

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation TI-Messenger ePA

Version: 1.2.0 CC
Revision: 1394632
Stand: 14.10.2025
Status: zur Abstimmung
freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemSpec_TI-M_ePA

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	13.06.202 4		initiale Erstellung	gematik
1.1.0	13.11.202 4		Einarbeitung Matrix-Update V1.11	gematik
1.1.1	09.12.202 4		Update TI-Messenger_24_3-1	gematik
1.1.2	12.03.202 5		Einarbeitung Patch TI-Messenger_25_1- 1	gematik
1.2.0 CC	14.10.202 5		Einarbeitung TI-Messenger_25_3 - zur Abstimmung freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes.....	5
1.1 Zielsetzung.....	5
1.2 Zielgruppe.....	5
1.3 Geltungsbereich.....	5
1.4 Abgrenzungen.....	5
1.5 Methodik.....	6
2 Systemüberblick.....	7
2.1 Akteure und Rollen.....	7
2.1.1 Rolle: "Versicherter"	7
2.2 Nachbarsysteme.....	7
2.2.1 Authentifizierungs-Dienst für Akteure in der Rolle "Versicherter"	8
2.2.2 VZD-FHIR-Directory	8
3 Zerlegung des Produkttyps (Systemkomponenten).....	9
3.1 TI-M Client ePA.....	9
3.1.1 VZD-FHIR-Directory	10
3.1.2 Auth Modul.....	10
3.1.3 Weitere Ergänzungen/Einschränkungen zur Matrix-Spezifikation.....	10
3.2 TI-M FD ePA.....	11
3.2.1 Registrierungs-Dienst.....	11
3.2.2 Messenger-Service.....	12
3.2.2.1 Schnittstelle für Authentifizierungsverfahren.....	12
3.2.2.2 Messenger-Proxy.....	12
3.2.2.3 Ergänzungen zur Matrix-Spezifikation.....	12
4 Übergreifende Festlegungen.....	14
4.1 Betrieb.....	14
5 Funktionsmerkmale.....	15
5.1 Einschränkung zu Anwendungsfall AF_10060 - Bereitstellung eines Messenger-Service für eine Organisation.....	15
5.2 Feature Identifikation und Login eines Benutzers.....	15
5.2.1 Anwendungsfall.....	16
5.3 Berechtigungsmanagement - Anpassungen.....	19
5.3.1 Unterbindung der Versicherteneinladung.....	19
5.3.1.1 Client-Server Prüfungen.....	19
5.3.1.2 Server-Server Prüfungen.....	20
5.3.1.3 Berechtigungsprüfung.....	21
5.3.2 Weitere Anpassungen.....	22
5.4 Löschen von Inhalten - Anpassungen.....	23
5.4.1 Serverseitiges Löschen.....	23

5.4.1.1 Matrix-Events.....	23
6 Anhang A - Verzeichnisse.....	24
6.1 Abkürzungen.....	24
6.2 Glossar.....	24
6.3 Abbildungsverzeichnis.....	24
6.4 Tabellenverzeichnis.....	25
6.5 Referenzierte Dokumente.....	25
6.5.1 Dokumente der gematik.....	25
6.5.2 Weitere Dokumente.....	26

1 Einordnung des Dokumentes

1.1 Zielsetzung

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

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller von Frontends für Versicherte (FdV) mit integriertem TI-M Client ePA, an Hersteller von TI-M FD ePA und an Anbieter, welche die beschriebenen Produkttypen betreiben.

1.3 Geltungsbereich

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

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzungen

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

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

1.5 Methodik

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

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

Anwendungsfälle und Anforderungen werden im Dokument wie folgt dargestellt:

<AF-ID> - <Titel des Anwendungsfalles>

Text / Beschreibung

[<=]

bzw.

<AFO-ID> - <Titel der Afo>

Text / Beschreibung

[<=]

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

2 Systemüberblick

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

2.1 Akteure und Rollen

Mit dieser Spezifikation werden die Versicherten als Akteure in die TI-Messenger Föderation eingebunden. Versicherte können zukünftig über einen TI-Messenger Client im Frontend des Versicherten der ePA (TI-M Client ePA) sicher und schnell Inhalte austauschen.

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

2.1.1 Rolle: "Versicherter"

Der TI-M ePA führt die Rolle "Versicherter" ein. Versicherten stehen die gleichen Funktionalitäten zur Verfügung wie einem Akteur in der Rolle "User" der Spezifikation [gemSpec_TI-M_Basis]. Diese Funktionalitäten können durch die Inhalte dieser Spezifikation erweitert oder eingeschränkt werden.

2.2 Nachbarsysteme

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

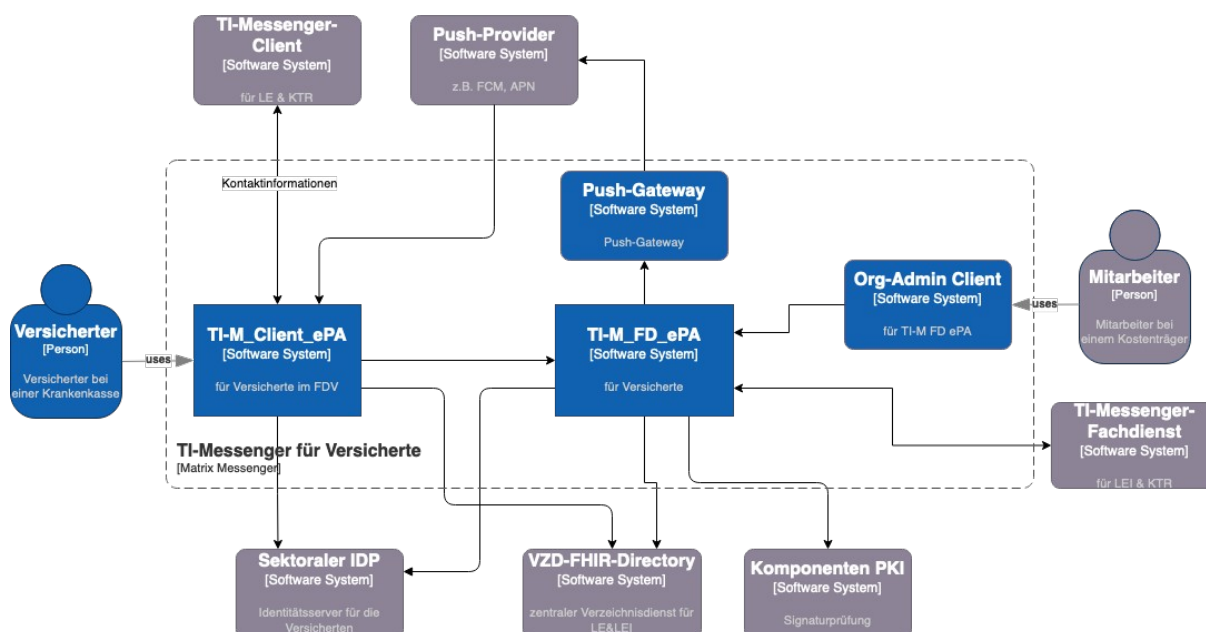


Abbildung 1: Kontextabgrenzung

Der TI-M Client ePA hat Schnittstellen

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

Der TI-M FD ePA hat Schnittstellen

- zum TI-M Client ePA für Versicherte,
- zum Org-Admin Client des Kostenträgers (KTR) zur Verwaltung der Akteure,
- zum sektoralen IDP. Es werden die gleichen Verfahren wie beim ePA FdV mit Single-Sign-On verwendet, wenn vorhanden (siehe [gemSpec_IDP_Sek]),
- zum FHIR-Verzeichnisdienst zur Pflege und zum Bezug der Föderationsliste,
- zur Komponenten PKI für die Erzeugung und Prüfung von Zertifikaten aus dem Vertrauensraum der TI,
- zu anderen TI-M FD, um innerhalb der TI-Messenger Föderation die Kommunikation mit Nutzern anderer TI-M FD zu ermöglichen und
- zum Push Gateway, um Benachrichtigungen für Nutzer zu versenden.

2.2.1 Authentifizierungs-Dienst für Akteure in der Rolle "Versicherter"

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

A_25488 -IDP-Sek_KTR

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

2.2.2 VZD-FHIR-Directory

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

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

3 Zerlegung des Produkttyps (Systemkomponenten)

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

3.1 TI-M Client ePA

Die folgende Grafik zeigt die Komponenten eines TI-M Clients ePA. Farblich hervorgehoben sind diejenigen Komponenten gegenüber der Basisspezifikation [gemSpec_TI-M_Basis], die im Rahmen der in dieser Spezifikation vorgestellten Features angepasst werden müssen (blau) und Komponenten, die neu hinzugekommen sind (grün).

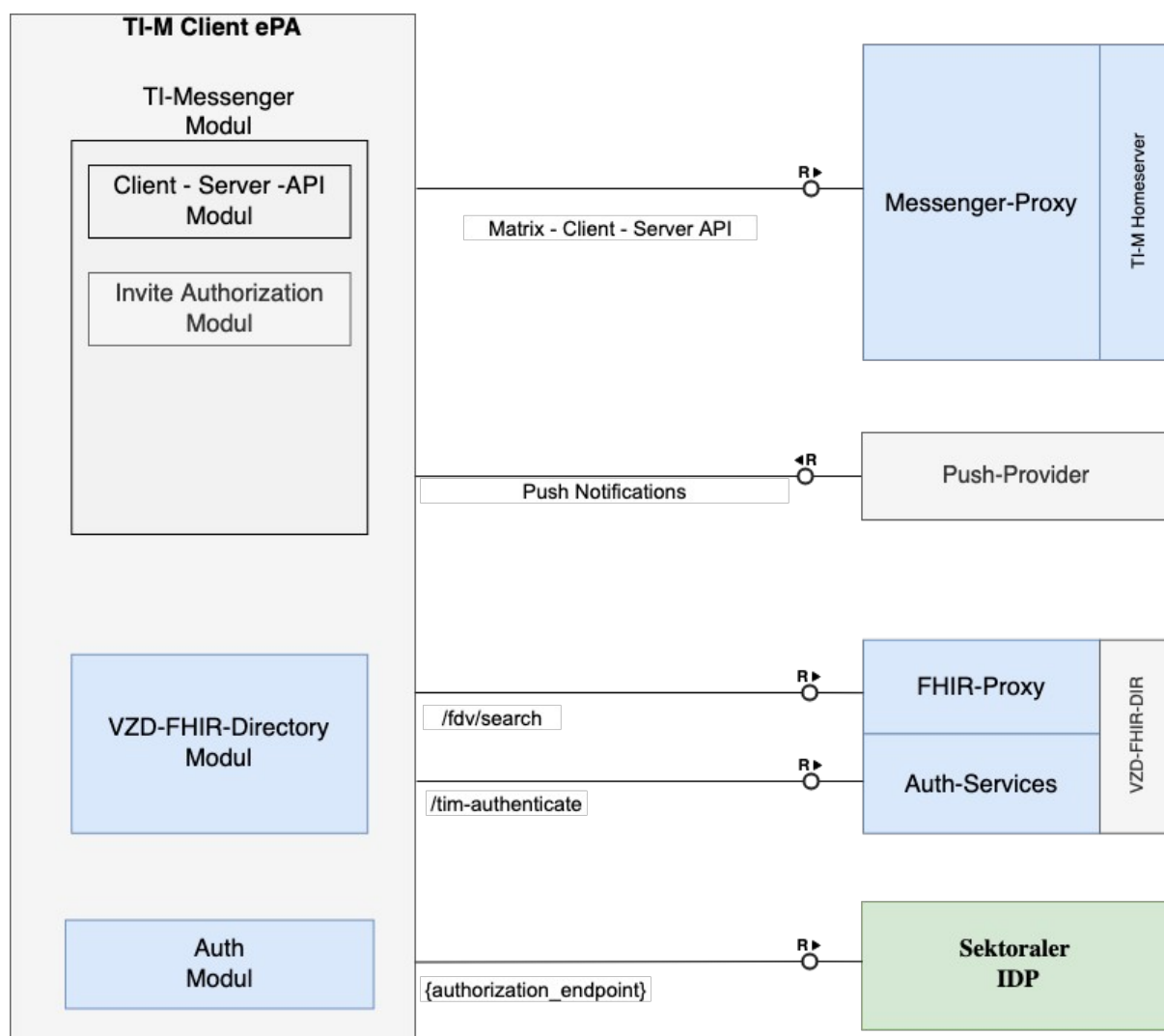


Abbildung 2: TI-M Client ePA Komponentendiagramm

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

A_26382 -Auftrennung separater Benutzeroberflächen in Module

Die TI-M Clients ePA MÜSSEN die Benutzeroberflächen und damit verbundenen Funktionalitäten derart modularisieren, dass der Client für Akteure in der Rolle "Versicherter" und der Org-Admin-Client unabhängig voneinander ausgeliefert und betrieben werden können.[<=]

A_26383-01 -Keine Administrationsfunktion für Akteure in der Rolle "Versicherter"

Anbieter von TI-M Clients ePA MÜSSEN sicherstellen, dass an Akteure in der Rolle "Versicherter" kein TI-M Client ePA mit Administrationfunktionalität für andere als das eigene Nutzerkonto ausgeliefert wird.[<=]

A_27055 -Maximales Inaktivitätsintervall bis zur Sperre des TI-M Clients

Das maximale Inaktivitätsintervall bis zur automatischen Sperre des TI-M Clients DARF NICHT größer sein als die maximale Dauer gemäß A_26512-*. [<=]

3.1.1 VZD-FHIR-Directory

A_25681-01 -VZD-FHIR-Directory Suche

Der TI-M Client ePA MUSS für die Suche im VZD-FHIR-Directory die Schnittstelle/fdv/search verwenden.[<=]

3.1.2 Auth Modul

Für die Interaktion mit dem sektoralen IDP wird auf Clientseite ein Authenticator-Modul bereitgestellt, dessen Anforderungen in [gemSpec_IDP_Sek] definiert sind. Für den TI-M Client ePA sind die Anforderungen an Clients aus der Spezifikation Identity Provider - Frontend ([gemSpec_IDP_Frontend] zu beachten und werden im Produktypsteckbrief aufgeführt.

3.1.3 Weitere Ergänzungen/Einschränkungen zur Matrix-Spezifikation

A_26015-01 -Unterbindung öffentlicher Räume (Client)

Der TI-M Client ePA DARF dem Akteur sowohl im Rahmen der Raumerzeugung als auch bei bestehenden Räumen NICHT erlauben eine oder mehrere der folgenden Einstellungen auszuwählen:

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

[<=]

3.2 TI-M FD ePA

Die folgende Grafik visualisiert die Komponenten eines TI-M FD ePA auf Serverseite, die im Rahmen der in diesem Dokument beschriebenen Features hinzukommen oder angepasst werden müssen. Farblich hervorgehoben sind diejenigen Komponenten gegenüber der Basisspezifikation [gemSpec_TI-M_Basis], die im Rahmen der in dieser Spezifikation vorgestellten Features angepasst werden müssen (blau) und Komponenten, die neu hinzugekommen sind (grün).

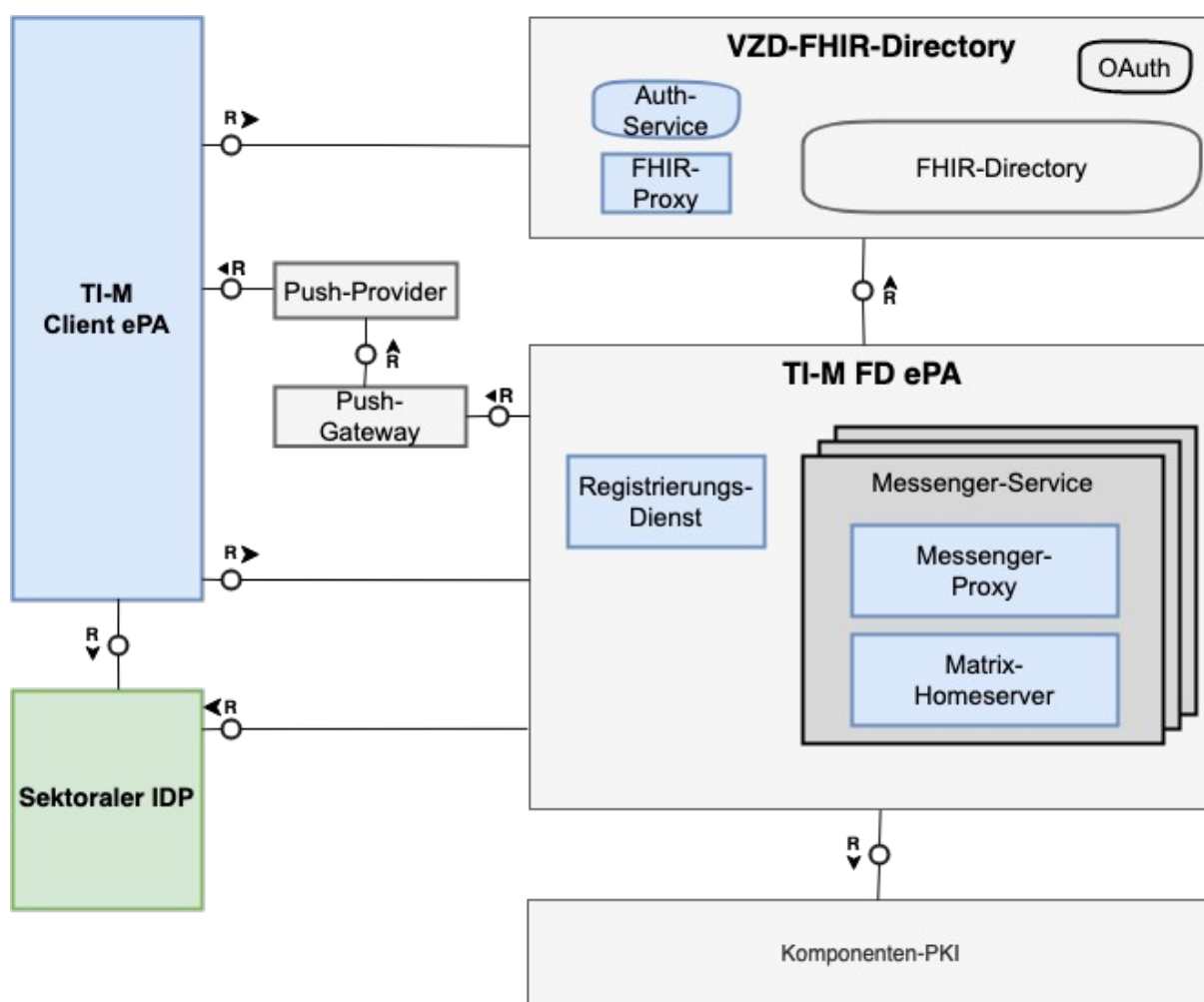


Abbildung 3: TI-Messenger-Service Komponentendiagramm

3.2.1 Registrierungs-Dienst

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

3.2.2 Messenger-Service

3.2.2.1 Schnittstelle für Authentifizierungsverfahren

Der Messenger-Service muss für die Authentifizierung der Akteure in der Rolle "Versicherter" an den sektoralen IDP angeschlossen werden. Anschließend können Inhalte des vom sektoralen IDP ausgestellten ID_TOKEN bei der Account Anlage verwendet werden (siehe [ML-150294 – Missing cross-reference](#) & [5.2.1-3- AF_10234 - Erzeugung des Display Name](#)). Für den TI-M FD ePA sind damit die Fachdienstanforderungen aus der Spezifikation Identity Provider – Nutzungsspezifikation für Fachdienste ([gemSpec_IDP_FD]) entsprechend bindend und im Produktpsteckbrief aufgeführt.

A_25696 -OIDC mit pushed authorization requests

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

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

3.2.2.2 Messenger-Proxy

Das Berechtigungsmanagement des Messenger-Proxy wird erweitert, um die direkte Versicherten-zu-Versicherte Kommunikation zu unterbinden (siehe [5.3- Berechtigungsmanagement - Anpassungen](#)). Zusätzlich kann der Proxy noch angepasst werden, um Pushed Authorization Requests gegenüber dem Sektoralen IDP zu realisieren (siehe [5.2- Feature Identifikation und Login eines Benutzers](#)).

3.2.2.3 Ergänzungen zur Matrix-Spezifikation

A_25996-01 -Unterbindung öffentlicher Räume (Fachdienst)

Der TI-M Fachdienst ePA MUSS Anfragen an den Endpunkten /createRoom und /rooms/{roomId}/state/{eventType}/{stateKey} mit HTTP 400 und M_INVALID_ROOM_STATE ablehnen wenn im resultierenden Raum eine oder mehrere der folgenden Einstellungen zutreffen würden:

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

[\leq]

Die Basisspezifikation [gemSpec_TI-M_Basis] garantiert die Möglichkeit von Profil- und Suchabfragen für den Fall, dass Nutzer gemeinsame Räume haben, trifft jedoch keine Aussage über das Verhalten in anderen Fällen. Während es z. B. sinnvoll sein kann, das Profil eines Leistungserbringers auch ohne gemeinsame Räume einzusehen, muss diese Möglichkeit für Versicherte grundsätzlich unterbunden werden. Da die MXID von Versicherten aus der KVNR gebildet wird, wäre es sonst mit einfachen Mitteln möglich, eine Zuordnung von KVNRs zu Displaynamen, Avatars oder anderen sensiblen Profilinformationen zu erstellen. Des Weiteren gibt es für Versicherte generell keinen sinnvollen Grund, andere Nutzer am Homeserver zu suchen. Die entsprechenden Endpunkte werden daher im Folgenden eingeschränkt.

A_26290 -Verbot von Profilabfragen ohne gemeinsame Räume

Der TI-M Fachdienst ePA MUSS Requests zu den folgenden Endpunkten mit einer HTTP 403 Response ablehnen, sofern der anfragende Nutzer keine gemeinsamen Räume mit dem angefragten Nutzer hat:

- GET `/_matrix/client/v3/profile/{userId}`
- GET `/_matrix/client/v3/profile/{userId}/avatar_url`
- GET `/_matrix/client/v3/profile/{userId}/displayname`

[<=]

A_26375 -Verbot von Suchabfragen

Der TI-M Fachdienst ePA MUSS am Endpunkt `/_matrix/client/v3/user_directory/search` die Auslieferung von Nutzerprofilen unterbinden, indem er das Feld `results` in seiner Response immer leer belässt. **[<=]**

Im Rahmen einer Vertreterregelung können sich, vermittelt durch z. B. einen Arzt, auch mehrere Versicherte gleichzeitig in einem Raum befinden. Hierbei gibt es den Spezialfall, dass der Arzt den Raum nach Abschluss der Unterhaltung verlässt und die verbliebenen Versicherten unkontrolliert weiterkommunizieren könnten. Um dieser Situation entgegenzuwirken, werden die Fachdienste im Folgenden verpflichtet, ihre Nutzer periodisch aus solchen verwaisten Räumen zu entfernen.

A_26348-01 -Periodische Entfernung von Nutzern aus verwaisten Räumen

Der TI-M Fachdienst ePA MUSS in regelmäßigen Abständen lokale Nutzer aus Räumen entfernen, in denen sich nur Versicherte befinden. Als im Raum befindlich MUSS dabei jeder Nutzer angesehen werden, dessen Membership den Wert `join` oder `invite` aufweist. Beim Entfernen von Nutzern MUSS deren Membership auf den Wert `leave` gesetzt werden, ohne dass der Raum als vergessen¹ markiert wird. Die Entscheidung, ob ein Nutzer Versicherter ist oder nicht, MUSS durch Abgleich des Domainteils der MXID gegen die aktuell am Messenger-Proxy verfügbare Föderationsliste erfolgen.

¹ `[Client-Server API/#post_matrixclientv3roomsroomidforget]` **[<=]**

A_26349 -Konfigurierbares Intervall für die periodische Entfernung von Nutzern aus verwaisten Räumen

Der TI-M Fachdienst MUSS das Intervall für die periodische Entfernung von lokalen Nutzern aus Räumen, in denen sich nur Versicherte befinden, konfigurierbar gestalten.

[<=]

Hinweis: Um einen Kompromiss zwischen Wirksamkeit und Kosteneffizienz zu erzielen wird ein tägliches Intervall empfohlen.

4 Übergreifende Festlegungen

4.1 Betrieb

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

- TI-M Fachdienst ePA

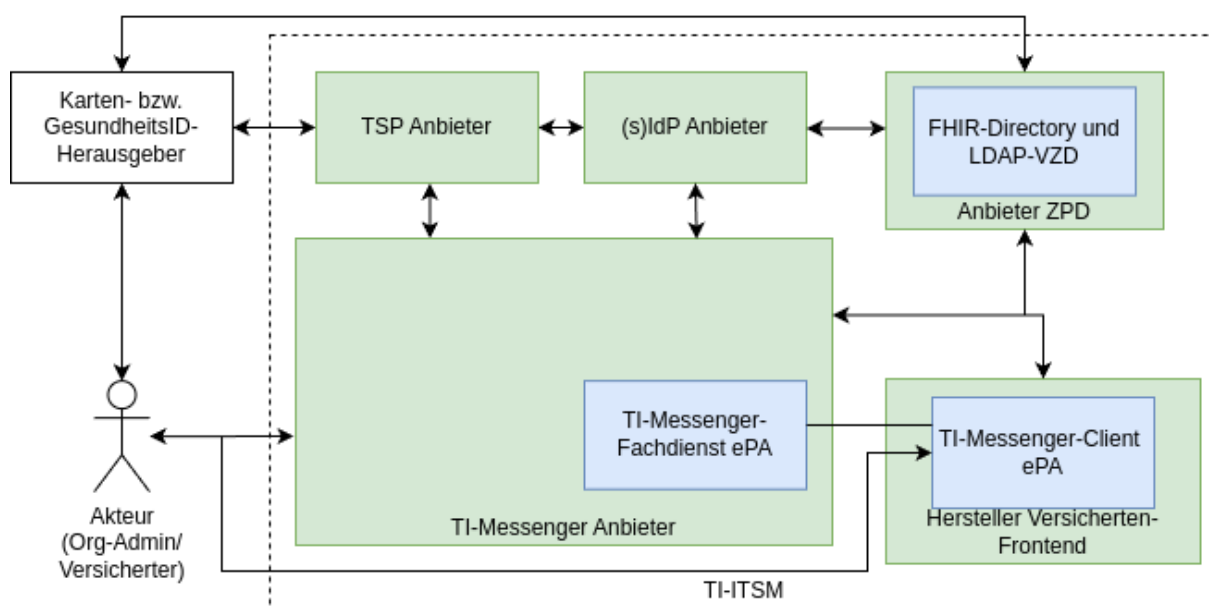


Abbildung 4 Betriebsmodell TI-M ePA

Hinweis zur Abbildung:

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

5 Funktionsmerkmale

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

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

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. Die Domain des Messenger-Service ist in der Föderationsliste als Domain für Versicherte zu hinterlegen.
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. Die Domain des Messenger-Service ist in der Föderationsliste hinterlegt worden und das Feld "isInsurance" wurde mit "true" belegt.

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

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

A_26000 -AF_10060 - Messenger-Service für ePA - Föderationslisteneintrag

Bei der Bereitstellung eines Messenger-Service für ePA MUSS beim Eintragen der Domain in der Föderationsliste der Wert von "isInsurance" mit "true" belegt werden.[<=]

5.2 Feature Identifikation und Login eines Benutzers

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

5.2.1 Anwendungsfall

AF_10234 -Identifikation und Login eines Benutzers

Damit Versicherte die Messenger-Funktion der ePA-App ihrer Krankenkasse nutzen können, müssen sich diese am IDP ihrer Krankenkasse identifizieren und erhalten damit Zugang zu deren TI-Messenger Service. Die Authentifizierung von Versicherten für die Registrierung von TI-Messenger Accounts und für das Login am Homeserver erfolgt am sektoralen IDP mittels OIDC.

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 /_matrix/client/v3 • {sidp}: ID des sektoralen IDPs, die vom Homeserver beauftragt 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

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.

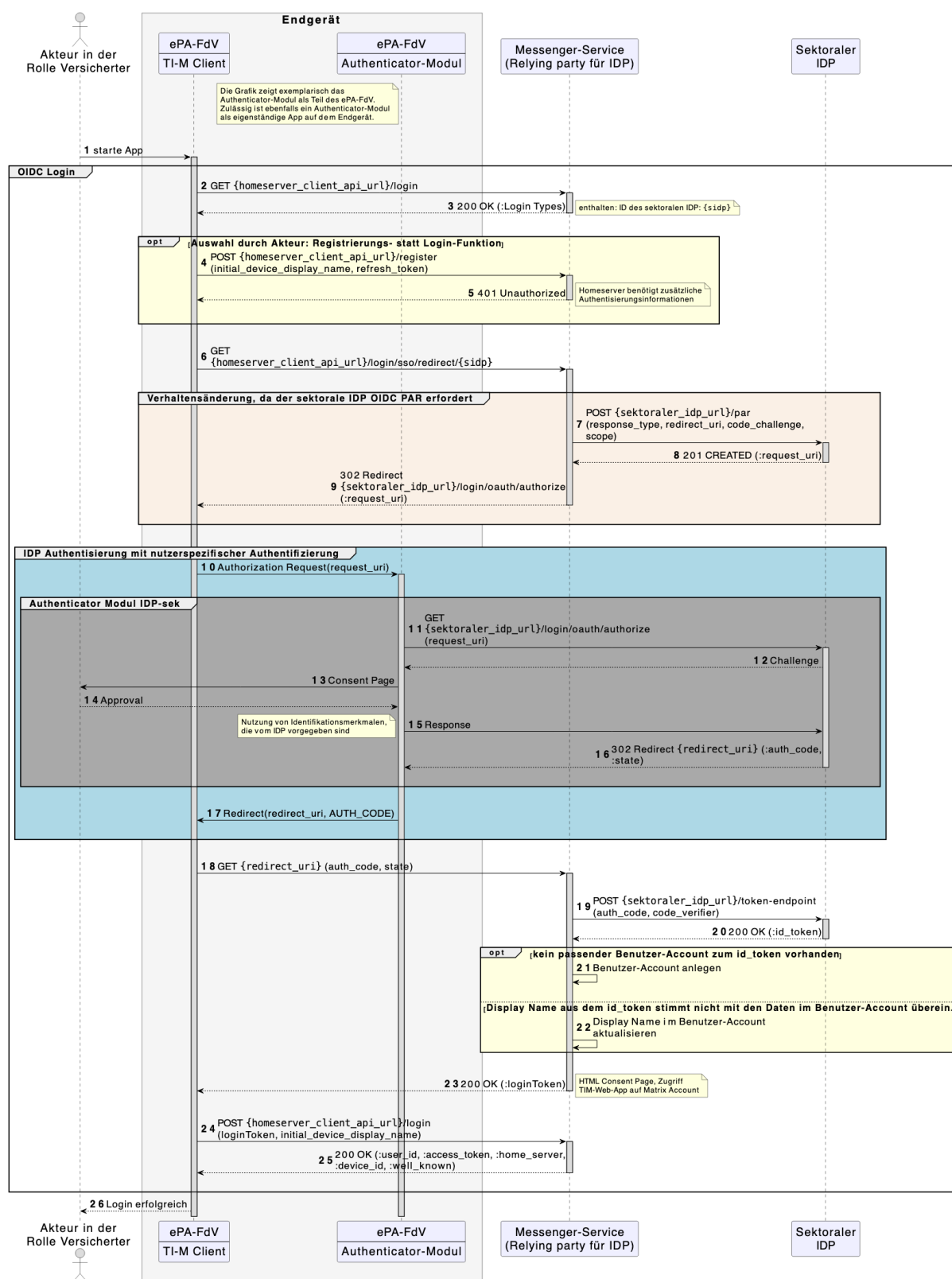


Abbildung 5 : Laufzeitsicht - Identifikation und Login eines Benutzers

[<=]

A_25706-01 -AF_10234 - Erzeugung der MXID bei Registrierung

Der TI-M FD ePA MUSS im Rahmen der Registrierung von Akteuren in der Rolle Versicherter den Localpart der MXID mit der KVNR im Lowercase-Format belegen.【<=】

Hinweis: Die KVNR kann aus dem Claim `urn:telematik:claims:id` des vom sektoralen IDP ausgestellten ID Tokens ermittelt werden.

A_25707 -AF_10234 - Erzeugung des Display Name

Der TI-M FD ePA SOLL im Fall der Registrierung oder des Logins den Display Name für die Accounts der Akteure in der Rolle Versicherter aus dem `id_token` vom sektoralen IDP übernehmen (`claim urn:telematik:claims:display_name`). Ist dies nicht möglich, so SOLL der TI-M FD ePA den Display Name sinnvoll aus anderen Bestandteilen des `id_token` zusammensetzen.【<=】

5.3 Berechtigungsmanagement - Anpassungen

5.3.1 Unterbindung der Versicherteneinladung

Der TI-M FD ePA soll verhindern, dass ein Versicherter einen anderen Versicherten einladen kann. Die folgende Grafik zeigt, welche Komponenten der Fachdienste, die zusätzliche Prüflogik übernehmen müssen. Die Versichertenprüfung soll an der Matrix-Client-Server-API durchgeführt werden sowie zur weiteren Absicherung ebenfalls an der Matrix-Server-Server-API zwischen den TI-M FD.

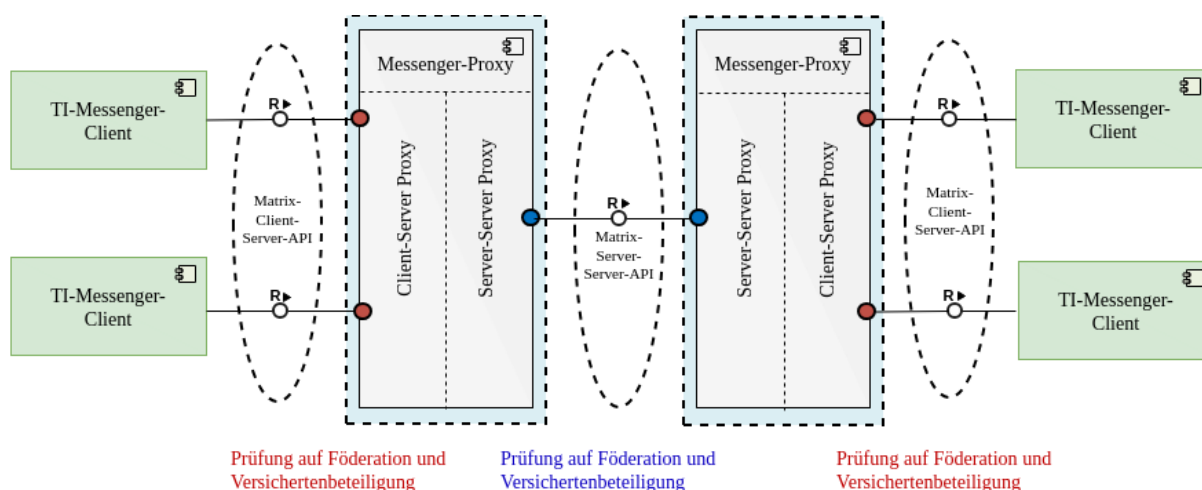



Abbildung 6: Prüfung auf Versichertenbeteiligung

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


Hinweis: Sofern ein Akteur, der nicht Versicherter ist, die Einladung(en) ausspricht, können auch mehrere Versicherte Teilnehmer eines Raumes sein und Nachrichten austauschen.

5.3.1.1 Client-Server Prüfungen

In der Funktion als Client-Server Proxy prüft der Messenger-Proxy, wie in der TI-M Basis beschrieben, eingehende Invite-Events der TI-M Clients (in der Abbildung 6 rot dargestellt) und fungiert so als Reverse-Proxy. Für den TI-M ePA muss der Messenger-Proxy zusätzlich zur in der TI-M Basis geforderten Föderationszugehörigkeit die

Versicherteneinladung nach  [ML-150398 - AF_10233 Versicherteneinladung unterbinden](#) verhindern.

5.3.1.2 Server-Server Prüfungen

In der Funktion als Server-Server Proxy prüft der Messenger-Proxy, wie in der TI-M Basis beschrieben, alle ausgehenden sowie eingehenden Events auf Föderationszugehörigkeit. Für den TI-M ePA muss die Prüfung zusätzlich die Versicherteneinladung nach  [ML-150398 - AF_10233 Versicherteneinladung unterbinden](#) verhindern.

AF_10233 -AF_10233 Versicherteneinladung unterbinden

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

Tabelle 3: AF - Versicherteneinladung unterbinden

Attribute	Bemerkung
Auslöser	Anfrage am Messenger Proxy
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>



Abbildung 7: Versicherteneinladung unterbinden

[<=]

A_25705 -AF_10233 - Versicherteneinladung unterbinden

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

A_25704 -AF_10233 - Versicherteneinladung erlauben

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

5.3.1.3 Berechtigungsprüfung

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

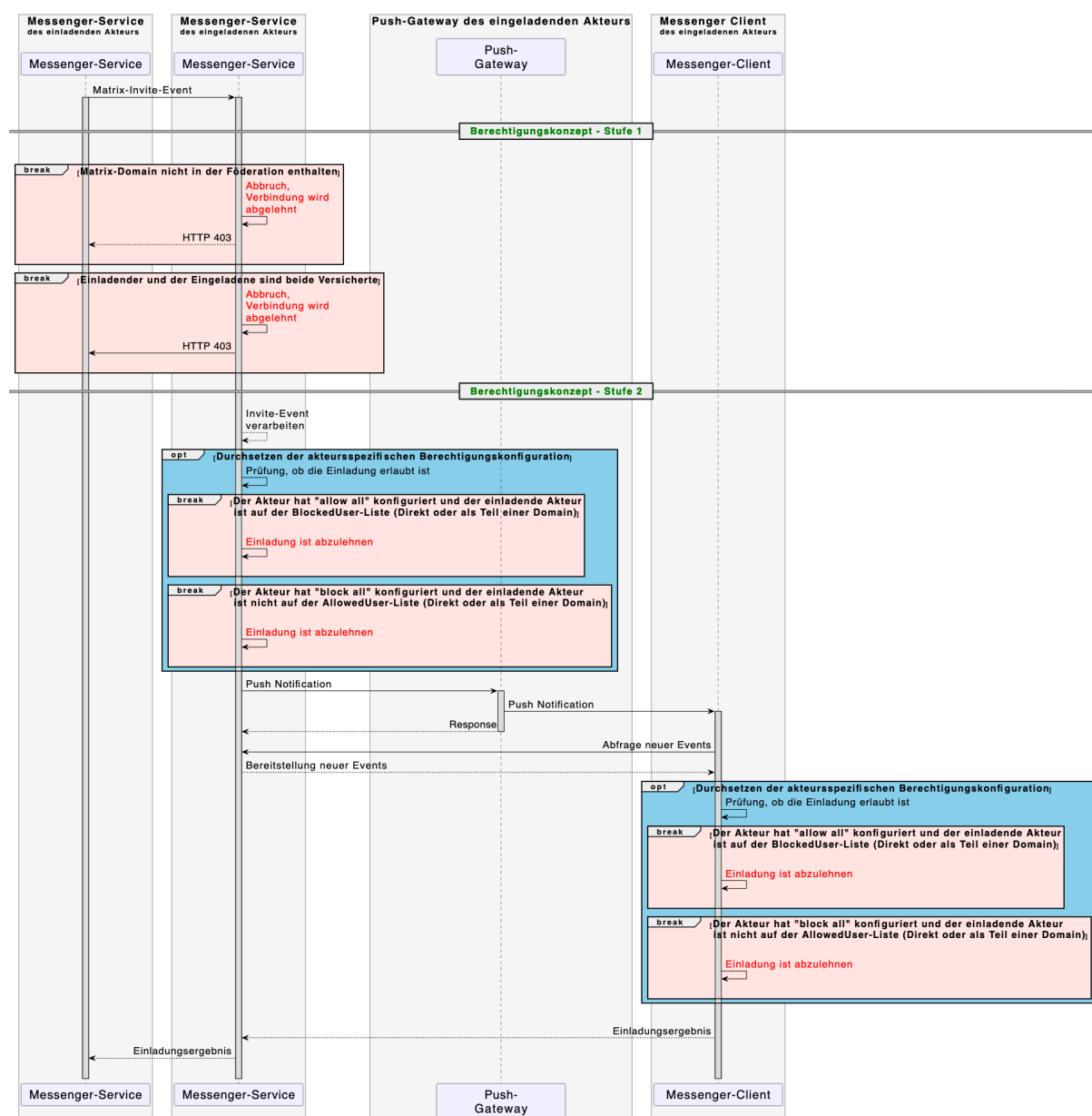


Abbildung 8: Berechtigungsprüfung TI-M_ePA

5.3.2 Weitere Anpassungen

A_25044-01 -Event Type für Berechtigungskonfiguration

Der TI-M Client ePA MUSS für die Ablage der Berechtigungskonfiguration in den Accountdaten des Matrix-Homeservers `de.gematik.tim.account.permissionconfig.epa.v1` als Event Type verwenden. [**<=**]

A_25258-01 -Schema der Berechtigungskonfiguration

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

5.4 Löschen von Inhalten - Anpassungen

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

5.4.1 Serverseitiges Löschen

5.4.1.1 Matrix-Events

Versicherte haben grundsätzlich die Hoheit über ihre Daten und Kommunikation. Im Gegensatz zu Mitarbeitern im Gesundheitswesen ist anzunehmen, dass Versicherte zudem kein Archivsystem haben, in das sie TI-M Inhalte exportieren können. Hier darf es daher keine serverseitige Löschung ohne vorherige Bestätigung durch den Versicherten geben, da sonst Inhalte unerwartet verloren gehen würden.

A_28338 -Serverseitige Löschung von Events nur nach Nutzerbestätigung

TI-M ePA Fachdienste DÜRFEN Matrix-Events NICHT ohne vorige Bestätigung aller lokalen Teilnehmer des Raumes löschen. Redactions sind von dieser Regelung ausgenommen.
[<=][<=]

6 Anhang A - Verzeichnisse

6.1 Abkürzungen

Tabelle 4: Im Dokument verwendete Abkürzungen

Kürzel	Erläuterung
ePA	elektronische Patientenakte
FD	Fachdienst
FdV	Frontend des Versicherten
IdP	Identity Provider
KTR	Kostenträger
PKI	Public Key Infrastructure
VZD	Verzeichnisdienst

6.2 Glossar

Tabelle 5: Im Dokument verwendete Begriffe

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

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

6.3 Abbildungsverzeichnis

Abbildung 1: Kontextabgrenzung.....	7
Abbildung 2: TI-M Client ePA Komponentendiagramm.....	9
Abbildung 3: TI-Messenger-Service Komponentendiagramm.....	11
Abbildung 4 Betriebsmodell TI-M ePA.....	14
Abbildung 5 : Laufzeitsicht - Identifikation und Login eines Benutzers.....	18

Abbildung 6: Prüfung auf Versichertenbeteiligung.....	19
Abbildung 7: Versicherteneinladung unterbinden.....	21
Abbildung 8: Berechtigungsprüfung TI-M_ePA.....	22

6.4 Tabellenverzeichnis

Tabelle 1: Einschränkung zu Anwendungsfall AF_10060.....	15
Tabelle 2: AF - Identifikation und Login eines Benutzers.....	16
Tabelle 3: AF - Versicherteneinladung unterbinden.....	20
Tabelle 4: Im Dokument verwendete Abkürzungen.....	24
Tabelle 5: Im Dokument verwendete Begriffe.....	24
Tabelle 6: Referenzierte Dokumente der gematik.....	25
Tabelle 7: Weitere Dokumente.....	26

6.5 Referenzierte Dokumente

6.5.1 Dokumente der gematik

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

Tabelle 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
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktivbetrieb
[gemSpec_IDP_FD]	gematik: Spezifikation Identity Provider - Nutzungsspezifikation für Fachdienste
[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)

6.5.2 Weitere Dokumente

Tabelle 7: Weitere Dokumente

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