungsfällen verwendet werden. Aus diesem Grund werden in der folgenden Tabelle
478 die verschiedenen Token näher beschrieben.

479

480 **Tabelle 3: Arten von Token**

Token	ausgestellt vom	Beschreibung
ID_TOKEN	IDP-Dienst	Dieses Token wird auf Basis von SmartCard-Identitäten vom zuständigen IDP-Dienst

Token	ausgestellt vom	Beschreibung
		<p>ausgestellt.</p> <p>Dieses Token wird vom Frontend des Registrierungs-Dienstes sowie den TI-Messenger-Clients verwendet, um sich gegenüber dem Registrierungs-Dienst oder dem Auth-Service des VZD-FHIR-Directory zu authentifizieren.</p>
Matrix-ACCESS_TOKEN	Matrix-Homeserver	<p>Nach der erfolgreichen initialen Registrierung oder 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.</p> <p>Mit dem Matrix-ACCESS_TOKEN MUSS sich ein Akteur mit einem existierenden Matrix-Account, an seinem Matrix-Homeserver authentisieren. Dieses Token MUSS im lokalen Speicher des TI-Messenger-Clients sicher abgespeichert werden, wird bei jeder weiteren Interaktion mit seinem Matrix-Homeserver verwendet und ist an die Session des jeweiligen TI-Messenger-Clients gebunden.</p>
Matrix-OpenID-Token	Matrix-Homeserver	<p>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.</p> <p>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.</p>
provider-accesstoken	OAuth des VZD-FHIR-Directory	Das provider-accesstoken wird dem Registrierungs-Dienst durch den OAuth-Service des VZD-FHIR-Directory bereitgestellt.

Token	ausgestellt vom	Beschreibung
		<p>Ein provider-accesstoken wird benötigt, wenn der Registrierungs-Dienst eines TI-Messenger-Fachdienstes, nach der Bereitstellung eines neuen Messenger-Service für eine Organisation, einen neuen Eintrag für diese Ressource im VZD-FHIR-Directory anlegen oder der Registrierungs-Dienst eine Föderationsliste vom FHIR-Proxy abfragen möchte. Der Registrierung-Dienst übergibt dazu vereinbarte Client-Credentials an den OAuth-Service des VZD-FHIR-Directory und erhält nach der erfolgreichen Prüfung dieser Credentials das provider-accesstoken.</p>
search-accesstoken	Auth-Service des VZD-FHIR-Directory	<p>Das search-accesstoken wird einem berechtigten Akteur durch den Auth-Service das VZD-FHIR-Directory bereitgestellt.</p> <p>Dieses wird für die Suche im VZD-FHIR-Directory benötigt und stellt sicher, dass nur berechtigte 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.</p>
owner-accesstoken	Auth-Service des VZD-FHIR-Directory	<p>Das owner-accesstoken wird einem berechtigten Akteur durch den Auth-Service das VZD-FHIR-Directory bereitgestellt.</p> <p>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 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 einen zuständigen IDP-Dienst benutzen. Das durch den IDP ausgestellte ID_TOKEN wird durch den Auth-Service des VZD-FHIR-Directory geprüft. Bei</p>

Token	ausgestellt vom	Beschreibung
		erfolgreicher Prüfung wird das owner-accesstoken vom Auth-Service ausgestellt.

481

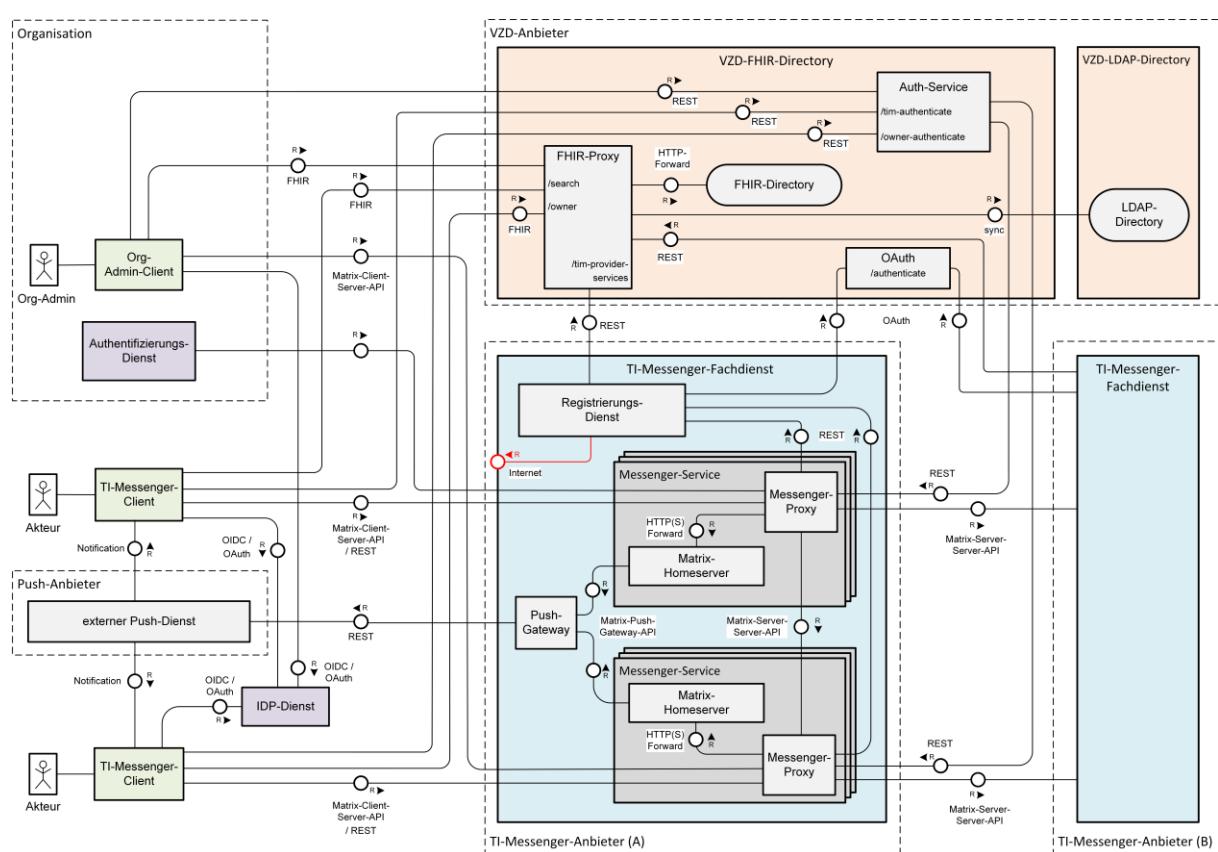
482

483

4 Systemzerlegung

484 Wie bereits im Kapitel "Systemüberblick" dargestellt sind bei der Umsetzung der
 485 Funktionalitäten des TI-Messenger-Dienstes mehrere Komponenten beteiligt, die durch
 486 verschiedene Anbieter bereitgestellt werden. Im Folgenden werden die jeweiligen
 487 beteiligten Komponenten des TI-Messenger-Dienstes weiter beschrieben.

488 Die folgende Abbildung zeigt alle an der TI-Messenger-Architektur beteiligten
 489 Komponenten mit deren Schnittstellen.
 490



491

492 **Abbildung 3: Komponenten der TI-Messenger-Architektur und deren Schnittstellen**

493

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

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

502 4.1 IDP-Dienst

503 Ein IDP-Dienst stellt JSON Web Token (JWT) für attestierte Identitäten aus. Er
504 übernimmt die Aufgabe der Identifikation der Akteure für den Fachdienst. Das bedeutet,
505 Fachdienste MÜSSEN keine Überprüfung der Akteure selbst implementieren, sondern
506 KÖNNEN davon ausgehen, dass der Besitzer des bei ihnen vorgetragenen "ID_TOKEN"
507 bereits identifiziert und authentifiziert wurde. Anwendungsfrontends können über die
508 Authentifizierung des Akteurs am IDP-Dienst Zugriff (gegen Vorlage des ausgestellten
509 ID_TOKEN) zu den von den Fachdiensten angebotenen Daten erhalten.

510 In der ersten Ausbaustufe des TI-Messengers-Dienstes MUSS der von der gematik
511 spezifizierte zentrale IDP-Dienst verwendet werden. Dieser ermöglicht die sichere
512 Identifikation der Akteure anhand der ihnen bereitgestellten Identifikationsmittel (SMC-B
513 / HBA). Die Identifikation des Akteurs wird anhand einer Smartcard und der Auswertung
514 des vom Authenticator-Modul an den IDP-Dienst übergebenen
515 Authentifizierungszertifikats (aus der Smartcard) sichergestellt. Das Authenticator-Modul
516 wird auf dezentraler Hardware zusammen mit dem Primärsystem oder auf dem mobilen
517 Endgerät des Akteurs betrieben. Das Authenticator-Modul für den zentralen IDP-
518 Dienst wird von der gematik bereitgestellt.

519 Werden zukünftig weitere zugelassene IDP-Dienste verfügbar KÖNNEN diese ebenfalls für
520 die Authentifizierung von Akteuren genutzt werden. Im Folgenden wird nur noch der
521 Begriff IDP-Dienst verwendet.

522 4.2 VZD-FHIR-Directory

523 Beim VZD-FHIR-Directory handelt es sich um einen zentralen Verzeichnisdienst der TI, der
524 die deutschlandweite Suche von Organisationen und Akteuren des TI-Messenger-Dienstes
525 ermöglicht. Das VZD-FHIR-Directory basiert auf dem FHIR-Standard zum Austausch von
526 definierten Informationsobjekten (FHIR-Ressourcen).

527 Der Verzeichnisdienst bietet zwei Arten von Verzeichnistypen an, die durchsucht werden
528 können. Für die Suche von Organisationseinträgen wird das Organisationsverzeichnis
529 (*HealthcareService*) und für die Suche von Akteuren das Personenverzeichnis
530 (*PractitionerRole*) verwendet. Im Organisationsverzeichnis sind alle auf eine
531 Organisation bezogenen Ressourcen hinterlegt die durch einen Akteur in der Rolle "Org-
532 Admin" der Organisation gepflegt werden. Das Personenverzeichnis bietet Akteuren in
533 der Rolle "User-HBA" die Möglichkeit, alle zu seiner *PractitionerRole* gehörenden FHIR-
534 Einträge zu konfigurieren. Für die Suche nach FHIR-Einträgen werden durch die TI-
535 Messenger-Clients FHIR-Schnittstellen am VZD-FHIR-Directory aufgerufen. Bei der
536 Verwendung der Schnittstellen MUSS sich der TI-Messenger-Client gegenüber dem VZD-
537 FHIR-Directory authentifizieren. Für die Authentifizierung werden die im Kapitel
538 "Verwendung der Token" beschriebenen accesstoken (search-accesstoken und owner-
539 accesstoken) verwendet. In der folgenden Tabelle werden die beiden Verzeichnistypen in
540 Abhängigkeit der jeweiligen Identität und den sich daraus ergebenden Berechtigungen
541 gezeigt.

542
543
544

545

Tabelle 4: Verzeichnistypen - Rechtekonzept

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

546

547 Zusätzlich zur Bereitstellung der Verzeichnistypen ermöglicht das VZD-FHIR-Directory
 548 ebenfalls die sektorenübergreifende Kommunikation. Hierfür wird die Matrix-Domain
 549 eines Messenger-Services durch einen Eintrag in das VZD-FHIR-Directory durch den
 550 Registrierungs-Dienst in die TI-Föderation aufgenommen. Für die Registrierung der
 551 Matrix-Domain wird durch den Registrierungs-Dienst eine REST-Schnittstelle am VZD-
 552 FHIR-Directory aufgerufen, die mittels OAuth2 Client Credentials Flow gesichert ist. Dies
 553 ermöglicht es TI-Messenger-Anbietern ihre betriebenen Messenger-Services in die TI-
 554 Messenger-Föderation aufzunehmen und zu verwalten.

555 Allgemein besteht das VZD-FHIR-Directory aus mehreren Teilkomponenten (FHIR-Proxy,
 556 Auth-Service, OAuth-Service und FHIR-Directory) die benötigt werden, um alle
 557 Funktionsmerkmale abilden zu können. Im Folgenden werden die Teilkomponenten
 558 weiter beschrieben. Weiterführende Informationen zum VZD-FHIR-Directory sind in [api-
 559 vzd] zu finden.

560

FHIR-Proxy

562 Der FHIR-Proxy ist eine Teilkomponente des VZD-FHIR-Directory. Alle Anfragen an das
 563 FHIR-Directory werden über den FHIR-Proxy verarbeitet. Der FHIR-Proxy stellt die
 564 folgenden drei Schnittstellen zur Verfügung, die durch die TI-Messenger-Clients sowie
 565 durch den Registrierungs-Dienst aufgerufen werden:

- 566 • /search (FHIR-Schnittstelle zur Suche)
- 567 • /owner (FHIR-Schnittstelle zur Pflege eigener Einträge)
- 568 • /tim-provider-services (REST-Schnittstelle zur Pflege eigener TIM Provider
 569 Einträge und MXIDs der Organisationen und Akteuren)

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

573

Auth-Service

575 Die Teilkomponente Auth-Service stellt den TI-Messenger-Clients die für den Aufruf der
 576 FHIR-Schnittstellen am FHIR-Proxy benötigen access-token aus. Hierbei werden die zwei
 577 folgenden REST-Schnittstellen:

- 578 • /tim-authenticate und

579 • /owner-authenticate
580 verwendet. Die Schnittstelle /tim-authenticate erwartet ein Matrix-OpenID-Token,
581 wohingegen bei der Schnittstelle /owner-authenticate ein ID_TOKEN übergeben
582 werden muss.

583
584 **OAuth**

585 Bei Aufruf der REST-Schnittstelle /tim-provider-services durch den Registrierungs-
586 Dienst am FHIR-Proxy wird ein accessstoken (provider-accessstoken) benötigt, welches von
587 der Teilkomponente OAuth ausgestellt wird. Hierfür MUSS sich der Registrierungs-Dienst
588 des TI-Messenger-Fachdienstes bei der Teilkomponente OAuth des VZD-FHIR-Directory
589 mittels OAuth2 Client Credentials Flow authentisieren. Zuvor MUSS der TI-Messenger-
590 Anbieter für seinen Registrierungs-Dienst beim VZD-Anbieter Client-Credentials
591 beantragen.

592
593 **FHIR-Directory**
594 Die Teilkomponente FHIR-Directory stellt das zentrale Verzeichnis der FHIR-Ressourcen
595 bereit.

596 **4.3 TI-Messenger-Fachdienst**

597 Der TI-Messenger-Fachdienst ist die zentrale Komponente des TI-Messenger-Dienstes zur
598 Ad-hoc-Kommunikation zwischen mehreren Akteuren. Für die Kommunikation mit den TI-
599 Messengers-Clients stellt der Fachdienst alle notwendigen Schnittstellen bereit. Für eine
600 fachdienstübergreifende Kommunikation werden alle Nachrichten an die in der TI-
601 Föderation gelisteten TI-Messenger-Fachdienste übermittelt. Es MUSS sichergestellt
602 werden, dass die Organisation die Akteure jederzeit identifizieren kann und das die
603 Organisationen Akteure jederzeit aus dem TI-Messenger-Dienst ausschließen können.
604 Daher MUSS die Kontrolle über die Identitäten bei der Organisation liegen. Hierbei ist
605 eine Delegierung, z. B. an einen Dienstleister zulässig. Jeder Anbieter, der einen TI-
606 Messenger-Fachdienst bereitstellt, MUSS einen Registrierungs-Dienst, ein Push-Gateway
607 sowie einen oder mehrere Messenger-Services betreiben. Im Folgenden werden die
608 einzelnen Komponenten weiter beschrieben.

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

614 **4.3.1 Registrierungs-Dienst**

615 Der Registrierungs-Dienst ist eine Komponente, die vom Hersteller des TI-Messenger-
616 Fachdienstes umgesetzt werden MUSS. Durch diese MÜSSEN im VZD-FHIR-Directory die
617 Matrix-Domains der TI-Messenger-Fachdienste, die an der Föderation des TI-Messengers
618 teilnehmen, eingetragen werden. Die Eintragung der Matrix-Domain SOLL automatisch
619 erfolgen. Ebenfalls KANN über den Registrierungs-Dienst das Accounting durchgeführt
620 werden. Dies wird von der gematik nicht normativ festgelegt.

621 Um einen benutzerfreundlichen Onboarding-Prozess zu gewährleisten MUSS der
622 Registrierungs-Dienst die Bereitstellung eines Messenger-Service über ein Frontend
623 ermöglichen (im Folgenden auch als Frontend des Registrierungs-Dienstes bezeichnet).

624 Nach der erfolgreichen Authentisierung einer Organisation, durch Validierung eines
625 ausgestellten ID_TOKEN von einem zuständigen IDP-Dienst, wird für einen Akteur in der
626 Rolle "Org-Admin" ein Administrations-Account im Registrierungs-Dienst angelegt. Das
627 ermöglicht es einem Akteur in der Rolle "Org-Admin" dezentrale Messenger-Service für
628 seine Organisation zu beantragen. Dazu MUSS das Frontend des Registrierungs-Dienstes
629 bei allen durch ihn unterstützten IDP-Diensten registriert sein. Vor dem Anlegen eines
630 neuen Messenger-Service MUSS der Registrierungs-Dienst prüfen, ob der beantragte
631 Domain-Name verfügbar ist und diesen zur TI-Messenger Föderation hinzufügen.

632 Neben der Registrierung neuer Messenger-Services, dient der Registrierungs-Dienst als
633 Middleware zwischen TI-Messenger-Services und dem VZD-FHIR-Directory und speichert
634 eine aktuelle Liste aller verifizierten Domains (Föderationsliste), damit diese von den
635 Messenger-Proxies des TI-Messenger-Fachdienstes abgerufen werden können (siehe
636 Kapitel [3.5- Berechtigungskonzept - Stufe 1](#)). Darüber hinaus wird am Registrierungs-
637 Dienst eine Freigabeliste bereitgestellt. Diese dient dem Messenger-Proxy zur Prüfung
638 von Berechtigungen bei der Kontaktaufnahme von anderen Akteuren (siehe Kapitel [3.5-
639 Berechtigungskonzept - Stufe 2](#)). Hierfür MUSS der Registrierungs-Dienst eine
640 Schnittstelle bereitstellen, mit der TI-Messenger-Clients Berechtigungen hinterlegen
641 können. Eine weitere Funktion des Registrierungs-Dienstes ist die Überprüfung auf
642 Einträge im VZD-FHIR-Directory. Diese dient ebenfalls dem Messenger-Proxy zur Prüfung
643 von Berechtigungen bei der Kontaktaufnahme von anderen Akteuren (siehe Kapitel [3.5-
644 Berechtigungskonzept - Stufe 3](#)).

645 **4.3.2 Push-Gateway**

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

650 **4.3.3 Messenger-Service**

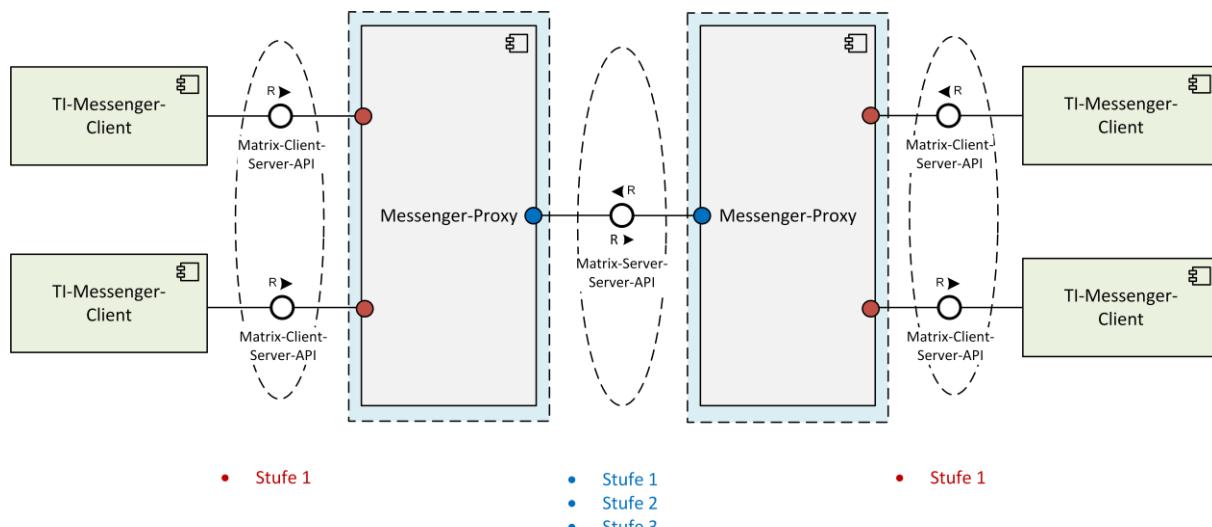
651 Ein Messenger-Service besteht aus einem Messenger-Proxy und einem Matrix-
652 Homeserver der gemäß der Spezifikation der Matrix Foundation implementiert ist.
653 Messenger-Services unterscheiden sich lediglich durch die jeweils unterstützten
654 Authentifizierungsverfahren. Es ist notwendig, dass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

659 **4.3.3.1 Messenger-Proxy**

660

661 Der Messenger-Proxy als Prüfinstanz aller eingehenden Anfragen zum Messenger-Service
662 ist für die Regelung der gemäß Matrix Client-Server-API und Matrix-Server-Server-API
663 geltenden Aufrufe zuständig. Die hierbei jeweils umzusetzenden Prüfregeln unterscheiden
664 sich und werden im Folgenden näher beschrieben. Die folgende Abbildung zeigt die
665 durchzuführenden Prüfungen in Abhängigkeit der beabsichtigten Kommunikation.

666



667

Abbildung 4: Darstellung der Berechtigungsprüfung am Messenger-Proxy

669

Client-Server Proxy

In der Funktion als Client-Server Proxy prüft der Messenger-Proxy eingehende `Invite`-Events der TI-Messenger-Clients (in der Abbildung rot dargestellt). Hierbei MUSS der Messenger-Proxy prüfen, ob die in der Anfrage enthaltenen Matrix-Domain zur TI-Föderation gehören (siehe Kapitel [3.5- Berechtigungskonzept](#) - Stufe 1). Nach erfolgreicher Prüfung, wird das `Invite`-Event an den Matrix-Homeserver weitergeleitet. Der Matrix-Homeserver prüft daraufhin, ob die beteiligten Akteure auf dem selben Matrix-Homeserver registriert sind. Ist dies nicht der Fall, wird das `Invite`-Event an den zuständigen Messenger-Proxy des Einzuladenden weitergeleitet. In diesem Fall findet die weiterer Prüfung beim Messenger-Proxy des Einzuladenden statt (Server-Server Proxy).

680

Server-Server Proxy

682 In der Funktion als Server-Server Proxy prüft der Messenger-Proxy eingehende Matrix-
683 Events anderer Messenger-Proxies. Hierbei MÜSSEN alle Stufen gemäß Kapitel 3.5-Berechtigungskonzept vom Messenger-Proxy geprüft werden (in der Abbildung blau
684 dargestellt). Ist keine der drei Stufen erfolgreich geprüft worden, dann MUSS der
685 Messenger-Proxy die Verbindung ablehnen.
686

687

Weiterführende Vorgaben

689 Die Komponente Messenger-Proxy MUSS für jeden Messenger-
690 Service separat bereitgestellt werden. Es ist nicht zwingend notwendig, diese auf die
691 Matrix-Server-Server-API und Matrix-Client-Server-API bezogenen Prüfungen durch
692 getrennte Komponenten zu realisieren. Die Art der Umsetzung bleibt dem TI-Messenger-
693 Fachdienst-Hersteller überlassen.

Bei einer Nutzung des Messenger-Services für eine Organisation dient der Messenger-Proxy zusätzlich als Schnittstelle für den Anschluss des Authentifizierungs-Dienstes der Organisation an den Ziel Matrix-Homeserver.

697

698

699 4.3.3.2 Matrix-Homeserver

700 Für den Betrieb des TI-Messenger-Dienstes MUSS der TI-Messenger-Anbieter mindestens
701 einen Matrix-Homeserver gemäß der Matrix-Foundation Spezifikation in der
702 sektorübergreifenden TI-Föderation betreiben. Es MÜSSEN alle Matrix-Homeserver die in
703 der Föderation verwendet werden den Anforderungen der Matrix Foundation Spezifikation
704 entsprechen. Über den Matrix-Homeserver findet die Ad-hoc-Kommunikation der
705 Akteure sowie weitere Nutzerinteraktionen (z. B. Starten neuer Räume etc.) statt.

706 4.4 TI-Messenger-Client

707 Ein TI-Messenger-Client ist eine mobile oder stationäre Anwendung. Diese basiert auf der
708 von der Matrix-Foundation definierten Spezifikation und ermöglicht die Ad-hoc-
709 Kommunikation von Akteuren über den TI-Messenger-Dienst. Im Kontext des TI-
710 Messenger-Dienstes wird zwischen zwei Ausprägungen des TI-Messenger-Clients
711 unterschieden. Diese ergeben sich aus den jeweiligen Rollen der Akteure, die im
712 Folgenden weiter beschrieben werden.

713 Für die Realisierung von Anwendungsfällen, die ausschließlich ein Administrator der
714 Organisation ausführt (siehe Kapitel 6- *Anwendungsfälle*, dem Akteur "Org-Admin"
715 zugeordneten Anwendungsfälle), MUSS ein TI-Messenger-Anbieter einen TI-Messenger-
716 Client mit Administrationsfunktionen anbieten (auch als Org-Admin-Client bezeichnet).
717 Diese erweiterte Funktionalität KANN auch in den TI-Messenger-Client für Akteure
718 integriert sein. TI-Messenger-Clients für Akteure (Akteure in der Rolle User / User-HBA)
719 unterstützen die von der Matrix-Spezifikation festgelegten Funktionalitäten sowie die
720 Abfragen im VZD-FHIR-Directory. Der geforderte mindestens bereitzustellende
721 Funktionsumfang wird in der [gemSpec_TI-Messenger-Client] beschrieben.

722

723

724

725

5 Übergreifende Festlegungen

726

5.1 Datenschutz und Sicherheit

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

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

738

5.2 Verwendete Standards

739

Matrix

740 Für den TI-Messenger-Dienst wird das offene Kommunikationsprotokoll der Matrix-
741 Foundation verwendet. Im Rahmen der Spezifikation wird das Server-Server- (gemäß
742 [Server-Server API]) und das Client-Server-Protokoll (gemäß [Client-Server API])
743 nachgenutzt. Für die Kommunikation der Matrix-Homeserver in der Föderation wird die
744 API gemäß [Server-Server API] verwendet. Der TI-Messenger-Client setzt bei der
745 Kommunikation mit den Matrix-Homeservern die API des Matrix-Client-Server-Protokolls
746 um. Für die Benachrichtigung der Akteure über eingehende Nachrichten wird ein Push-
747 Gateway verwendet, welches gemäß [Push Gateway API] nachgenutzt wird. Bei der
748 Kommunikation werden REST-Webservices über HTTPS (JSON-Objekte) aufgerufen.
749

750

751

OpenID-Connect

752 Das VZD-FHIR-Directory, der Registrierungs-Dienst sowie die TI-Messenger-Clients
753 nutzen im Rahmen der Authentifizierung ID_TOKEN in Form eines JSON-Web-Token
754 (JWT) gemäß [OpenID].
755

756

FHIR

757 Die TI-Messenger-Clients nutzen die FHIR-Schnittstellen der Teilkomponente FHIR-Proxy
758 des VZD-FHIR-Directorys gemäß dem FHIR-Standard [FHIR] mit einer RESTful API.

759 5.3 Authentifizierung und Autorisierung**760 5.3.1 Authentifizierung von Akteuren am Messenger-Service**

761 Für die Authentifizierung von Akteuren werden die durch den jeweiligen Matrix-
762 Homeserver bereitgestellten Authentifizierungsverfahren genutzt. Dies ermöglicht es z.
763 B. Krankenhäusern ihre eigene Benutzerverwaltung (z. B. Active Directory) zu nutzen,
764 oder Verbänden ihre eigenen Identitätsserver (IDP-Dienst) zu verwenden. Die
765 Abstimmung, welches Authentifizierungsverfahren verwendet wird, trifft die Organisation
766 mit dem jeweiligen TI-Messenger-Anbieter. Die Benutzerverwaltung erfolgt durch
767 autorisierte Mitarbeiter in der jeweiligen Organisation (Akteur in der Rolle "Org-
768 Admin"). Die Administration der verwendeten Authentifizierungsmethoden MÜSSEN unter
769 der Kontrolle der jeweiligen Organisation sein.

770

771 5.3.2 Authentifizierung am VZD-FHIR-Directory

772 Die Authentifizierung für den Lese- und Schreibzugriff auf das FHIR-Directory erfolgt mit
773 Hilfe von Identitätstoken. Die jeweilige Überprüfung der Identitätstoken erfolgt am FHIR-
774 Proxy des VZD-FHIR-Directory. Die Authentifizierung der Komponenten Registrierungs-
775 Dienst und TI-Messenger-Client wird im Folgenden weiter beschrieben.

776

777 Registrierungs-Dienst

778 Die Authentifizierung des Registrierungs-Dienstes am VZD-FHIR-Directory erfolgt mittels
779 OAuth am OAuth-Service des VZD-FHIR-Directory. Nach erfolgreicher Authentifizierung
780 mit vereinbarten Client-Credentials wird dem Registrierungs-Dienst ein provider-
781 accesstoken ausgestellt.

782

783 TI-Messenger-Client

784 TI-Messenger-Clients MÜSSEN sich gegenüber dem Auth-Service des VZD-FHIR-
785 Directory mit Hilfe eines ID_TOKENS oder des Matrix-OpenID-Token
786 authentifizieren. Dem Matrix-OpenID-Token des Matrix-Homeservers wird vertraut, wenn
787 der ausstellende Matrix-Homeserver als Matrix-Domain einer verifizierten Organisations-
788 Ressource im VZD-FHIR-Directory eingetragen wurde. Der Auth-Service des VZD-FHIR-
789 Directory stellt nach erfolgreicher Prüfung des jeweiligen Matrix-OpenID-Token ein
790 search-accesstoken aus. Dem ID_TOKEN wird vertraut, wenn der ausstellende IDP-
791 Dienst beim VZD-FHIR-Directory registriert ist und somit das Token durch den Auth-
792 Service validiert werden kann. Nach erfolgreicher Prüfung des ID_TOKEN durch den
793 Auth-Service des VZD-FHIR-Directory wird ein owner-accesstoken ausgestellt.

794 5.3.3 Autorisierung am Messenger-Service

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

800 5.3.4 Autorisierung am VZD-FHIR-Directory

801 **Registrierungs-Dienst**

802 Für den Schreibzugriff des Registrierungs-Dienstes autorisiert dieser sich gegenüber dem
803 FHIR-Proxy des VZD-FHIR-Directory mit einem provider-accesstoken, welches vom
804 OAuth-Service des VZD FHIR-Directory ausgestellt wurde.

805 **TI-Messenger-Client**

806 Für den Lesezugriff autorisieren sich TI-Messenger-Clients gegenüber dem FHIR-Proxy
807 des VZD-FHIR-Directory mit einem search-accesstoken, welches vom Auth-Service des
808 VZD FHIR-Directory ausgestellt wurde. Für den Schreibzugriff nutzen TI-Messenger-
809 Clients das owner-accesstoken, welches vom Auth-Service des VZD FHIR-Directory
810 ausgestellt wurde.
811

812 5.4 Rechtekonzept VZD-FHIR-Directory

813 Im folgenden Kapitel wird beschrieben, wie der Lese- und Schreibzugriff durch die TI-
814 Messanger-Clients und dem Registrierungs-Dienst auf dem VZD-FHIR-Directory erfolgt.

815 5.4.1 Lesezugriff

816 **Registrierungs-Dienst**

817 Die TI-Messenger-Fachdienste erhalten die Möglichkeit, mittels ihres Registrierungs-
818 Dienstes die Föderationsliste vom FHIR-Proxy des VZD-FHIR-Directory abzurufen. Hierfür
819 MUSS die Schnittstelle /tim-provider-services am FHIR-Proxy des VZD-FHIR-
820 Directory unter Vorlage des provider-accesstoken aufgerufen werden.

821

822

823 **TI-Messenger-Clients**

824 Durch den Aufruf der Schnittstelle /search am FHIR-Proxy des VZD-FHIR-Directory
825 KANN ein TI-Messenger-Client unter Vorlage des search-accesstoken Suchanfragen an
826 das FHIR-Directory stellen. Die Suchergebnisse sind abhängig von den eingetragenen
827 FHIR-Ressourcen und deren Sichtbarkeit.

828 5.4.2 Schreibzugriff

829 **Registrierungs-Dienst**

830 Die TI-Messenger-Fachdienste erhalten die Möglichkeit, mittels ihres Registrierungs-
831 Dienstes Messenger-Services in die TI-Föderation aufzunehmen. Hierfür MUSS die
832 Schnittstelle /tim-provider-services am FHIR-Proxy des VZD-FHIR-Directory unter
833 Vorlage des provider-accesstoken aufgerufen werden.

834

835 **TI-Messenger-Clients**

836 Durch den Aufruf der Schnittstelle /owner am FHIR-Proxy des VZD-FHIR-Directory erhält
837 ein Akteur unter Vorlage des owner-accesstoken Schreibzugriffe auf das FHIR-Directory.
838 In der folgenden Tabelle wird die zu verändernde FHIR-Ressource in Abhängigkeit zu der
839 verwendeten Identität eines Akteurs beschrieben (siehe dazu auch die Tabelle
840 "Verzeichnistypen - Rechtekonzept").

841

842 Tabelle 5: Schreibzugriff - VZD-FHIR-Ressourcen

Rolle	Identität	FHIR-Ressource	Beschreibung
Org-Admin	SMC-B	HealthcareService	Die Nutzung einer SMC-B ermöglicht es einem Akteur in der Rolle "Org-Admin" mit Hilfe eines TI-Messenger-Clients mit Administrationsfunktion FHIR-Ressourcen (<i>Endpoint</i>) im Namen der Organisation in das Organisationsverzeichnis einzutragen. Die Einträge im Organisationsverzeichnis beginnen immer mit einer <i>HealthcareService</i> Ressource.
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 (<i>Endpoint</i>), im Personenverzeichnis zu erweitern, um für andere Leistungserbringer anschreibbar zu werden oder um andere Leistungserbringer anzuschreiben. Die Einträge im Personenverzeichnis beginnen immer mit einer <i>PractitionerRole</i> Ressource.

843

844

845 **5.5 Funktionsaccounts**

846 Die Verwendung von Funktionsaccounts bietet Akteuren die Möglichkeit einzelne
 847 Unterstrukturen einer Organisation im Gesundheitswesen zu erreichen. Dabei ist es nicht
 848 notwendig, dass der Akteur die genaue interne Struktur der Organisation kennt. Um
 849 Funktionsaccounts innerhalb einer Organisation zu ermöglichen, werden Chatbots als
 850 Akteure eingesetzt, die Anfragen automatisiert verarbeiten. Ein Funktionsaccount wird als
 851 eine *Endpoint*-Ressource eines *HealthcareService* einer Organisation angelegt und dessen
 852 MXID einem Chatbot zugeordnet. Somit kann eine Unterstruktur einer Organisation über
 853 den Funtionsaccount und dessen hinterlegte MXID im VZD-FHIR-Directory von einem
 854 Akteur gefunden werden. Bei Aufruf eines Funktionsaccounts durch ein *Invite*-Event
 855 eines TI-Messenger-Client MUSS der TI-Messenger-Fachdienst den zugeordneten Chatbot
 856 des Funktionsaccounts in einen gemeinsamen Raum hinzufügen.

857

858 **Chatbot**

859 Chatbots sind spezielle Akteure, die stellvertretend für eine Unterstruktur einer
 860 Organisation von einem die Kommunikation initiiierenden Akteur eingeladen werden
 861 können. Chatbots KÖNNEN die Kommunikation vollständig automatisiert abschließen (z.
 862 B. Terminvergabe) oder in der Organisation hinterlegte natürliche Personen dem Chat
 863 hinzuziehen (z. B. Ausstellen eines Rezeptes). Beispiele für Chatbots sind unter [Matrix
 864 Bots] zu finden. Treten Chatbots als Kommunikationsteilnehmer des TI-Messengers auf,
 865 so MÜSSEN diese im jeweiligen Chat als Chatbot gekennzeichnet werden.

866 Im Folgenden wird ein Beispiel für eine mögliche Zuordnung für die Abbildung von
 867 Funktionsaccounts innerhalb einer Organisation mit deren Unterstrukturen dargestellt.
 868

869 **Tabelle 6: Beispiel für Funktionsaccounts**

Abteilung	Funktionsaccount	Akteur (MXID)	Displayname
Kardiologie	FA_Kardiologie	@MXID_Bot01:<domain>.de @MXID_01:<domain>.de @MXID_02:<domain>.de	Chatbot (FA_Kardiologie) Maltilde Dennert (Arzt) Sarah Fritsche (MFA)
Neurologie	FA_Neurologie	@MXID_Bot02:<domain>.de @MXID_03:<domain>.de	Chatbot (FA_Neurologie) Gerd Gotsch (MFA)
Radiologie	FA_Radiologie	@MXID_Bot03:<domain>.de @MXID_04:<domain>.de	Chatbot (FA_Radiologie) Wilfried Fruechtl (Assistenzarzt)

870
 871 Der Chatbot KANN automatisiert Anfragen von Akteuren (z. B. für Terminanfragen,
 872 Medikationsentscheidung) bearbeiten oder bei Bedarf die zugeordneten und zu diesem
 873 Zeitpunkt verfügbaren Akteure in den Chatraum einladen. Die dem Chatbot zur
 874 Verfügung stehenden Akteure (in der Spalte blau hinterlegt) sind in der Konfiguration des
 875 Chatbots zu definieren.

876 *Hinweis: Für die Kommunikationsübernahme durch einen Chatbot ist es empfehlenswert,*
 877 *diesen jederzeit erreichbar zu machen.*

878

879 Im Folgenden wird die Interaktion eines externen Akteurs mit einem Funktionsaccount
 880 gezeigt.

881

882 **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

883

2. Konfiguration von Funktionsaccounts:

- Der Akteur in der Rolle "Org-Admin" legt einen Funktionsaccount (organisationsbezogene MXID) als einen *Endpoint* 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

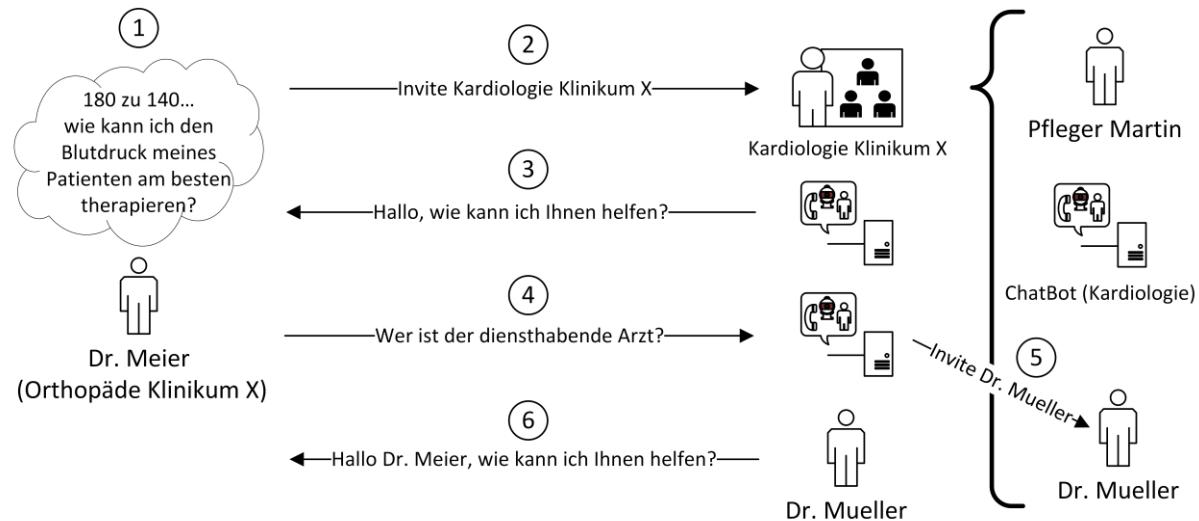
884

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

885

886



887

888

Abbildung 5: Beispiel einer Iteraktion mit einem Chatbot

889

890 5.6 Test

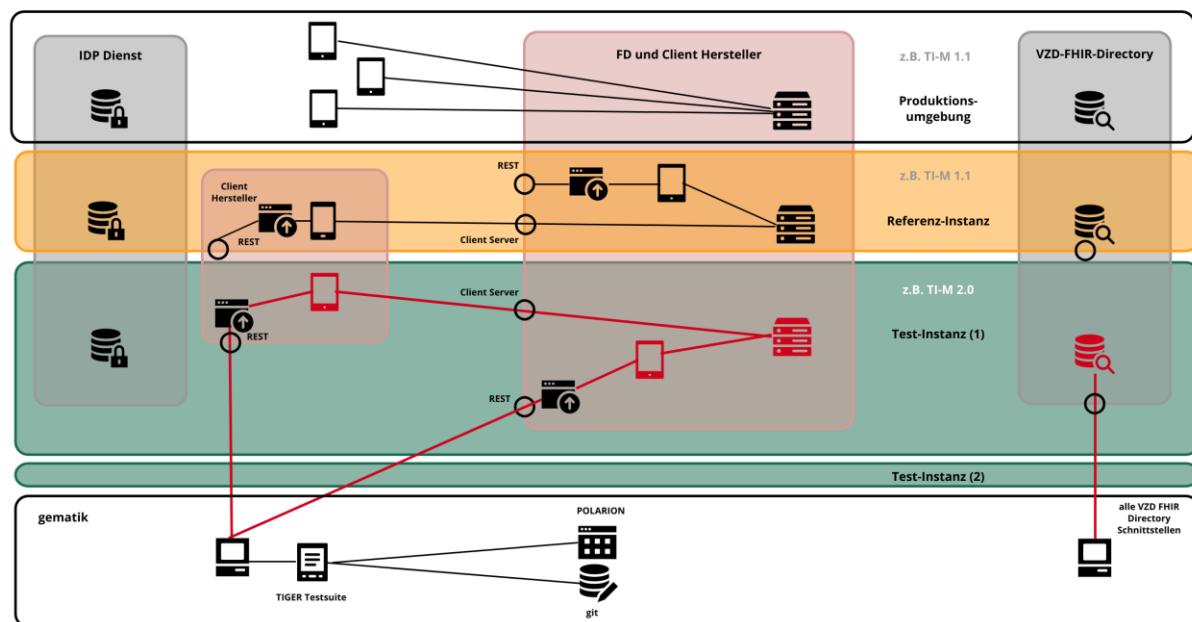
891 Der TI-Messenger-Anbieter MUSS eine Referenz-Instanz und mindestens eine Test-
 892 Instanz des TI-Messenger-Fachdienstes und TI-Messenger-Clients bereitstellen und
 893 betreiben. Die Referenz-Instanz hat die gleiche Version wie die Produktionsumgebung
 894 und kann von anderen Herstellern für Tests und Entwicklung gegen die zugelassene
 895 Version benutzt werden. Weiterhin wird die Referenz-Instanz für die Reproduktion
 896 aktueller Fehler-Probleme aus der Produktionsumgebung genutzt. Der Zugriff auf die
 897 Referenz-Instanz MUSS für die gematik zur Fehleranalyse gewährleistet sein.
 898 Die Test-Instanz dient den Herstellern bei der Entwicklung neuer TI-Messenger-Clients
 899 und TI-Messenger Fachdienste Versionen, den IOP-Tests zwischen den verschiedenen TI-
 900 Messenger-Anbietern und wird auch von der gematik für die Zulassung genutzt.
 901 Der TI-Messenger-Anbieter MUSS die verschiedenen Benutzer der Referenz-Instanz und
 902 der Test-Instanz koordinieren (Verwaltung eines Test-/Nutzungsplans). Bei Bedarf
 903 (Entwicklung verschiedener Versionen, hoher Auslastung durch andere Hersteller oder
 904 durch die gematik) MUSS der TI-Messenger-Anbieter auch mehrere Test-Instanzen mit
 905 der gleichen oder mit verschiedenen Versionen bereitstellen und betreiben.

906

907

908

909



910

911

Abbildung 6: TI-Messenger-Dienst Instanzen

912

913 **5.7 Betrieb**

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

- 915 • TI-Messenger-Fachdienst(e) und
916 • TI-Messenger-Client(s)

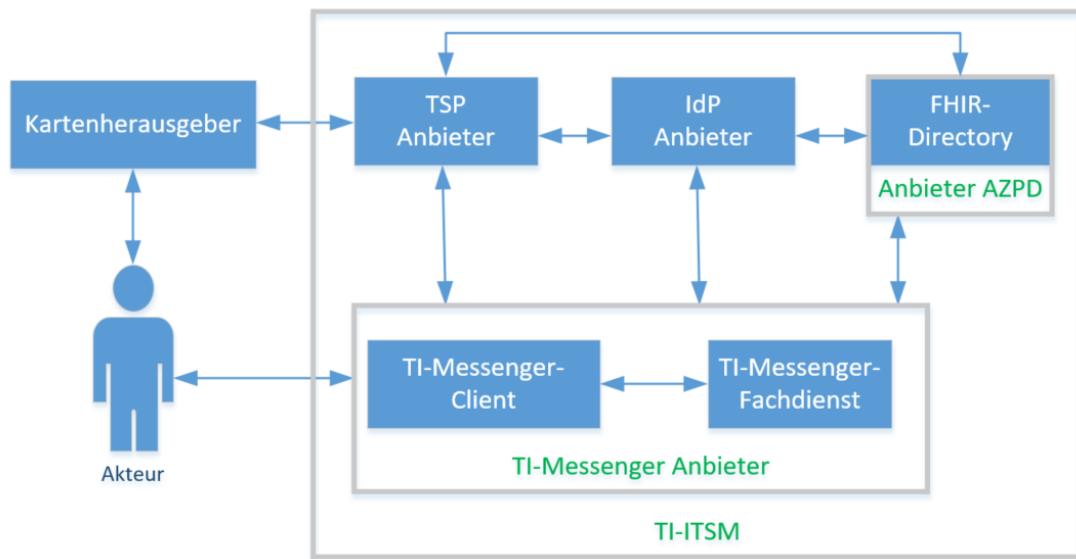
917 Der TI-Messenger-Anbieter MUSS mindestens einen TI-Messenger-Fachdienst und einen
918 TI-Messenger-Client (jeweils oder gebündelt mit Messaging- und Org-Admin-
919 Funktionalität) anbieten.

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

923 Der TI-Messenger-Anbieter MUSS seinen Nutzern und Organisationen einen Helpdesk
924 entsprechend [gemKPT_Betr] anbieten, welcher auch Störungen zu allen verantworteten
925 TI-Messenger-Clients und TI-Messenger-Fachdiensten entgegennimmt.

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

929



930

931

932

933

Abbildung 7: Ausschnitt - TI-Messenger-Anbieter im TI-ITSM

934

6 Anwendungsfälle

935

936 Die nachfolgend beschriebenen Anwendungsfälle sind spezifisch für den TI-Messenger-
937 Dienst und weichen daher teilweise von der Matrix-Client-Server-API ab. Das gleiche gilt
938 für die auf dem Matrix-Server-Server-Protokoll ([Server-Server API]) basierenden
939 Anwendungsfälle. Das bedeutet, dass alle Anwendungsfälle, die gemäß Matrix-Client-
940 Server-Protokoll umgesetzt werden, an dieser Stelle nicht weiter aufgeführt sind.
941 Stattdessen wird hier auf die Matrix-Client-Server-API verwiesen ([Client-Server API]).

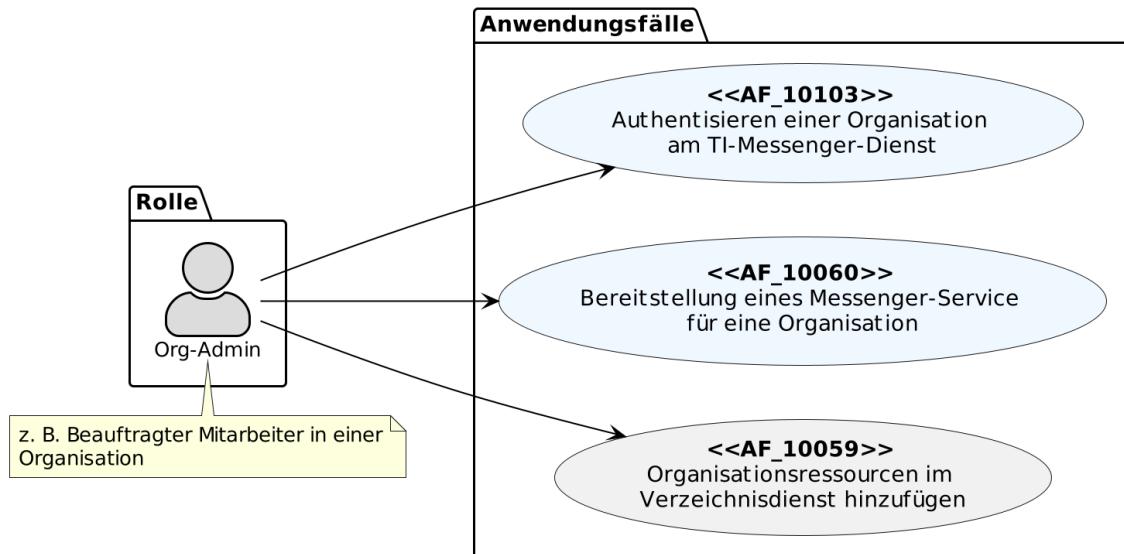
942 Im Kontext des TI-Messenger-Dienstes nehmen Akteure unterschiedliche Rollen ein
943 (siehe Kapitel [3.1 - Akteure und Rollen](#)). Entsprechend der eingenommenen Rolle eines
944 Akteurs werden unterschiedliche Anwendungsfälle ausgelöst. Für die Rollen "Org-Admin"
945 und User/User-HBA" wird dies in den folgenden Abbildungen dargestellt.

946

Rolle: Org-Admin

948 Ein Akteur in der Rolle "Org-Admin" KANN ein beauftragter Mitarbeiter in einer
949 Organisation oder ein beauftragter Administrator des TI-Messenger-Anbieters sein. Für
950 seine administrativen Tätigkeiten löst dieser Akteur, unter Nutzung einer freigeschalteten
951 SMC-B, im Kontext des TI-Messenger-Dienstes die folgenden Anwendungsfälle aus.

952



953

Abbildung 8: Org-Admin - Übersicht Anwendungsfälle

955

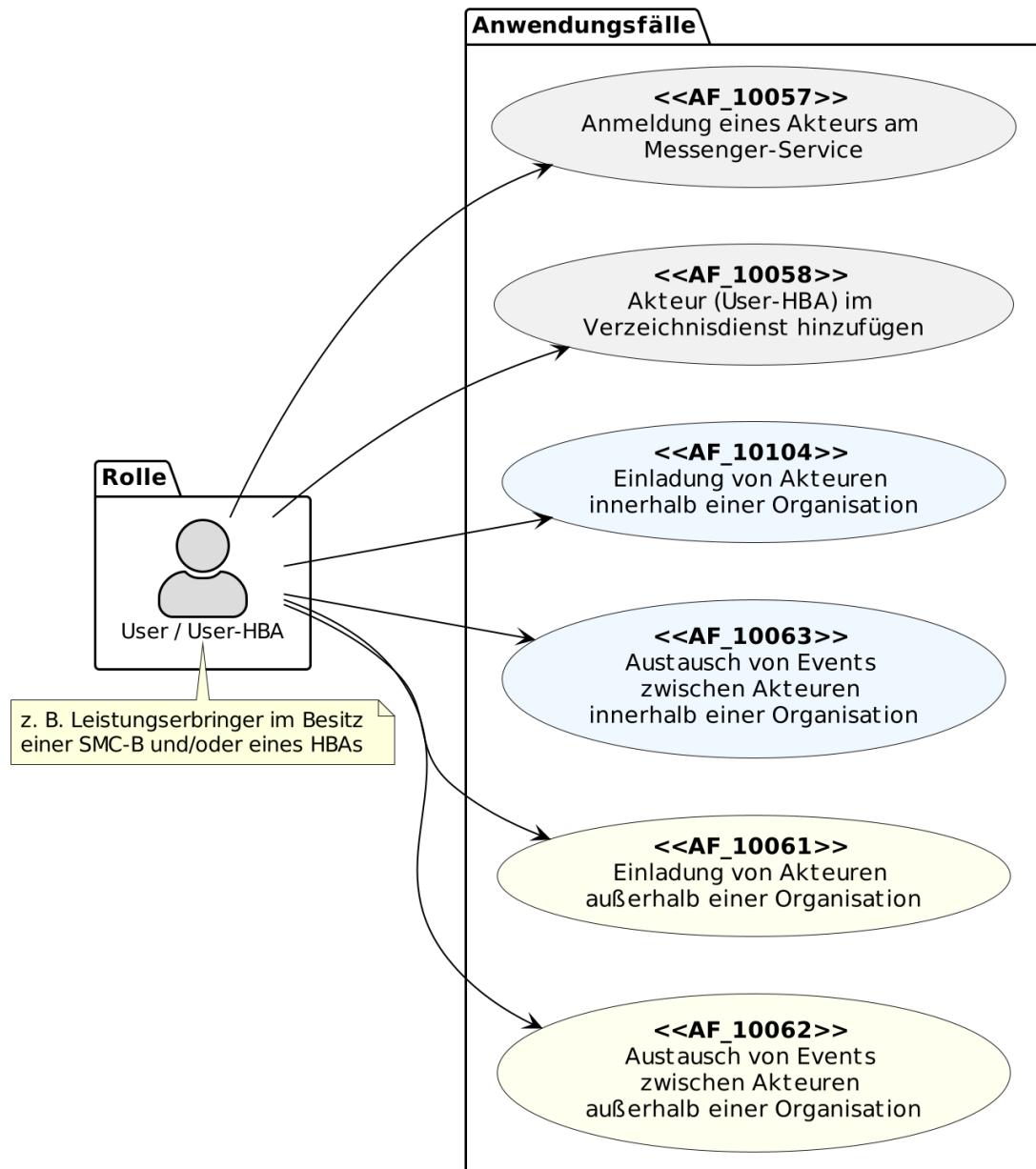
956 Der Anwendungsfall "AF_10060 - Bereitstellung eines Messenger Service für eine
957 Organisation" setzt die erfolgreiche Authentifizierung der Organisation durch den
958 Anwendungsfall "AF_10103 - Authentisieren einer Organisation am TI-Messenger-Dienst"
959 voraus. Werden durch eine Organisation mehrere Messenger-Services benötigt (z. B. im
960 Krankenhausumfeld) KANN der Anwendungsfall mehrfach ausgeführt werden. Mit der
961 farblichen Zuordnung soll auf eine funktionale Beziehung zwischen den einzelnen
962 Anwendungsfällen hingewiesen werden.

963 Eine weitere Aufgabe des Org-Admin, welche hier nicht weiter in einem Anwendungsfall
 964 gezeigt wird, ist die Einrichtung von Funktionsaccounts.

965

966 **Rolle: User / User-HBA**

967 Ein Akteur in der Rolle "User / User-HBA" KANN die folgenden Anwendungsfälle auslösen.
 968



969
 970

971 **Abbildung 9: User / User HBA - Übersicht Anwendungsfälle**
 972

973 Der Anwendungsfall "AF_10058 - Akteur (User-HBA) im Verzeichnisdienst hinzufügen"
 974 KANN nur von einen Akteur in der Rolle "User-HBA" ausgeführt werden. Alle anderen
 975 gezeigten Anwendungsfälle KÖNNEN von den Akteuren in der Rolle "User / User-HBA"

976 ausgeführt werden. Mit der farblichen Zuordnung soll auf eine funktionale Beziehung
 977 zwischen den einzelnen Anwendungsfällen hingewiesen werden.

978 *Hinweis: In den folgenden Anwendungsfällen wird auf Abläufe verwiesen, die im Anhang*
 979 *B zu finden sind. Ebenfalls können für eine bessere Lesbarkeit die in den jeweiligen*
 980 *Anwendungsfällen dargestellten Laufzeitsichten als PlantUML-Quelle in [api-messenger]*
 981 *unter src/plantuml und in Diagrammform unter /images/diagrams abgerufen werden.*

982

983 **6.1 AF - Authentisieren einer Organisation am TI-Messenger- 984 Dienst**

985 **AF_10103 - Authentisieren einer Organisation am TI-Messenger-Dienst**

986 Mit diesem Anwendungsfall authentisiert ein Akteur, in der Rolle "Org-Admin", seine
 987 Organisation bei einem TI-Messenger-Anbieter. Für die Authentisierung einer
 988 Organisation stellt der TI-Messenger-Fachdienst eine Schnittstelle an
 989 seinem Registrierungs-Dienst bereit. Diese wird über das Frontend des Registrierungs-
 990 Dienstes für die Authentisierung verwendet. Die Authentisierung der Organisation erfolgt
 991 individuell und nutzungsabhängig durch einen Akteur in der Rolle "Org-Admin". Für die
 992 Verifizierung der Organisation MUSS bei der Authentisierung am IDP-Dienst eine
 993 freigeschaltete SMC-B verwendet werden. Als Nachweis zur Prüfung auf eine gültige
 994 Organisation MUSS der Registrierungs-Dienst die im ID_TOKEN enthaltene ProfessionOID
 995 gegen die OID-Festlegung für Institutionen prüfen. Bei erfolgreicher Verifizierung der
 996 Organisation wird ein Administrator-Account für die Organisation am Registrierungs-
 997 Dienst angelegt. Dies ermöglicht es einem Administrator Messenger-Services zu
 998 registrieren und seiner Organisation am TI-Messenger-Dienst teilzunehmen.
 999

1000 **Tabelle 7: Tabelle : AF - Authentisieren einer Organisation am TI-Messenger-Dienst**

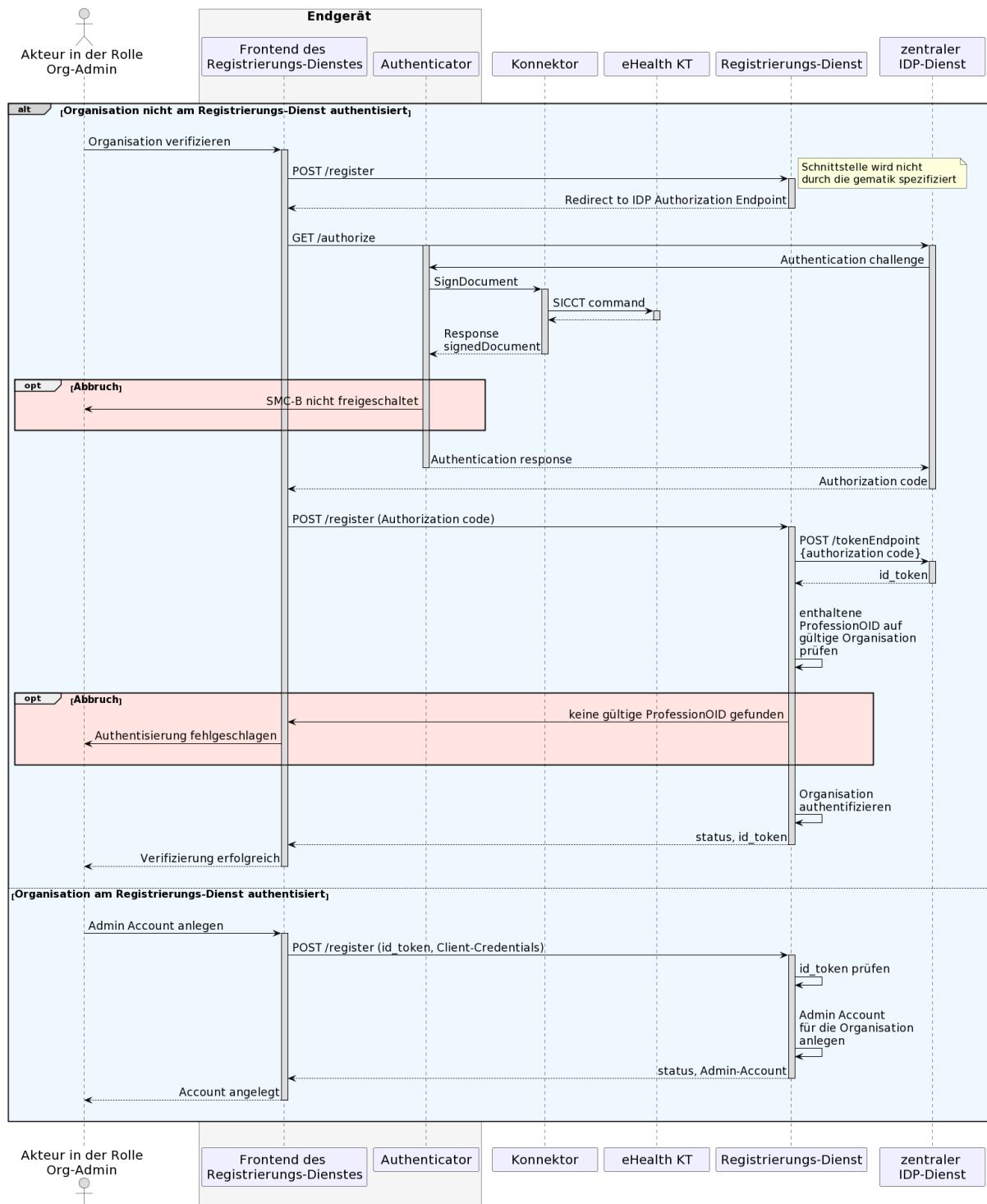
AF_10103	Authentisieren einer Organisation am TI-Messenger-Dienst
Akteur	Beauftragter Mitarbeiter einer Organisation in der Rolle "Org-Admin"
Auslöser	Eine Organisation des deutschen Gesundheitswesens möchte am TI-Messenger-Dienst teilnehmen und benötigt die Berechtigung einen Messenger-Service zu registrieren
Komponenten	<ul style="list-style-type: none"> • Frontend des Registrierungs-Dienstes, • Authenticator, • Konnektor, • eHealth Kartenterminal mit gesteckter SMC-B, • Registrierungs-Dienst, • IDP-Dienst

Vorbedingung	<ol style="list-style-type: none"> 1. Der Akteur kann über ein Frontend des Registrierungs-Dienstes für die Kommunikation auf den Registrierungs-Dienst zugreifen. 2. Das verwendete Frontend des Registrierungs-Dienstes ist bei einem zuständigen IDP-Dienst registriert. 3. Der Akteur kann den Authenticator des jeweiligen TI-Messenger-Anbieters verwenden. 4. Die im eHealth Kartenterminal gesteckte SMC-B ist freigeschaltet.
Eingangsdaten	Identität der Organisation, SMC-B
Ergebnis	Die Organisation wurde am Registrierungs-Dienst des TI-Messenger-Fachdienstes verifiziert
Ausgangsdaten	ID_TOKEN, Admin-Account, Status
Akzeptanzkriterien	   ,  

1001

1002 In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den
 1003 Anwendungsfall genutzt werden, dargestellt. Für die Authentisierung einer Organisation
 1004 wird in der Laufzeitsicht der zentrale IDP-Dienst der TI verwendet. Die Nutzung anderer
 1005 IDP-Dienste ist auch möglich.

1006



1007

1008 **Abbildung 10: Laufzeitsicht - Authentisieren einer Organisation am TI-Messenger-Dienst**

1009 [<=]

1010

1011 **Akzeptanzkriterien für den Anwendungsfall: Authentisieren einer Organisation
am TI-Messenger-Dienst (AF_10103)**

1013

**1014 ML-128757 - AF_10103 - Verifizierung der Organisation als Akteur in der Rolle
1015 Org-Admin**

1016 Nur ein Akteur in der Rolle "Org-Admin" darf seine Organisation gegenüber dem TI-
1017 Messenger-Fachdienst authentifizieren.

1018 [<=]

1019 ML-128759 - AF_10103 - Organisation wurde erfolgreich verifiziert

1020 Die Organisation wurde beim TI-Messenger-Fachdienst erfolgreich mit einer Identität
1021 einer Organisation des Gesundheitswesens verifiziert

1022 [<=]

1023 ML-128758 - AF_10103 - ID-Token wurden ausgestellt und übergeben

1024 Das vom IDP-Dienst ausgestellte ID_TOKEN ist gültig und liegt dem Frontend des
1025 Registrierungs-Dienstes vor.

1026 [<=]

1027 ML-129853 - AF_10103 - Administrator Account angelegt

1028 Ein Administrator Account für die Organisation wurde erfolgreich am Registrierungs-
1029 Dienst angelegt.

1030 [<=]

1031 ML-132446 - AF_10103 - TI-M Rohdatenerfassung und -lieferung

1032 Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-
1033 Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die
1034 definierte Schnittstelle der Rohdatenerfassung versendet.[<=]

1035

**1036 6.2 AF - Bereitstellung eines Messenger-Service für eine
1037 Organisation****1038 AF_10060 - Bereitstellung eines Messenger-Service für eine Organisation**

1039 Mit diesem Anwendungsfall wird einer zuvor am Registrierungs-Dienst authentifizierten
1040 Organisation ein Messenger-Service für diese Organisation durch einen Akteur in der
1041 Rolle "Org-Admin" bereitgestellt. Die Beantragung zur Bereitstellung eines Messenger-
1042 Service wird durch den Akteur in der Rolle "Org-Admin" am Frontend des Registrierungs-
1043 Dienstes vorgenommen. Dieser MUSS sich zuvor mit dem Admin-Account der
1044 Organisation am Registrierungs-Dienst anmelden. Für eine zeitnahe Adaption des TI-
1045 Messenger-Dienstes MUSS eine schnelle Bereitstellung von Messenger-Services
1046 gewährleistet sein. TI-Messenger-Anbieter sind verpflichtet, Prozesse zu etablieren,
1047 damit Messenger-Services für Organisationen schnell und ggf. automatisiert bereitgestellt
1048 werden können. Nach erfolgreicher Bereitstellung eines Messenger-Service wird dieser in
1049 die Föderation des TI-Messenger-Dienstes aufgenommen. Werden mehrere Messenger-
1050 Services für eine Organisation benötigt KANN dieser Anwendungsfall mehrfach
1051 ausgeführt werden.
1052

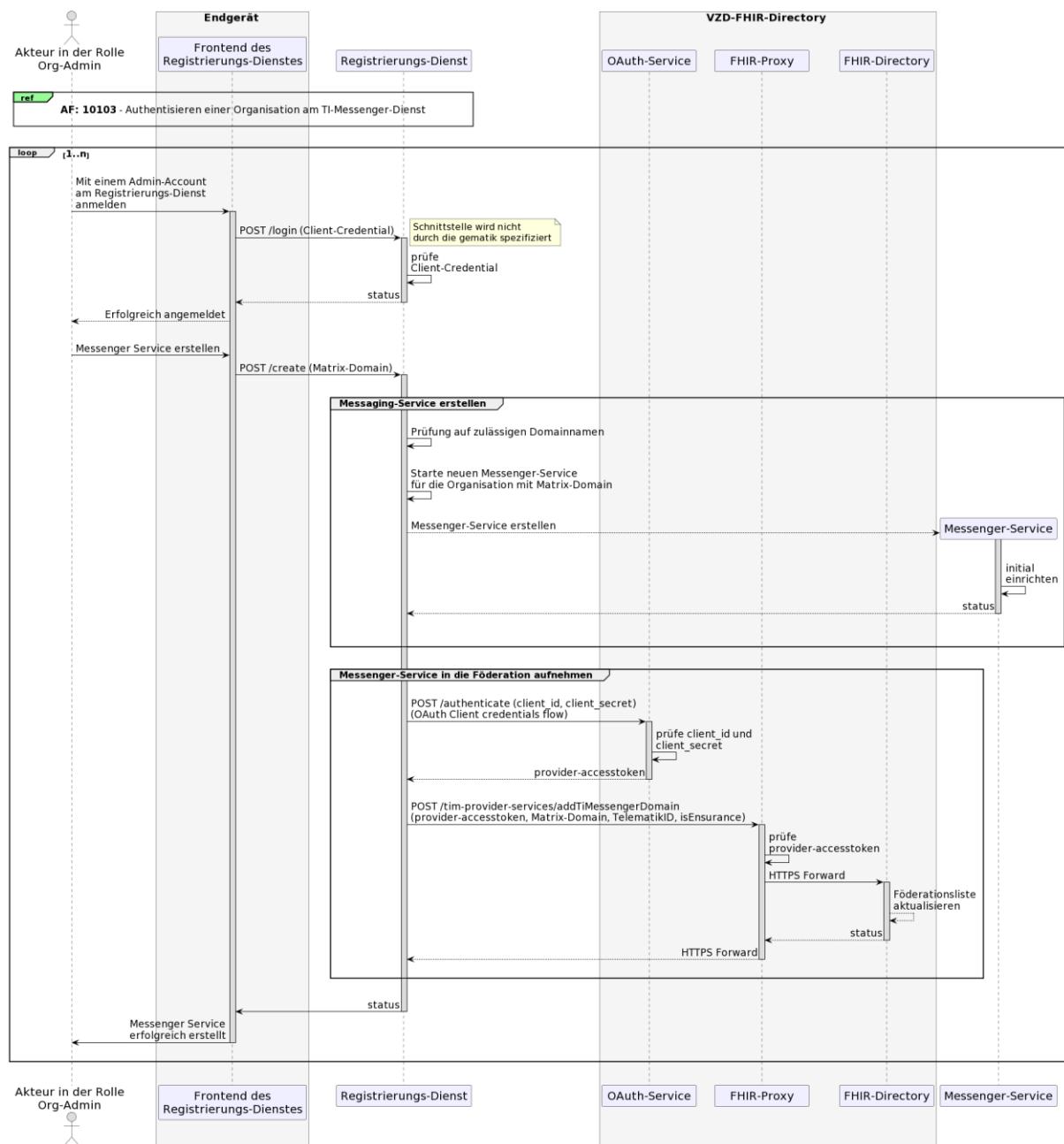
1053 **Tabelle 8: AF - Bereitstellung eines Messenger-Service für eine Organisation**

AF_10060	Bereitstellung eines Messenger-Service für eine Organisation
-----------------	---

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

1054

1055 In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den
 1056 Anwendungsfall genutzt werden, dargestellt. Für den Anwendungsfall wird die
 1057 erfolgreiche Authentifizierung der Organisation mit Hilfe des Anwendungsfalls "AF_10103
 1058 - Authentisieren einer Organisation am TI-Messenger-Dienst" vorausgesetzt. Die
 1059 Komponente Messenger-Service für die Organisation wird im Verlauf des
 1060 Anwendungsfalles zu einem späteren Zeitpunkt erstellt.
 1061



1062

1063 **Abbildung 11: Laufzeitsicht - Bereitstellung eines Messenger-Service für eine**
1064 **Organisation**

1065 [=<]

1066

1067 **Akzeptanzkriterien für den Anwendungsfall: Bereitstellung eines Messenger-**
1068 **Service für eine Organisation (AF_10060)**

1069

1070 **ML-123648 - AF_10060 - Messenger-Service bereitstellen nur als Akteur in der**
1071 **Rolle Org-Admin**

1072 Nur ein Akteur in der Rolle "Org-Admin" darf einen Messenger-Service bereitstellen.
1073 [=<]

1074 **ML-123649 - AF_10060 - Messenger-Service wurde erzeugt**

1075 Ein neuer Messenger-Service wurde mit dem gewählten Domainbezeichner erzeugt.
 1076 [=<]
 1077 **ML-123650 - AF_10060 - Messenger-Service im VZD-FHIR-Directory existiert**
 1078 Für den erzeugten Messenger-Service wurde ein neuer Eintrag im VZD-FHIR-Directory
 1079 angelegt
 1080 [=<]
 1081 **ML-132585 - AF_10060 - TI-M Rohdatenerfassung und -lieferung**
 1082 Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-
 1083 Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die
 1084 definierte Schnittstelle der Rohdatenerfassung versendet.[=<]
 1085

1086 **6.3 AF - Organisationsressourcen im Verzeichnisdienst hinzufügen**

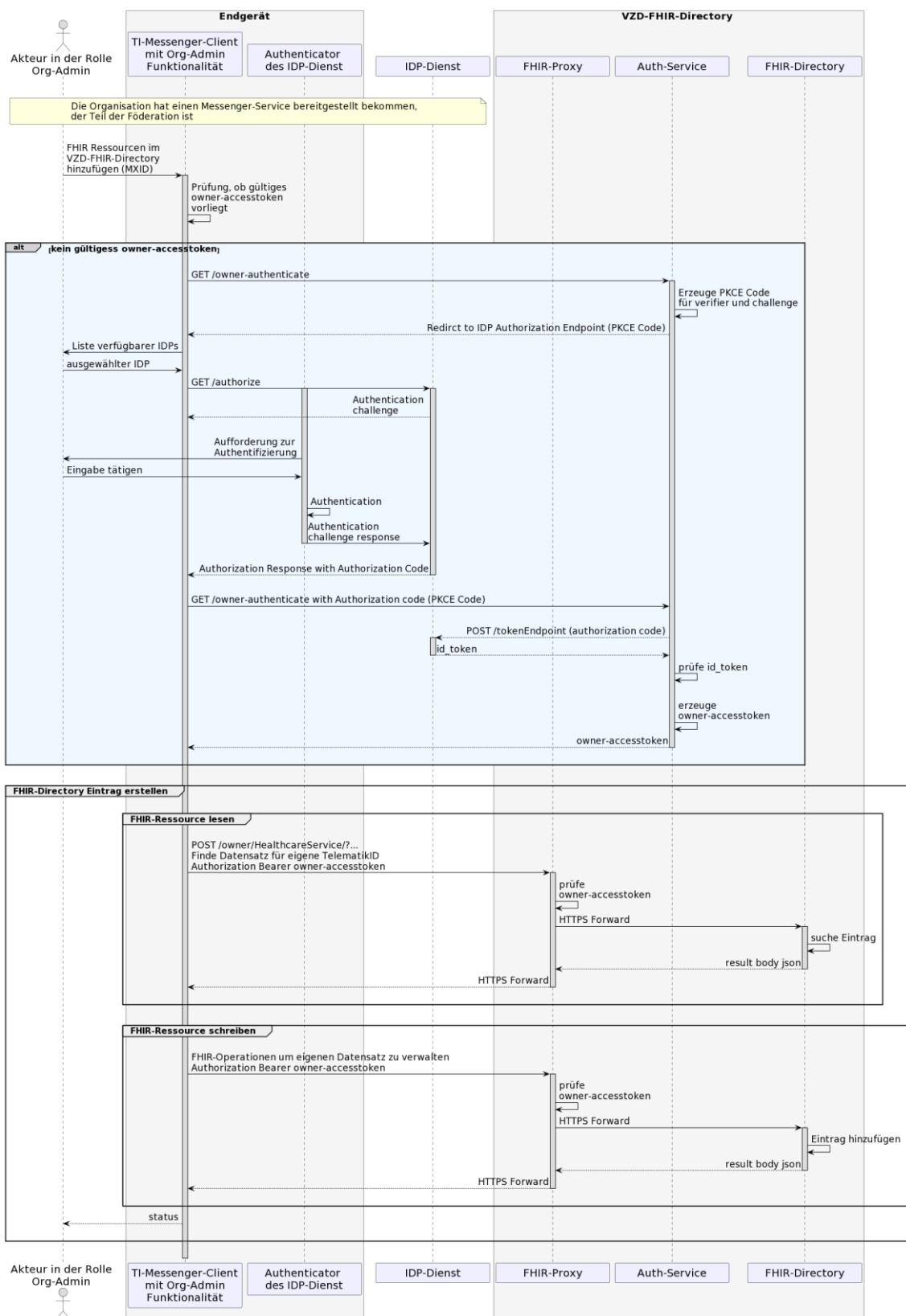
1087 **AF_10059 - Organisationsressourcen im Verzeichnisdienst hinzufügen**
 1088 Mit diesem Anwendungsfall macht ein Akteur in der Rolle "Org-Admin" Akteure seiner
 1089 Organisation im TI-Messenger-Dienst für andere Akteure auffindbar und erreichbar.
 1090 Dafür werden FHIR-Ressourcen mit ihrer jeweiligen MXID im Organisationsverzeichnis
 1091 (*HealthcareService*) des VZD-FHIR-Directory hinterlegt. Organisationen KÖNNEN mehrere
 1092 FHIR-Ressourcen pro Organisation administrieren und somit eingehende
 1093 Kommunikationsprozesse organisatorisch und thematisch strukturieren.
 1094

1095 **Tabelle 9: AF - Organisationsressourcen im Verzeichnisdienst hinzufügen**

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

Vorbedingungen	<ol style="list-style-type: none"> 1. Für die Organisation wurde ein Messenger-Service bereitgestellt und eine FHIR-Ressource im VZD-FHIR-Directory erzeugt. 2. Der Administrator der Organisation verfügt über einen TI-Messenger-Client (mit erweiterter Org-Admin Funktionalität). 3. Das VZD-FHIR-Directory ist bei einem zuständigen IDP-Dienst registriert. 4. Der Administrator der Organisation kann sich an einem zuständigen IDP-Dienst authentisieren.
Eingangsdaten	SMC-B, FHIR-Organisations-Ressourcen
Ergebnis	FHIR-Organisations-Ressourcen aktualisiert, Status
Ausgangsdaten	Aktualisierte VZD-FHIR-Directory-Datensätze
Akzeptanzkriterien	 ML-123626 ,  ML-123627 ,  ML-132586

1096
 1097 In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den
 1098 Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es sich um eine
 1099 **vereinfachte Laufzeitansicht** in der zum Beispiel die TLS-Terminierung am FHIR-Proxy
 1100 auf Grund der Übersichtlichkeit nicht berücksichtigt wurde.
 1101



1102

1103

Abbildung 12: Laufzeitsicht - Organisationsressourcen im Verzeichnisdienst hinzufügen

1104

1105
1106
1107
1108

Akzeptanzkriterien für den Anwendungsfall: Organisationsressourcen im Verzeichnisdienst hinzufügen (AF_10059)

ML-123627 - AF_10059 - Organisationsressourcen im VZD-FHIR-Directory hinzufügen

Nach erfolgreicher Authentisierung an einem zuständigen IDP-Dienst als Administrator einer Organisation kann der Akteur in der Rolle "Org-Admin" die MXID eines Akteurs seiner Organisation in den *HealthcareService* in einen *Endpoint* eintragen und Unterstrukturen für die Organisation anlegen. Der Akteur in der Rolle "Org-Admin" wird über den Erfolg der Operation informiert.

[<=]

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

Der Akteur in der "RolleOrg-Admin" darf nur FHIR-Ressourcen seiner eigenen Organisation (inklusive der Unterstrukturen) ändern.

[<=]

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.[<=]

1126

6.4 AF - Anmeldung eines Akteurs am Messenger-Service

AF_10057 - Anmeldung eines Akteurs am Messenger-Service

Mit diesem Anwendungsfall meldet sich ein Akteur an einem in der TI-Föderation zuständigen Messenger-Service an und registriert seinen TI-Messenger-Client als Endgerät. Der Akteur 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 beispielweise durch ein QR-Code-Scan unterstützt werden. Die Authentifizierung erfolgt hierbei nach den Vorgaben der jeweiligen Organisation. Nach der erfolgreichen Anmeldung eines Akteurs am Messenger-Service KÖNNEN die von ihm angebotenen Dienste verwendet werden.

1137

Tabelle 10: AF - Anmeldung eines Akteurs am Messenger-Service

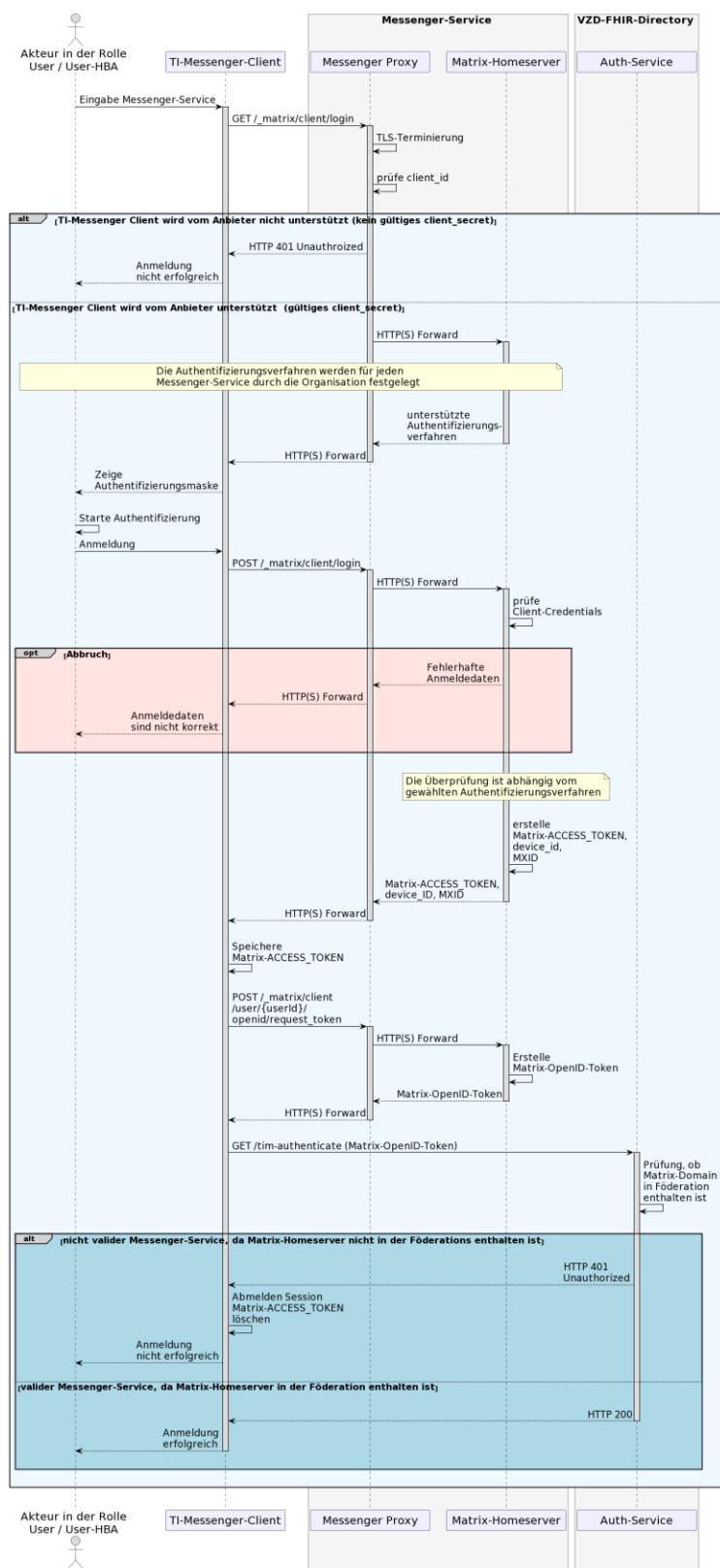
AF_10057	Anmeldung eines Akteurs am Messenger-Service
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der "Rolle User / User-HBA"
Auslöser	Ein Akteur möchte sich mit seinem TI-Messenger-Client bei einem Messenger-Service anmelden.
Komponenten	<ul style="list-style-type: none"> • TI-Messenger-Client, • Messenger-Proxy, • Messenger-Homeserver,

	<ul style="list-style-type: none"> • FHIR-Proxy, • FHIR-Directory.
Vorbedingungen	<ol style="list-style-type: none"> 1. Der Akteur verfügt über einen vom Anbieter unterstützten TI-Messenger-Client. 2. Der Akteur kennt die URL des Messenger-Services oder die URL ist bereits in seinem TI-Messenger-Client konfiguriert. 3. Der Akteur kann sich durch ein beim Matrix-Homeserver unterstütztes Authentisierungsverfahren identifizieren. Wird durch die Organisation ein eigenes Authentifizierungsverfahren verwendet MUSS eine Anbindung an den Matrix-Homeserver erfolgt sein. 4. Der verwendete Matrix-Homeserver ist in die Föderation integriert (valider Messenger-Service).
Eingangsdaten	URL des Matrix-Homeservers
Ergebnis	Es wurde ein TI-Messenger Account für einen Akteur in der Rolle "User / User-HBA" erzeugt.
Ausgangsdaten	Matrix-ACCESS_TOKEN, MXID, device_id Status
Akzeptanzkriterien	    

1139
 1140
 1141
 1142
 1143
 1144
 1145

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. In dieser wird der Prozess einer Anmeldung eines Akteurs an einem Messenger-Service dargestellt. Sollte ein Akteur noch nicht an einem Matrix-Homeserver registriert sein, dann wird zunächst eine Registrierung des Akteurs mit der Operation `POST /matrix/client/register` durchgeführt. Der Ablauf der Registrierung ist analog dem des Login-Verfahrens.

1146



Akteur in der Rolle
User / User-HBA

1147

1148

Abbildung 13: Laufzeitsicht - Anmeldung eines Akteurs am Messenger-Service

1149 [<=]

1150

1151 **Akzeptanzkriterien für den Anwendungsfall: Anmeldung eines Akteurs am**
1152 **Messenger-Service (AF_10057)**

1153

1154 **ML-123571 - AF_10057 - Akteur kann sich erfolgreich an einem gültigen**
1155 **Messenger-Service anmelden**

1156 Ein Akteur hat sich erfolgreich an einem gültigen Messenger-Service angemeldet und mit
1157 einem zugelassenen Authentifizierungsverfahren erfolgreich authentisiert. Es MUSS
1158 sichergestellt werden, dass die Anmeldung an Messenger-Services, die nicht Teil der
1159 Föderation sind, nicht möglich ist.

1160 [=<]

1161 **ML-123576 - AF_10057 - Der Messenger-Service stellt dem TI-Messenger-Client**
1162 **ein Access-Token aus**

1163 Nach erfolgreicher Anmeldung hat der Messenger-Service dem TI-Messenger-Client ein
1164 Matrix-ACCESS_TOKEN ausgestellt.

1165 [=<]

1166 **ML-123575 - AF_10057 - Speicherung Access-Token durch TI-Messenger-Client**

1167 Der TI-Messenger-Client speichert das ihm übergebene Matrix-ACCESS_TOKEN zur
1168 Verwendung in den folgenden Anwendungsfällen.

1169 [=<]

1170 **ML-129870 - AF_10057 - Akteur kann sich an einen nicht validen Messenger-**
1171 **Service nicht anmelden**

1172 Ein Akteur kann sich nicht bei einem öffentlichen Matrix-Homeserver anmelden, der nicht
1173 in die TI-Föderation integriert ist.

1174 [=<]

1175 **ML-132587 - AF_10057 - TI-M Rohdatenerfassung und -lieferung**

1176 Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-
1177 Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die
1178 definierte Schnittstelle der Rohdatenerfassung versendet. [=<]

1179

1180 **6.5 AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen**

1181 **AF_10058 - Akteur (User-HBA) im Verzeichnisdienst hinzufügen**

1182 Mit diesem Anwendungsfall wird ein Akteur in der Rolle "User-HBA" für andere Akteure
1183 anderer Messenger-Services auffindbar und erreichbar. Dafür werden FHIR-Ressourcen
1184 mit ihrer jeweiligen MXID im Personenverzeichnis (*PractitionerRole*) des VZD-FHIR-
1185 Directory hinterlegt. Zusätzlich besteht die Möglichkeit die Sichtbarkeit für andere
1186 Akteure einzuschränken. Dieser Anwendungsfall KANN direkt mit dem initialen
1187 Anmeldevorgang eines Akteurs am Messenger Service (siehe Anwendungsfall: "AF_10057
1188 - Anmeldung eines Akteurs am Messenger-Service") kombiniert werden. Hierfür wird der
1189 Akteur in der Rolle "User-HBA" während des Anmeldevorgangs durch den TI-Messenger-
1190 Client gefragt, ob dieser im Besitz eines HBAs ist.
1191

1192 **Tabelle 11: AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen**

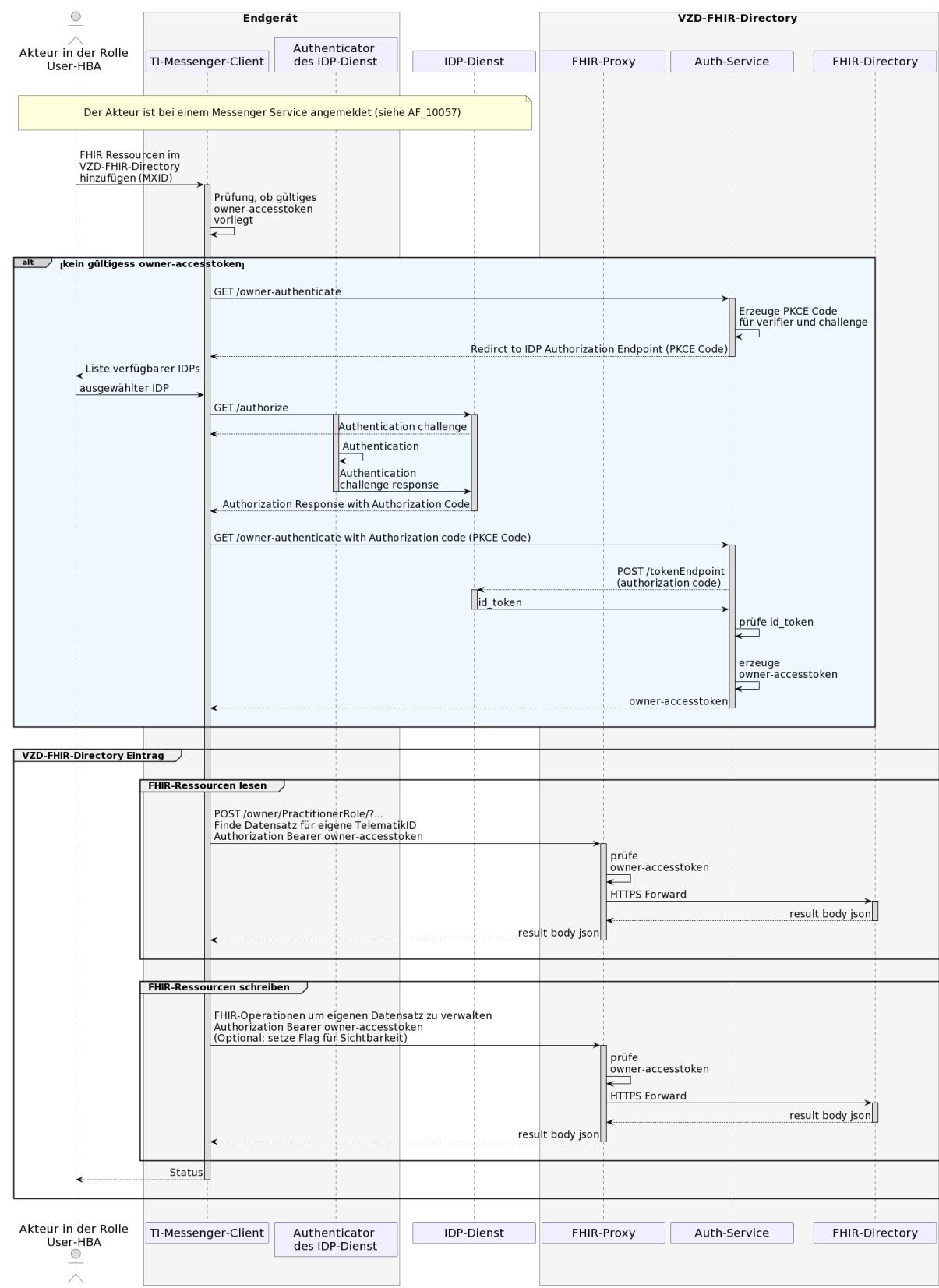
AF_10058	Akteur (User-HBA) im Verzeichnisdienst hinzufügen
----------	---

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 des IDP-Dienst, • IDP-Dienst, • FHIR-Proxy, • Auth-Service, • FHIR-Directory .
Vorbedingungen	<ol style="list-style-type: none"> 1. Der Akteur ist bei einem gültigen Messenger-Service angemeldet (siehe AF_10057). 2. Der Akteur verfügt über einen zugelassenen TI-Messenger-Client. 3. Das VZD-FHIR-Directory ist bei einem zuständigen IDP-Dienst registriert. 4. Der Akteur kann sich am IDP-Dienst authentisieren.
Eingangsdaten	HBA, FHIR-Practitioner-Ressourcen
Ergebnis	FHIR-Practitioner-Ressourcen aktualisiert, Status
Ausgangsdaten	aktualisierter Practitioner-Datensatz
Akzeptanzkriterien	 ML-123611,  ML-123612 ,  ML-132588

1193

1194 In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den
 1195 Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es sich um eine
 1196 **vereinfachte Laufzeitansicht** in der zum Beispiel die TLS-Terminierung am FHIR-Proxy
 1197 auf Grund der Übersichtlichkeit nicht berücksichtigt wurde.
 1198

1199



1200

1201

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

1202

1203

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

1206

ML-123612 - AF_10058 - Akteur als Practitioner hinzufügen

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

1210 [=<]

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

Der Akteur in der Rolle "User-HBA" darf nur die eigene FHIR-Ressourcen ändern.

1214 [=<]

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-Fachdienst erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet. [=<]

1219

6.6 AF - Föderationszugehörigkeit eines Messenger-Service prüfen**AF_10064 - Föderationszugehörigkeit eines Messenger-Service prüfen**

Dieser Anwendungsfall prüft, ob ein Messenger-Service zugehörig zur TI-Messenger-Föderation ist und gilt für alle Anwendungsfälle, welche die Matrix-Domain eines anderen Messenger-Services überprüfen müssen. Für die Prüfung der Zugehörigkeit der Matrix-Domain zur TI-Messenger-Föderation, verwendet der Messenger-Proxy eine Föderationsliste die vom Registrierungs-Dienst seines TI-Messenger-Fachdienstes bereitgestellt wird. Die Speicherdauer der Föderationsliste des Messenger-Proxies ist limitiert. Die Aktualisierung der Föderationsliste erfolgt wie in Anhang B 8.2 "Aktualisierung der Föderationsliste" beschrieben.

1230

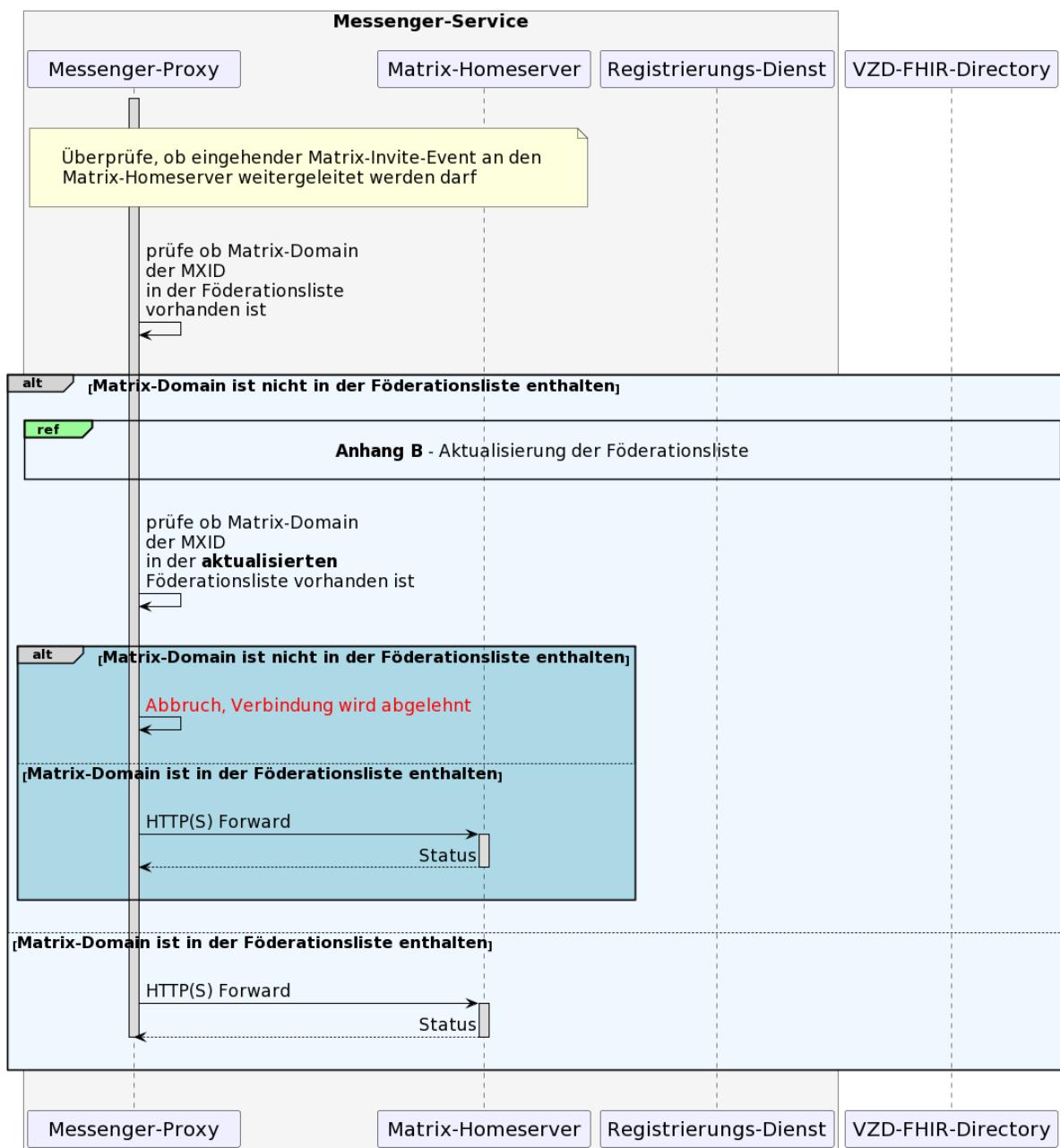
1231

Tabelle 12: Föderationszugehörigkeit eines Messenger-Service prüfen

AF_10064	Föderationszugehörigkeit eines Messenger-Service prüfen
Akteur	-
Auslöser	Der Messenger-Proxy empfängt einen <code>Invite-Event</code> und MUSS die im Request enthaltenen MXIDs auf Domain-Zugehörigkeit zur TI-Messenger-Föderation prüfen.
Komponenten	<ul style="list-style-type: none"> • Messenger-Proxy, • Matrix-Homeserver.
Vorbedingungen	keine
Eingangsdaten	<code>Invite-Event</code>
Ergebnis	Der Messenger-Proxy ermittelt mittels der Föderationsliste, ob die Matrix-Domain des anderen Messenger-Service Teil der TI-Messenger-Föderation ist.
Ausgangsdaten	Status vom Matrix-Homeserver und Weiterleitung
Akzeptanzkriterien	 ML-123672 ,  ML-123891 ,  ML-123893 ,  ML-132589

1232

1233 In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den
 1234 Anwendungsfall genutzt werden, dargestellt. Das auslösende Matrix-Event am
 1235 Messenger-Proxy wird in der folgenden Abbildung nicht gezeigt. Die Aktualisierung der
 1236 Föderationsliste ist in Anhang B "Aktualisierung der Föderationsliste" hinreichend
 1237 beschrieben.
 1238



1239

1240

1241 **Abbildung 15: Laufzeitsicht - Föderationszugehörigkeit eines Messenger-Service prüfen**

1242 [=<]

1243

1244 **Akzeptanzkriterien für den Anwendungsfall: Föderationszugehörigkeit eines
Messenger-Service prüfen (AF_10064)**

1245

1246 **ML-123672 - AF_10064 - Föderationsliste vom VZD-FHIR-Directory abrufen**1247 Der Registrierungs-Dienst des TI-Messenger-Fachdienstes MUSS die Föderationsliste
erfolgreich vom FHIR-Proxy des VZD-FHIR-Directory abrufen.

1248 [=<]

1249 **ML-123893 - AF_10064 - Aktualität - Föderationsliste Messenger-Proxy**

1252 Es MUSS sichergestellt werden, dass die Föderationsliste des Messenger-Proxy aktuell ist.
 1253 Dafür MUSS der Messenger-Proxy mindestens einmal täglich eine aktuelle Liste bei dem
 1254 Registrierungs-Dienst anfordern.

1255 [<=]

ML-123891 - AF_10064 - Matrix-Domain Teil der Föderationsliste & Aktualitätscheck

1258 Es MUSS sichergestellt werden, dass der Registrierungs-Dienst die Föderationsliste auf
 1259 Aktualität überprüft, bevor eine aktualisierte Liste durch den Messenger-Proxy abgerufen
 1260 werden kann. Ebenfalls MUSS sichergestellt werden, dass der Messenger-Proxy
 1261 tatsächlich überprüft, ob die Matrix-Domain des anderen Messenger-Service Teil der
 1262 Föderationsliste ist.

1263 [<=]

ML-132589 - AF_10064 - TI-M Rohdatenerfassung und -lieferung

1264 Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-
 1265 Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die
 1266 definierte Schnittstelle der Rohdatenerfassung versendet. [<=]

1268

1269 6.7 AF - Einladung von Akteuren innerhalb einer Organisation

AF_10104 - Einladung von Akteuren innerhalb einer Organisation

1270 In diesem Anwendungsfall wird ein Akteur der zu einer gemeinsamen Organisation
 1271 gehört in einen Raum eingeladen um Aktionen auszuführen. Für die Suche von Akteuren
 1272 innerhalb einer gemeinsamen Organisation durchsucht ein TI-Messenger-Client das
 1273 Nutzerverzeichnis seiner Organisation auf dem Matrix-Homeserver. In diesem
 1274 Anwendungsfall prüft der Messenger-Proxy ob die im Invite-Event enthaltenen Matrix-
 1275 Domains Teil der TI-Föderation sind (siehe Berechtigungskonzept - Stufe 1). Ist dies der
 1276 Fall erfolgt die Weiterleitung an den zugehörigen Matrix-Homeserver. Dieser prüft ob die
 1277 beteiligten Akteure bei ihm registriert sind. Ist dies nicht der Fall, handelt es sich bei dem
 1278 einzuladenden Akteur nicht um einen Akteur innerhalb der Organisation und das Invite-
 1279 Event wird an den Matrix- Homeserver des einzuladenden Akteurs weitergeleitet. Der
 1280 Anwendungsfall "AF_10061 - Einladung von Akteuren außerhalb einer Organisation" zeigt
 1281 den sich daraus ergebenden Verlauf.

1283

1284 **Tabelle 13: Einladung von Akteuren innerhalb einer Organisation**

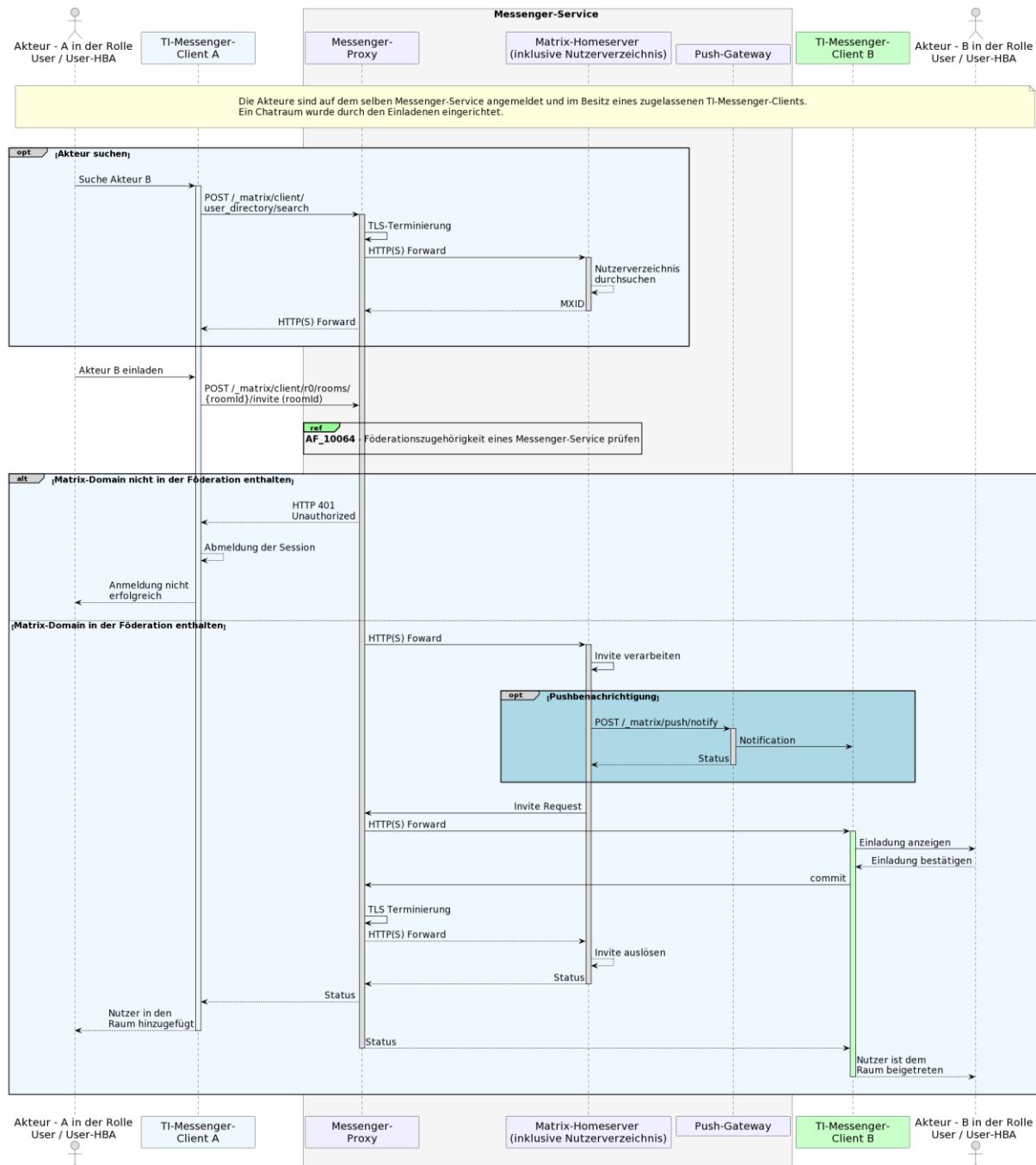
AF_10104	Einladung von Akteuren innerhalb einer Organisation
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle "User / User-HBA"
Auslöser	Akteur A möchte Akteur B seiner Organisation in einen gemeinsamen Raum einladen.
Komponenten	<ul style="list-style-type: none"> • TI-Messenger Client A + B, • Messenger-Proxy, • Matrix-Homeserver, • Push-Gateway.

Vorbedingungen	<ol style="list-style-type: none"> 1. Die Akteure sind am selben Messenger-Service angemeldet. 2. Jeder Akteur hat einen zugelassenen TI-Messenger-Client. 3. Ein Chatraum wurde durch den Einladenden eingerichtet.
Eingangsdaten	Invite-Event
Ergebnis	Akteur A und Akteur B sind beide in einem gemeinsamen Chatraum. Optional erfolgt eine Benachrichtigung an Akteur B über die Einladung in den Chatraum.
Ausgangsdaten	Status
Akzeptanzkriterien	 ML-123896 ,  ML-129415 ,  ML-129414 ,  ML-132590

1285
 1286
 1287
 1288
 1289
 1290
 1291
 1292
 1293

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Der für die zukünftige Kommunikation genutzte Chatraum wurde durch den einladenden Akteur bereits erstellt. Die folgende Darstellung zeigt lediglich die Einladung zwischen zwei Akteuren. Weitere Akteure können unabhängig von dieser Laufzeitsicht eingeladen werden (Hinweis: Group-Messaging). Für die vereinfachte Darstellung wird vorausgesetzt, dass die TI-Messenger-Clients der beteiligten Akteure online sind. Ebenfalls wird davon ausgegangen, dass beide Akteure am selben Matrix-Homeserver registriert sind.

1294



Akteur - A in der Rolle
User / User-HBA

TI-Messenger-Client A

Messenger-Proxy

Matrix-Homeserver
(inklusive Nutzerverzeichnis)

Push-Gateway

TI-Messenger-Client B

Akteur - B in der Rolle
User / User-HBA

1295

1296

Abbildung 16: Einladung von Akteuren innerhalb einer Organisation

1297 [\Leftarrow]

1298

1299 **Akzeptanzkriterien für den Anwendungsfall: Einladung von Akteuren innerhalb
einer Organisation (AF_10104)**

1300 **ML-123896 - AF_10104 - Matrix-Homeserver nach Akteuren durchsuchen**

1301 Der TI-Messenger-Client zeigt eine Liste aller Akteuren eines Matrix-Homeservers an.

1302 [\Leftarrow]

1305 **ML-129415 - AF_10104 - Messenger-Proxy prüft TI-Föderationszugehörigkeit**
1306 Der Messenger-Proxy lehnt den `Invite-Event` ab, wenn die Matrix-Domain nicht zur TI-
1307 Föderation gehört.
1308 [<=]

1309 **ML-129414 - AF_10104 - Akteure sind dem Chatraum beigetreten**
1310 Alle Chat-Parteien sind erfolgreich im Chatraum vorhanden.
1311 [<=]

1312 **ML-132590 - AF_10104 - TI-M Rohdatenerfassung und -lieferung**
1313 Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-
1314 Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die
1315 definierte Schnittstelle der Rohdatenerfassung versendet.[<=]

1316

1317 **6.8 AF - Austausch von Events zwischen Akteuren innerhalb einer**
1318 **Organisation**

1319 **AF_10063 - Austausch von Events zwischen Akteuren innerhalb einer**
1320 **Organisation**

1321 Dieser Anwendungsfall ermöglicht es Akteuren, welche sich in einem gemeinsamen Raum
1322 innerhalb eines Messenger-Service befinden, Nachrichten auszutauschen und weitere
1323 durch die Matrix-Spezifikation festgelegte Aktionen (Events) auszuführen.
1324

1325

Tabelle 14 Austausch von Events zwischen Akteuren innerhalb einer Organisation

AF_10063	Austausch von Events zwischen Akteuren innerhalb einer Organisation
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle "User / User-HBA"
Auslöser	Alle Matrix-Events die innerhalb eines Messenger-Service einer Organisation ausgeführt werden
Komponenten	<ul style="list-style-type: none"> • TI-Messenger Client A + B, • Messenger-Proxy, • Matrix-Homeserver, • Push-Gateway.
Vorbedingungen	<ol style="list-style-type: none"> 1. Die Akteure sind am selben Messenger-Service angemeldet. 2. Jeder Akteur hat einen zugelassenen TI-Messenger-Client. 3. Die Teilnehmer sind einem gemeinsamen Raum beigetreten.
Eingangsdaten	Matrix-Event
Ergebnis	Matrix-Event wurde erfolgreich verarbeitet
Ausgangsdaten	Abhängig vom Matrix-Event
Akzeptanzkriterien	 ML-123669 ,  ML-123670 ,  ML-132591

1326

1327

1328

1329

1330

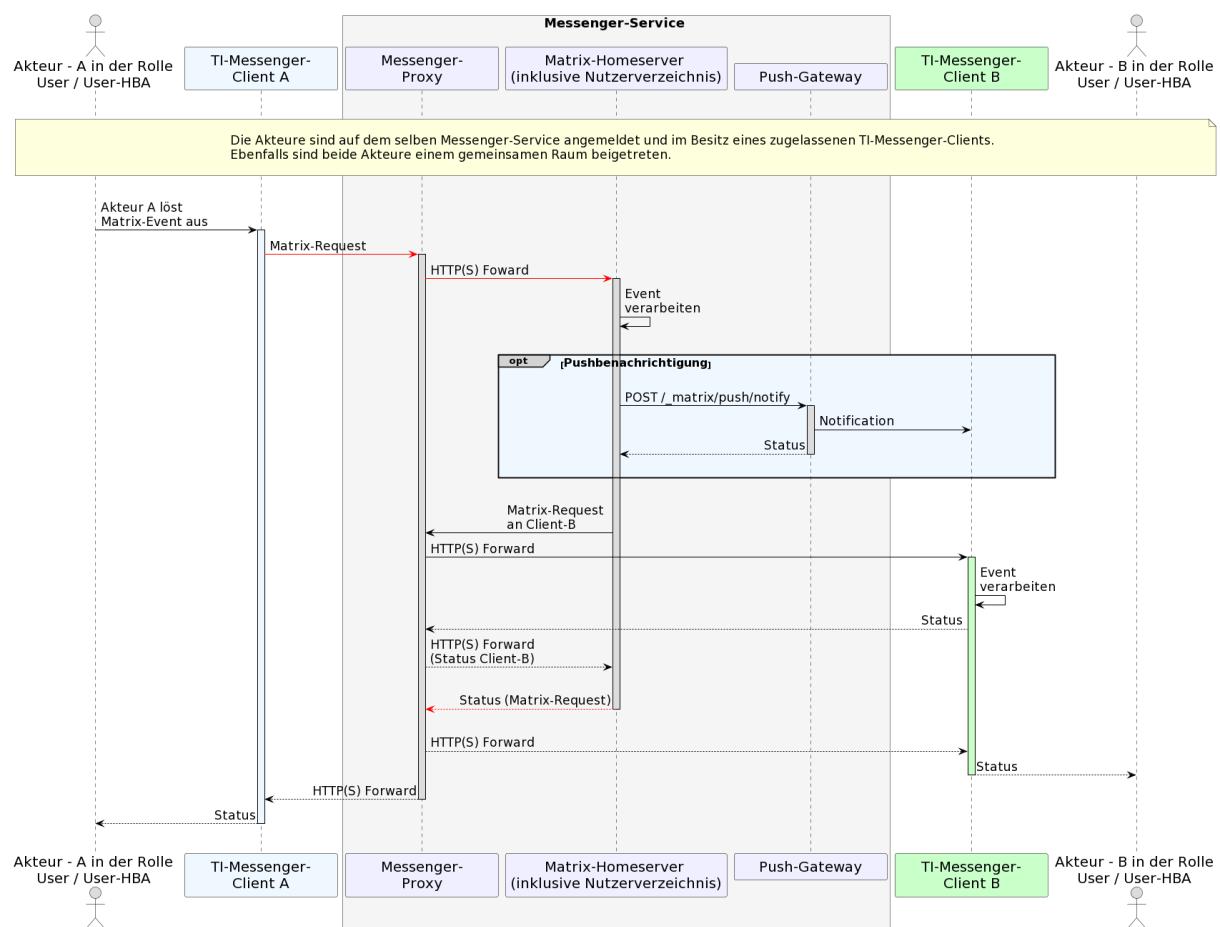
1331

1332

1333

1334

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es sich um eine **vereinfachte Laufzeitansicht** in der zum Beispiel die TLS-Terminierung am Messenger-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde. Die in der Abbildung rot dargestellten Linien symbolisieren den Kommunikationsverlauf des auslösenden Matrix-Request. Für die vereinfachte Darstellung wird vorausgesetzt, dass die TI-Messenger-Clients der beteiligten Akteure online sind.



1335

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

1336 [=>]

1339
1340 **Akzeptanzkriterien für den Anwendungsfall: Austausch von Events zwischen
1341 Akteuren innerhalb einer Organisation (AF_10063)**
1342

ML-123670 - AF_10063 - Chatnachricht wird verarbeitet

1344 Eine Chatnachricht vom TI-Messenger-Client A an TI-Messenger-Client B wurde vom
1345 Matrix-Homeserver erfolgreich verarbeitet.

1346 [=>]

ML-123669 - AF_10063 - Auslösen einer Benachrichtigung

1348 Der Matrix-Homeserver löst eine Benachrichtigung des TI-Messenger-Clients vom
1349 Empfänger über das mit dem TI-Messenger-Client verbundene Push-Gateway des TI-
1350 Messenger-Anbieters aus.

1351 [=>]

ML-132591 - AF_10063 - TI-M Rohdatenerfassung und -lieferung

1353 Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-
1354 Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die
1355 definierte Schnittstelle der Rohdatenerfassung versendet. [=>]

1356

1357 **6.9 AF - Einladung von Akteuren außerhalb einer Organisation**1358 **AF_10061 - Einladung von Akteuren außerhalb einer Organisation**

1359 In diesem Anwendungsfall wird ein Akteur außerhalb einer Organisation eingeladen. Für
1360 die Suche von Akteuren außerhalb der Organisation KANN das VZD-FHIR-Directory
1361 verwendet werden. Ist die MXID des gesuchten Akteurs dort nicht vorhanden MUSS die
1362 Kontaktaufnahme auch über einen QR-Code Scan erfolgen. Im Gegensatz zu einer
1363 Einladung von Akteuren innerhalb einer Organisation (siehe "AF_10063 -Austausch von
1364 Events innerhalb einer Organisation"), prüft in diesem Anwendungsfall der Messenger-
1365 Proxy des Einzuladenden zusätzlich die im Kapitel "Berechtigungskonzept" festgelegten
1366 Kriterien (Stufe 1 - 3).
1367

1368

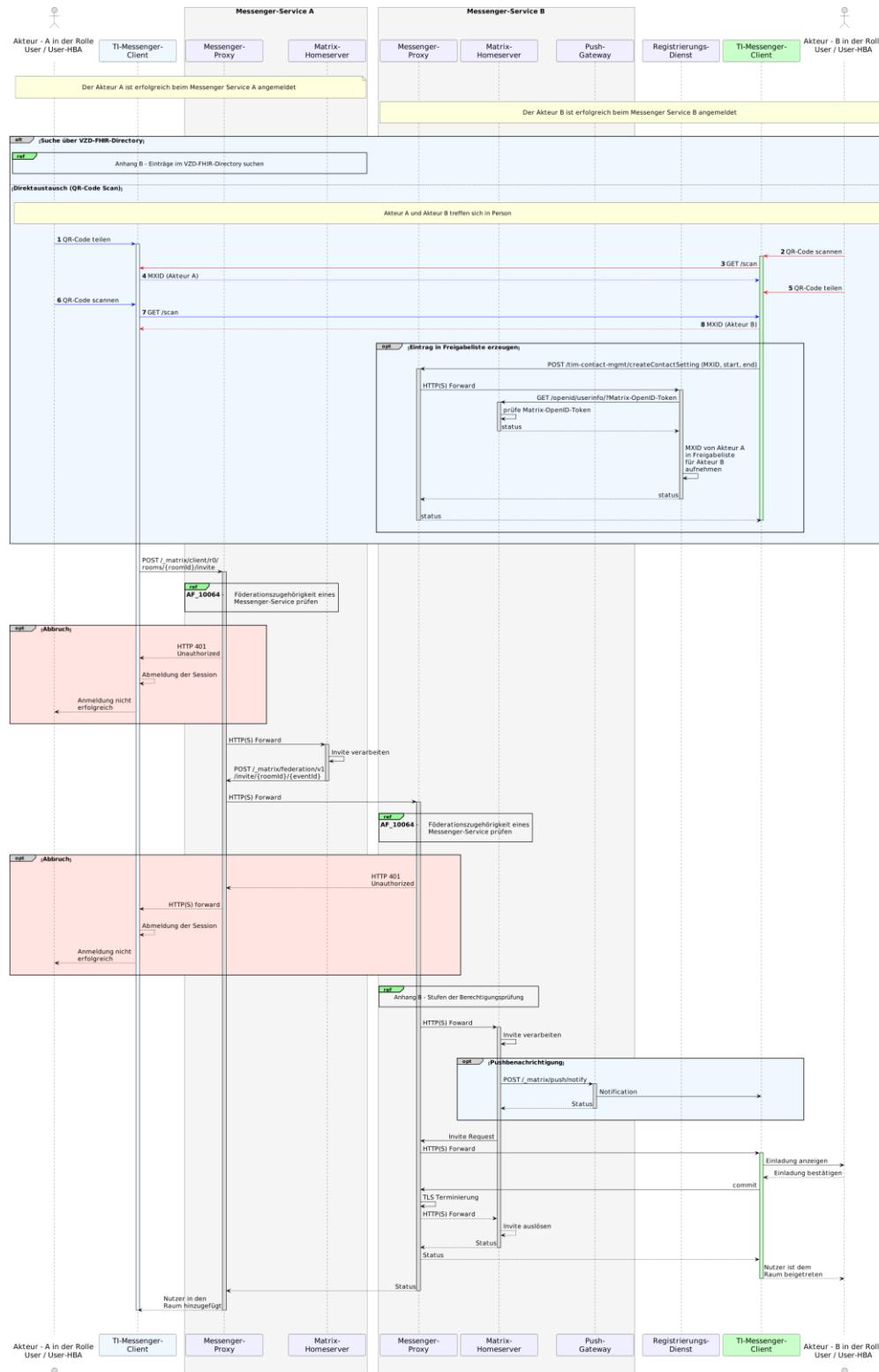
Tabelle 15 AF - Einladung von Akteuren außerhalb einer Organisation

AF_10061	Einladung von Akteuren außerhalb einer Organisation
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der "Rolle User / User-HBA"
Auslöser	Akteur A möchte mit Akteur B außerhalb einer Organisation einen gemeinsamen Chatraum einrichten.
Komponenten	<ul style="list-style-type: none"> • TI-Messenger Client A + B, • Messenger-Proxy A + B, • Matrix-Homeserver A + B, • VZD-FHIR-Directory, • Push-Gateway B.
Vorbedingungen	<ol style="list-style-type: none"> 1. Die Akteure verfügen über einen zugelassenen TI-Messenger-Client. 2. Die Akteure kennen die URL ihres Messenger-Service oder die URL ist bereits in ihren TI-Messenger-Clients konfiguriert. 3. Die Akteure sind am Messenger-Services angemeldet (siehe AF_10057) 4. Die verwendeten Messenger-Services sind Bestandteile der TI-Messenger-Föderation.
Eingangsdaten	Invite-Event
Ergebnis	Akteur A und Akteur B sind beide in einem gemeinsamen Chatraum. Optional erfolgt eine Benachrichtigung an Akteur B über die Einladung in den Chatraum.
Ausgangsdaten	Status
Akzeptanzkriterien	 ML-123654 ,  ML-123663 ,  ML-132592

1369

1370 In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den
 1371 Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es um eine **vereinfachte**
 1372 **Laufzeitansicht** in der zum Beispiel die TLS-Terminierung am Messenger-Proxy auf
 1373 Grund der Übersichtlichkeit nicht berücksichtigt wurde. Ebenfalls wurde für eine
 1374 vereinfachte Darstellung darauf verzichtet eine eventuell notwendige Aktualisierung der
 1375 Föderationsliste vom eigenem Registrierungs-Dienst zu zeigen. Der Abruf der
 1376 Föderationsliste ist im Anhang B "Aktualisierung der Föderationsliste" hinreichend
 1377 beschrieben. Für die vereinfachte Darstellung wird vorausgesetzt, dass die TI-
 1378 Messenger-Clients der beteiligten Akteure online sind. Der in der Abbildung dargestellte
 1379 Registrierungs-Dienst gehört zu dem TI-Messenger-Fachdienst des Messenger-Service B.

1380



1381

1382

1383 **Abbildung 18: Laufzeitsicht - Einladung von Akteuren außerhalb einer Organisation**

1384 [<=]

1385 **Akzeptanzkriterien für den Anwendungsfall: Einladung von Akteuren außerhalb
1386 einer Organisation (AF_10061)**

1387

1388 **ML-123654 - AF_10061 - Suche im VZD-FHIR-Directory**

1389 Ein Messenger-Client kann erfolgreich im VZD-FHIR-Directory nach einem Chatpartner
1390 suchen.

1391 [\leq]

1392 Ein Beispiel für einen `Invite`-Event ist im Dokument [gemSpec_TI-Messenger-
1393 FD#Messenger Proxy] zu finden.

1394

1395 **ML-123663 - AF_10061 - Akteure sind dem Chatraum beigetreten**

1396 Alle Chat Parteien sind erfolgreich im Chatraum vorhanden.

1397 [\leq]

1398 **ML-132864 - Berechtigungsprüfung aller Stufen**

1399 Die Berechtigungsprüfung der Stufen 1-3 wurden berücksichtigt.

1400 [\leq]

1401 **ML-132592 - AF_10061 - TI-M Rohdatenerfassung und -lieferung**

1402 Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-
1403 Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die
1404 definierte Schnittstelle der Rohdatenerfassung versendet. [\leq]

1405

1406 **6.10 AF - Austausch von Events zwischen Akteuren außerhalb
1407 einer Organisation**

1408 **AF_10062 - Austausch von Events zwischen Akteuren außerhalb einer
1409 Organisation**

1410 In diesem Anwendungsfall können Akteure welche sich in einem gemeinsamen Raum
1411 befinden Nachrichten austauschen und andere durch die Matrix-Spezifikation festgelegte
1412 Aktionen ausführen. Dieser Anwendungsfall setzt ein erfolgreiches `Invite`-Event eines
1413 oder mehrerer beteiligter Akteure voraus. In diesem Anwendungsfall sind die beteiligten
1414 Akteure in einem gemeinsamen Chatraum und auf unterschiedlichen Messenger-Services
1415 verteilt.

1416

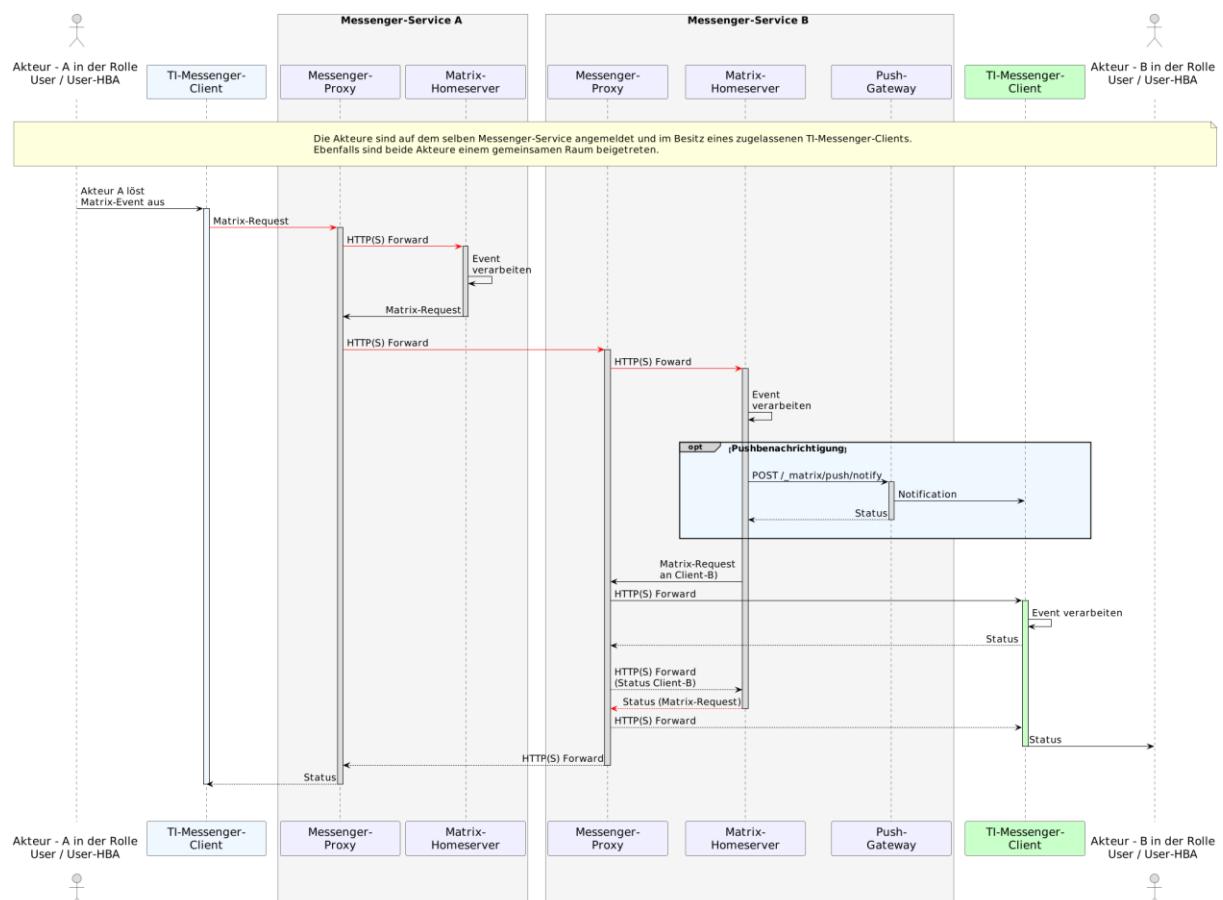
1417

Tabelle 16: AF - 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. 3. Die Messenger-Proxys überprüfen die Zugehörigkeit der beteiligten Messenger-Services (siehe AF_10064)
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

1418

1419 In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den
 1420 Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es um eine **vereinfachte**
 1421 **Laufzeitansicht** in der zum Beispiel die TLS-Terminierung am Messenger-Proxy auf
 1422 Grund der Übersichtlichkeit nicht berücksichtigt wurde. Es wird in dem Anwendungsfall
 1423 von lediglich zwei beteiligten Akteuren ausgegangen. Auf die bei der Prüfung zur
 1424 Föderationsliste, durch den Messenger-Proxy, notwendigen Interaktionen wurde in dieser
 1425 Laufzeitsicht verzichtet. Für eine ausführliche Beschreibung dieser Prüfung wird auf den
 1426 Anwendungsfall "AF_10064 -Föderationszugehörigkeit eines Messenger-Service prüfen"
 1427 verwiesen. Die in der Abbildung rot dargestellten Linien symbolisieren den
 1428 Kommunikationsverlauf des auslösenden Matrix-Request. Für die vereinfachte
 1429 Darstellung wird vorausgesetzt, dass die TI-Messenger-Clients der beteiligten Akteure
 1430 online sind.
 1431



1432

Abbildung 19: Laufzeitsicht - Austausch von Events zwischen Akteuren außerhalb einer Organisation

1435 [=<]

1436

1437 **Akzeptanzkriterien für den Anwendungsfall: Austausch von Nachrichten**
1438 **zwischen Akteuren außerhalb einer Organisation (AF_10062)**

1439

1440 **ML-123665 - AF_10062 - Messenger-Proxy des Senders prüft Domain des Empfängers**

1442 Der Messenger-Proxy des Senders prüft die Domain des Empfängers auf Zugehörigkeit zur TI-Messenger-Föderation.

1444 [=<]

1445 **ML-123666 - AF_10062 - Messenger-Proxy des Empfängers prüft Domain des Senders**

1447 Der Messenger-Proxy des Empfängers prüft die Domain des Senders auf Zugehörigkeit zur TI-Messenger-Föderation.

1449 [=<]

1450 **ML-123667 - AF_10062 - Auslösen einer Notifikation**

1451 Der Matrix-Homeserver des Empfängers löst eine Benachrichtigung des Messenger-Clients über sein Push-Gateway aus.

1453 [=<]

1454 **ML-123668 - AF_10062 - Nachricht wird angezeigt**

1455 Die Nachricht wird dem Empfänger im gemeinsamen Raum angezeigt.
1456 [≤]

1457 **ML-132593 - AF_10062 - TI-M Rohdatenerfassung und -lieferung**
1458 Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-
1459 Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die
1460 definierte Schnittstelle der Rohdatenerfassung versendet.[≤]

1461

1462

7 Anhang A – Verzeichnisse

1463

7.1 Abkürzungen

Kürzel	Erläuterung
AD	Active Directory
AF	Anwendungsfall
AZPD	Anbieter zentrale Plattformdienste
FHIR	Fast Healthcare Interoperable Resources
HBA	Heilberufsausweis
HTTP	Hypertext Transfer Protocol
IDP	Identity Provider
JSON	JavaScript Object Notation
JWT	JSON Web Token
LDAP	Lightweight Directory Access Protocol
LE	Leistungserbringer
MXID	Matrix-User-ID
OAuth	Open Authorization
PTA	Pharmazeutisch-technischer Assistent
REST	Representational State Transfer
SMC-B	Institutionenkarte (Security Module Card Typ B)
SSO	Single Sign-on
TI	Telematikinfrastruktur

TI-ITSM	IT-Service-Management der TI
TI-M	TI-Messenger
TSP	Trust Service Provider
VZD	Verzeichnisdienst

1464 **7.2 Glossar**

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

1465 Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung
 1466 gestellt.

1467 **7.3 Abbildungsverzeichnis**

1468	Abbildung 1: Komponenten der TI-Messenger-Architektur (vereinfachte Darstellung)....	9
1469	Abbildung 2: Benachbarten Produkttypen des TI-Messenger-Dienstes	14
1470	Abbildung 3: Komponenten der TI-Messenger-Architektur und deren Schnittstellen	22
1471	Abbildung 4: Darstellung der Berechtigungsprüfung am Messenger-Proxy	27
1472	Abbildung 5: Beispiel einer Iteraktion mit einem Chatbot.....	35
1473	Abbildung 6: TI-Messenger-Dienst Instanzen	36
1474	Abbildung 7: Ausschnitt - TI-Messenger-Anbieter im TI-ITSM.....	37
1475	Abbildung 8: Org-Admin - Übersicht Anwendungsfälle.....	38
1476	Abbildung 9: User / User HBA - Übersicht Anwendungsfälle	39
1477	Abbildung 10: Laufzeitsicht - Authentisieren einer Organisation am TI-Messenger-Dienst	42
1479	Abbildung 11: Laufzeitsicht - Bereitstellung eines Messenger-Service für eine Organisation	45
1481	Abbildung 12: Laufzeitsicht - Organisationsressourcen im Verzeichnisdienst hinzufügen	48
1482	Abbildung 13: Laufzeitsicht - Anmeldung eines Akteurs am Messenger-Service	51
1483	Abbildung 14: Laufzeitsicht - Akteur (User-HBA) im Verzeichnisdienst hinzufügen	54

1484	Abbildung 15: Laufzeitsicht - Föderationszugehörigkeit eines Messenger-Service prüfen	57
1485	Abbildung 16: Einladung von Akteuren innerhalb einer Organisation	60
1486	Abbildung 17: Laufzeitsicht - Austausch von Events zwischen Akteuren innerhalb einer	
1487	Organisation	63
1488	Abbildung 18: Laufzeitsicht - Einladung von Akteuren außerhalb einer Organisation.....	66
1489	Abbildung 19: Laufzeitsicht - Austausch von Events zwischen Akteuren außerhalb einer	
1490	Organisation	69
1491	Abbildung 20: Laufzeitansicht - Einträge im VZD-FHIR-Directory suchen	76
1492	Abbildung 21: Laufzeitansicht - Aktualisierung der Föderationsliste	77
1493	Abbildung 22: Laufzeitansicht - Stufen der Berechtigungsprüfung.....	78
1494		

1495 **7.4 Tabellenverzeichnis**

1496	Tabelle 1: Akteure und Rollen	10
1497	Tabelle 2: Kommunikationsmatrix	16
1498	Tabelle 3: Arten von Token	18
1499	Tabelle 4: Verzeichnistypen - Rechtekonzept	24
1500	Tabelle 5: Schreibzugriff - VZD-FHIR-Ressourcen	32
1501	Tabelle 6: Beispiel für Funktionsaccounts.....	33
1502	Tabelle 7: Tabelle : AF - Authentisieren einer Organisation am TI-Messenger-Dienst....	40
1503	Tabelle 8: AF - Bereitstellung eines Messenger-Service für eine Organisation	43
1504	Tabelle 9: AF - Organisationsressourcen im Verzeichnisdienst hinzufügen.....	46
1505	Tabelle 10: AF - Anmeldung eines Akteurs am Messenger-Service	49
1506	Tabelle 11: AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen	52
1507	Tabelle 12: Föderationszugehörigkeit eines Messenger-Service prüfen	56
1508	Tabelle 13: Einladung von Akteuren innerhalb einer Organisation	58
1509	Tabelle 14 Austausch von Events zwischen Akteuren innerhalb einer Organisation	62
1510	Tabelle 15 AF - Einladung von Akteuren außerhalb einer Organisation.....	65
1511	Tabelle 16: AF - Austausch von Events zwischen Akteuren außerhalb einer Organisation	68
1512		
1513		

1514 **7.5 Referenzierte Dokumente**

1515 **7.5.1 Dokumente der gematik**

1516 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument
1517 referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der

1518 vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und
1519 Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und
1520 Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht
1521 aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der
1522 aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die
1523 vorliegende Version aufgeführt wird.

1524

[Quelle]	Herausgeber: Titel
[api-messenger]	gematik: api-ti-messenger https://github.com/gematik/api-ti-messenger/
[api-vzd]	gematik: Verzeichnisdienst der Telematikinfrastruktur https://github.com/gematik/api-vzd
[gemKPT_TI_Messenger]	gematik: Konzeptpapier TI-Messenger
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktivbetrieb
[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

1525

7.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[Client-Server API]	Matrix Foundation: Matrix Specification - Client-Server API https://spec.matrix.org/v1.2/client-server-api/
[FHIR]	HL7 FHIR Dokumentation https://www.hl7.org/fhir/documentation.html
[Matrix Specification]	Matrix Foundation: Matrix Specification https://spec.matrix.org/v1.2/
[OpenID]	OpenID Foundation https://openid.net/developers/specs/
[Push Gateway API]	Matrix Foundation: Matrix Specification - Push Gateway API https://spec.matrix.org/v1.2/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/v1.2/server-server-api/
[Matrix Bots]	Matrix Bot Implementierungen https://matrix.org/bots/

1526

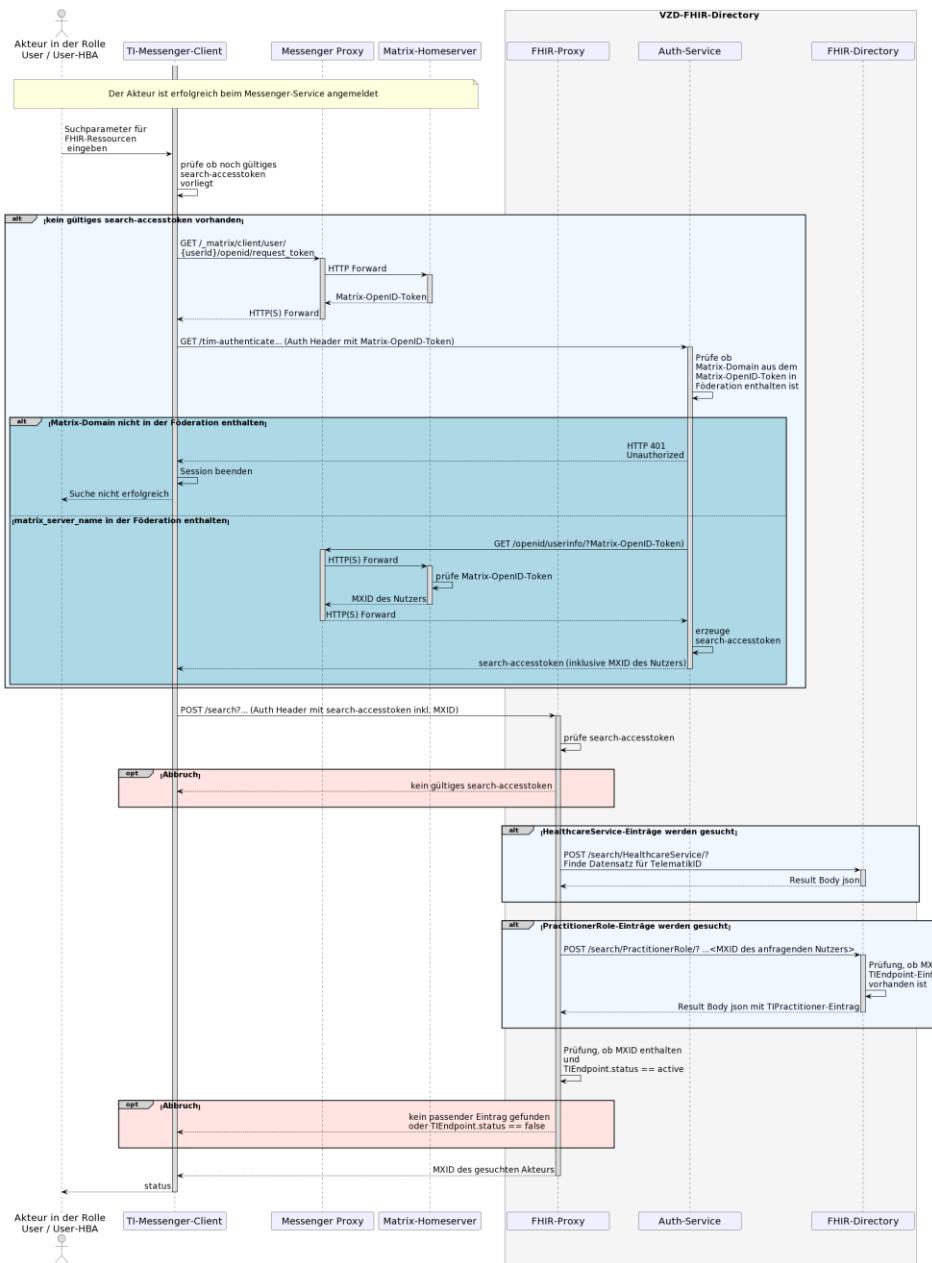
1527

8 Anhang B - Abläufe

1528

8.1 Einträge im VZD-FHIR-Directory suchen

1529 Die folgende Abbildung beschreibt, wie ein Akteur im VZD-FHIR-Directory nach
 1530 *HealthcareService*- und *PractitionerRole* Ressourcen sucht. Dies setzt eine erfolgreiche
 1531 Anmeldung des Akteurs an einem Messenger-Service voraus. Der dargestellte Ablauf
 1532 zeigt alle prinzipiell notwendigen Kommunikationsbeziehungen. Weitergehende
 1533 Informationen zum Ablauf sind in der [gemSpec_VZD_FHIR_Directory] zu finden.
 1534



1535

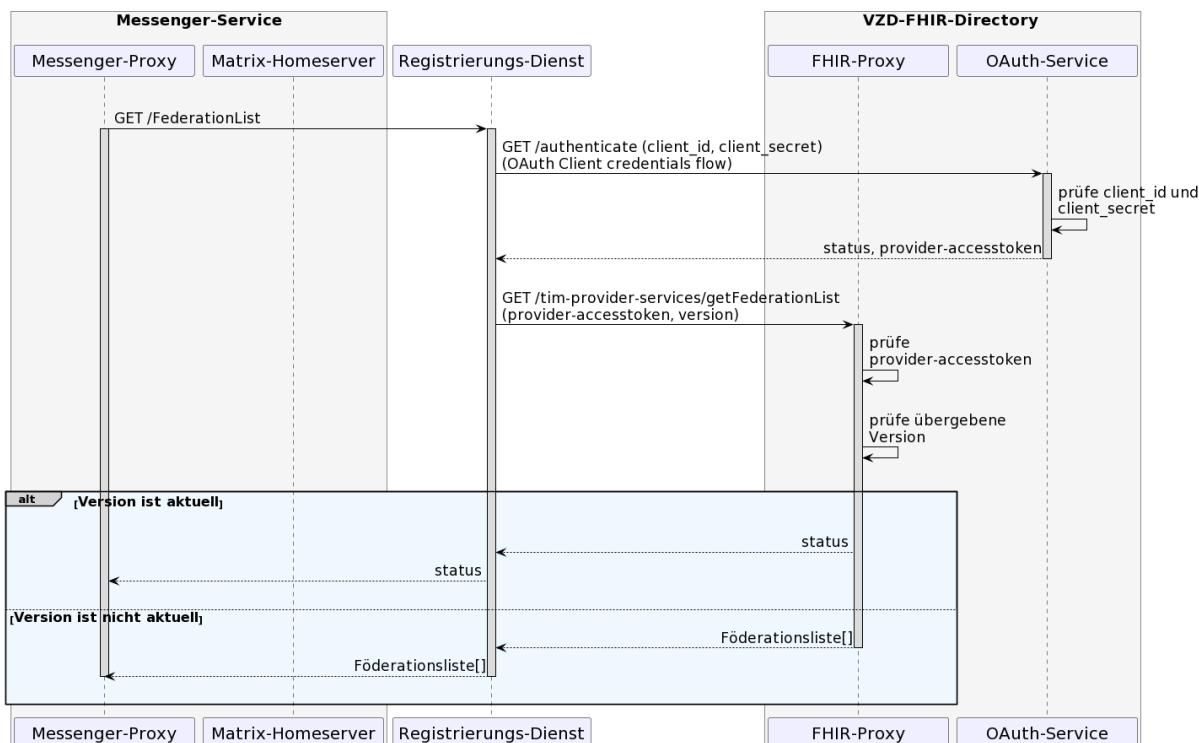
Abbildung 20: Laufzeitansicht - Einträge im VZD-FHIR-Directory suchen

1537

1538 8.2 Aktualisierung der Föderationsliste

1539 Die folgende Abbildung beschreibt, wie der Messenger-Proxy seine lokal vorgehaltene
 1540 Föderationsliste aktualisiert. Für die Aktualisierung der Föderationsliste MUSS der
 1541 Messenger-Proxy diese beim Registrierungs-Dienst seines TI-Messenger-Fachdienstes
 1542 anfragen. Die Häufigkeit der Anfrage einer neuen Liste wird durch den Anbieter
 1543 festgelegt, Ziel sollte eine möglichst aktuelle Föderationsliste sein (mindestens jedoch
 1544 einmal am Tag). Hierbei übergibt der Messenger-Proxy die durch ihn gespeicherte
 1545 Version der Föderationsliste im Aufruf an den Registrierungs-Dienst. Bei
 1546 Übereinstimmung der Version wird für den Messenger-Proxy keine neue Föderationsliste
 1547 durch den Registrierungs-Dienst bereitgestellt. Ist die Version größer als die vom
 1548 Messenger-Proxy übergebene, dann wird durch den Registrierungs-Dienst eine
 1549 aktualisierte Föderationsliste zur Verfügung gestellt. Bei jeder Anfrage eines Messenger-
 1550 Proxys beim Registrierungs-Dienst nach einer aktuellen Föderationsliste MUSS auch der
 1551 Registrierungs-Dienst die Aktualität beim FHIR-Proxy prüfen indem er die von ihm
 1552 gespeicherte Version der Föderationsliste beim Aufruf am FHIR-Proxy übergibt. Ein
 1553 Download der Föderationsliste ist nur notwendig, wenn eine neuere Version auf dem
 1554 FHIR-Proxy existiert. Die Struktur der Föderationsliste ist in
 1555 [gemSpec_VZD_FHIR_Directory] beschrieben.

1556



1557

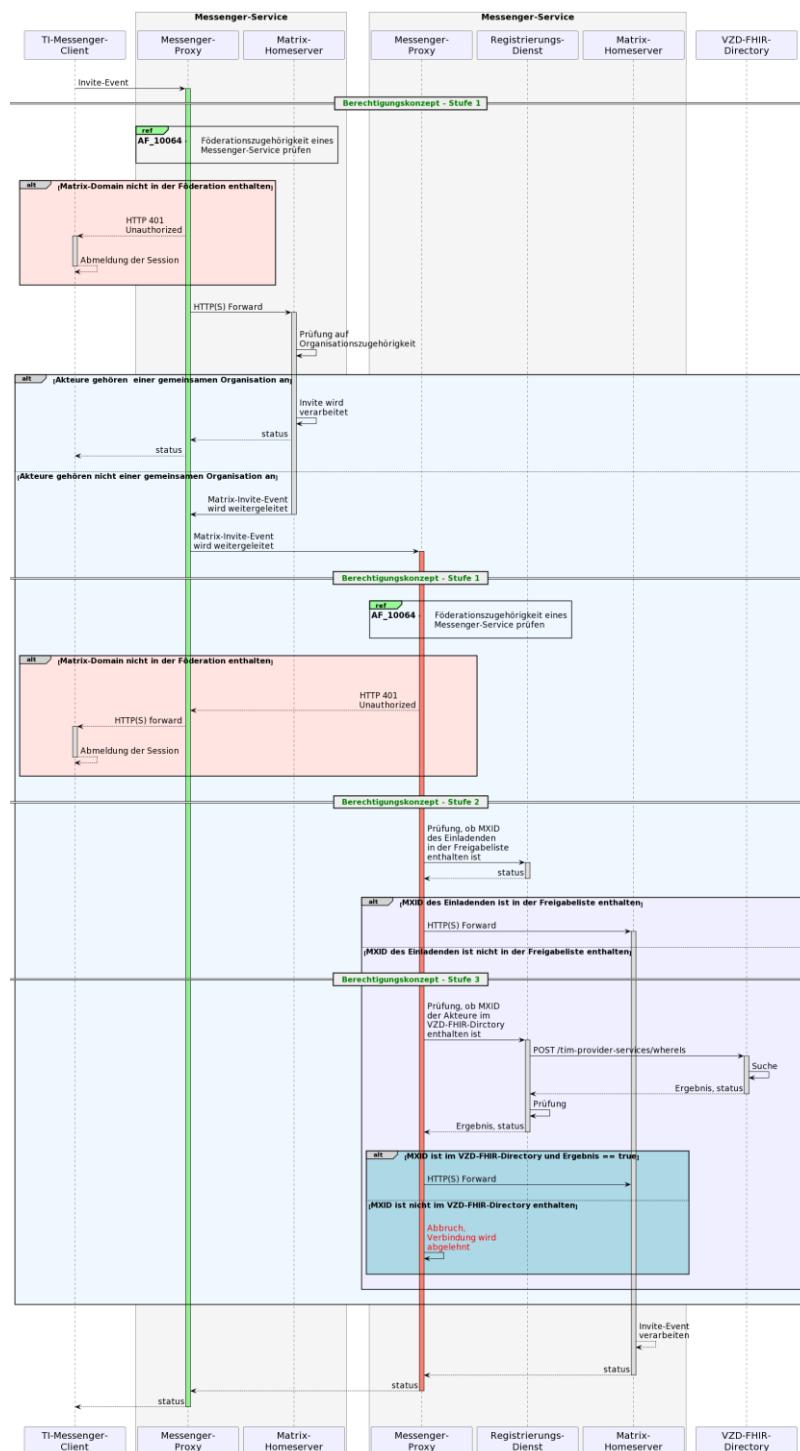
1558 Abbildung 21: Laufzeitansicht - Aktualisierung der Föderationsliste

1559

1560 8.3 Stufen der Berechtigungsprüfung

1561 Die folgende Abbildung beschreibt, wie die Berechtigungsprüfung eingehender Matrix-Anfragen am Messenger-Proxy erfolgen MUSS. Das Berechtigungskonzept basiert auf einer dreistufigen Prüfung, die in Kapitel "Berechtigungskonzept" beschrieben ist. Es wird auf die Erwähnung notwendiger Authentifizierungen an dieser Stelle verzichtet.

1565



1566

1567

Abbildung 22: Laufzeitanansicht - Stufen der Berechtigungsprüfung