

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation TI-Messenger (ePA)

Version: 1.0.0_CC
Revision: 875961
Stand: 28.03.2024
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemSpec_TI-M_ePA

29

30

Dokumentinformationen

Änderungen zur Vorversion

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

34

35

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0_CC	28.03.2024		initiale Erstellung	gematik

37

38

Inhaltsverzeichnis

39	1 Einordnung des Dokumentes	5
40	1.1 Zielsetzung	5
41	1.2 Zielgruppe	5
42	1.3 Geltungsbereich	5
43	1.4 Abgrenzungen	5
44	1.5 Methodik	6
45	2 Systemüberblick	7
46	2.1 Akteure und Rollen	7
47	2.2 Nachbarsysteme	7
48	2.2.1 Authentifizierungs-Dienst für Akteure in der Rolle "Versicherter"	8
49	2.2.2 VZD-FHIR-Directory	8
50	3 Zerlegung des Produkttyps (Systemkomponenten)	9
51	3.1 TI-M Client ePA.....	9
52	3.1.1 VZD-FHIR-Directory	10
53	3.1.2 Auth Modul.....	10
54	3.2 TI-M FD ePA	11
55	3.2.1 Registrierungs-Dienst	12
56	3.2.2 Messenger-Service	12
57	3.2.2.1 Schnittstelle für Authentifizierungsverfahren	12
58	3.2.2.2 Messenger-Proxy.....	14
59	4 Übergreifende Festlegungen	15
60	4.1 Betrieb.....	15
61	5 Funktionsmerkmale	16
62	5.1 Einschränkung zu Anwendungsfall AF_10060 - Bereitstellung eines	
63	Messenger-Service für eine Organisation	16
64	5.2 Feature Identifikation und Login eines Benutzers	16
65	5.2.1 Anwendungsfall	16
66	5.3 Berechtigungsmanagement - Unterbindung der Versicherteneinladung ..	19
67	5.3.1 Client-Server Prüfungen.....	20
68	5.3.2 Server-Server Prüfungen	20
69	5.3.3 Berechtigungsprüfung.....	22
70	5.4 Push-Benachrichtigung im FDV	23
71	6 Anhang A – Verzeichnisse	26
72	6.1 Abkürzungen	26
73	6.2 Glossar	26

74	6.3	Abbildungsverzeichnis	26
75	6.4	Tabellenverzeichnis	27
76	6.5	Referenzierte Dokumente	27
77	6.5.1	Dokumente der gematik.....	27
78	6.5.2	Weitere Dokumente.....	28
79			
80			

81 **1 Einordnung des Dokumentes**

82 **1.1 Zielsetzung**

83 Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und
84 Zulassung der Produkttypen TI-M_Client_ePA und TI-M_FD_ePA. Dieses Dokument
85 erweitert die Basisspezifikation [gemSpec_TI-M_Basis] um die für die genannten
86 Produkttypen notwendigen Anpassungen. Für die Produkte gelten weiterhin die in der
87 Basisspezifikation beschriebenen Funktionalitäten, sofern Sie nicht in diesem Dokument
88 erweitert oder eingeschränkt werden.

89 **1.2 Zielgruppe**

90 Das Dokument richtet sich an Hersteller von Frontends für Versicherte mit integriertem
91 TI-M Client ePA und an Hersteller von TI-M FD ePA.

92 **1.3 Geltungsbereich**

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

Schutzrechts-/Patentrechtshinweis

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

98 **1.4 Abgrenzungen**

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

103 Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept-
104 und Spezifikationsdokumenten. Diese sind in den Produkttypsteckbriefen der
105 Produkttypen TI-M_Client_ePA und TI-M_FD_ePA verzeichnet.

106 1.5 Methodik

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

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

117 Anwendungsfälle und Anforderungen werden im Dokument wie folgt dargestellt:

118 **<AF-ID> - <Titel des Anwendungsfalles>**

119 Text / Beschreibung

120 [**<=**]

121 bzw.

122 **<AFO-ID> - <Titel der Afo>**

123 Text / Beschreibung

124 [**<=**]

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

127

2 Systemüberblick

128 Für die Einbindung der Versicherten werden basierend auf der Basisspezifikation
 129 [gemSpec_TI-M_Basis] Anpassungen vorgenommen, die auf Clientseite im Produkt TI-M
 130 Client ePA und auf Serverseite im Produkt TI-M FD ePA aufgehen.

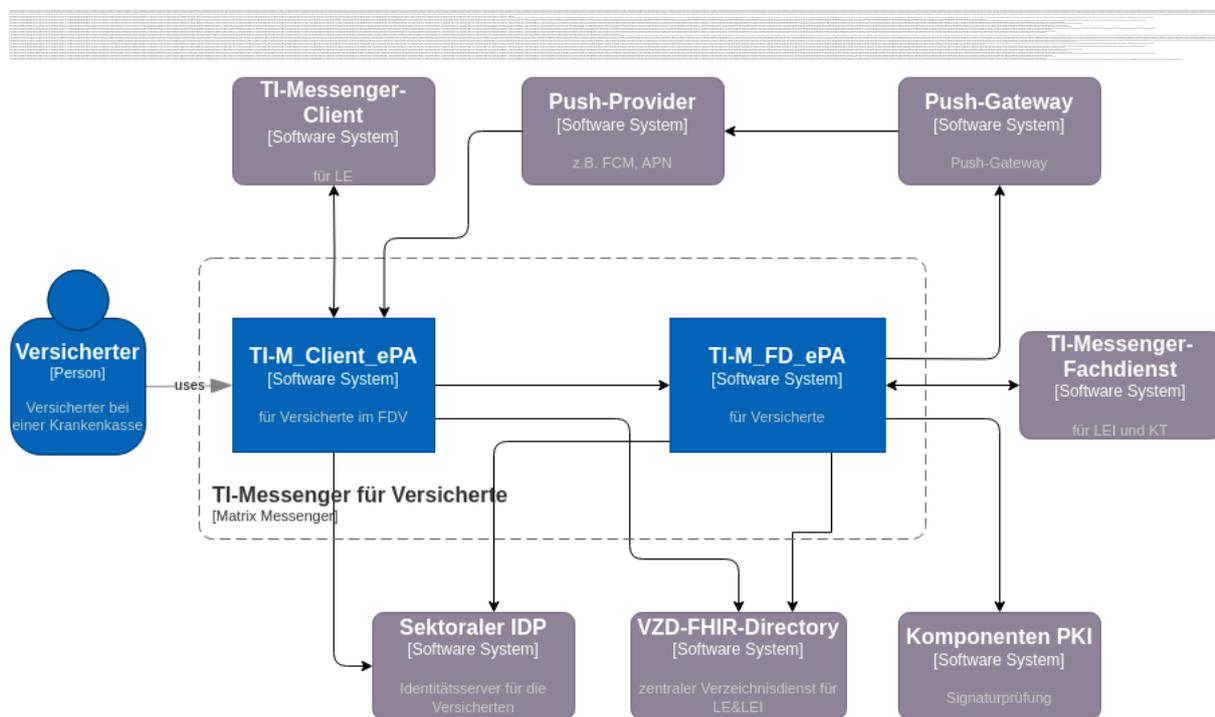
131 2.1 Akteure und Rollen

132 Mit dieser Spezifikation werden die Versicherten als Akteure in die TI-Messenger
 133 Föderation eingebunden. Versicherte können zukünftig über einen TI-Messenger Client im
 134 Frontend des Versicherten der ePA (TI-M Client ePA) sicher und schnell medizinische
 135 Inhalte austauschen. Versicherten stehen die gleichen Funktionalitäten, wie einem Akteur
 136 in der Rolle "User" der Spezifikation [gemSpec_TI-M_Basis] zur Verfügung, die durch die
 137 Inhalte dieser Spezifikation erweitert oder eingeschränkt werden.

138 Der Messenger-Service wird für den Versicherten immer von der jeweiligen Krankenkasse
 139 bereitgestellt.

140 2.2 Nachbarsysteme

141 Die folgende Grafik zeigt die Schnittstellen zu Nachbarsysteme für den TI-M Client ePA
 142 und den TI-M FD ePA.



177

178

Abbildung 1: Kontextabgrenzung

179 Der TI-M Client ePA hat Schnittstellen

- 180 • zu anderen TI-M Clients zum Austausch von Kontaktinformationen,
- 181 • zum sektoralen IDP. Es werden die gleichen Verfahren wie beim ePA FdV (mit
182 Single Sign On, wenn vorhanden (siehe [gemSpec_IDP_Frontend])) verwendet,
- 183 • zum VZD-FHIR-Directory zur Suche nach Kontakten in Organisationen oder im
184 Verzeichnis der Practitioner,
- 185 • zum externen Push Provider um Benachrichtigungen zu erhalten und
- 186 • zum TI-M FD ePA für Versicherte.

187 Der TI-M FD ePA hat Schnittstellen

- 188 • zum TI-M Client ePA für Versicherte,
- 189 • zum sektoralen IDP. Es werden die gleichen Verfahren wie beim ePA FdV mit
190 Single-Sign-On verwendet, wenn vorhanden (siehe [gemSpec_IDP_Sek]),
- 191 • zum FHIR-Verzeichnisdienst zur Pflege und zum Bezug der Föderationsliste,
- 192 • zur Komponenten PKI für die Erzeugung und Prüfung von Zertifikaten aus dem
193 Vertrauensraum der TI,
- 194 • zu anderen TI-M FD, um innerhalb der TI-Messenger Föderation die
195 Kommunikation mit Nutzern anderer TI-M FD zu ermöglichen und
- 196 • zum Push Gateway, um Benachrichtigungen für Nutzer zu versenden.

197 **2.2.1 Authentifizierungs-Dienst für Akteure in der Rolle** 198 **"Versicherter"**

199 Für die Verwaltung der Identitäten der Akteure in der Rolle "Versicherter" stellen die
200 Krankenkassen einen sektoralen IDP bereit. Die Spezifikation für den sektoralen IDP ist
201 unter [gemSpec_IDP_sek] zu finden. Für den TI-M ePA bindend sind Anforderungen aus
202 dem Dokument [gemSpec_IDP_Frontend] für den Client und Anforderungen aus
203 [gemSpec_IDP_FD] für den Fachdienst, die den jeweiligen Produkttypsteckbriefen zu
204 entnehmen sind und deren Inhalte zusätzlich in den Kapiteln zum Client (3.1.2- Auth
205 Modul) und zum Fachdienst (3.2.2.1- Schnittstelle für Authentifizierungsverfahren)
206 aufgeführt werden.

207 **A_25488 - IDP-sek_KTR**

208 Als Authentifizierungs-Dienst für die Akteure in der Rolle "Versicherter" MUSS der
209 sektorale IDP mit Anbieterzulassung nach [gemAnbT_IDP-Sek_KTR_ATV] verwendet
210 werden, der die Akteure für die Fachdienste ePA, eRezept und TI-M beheimatet. [<=]

211 **2.2.2 VZD-FHIR-Directory**

212 Beim VZD-FHIR-Directory gibt es gegenüber der Basisspezifikation nur minimale
213 Anpassungen.

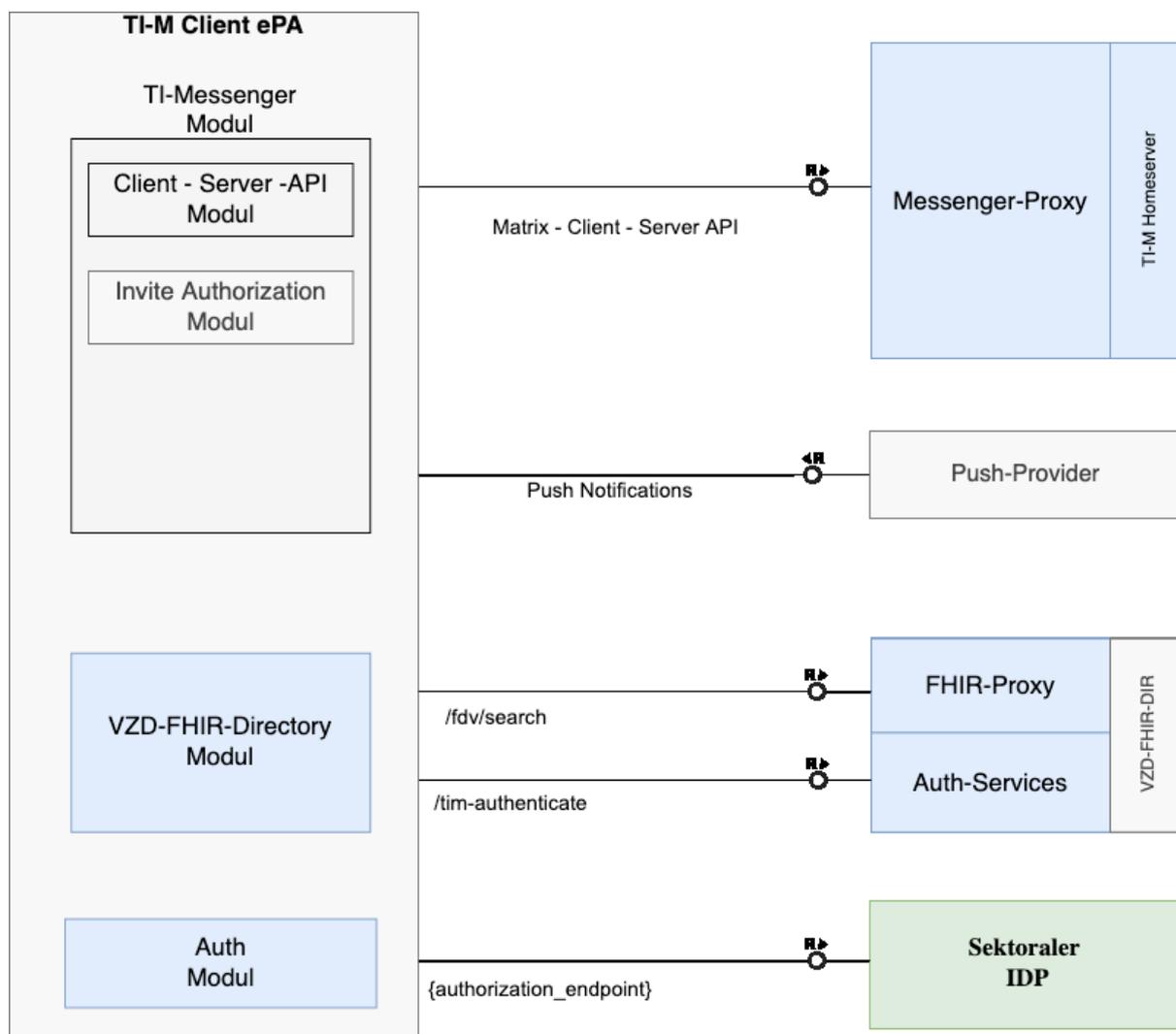
- 214 • Nach der Authentisierung wird für die Akteure ein individueller searchaccess-token
215 bereitgestellt.
- 216 • Für die Suche der Akteure in der Rolle "Versicherter" wurde ein eigener Endpunkt
217 bereitgestellt (3.1.1- VZD-FHIR-Directory).

218 **3 Zerlegung des Produkttyps (Systemkomponenten)**

219 In den folgenden Kapiteln werden die Komponenten des Clients und der Services in einer
 220 Bausteinansicht visualisiert.

221 **3.1 TI-M Client ePA**

222 Die folgende Grafik zeigt die Komponenten eines TI-M Clients ePA. Farblich
 223 hervorgehoben sind diejenigen Komponenten, die im Rahmen der in dieser Spezifikation
 224 vorgestellten Features angepasst werden müssen (blau) und Komponenten, die neu
 225 hinzugekommen sind (grün).



226
 227 **Abbildung 2: TI-M Client ePa Komponentendiagramm**

228 Neu hinzugekommen ist für die User Authentifizierung der Sektorale IDP auf den in
 229 Kapitel 2.2.1- Authentifizierungs-Dienst für Akteure in der Rolle "Versicherter"
 230 eingegangen wird. Am VZD-FHIR-Directory ändert sich lediglich der Endpunkt für die
 231 Suche, da für Akteure in der Rolle "Versicherter" ein neuer Endpunkt bereitgestellt wird.

232 3.1.1 VZD-FHIR-Directory

233 A_25681 - VZD-FHIR-Directory Suche

234 Der TI-M Client ePA MUSS Akteuren in der Rolle Versicherter die Suche im VZD-FHIR-
 235 Directory über die Schnittstelle `/fdv/search` anbieten. [\leq]

236 3.1.2 Auth Modul

237 Für die Interaktion mit dem sektoralen IDP wird auf Clientseite ein Authenticator-Modul
 238 bereitgestellt, dessen Anforderungen in [gemSpec_IDP_Sek] definiert sind. Für den TI-M
 239 Client ePA sind die folgenden Anforderungen zu beachten, die der Spezifikation für
 240 Frontends ([gemSpec_IDP_Frontend] entsprechend referenziert wurden und somit Teil
 241 des Produktypsteckbriefes werden.

Afo-ID	Title	Description
A_23083	Auslösung der Benutzerauthentifizierung	Das Anwendungsfrontend SOLL, wenn es eine Authentifizierung über den sektoralen IDP unterstützt, zur Auslösung der Benutzerauthentifizierung einen OAuth Authorization Request an den zugehörigen Authorization-Server schicken.
A_23086	Aufruf des Authorization-Servers	Das Anwendungsfrontend MUSS, wenn es eine Authentifizierung über den sektoralen IDP unterstützt, den <code>AUTHORIZATION_CODE</code> vom Authenticator-Modul annehmen und an den Authorization-Server weiterleiten.
A_24756	Unterstützung eines SSO innerhalb eines Anwendungskontextes	Will ein Fachdienst ein SSO innerhalb eines Anwendungskontextes unterstützen, so MUSS das Frontend des Fachdienstes den Authorization Request, mit der vom Authorization-Server des Fachdienstes empfangener URI-PAR (siehe [gemSpec_IDP_Sek] Tabelle "Ablaufbeschreibung App-App-Flow" Schritt 5) über das vom Authenticator-Modul bereitgestellte API direkt an dieses senden (siehe A_24748).

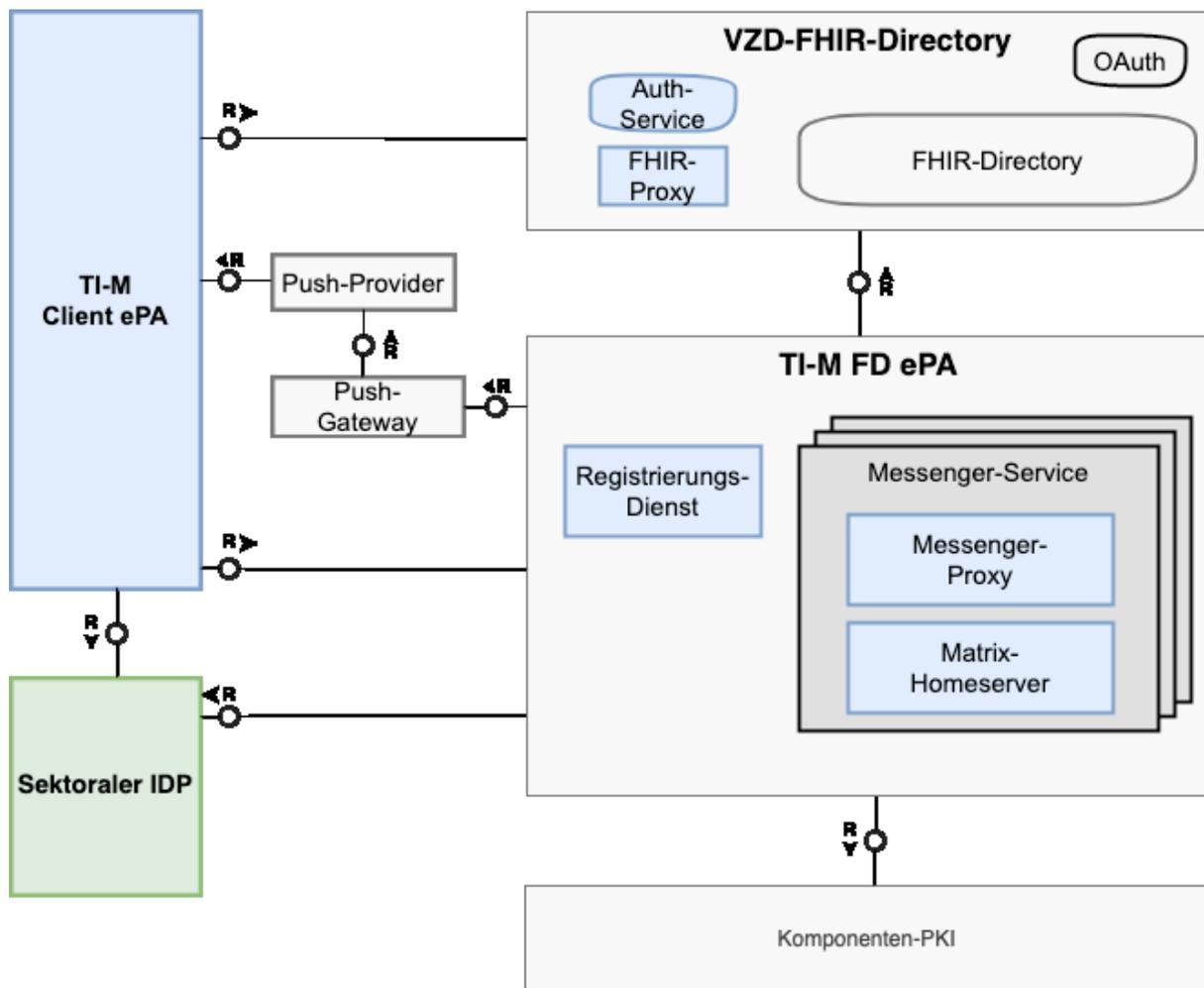
A_24916 Annahme eines Authorization Code

Will ein Fachdienst ein SSO innerhalb eines Anwendungskontextes unterstützen, so MUSS das Frontend des Fachdienstes eine Schnittstelle anbieten, dem das Authenticator-Modul das vom sektoralen IDP nach erfolgreicher Nutzerauthentisierung ausgestellten AUTH_CODE übergeben kann (siehe [gemSpec_IDP_Sek] Tabelle "Ablaufbeschreibung App-App-Flow" Schritt 8).

242 [4 items found](#)

243 **3.2 TI-M FD ePA**

244 Die folgende Grafik visualisiert die Komponenten eines TI-M FD ePA auf Serverseite, die
 245 im Rahmen der in diesem Dokument beschriebenen Features hinzukommen oder
 246 angepasst werden müssen. Farblich hervorgehoben sind diejenigen Komponenten, die im
 247 Rahmen der in dieser Spezifikation vorgestellten Features angepasst werden müssen
 248 (blau) und Komponenten, die neu hinzugekommen sind (grün).



249 **Abbildung 3: TI-Messenger-Service Komponentendiagramm**

250

251 3.2.1 Registrierungs-Dienst

252 Der Registrierungs-Dienst wird angepasst, da nur Kostenträger in die Lage versetzt
 253 werden sollen, Messenger-Services für Akteure in der Rolle "Versicherter" zu bestellen
 254 (siehe 5.1- Einschränkung zu Anwendungsfall AF_10060 - Bereitstellung eines Messenger-
 255 Service für eine Organisation).

256 3.2.2 Messenger-Service

257 3.2.2.1 Schnittstelle für Authentifizierungsverfahren

258 Der Messenger-Service muss für die Authentifizierung der Akteure in der Rolle
 259 "Versicherter" an den sektoralen IDP angeschlossen werden. Anschließend können
 260 Inhalte des vom sektoralen IDP ausgestellten `ID_TOKEN` bei der Account Anlage verwendet
 261 werden. (siehe  ML-150294- AF_10234 - Erzeugung der MXID. (Bei Registrierung)
 262 & 5.2.1-5- AF_10234 - Erzeugung des Display Name). Für den TI-M FD ePA sind die
 263 folgenden Anforderungen zu beachten, die in der Spezifikation für Frontends
 264 ([gemSpec_IDP_FD] entsprechend referenziert wurden und somit Teil des
 265 Produkttypsteckbriefes werden.

Afo-ID	Title	Description
A_22860-01	Prüfung benötigter "scopes" und "claims"	Fachdienste MÜSSEN erhaltene <code>ID_TOKEN</code> auf das Vorhandensein der benötigten <code>scopes</code> und <code>claims</code> überprüfen.
A_22861	Aktualisierung der bekannten Signaturschlüssel bei unbekannter "kid" der Signatur	Bei der Überprüfung eines <code>ID_TOKEN</code> MUSS der Fachdienst, wenn der vom sektoralen Identity Provider verwendete Signatur-Schlüssel ihm unbekannt ist, das Entity Statement des sektoralen Identity Provider sowie die Schlüssel hinter einer eventuell verwendeten <code>signed_jwks_uri</code> herunterladen und auf Vorhandensein der verwendeten <code>kid</code> prüfen.
A_23004	Anforderung eines Vertrauensniveaus	Fachdienste MÜSSEN eine Authentisierung auf dem für den Zugriff auf ihre Fachdaten notwendigen Vertrauensniveau im Parameter <code>acr_values</code> des Pushed Authorization-Request anfragen oder, wenn nur ein Wert infrage kommt diesen im Feld <code>default_acr_values</code> ihres Entity Statements nennen.
A_23005	Verifikation des durchgeführten Vertrauensniveaus	Fachdienste MÜSSEN prüfen, ob das im <code>ID_TOKEN</code> im Feld <code>acr</code> gelistete Vertrauensniveau der durchgeführten Authentisierung für den Zugriff auf ihre Fachdaten ausreicht.

A_23037 Robustheit bei fehlenden Daten	Sind einzelne <code>claims</code> des angefragten <code>scopes</code> nicht im <code>ID_TOKEN</code> enthalten oder leer, weil beispielsweise der Nutzer die Herausgabe verweigert oder Daten nicht hinterlegt wurden, so MUSS der Fachdienst das <code>ID_TOKEN</code> trotzdem akzeptieren und innerhalb der Fachanwendung geeignet reagieren.
A_23049 Überprüfung des "ID_TOKEN" durch den Authorization-Server	<p>Zugriffsgeschützte Fachdienste MÜSSEN vor Gewährung des Zugriffs, den erhaltenen <code>ID_TOKEN</code> wie folgt prüfen. Nur nach erfolgreicher Überprüfung darf der Zugriff gewährt werden.</p> <ol style="list-style-type: none"> 1. Das <code>ID_TOKEN</code> muss valide signiert sein durch einen Schlüssel des ausstellenden sektoralen Identity Provider 2. Das <code>ID_TOKEN</code> muss zeitlich gültig sein (Felder: <code>iat</code>, <code>exp</code>) 3. Das <code>ID_TOKEN</code> muss im Feld <code>aud</code> den jeweiligen Fachdienst eingetragen haben. 4. Falls es sich um eine pseudonyme Benutzeranmeldung handelt, muss die Kombination der Felder <code>iss</code> und <code>sub</code> auf den Benutzer zugeordnet werden. 5. Das Feld <code>nonce</code> MUSS mit der ausgelösten Authentisierungsanfrage übereinstimmen.
A_23183 Veröffentlichen der TLS Authentisierungsschlüssel	<p>Authorization-Server MÜSSEN sicherstellen, dass die für die TLS Client Authentisierung gegenüber sektoralen IDPs verwendeten Schlüssel über das Entity Statement validiert werden können, indem für diese Zertifikate im Schlüsselsatz (jwks) des Fachdienstes abgelegt werden. ("use = sig", x5c Objekt gesetzt). Nach [RFC8705-section 2.2 (https://www.rfc-editor.org/rfc/rfc8705.html#name-self-signed-certificate-mut)] ist der Authorization-Server erfolgreich authentifiziert, wenn das Zertifikat, das er während des Handshakes vorgelegt hat, mit einem der für diesen bestimmten Client registrierten Zertifikate übereinstimmt.</p>
A_23195 Entschlüsseln der ID_TOKEN	Der Fachdienst MUSS das erhaltene <code>ID_TOKEN</code> vor der Verwendung mit seinem korrespondierenden privaten Entschlüsselungskey entsprechend der "kid" in Header entschlüsseln.

[8 items found](#)

266

267

268

A_25696 - OIDC mit pushed authorization requests

269 Der TI-Messenger Service für ePA MUSS für die Registrierung eines neuen Accounts und
270 für das Login eines Akteurs in der Rolle Versicherter den OIDC authorization code flow
271 mit pushed authorization requests am sektoralen IDP unterstützen. [<=]

272 *Hinweis:* Die vom sektoralen IDP grundsätzlich unterstützten Authentifizierungsverfahren
273 sind in [gemSpec_IDP_Sek#Authentifizierungsverfahren] beschrieben.

274 **3.2.2.2 Messenger-Proxy**

275 Das Berechtigungsmanagement des Messenger-Proxy wird erweitert, um die direkte
276 Versicherten-zu-Versicherte Kommunikation zu unterbinden (siehe 5.3-
277 Berechtigungsmanagement - Unterbindung der Versicherteneinladung). Zusätzlich kann
278 der Proxy noch angepasst werden, um Pushed Authorization Requests gegenüber dem
279 Sektoralen IDP zu realisieren (siehe 5.2- Feature Identifikation und Login eines Benutzers
280).

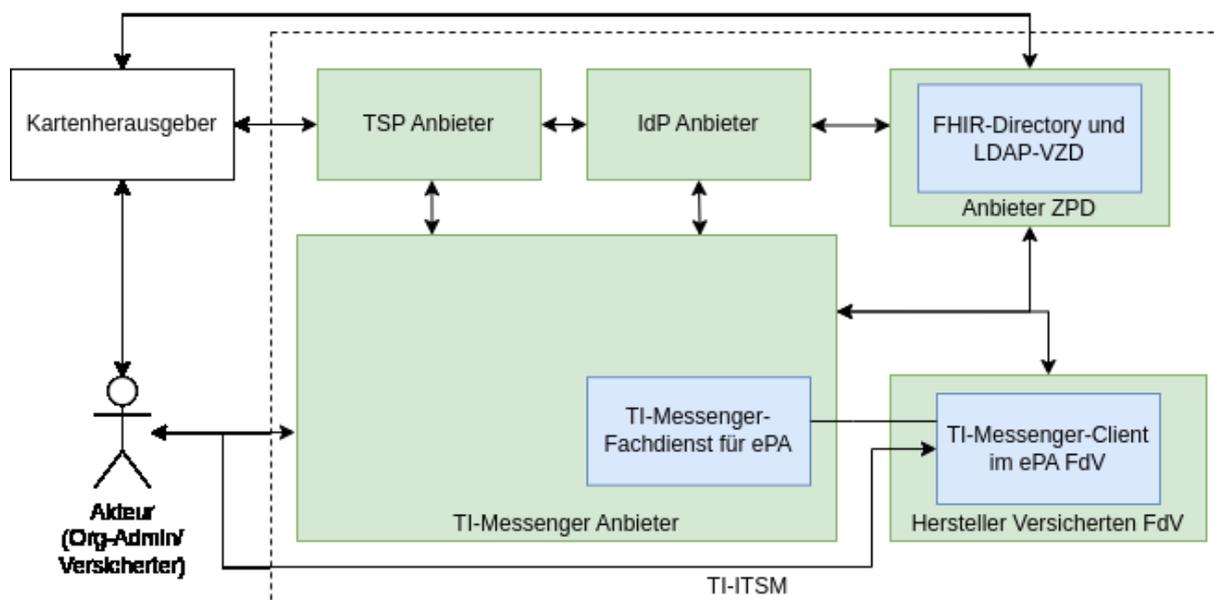
281

4 Übergreifende Festlegungen

4.1 Betrieb

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

- TI-M FD für ePA



285

286

Abbildung 4 Betriebsmodell TI-M ePA

287

Hinweis zur Abbildung:

Die Produktverantwortung für das Produkt TI-M Client ePA, welches im ePA FdV integriert ist, liegt beim Hersteller des Versicherten Frontends (siehe auch [gemKPT_Betr]).

290

291

5 Funktionsmerkmale

5.1 Einschränkung zu Anwendungsfall AF_10060 - Bereitstellung eines Messenger-Service für eine Organisation

294 Der nachfolgende Anwendungsfall beschreibt die Ergänzungen zur Einschränkung an
295 "AF_10060 - Bereitstellung eines Messenger-Service für eine Organisation".

296 **Tabelle 1: Einschränkung zu Anwendungsfall AF_10060**

AF_10060	Bereitstellung eines Messenger-Service für eine Organisation
Beschreibung / Motivation	Um den Messenger-Service für Akteure in der Rolle "Versicherter" von anderen Produkttypen differenzieren zu können, soll dieser ausschließlich nur (im Auftrag) von gesetzlichen und privaten Krankenversicherungen angelegt werden dürfen.
Vorbedingung	Ein Akteur in der Rolle "Org-Admin" hat die Organisation mit einer SM(C)-B KTR bzw. über das KIM-Verfahren mit einer professionOID für Kostenträger:1.2.276.0.76.4.59 registriert.
Ergebnis	Ein Messenger-Service für Akteure in der Rolle "Versicherter" darf ausschließlich von Kostenträgern im Gesundheitswesen (=professionOID1.2.276.0.76.4.59) instanziiert werden.

297

A_25690 - AF_10060 - Messenger-Service für ePA Bereitstellung nur für Kostenträger

300 Ein Messenger Service für ePA MUSS nur von Kostenträgern im Gesundheitswesen
301 (=professionOID 1.2.276.0.76.4.59) bereitgestellt werden können.[<=]

5.2 Feature Identifikation und Login eines Benutzers

303 Versicherte erhalten von ihrer Krankenkasse eine App, die es ihnen ermöglicht, den TI-
304 Messenger innerhalb des ePA FdV zu nutzen. Die Krankenkasse stellt den Versicherten
305 Identifizierungsmöglichkeiten gemäß [gemSpec_IDP_Sek#Identifizierung und
306 Authentifizierung des Nutzers] und einen IDP bereit, der es ermöglicht, die Versicherten
307 der Krankenkasse zu authentifizieren und Identitätsinformationen der Versicherten in den
308 Diensten der TI (wie hier am TI-Messenger Service) zu nutzen.

5.2.1 Anwendungsfall

AF_10234 - Identifikation und Login eines Benutzers

310 Damit Versicherte die Messenger-Funktion der ePA-App ihrer Krankenkasse nutzen
311 können, müssen sich diese am IDP ihrer Krankenkasse identifizieren und erhalten damit
312 Zugang zu deren TI-Messenger Service. Die Authentifizierung von Versicherten für die
313

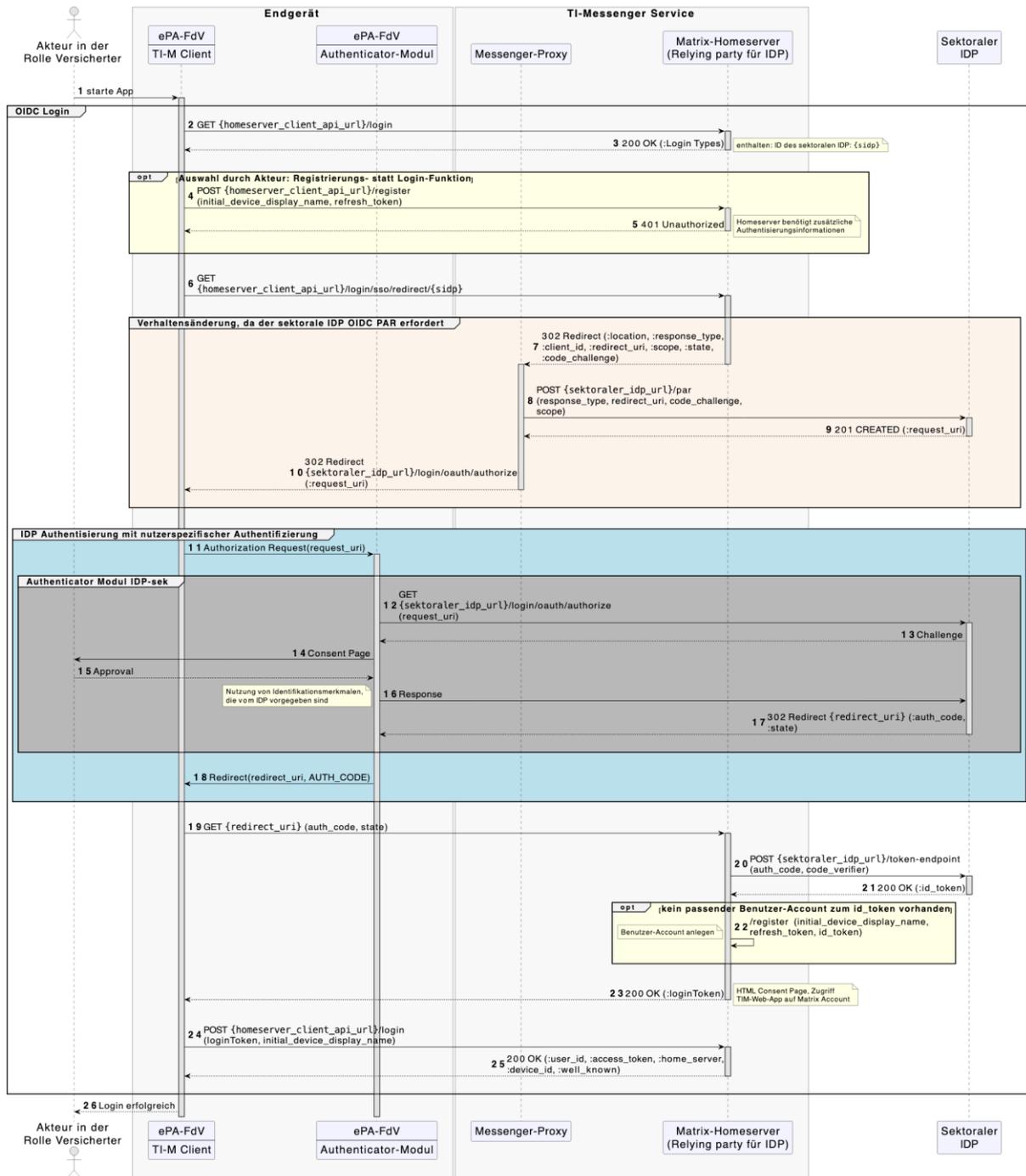
314 Registrierung von TI-Messenger Accounts und für das Login am Homeserver erfolgt am
315 sektoralen IDP mittels OIDC.

316 **Tabelle 2: AF - Identifikation und Login eines Benutzers**

Attribute	Bemerkung
Akteur	Versicherter, welcher gleichzeitig auch das ePA-FdV benutzt.
Auslöser	Der Akteur benutzt die Login- oder Registrierungs-Funktion seines TI-M Clients
Komponenten	<ul style="list-style-type: none"> • TI-M Client im ePA-FdV • Messenger-Proxy • Matrix-Homeserver (als Relying Party des sektoralen IDP) • Sektoraler IDP
Eingangsdaten	Login-Call am aufgerufenen Client des Akteurs
Ergebnis	<ol style="list-style-type: none"> 1. Der Akteur erhält einen nutzbaren Zugang zum TI-Messenger Service seiner Krankenkasse (bei Nutzung der Registrierungsfunktion). 2. Akteur ist mit seinem Client am Matrix Homeserver eingeloggt und kann anschließend über diesen kommunizieren.
Ausgangsdaten	<ul style="list-style-type: none"> • Neuer Nutzeraccount auf dem Homeserver (bei Nutzung der Registrierungsfunktion) • aktive User-Session im TI-M Client unter Benutzung eines gültigen access token
Diagrammvariablen	<ul style="list-style-type: none"> • {homeserver_client_api_url}: Hostname des Matrix-Homeserver, z.B. https://myprovider.homeserver-tim.de, zzgl. Basispfad zum gültigen Client-API <code>/_matrix/client/v3</code> • {sidp}: ID des sektoralen IDPs, die vom Homeserver beauskunftet wird • {sektoraler_idp_url}: Der am Homeserver konfigurierte FQDN des sektoralen IDP als OIDC IDP • {redirect_uri}: Die vollständige Callback-Adresse für den OIDC Flow • {client_url}: URL der TI-M Clients

317
318
319
320
321
322
323
324

Die Laufzeitsicht zeigt sowohl die Registrierung eines Benutzer-Accounts als auch den Login eines Akteurs am Homeserver des TI-Messengers Service. Die in der Box "Verhaltensänderung, ..." dargestellte Änderung betrifft notwendige Anpassungen am Messenger-Proxy, um damit Redirects vom Homeserver aufzufangen, auszuwerten und anhand der Auswertung über einen entsprechende Endpoint am sektoralen IDP einen PAR (ein Pushed Authorization Request) nach dessen Vorgaben zu erstellen.



325
326
327

Abbildung 5 : Laufzeitsicht - Identifikation und Login eines Benutzers

[<=]

328 Die in diesem Anwendungsfall beschriebene Laufzeitsicht kann beispielhaft mit konkreten
329 Übergabe- und Rückgabewerten anhand von [OIDC Login] nachvollzogen werden.

330 **A_25706 - AF_10234 - Erzeugung der MXID (Bei Registrierung)**

331 Der TI-M FD ePA MUSS im Fall der Registrierung die MXID für die Accounts von Akteuren
332 in der Rolle Versicherter nach folgender Bildungsregel erzeugen: @<pseudonymisierte
333 KVNR>:<Matrix-Domain der Krankenkasse für Versicherte>. Die KVNR zur
334 Verarbeitung durch die Pseudonymisierungsfunktion entnimmt der Matrix-Homeserver
335 aus dem id_token, das vom sektoralen IDP ausgestellt wurde (claim
336 urn:telematik:claims:id).[<=]

337 **A_25714 - AF_10234 - Pseudonymisierung der KVNR**

338 Die Pseudonymisierung der KVNR zur Verwendung als Local-Part bei Bildung der MXID
339 für Versicherte MUSS mittels SHA-384 erfolgen.[<=]

340 **A_25715 - AF_10234 - Form der SHA-384-Prüfsumme**

341 Die SHA-384-Prüfsumme der KVNR, welche als localpart der MXID für Versicherte
342 fungiert, MUSS in ihrer hexadezimalen Darstellung verwendet werden, sodass sich eine
343 96-stellige Zeichenkette für den localpart ergibt. Gemäß der Matrix-Spezifikation zur
344 Bildung von MXIDs (<https://spec.matrix.org/v1.3/appendices/#user-identifiers>), sind
345 die bei hexadezimaler Darstellung zulässigen Buchstaben [a-f] klein zu schreiben.[<=]

346 **A_25707 - AF_10234 - Erzeugung des Display Name**

347 Der TI-M FD ePA SOLL im Fall der Registrierung den Display Name für die Accounts der
348 Akteure in der Rolle Versicherter aus dem id_token vom sektoralen IDP übernehmen
349 (claim urn:telematik:claims:display_name).[<=]

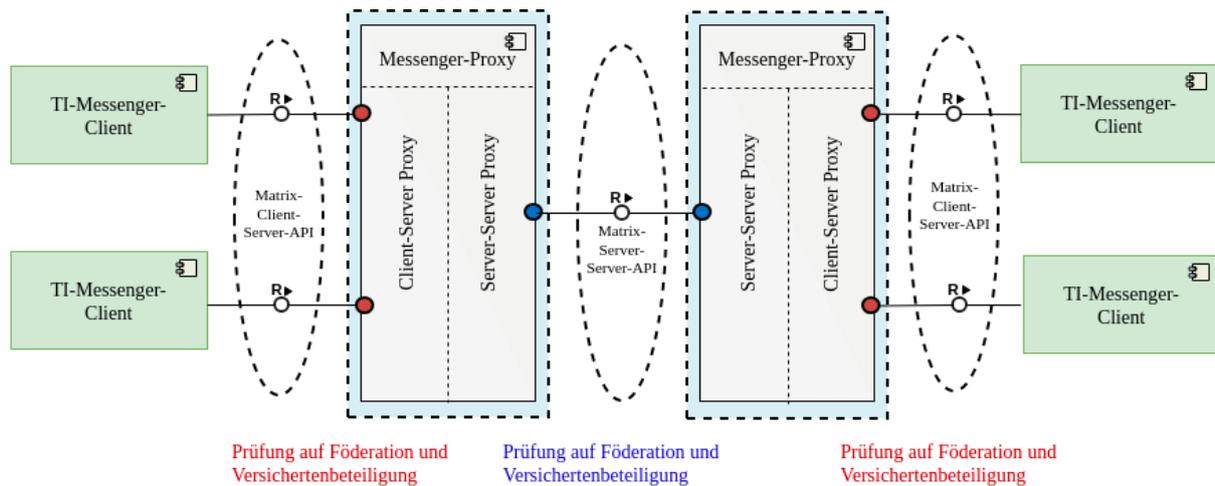
350 **A_25712 - AF_10234 - TI-M Rohdatenerfassung und -lieferung**

351 Die Rohdaten wurden entsprechend der Rohdatendefinition für den TI-M FD ePA
352 erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung
353 versendet.[<=]

354 **5.3 Berechtigungsmanagement - Unterbindung der** 355 **Versicherteneinladung**

356 Der TI-M FD ePA soll verhindern, dass ein Versicherter einen anderen Versicherten
357 einladen kann. Sofern ein Akteur, der nicht Versicherter ist, den Chat angelegt hat und
358 mehr als einen Versicherten eingeladen hat, können die Versicherten auch über diesen
359 Gruppenchat Nachrichten austauschen. Die folgende Grafik zeigt, welche Komponenten
360 der Fachdienste, die zusätzliche Prüflöge übernehmen müssen. Die Versichertenprüfung
361 soll an der Matrix-Client-Server-API durchgeführt werden sowie zur weiteren Absicherung
362 ebenfalls an der Matrix-Server-Server-API zwischen den TI-M FD.

363



364

365

Abbildung 6: Prüfung auf Versichertenbeteiligung

366 Die Anpassungen an der Prüflogik des Messenger-Proxy werden in den folgenden Kapiteln
 367 näher erläutert.

368 5.3.1 Client-Server Prüfungen

369 In der Funktion als Client-Server Proxy prüft der Messenger-Proxy, wie in der TI-M Basis
 370 beschrieben, eingehende Invite- Events der TI-M Clients (in der Abbildung 6 rot
 371 dargestellt) und fungiert so als Reverse-Proxy. Für den TI-M ePA muss der Messenger-
 372 Proxy zusätzlich zur in der TI-M Basis geforderten Föderationszugehörigkeit die
 373 Versicherteneinladung nach [ML-150398 - AF 10233 Versicherteneinladung unterbinden](#)
 374 verhindern.

375 5.3.2 Server-Server Prüfungen

376

377 In der Funktion als Server-Server Proxy prüft der Messenger-Proxy, wie in der TI-M Basis
 378 beschrieben, alle ausgehenden sowie eingehenden Events auf Föderationszugehörigkeit.
 379 Für den TI-M ePA muss die Prüfung zusätzlich die Versicherteneinladung nach [ML-
 380 150398 - AF 10233 Versicherteneinladung unterbinden](#) verhindern.

381 AF_10233 - AF_10233 Versicherteneinladung unterbinden

382 Dieser Anwendungsfall erweitert die in der TI-M Basis definierte Prüflogik für den
 383 Messenger-Proxy, neben der Föderationsprüfung ist zusätzlich zu prüfen, dass der
 384 Einladende und der Eingeladene nicht der Gruppe Versicherte zuzuordnen sind. Für die
 385 Prüfung der Zugehörigkeit verwendet der Messenger-Proxy die Information `isInsurance`
 386 aus der Föderationsliste.

387 **Tabelle 3: AF - Versicherteneinladung unterbinden**

Attribute	Bemerkung
Auslöser	Anfrage am Messenger Proxy

Attribute	Bemerkung
Komponenten	Messenger-Proxy
Vorbedingung	<p>Szenario 1: Beide Kommunikationspartner haben einen Benutzeraccount mit einer Domain, welche in der Föderationsliste als "isInsurance" gekennzeichnet wurde (Kennzeichen für eine Versichertendomain).</p> <p>Szenario 2: Mind. einer der Kommunikationspartner hat einen Benutzeraccount mit einer Domain, welche in der Föderationsliste NICHT als "isInsurance" gekennzeichnet wurde.</p>
Eingangsdaten	Matrix Invite Event
Ergebnis	<p>Szenario 1: Ablehnung der Einladung, wenn der Sender und der Empfänger beides Akteure in der Rolle Versicherter sind.</p> <p>Szenario 2: Weiterleitung der Einladung, wenn der Sender oder der Empfänger kein Akteur in der Rolle Versicherter ist.</p>

388



389

390

Abbildung 7: Versicherteneinladung unterbinden

391 [<=]

392 **A_25705 - AF_10233 - Versicherteneinladung unterbinden**

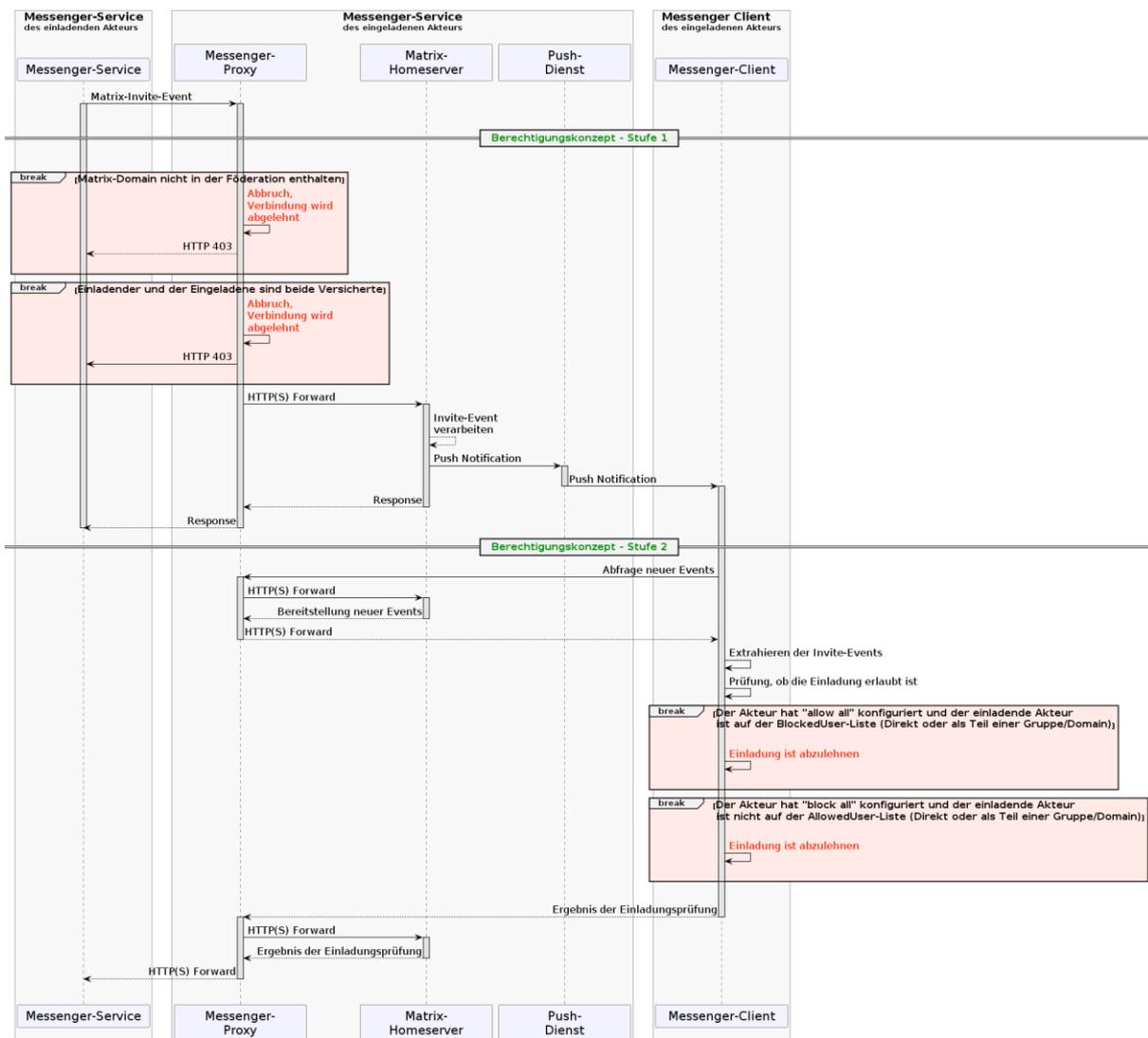
393 Der Messenger-Proxy des TI-M FD ePA MUSS im Rahmen der Client-Server Prüfungen
 394 Anfragen auf Invite-Events prüfen. Sind der Sender und der Empfänger beide Akteure in
 395 der Rolle Versicherter dann MUSS die Einladung vom TI-Messenger-Proxy abgelehnt
 396 werden. Ein Akteur ist als Versicherter zu identifizieren, wenn die Domain seiner MXID
 397 über den Wert "true" im Feld "isInsurance" innerhalb der Föderationsliste verfügt. [<=]

398 **A_25704 - AF_10233 - Versicherteneinladung erlauben**
 399 Der Messenger-Proxy des TI-M FD ePA MUSS im Rahmen der Server-Server Prüfungen
 400 Anfragen auf Invite-Events prüfen. Ist der Sender oder der Empfänger KEIN Akteur in der
 401 Rolle Versicherter, dann MUSS die Einladung vom TI-Messenger-Proxy weitergeleitet
 402 werden. Ein Akteur ist als Versicherter zu identifizieren, wenn die Domain seiner MXID
 403 über den Wert "true" im Feld "isInsurance" innerhalb der Föderationsliste verfügt. [<=]

404 **A_25713 - AF_10233 - TI-M Rohdatenerfassung und -lieferung**
 405 Die Rohdaten wurden entsprechend der Rohdatendefinition für den TI-M FD ePA
 406 erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung
 407 versendet. [<=]

408 5.3.3 Berechtigungsprüfung

409 Die folgende Grafik zeigt in der Zusammenfassung die für den TI-M ePA anzuwendenden
 410 Prüfregeln, am Beispiel der Verarbeitung eines Invite Events auf Seiten des Messenger-
 411 Service des eingeladenen Akteurs.



412

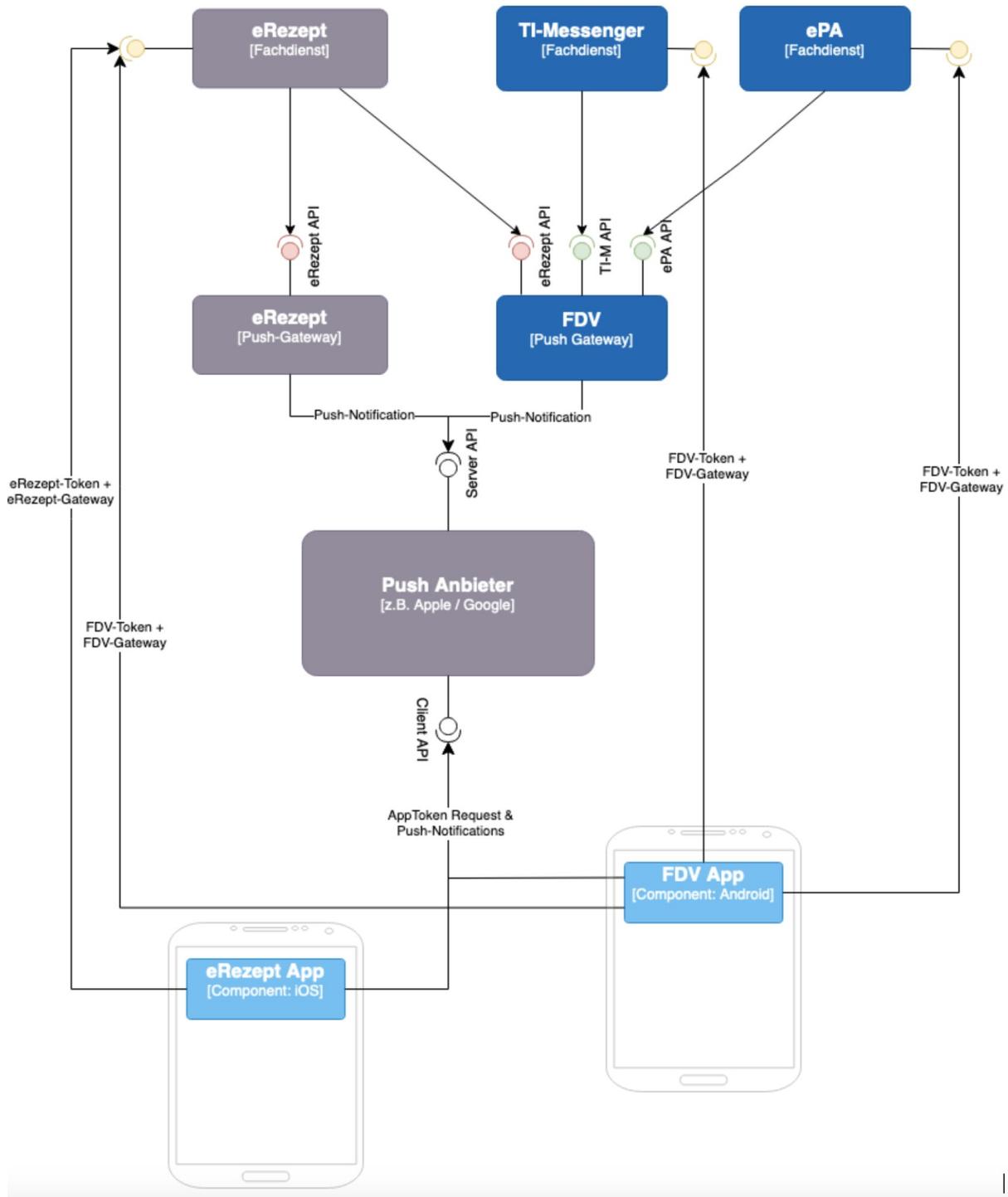
413

Abbildung 8: Berechtigungsprüfung TI-M_ePA

414 **5.4 Push-Benachrichtigung im FDV**

415 Eine besondere Herausforderung beim FDV besteht darin, dass eine App (das FDV) die
416 Client-Logik zur Kommunikation mit drei unterschiedlichen Fachdiensten (ePA, E-Rezept,
417 TI-M) sicherstellen muss. Um die Flexibilität hinsichtlich multipler Fachdienste und
418 unterschiedlicher Clients sicherzustellen, muss das Push-Gateway für andere Fachdienste
419 entsprechend separate Endpunkte zur Verfügung zu stellen, deren Ausgestaltung über
420 die kommenden Spezifikationsreleases zum ePA-FDV oder dem E-Rezept im ePA-FDV
421 erfolgen wird.

422 Die nachfolgende Grafik illustriert exemplarisch das zukünftige Szenario. Hier existiert
423 bereits ein E-Rezept-Fachdienst, der über ein Push-Gateway die Push-Dienste von Google
424 und Apple angebunden hat, um die E-Rezept-App sowohl unter Android als auch unter
425 iOS mit Push-Benachrichtigungen zu versorgen. In diesem Szenario möchte eine Beispiel-
426 Krankenkasse dem Versicherten eine App ("FDV App") zur Verfügung stellen, die Push-
427 Benachrichtigungen der integrierten Fachdienste ePA, E-Rezept und TI-Messenger
428 verarbeiten kann. Hierzu ist es notwendig, den bereits existierenden E-Rezept-Fachdienst
429 anzubinden sowie auf Seiten des Versicherten (in der "FDV App") die Benachrichtigungen
430 technisch von einander zu trennen.



431
432

Abbildung 9: Push-Gateway

433 Wie die Abbildung zeigt, stellt die Beispiel-Krankenkasse ein Push-Gateway für ihre FdV-
 434 App zur Verfügung und registriert die App beim Push-Anbieter. Durch die Registrierung
 435 erhält die App vom Anbieter ein Token, über welches die Anwendung beim Senden von
 436 Push-Benachrichtigungen eindeutig identifiziert werden kann. Dieses Token und die
 437 Information, welches Gateway zu verwenden ist, stellt die App den von ihr genutzten
 438 Fachdiensten zur Verfügung. Dazu ist es notwendig, dass die in der Grafik gelb
 439 markierten Schnittstellen öffentlich verfügbar und für beliebige Clients nutzbar sein

440 müssen. Die Schnittstellen erlauben einem Client dem Fachdienst das zu nutzende Push-
441 Gateway und den zu verwendenden Provider zu definieren. Zusätzlich muss der Client
442 über die Schnittstelle den Token bereitstellen können, über den die App vom Push-
443 Provider eindeutig zu identifizieren ist (Bsp.: [Client-Server
444 API]/#post_matrixclientv3pushersset). Ebenfalls müssen die Schnittstellen der
445 Fachdienste zu den Gateways öffentlich einsehbar sein, damit die gematiker
446 Krankenkasse an ihrem Push-Gateway eine Schnittstelle bereitstellen kann, die vom E-
447 Rezept-Fachdienst auch verstanden wird (Bsp.: [Push Gateway
448 API]/#post_matrixpushv1notify). Die beiden deckungsgleichen Schnittstellen sind rot
449 markiert. Die grün markierten Schnittstellen am Push Gateway der gematiker
450 Krankenkasse werden im Beispielszenario nicht von anderen Apps genutzt, Müssen
451 jedoch auch öffentlich verfügbar sein, damit andere App-Entwickler für ihre
452 Anwendungen ein Push-Gateway mit identischen Schnittstellen bereitstellen können. Das
453 vorgestellte Szenario hat den Vorteil, dass die Push-Anbieter spezifischen Credentials
454 beim Push-Gateway des App-Anbieters verbleiben können und dass es dem App Anbieter
455 überlassen ist zu entscheiden, wie er die Trennung der Inhalte übernimmt. Z.B. kann die
456 gematiker Krankenkasse selbst in der Logik ihres Gateways entscheiden, ob sie in den
457 Inhalt der Benachrichtigung einen Indikator aufnimmt, welcher Fachdienst die
458 Benachrichtigung gesendet hat oder z.B. bei Nutzung von FCM diese Unterscheidung über
459 eigene Topics für die verschiedenen Fachdienste realisiert.

460 **6 Anhang A – Verzeichnisse**

461 **6.1 Abkürzungen**

462 **Tabelle 4: Im Dokument verwendete Abkürzungen**

Kürzel	Erläuterung

463 **6.2 Glossar**

464 **Tabelle 5: Im Dokument verwendete Begriffe**

Begriff	Erläuterung

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

467 **6.3 Abbildungsverzeichnis**

468 |Abbildung 1: Kontextabgrenzung 7
 469 |Abbildung 2: TI-M Client ePa Komponentendiagramm 9
 470 |Abbildung 3: TI-Messenger-Service Komponentendiagramm11
 471 |Abbildung 4 Betriebsmodell TI-M ePA15
 472 |Abbildung 5 : Laufzeitsicht - Identifikation und Login eines Benutzers18
 473 |Abbildung 6: Prüfung auf Versichertenbeteiligung20
 474 |Abbildung 7: Versicherteneinladung unterbinden21
 475 |Abbildung 8: Berechtigungsprüfung TI-M_ePA.....22
 476 |Abbildung 9: Push-Gateway24
 477 |

478 **6.4 Tabellenverzeichnis**

479 [Tabelle 1: Einschränkung zu Anwendungsfall AF_1006016
 480 Tabelle 2: AF - Identifikation und Login eines Benutzers17
 481 Tabelle 3: AF - Versicherteneinladung unterbinden20
 482 Tabelle 4: Im Dokument verwendete Abkürzungen26
 483 Tabelle 5: Im Dokument verwendete Begriffe26
 484 Tabelle 6: Referenzierte Dokumente der gematik27
 485 Tabelle 7: Weitere Dokumente28
 486 |

487 **6.5 Referenzierte Dokumente**

488 **6.5.1 Dokumente der gematik**

489 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument
 490 referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der
 491 vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und
 492 Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und
 493 Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht
 494 aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der
 495 aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die
 496 vorliegende Version aufgeführt wird.

497 **Tabelle 6: Referenzierte Dokumente der gematik**

[Quelle]	Herausgeber: Titel
[gemAnbT_IDP-Sek_KTR_ATV]	Anbietertypsteckbrief Prüfvorschrift Anbieter Sektoraler Identity Provider für den Sektor Kostenträger
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar
[gemSpec_IDP_Frontend]	gematik: Spezifikation Identity Provider - Frontend
[gemSpec_IDP_Sek]	gematik: Spezifikation Sektoraler Identity Provider
[gemSpec_TI-M_Basis]	gematik: Spezifikation TI-Messenger (Basis)
[OIDC Login]	Detaildarstellung OIDC Registrierung und Login https://github.com/gematik/api-ti-messenger/blob/tim-epa-fdv/images/diagrams/TI-M_ePA/TI-Messenger_OIDC_Login.png

498 **6.5.2 Weitere Dokumente**499 **Tabelle 7: Weitere Dokumente**

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[Client-Server API]	Matrix Foundation: Matrix Specification - Client-Server API https://spec.matrix.org/v1.3/client-server-api/
[Push Gateway API]	Matrix Foundation: Matrix Specification - Push Gateway API https://spec.matrix.org/v1.3/push-gateway-api/
[Server-Server API]	Matrix Foundation: Matrix Specification - Server-Server API https://spec.matrix.org/v1.3/server-server-api/

500

501