

1.3.1 Dokumentation

Konfiguration

[TI-CA Zertifikate](#)

[Umgebungsvariablen](#)

[URLs der adressierten Systeme](#)

[Konfigurationen TIaaS Arbeitsumgebung](#)

[DIGA Informationen](#)

[ePA Umgebung](#)

[Uvicorn Worker](#)

[ePA Provider Mapping](#)

[Endpunkt](#)

[API-Übersicht:](#)

[API-Dokumentation: POST /send-document/](#)

[Request Body](#)

[Beispiel Request in Python:](#)

[Rückgabewerte /send-document](#)

[ErrorCodes /send-document](#)


[API-Dokumentation: POST /localize-record/](#)

[Request Body](#)

[Beispiel Request in Python](#)

[ErrorCodes /localize-record:](#)

[API-Dokumentation: GET /info](#)

 **Gültig ab Version: 1.3.1**

Dies ist die Dokumentation für die Verwendung des “**_fbeta ePA Service**”. Im Folgenden werden wichtige Konfigurationsdetails aufgeführt und erläutert. Anschließend werden die Details der API-Schnittstelle beschrieben und ein Beispiel für die Integration in ein Produktivsystem gegeben.

Konfiguration

TI-CA Zertifikate

Legen Sie Ihr p12-Zertifikat in das Verzeichnis `/config` ab. Das Zertifikat wird bei Operationen die mit dem Konnektor kommunizieren mit einbezogen. Lediglich das Passwort für das Zertifikat muss als Umgebungsvariable `KONNEKTOR_CERT_PW` hinterlegt werden.

```
▼ config
  KVS_Client_172.026.002.093.p12
```

Umgebungsvariablen

Folgende Umgebungsvariablen müssen in der Datei `.env` gesetzt werden:

URLs der adressierten Systeme

- `KONNEKTOR_URL` : URL des Konnektors
(`'https://konnektor-2.ru.tiaas.rise-ti.de'`)
- `USER_AGENT` : User Agent String für HTTP-Requests
(`'usrAgent/1.1.0'`)
- `KONNEKTOR_CERT_PW` : Passwort für das p12 Zertifikat
- `KONNEKTOR_JWS_URL` : URL zum JWS-Zertifikat des Konnektors – wird zur Identitätsprüfung bei der Kommunikation benötigt. Vom Konnektor-/TI-as-a-Service-Anbieter erhältlich (zeigt typischerweise auf eine `.jws`-Datei).
(ACHTUNG!) Wenn diese Variable gesetzt ist, aber kein valides Konnektor-CA-Bundle aufgebaut werden kann, startet der Service nicht.

- Für RISE gelten folgende URLs:

```
1 | RU: https://client.rise-tiaas.de/update-tiaas-ru/trusted-server-certs-ru.jws  
2 | PU: https://client.rise-tiaas.de/update-tiaas-pu/trusted-server-certs.jws
```

- `KONNEKTOR_ALLOW_INSECURE_TLS` : Flag für unsicheren TLS-Modus bei der Konnektor-Verbindung (`true` / `false` , Default: `false`).

(ACHTUNG!) Bei `true` wird die TLS-Zertifikatsprüfung gegenüber dem Konnektor explizit deaktiviert. Dieser Modus ist unsicher und nicht für Produktion geeignet.

Ist kein valides Konnektor-CA-Bundle verfügbar, startet der Service ab sofort nur noch mit expliziter Freigabe über `KONNEKTOR_ALLOW_INSECURE_TLS=true` .

Konfigurationen TIaaS Arbeitsumgebung

- `MANDANT_ID` : ID des eingerichteten Mandanten im Konnektor
(`'Test'`)
- `CLIENT_SYSTEM_ID` : ID des eingerichteten Client-Systems im Konnektor
(`'Test_Clientsystem'`)
- `WORKPLACE_ID` : ID des eingerichteten Arbeitsplatzes im Konnektor
(`'Test-Arbeitsplatz'`)
- `USER_ID` : ID des eingerichteten Users (Optional)

DIGA Informationen

- `DIGA_NAME` : Name Ihrer DiGA (Name der Verordnungseinheit)
('DIGA-Hersteller')
- `DIGA_MANUFACTURER` : Name des DiGA-Herstellers
('Sina Gr..fin ..zTEST-ONLY')

ePA Umgebung

- `EPA_ENVIRONMENT` : ePA-Umgebung `RU (RU REF)` , `RT (RU DEV)` or `PROD`
- (**Deprecated** ab Version 1.1.2 - Provider wird automatisch aus dem Provider-Mapping bezogen) `EPA_PROVIDER_NUMBER` : Nummer für ePA-Provider (`IBM=1`, `RISE=2`) (`epa-as-<provider-number>`)

Uvicorn Worker

- `UVICORN_WORKERS` : Anzahl der API-Worker für eine parallelisierte Verarbeitung (Default-Wert: 1)

ePA Provider Mapping

```
1 RECORD_PROVIDER_1 = 'IBM'  
2 RECORD_PROVIDER_2 = 'Bitmarck Technik'  
3 RECORD_PROVIDER_X = 'PROVIDERNAME' [...]
```

Endpunkt

API-Übersicht:

Eine Übersicht aller API-Endpunkte, sowie Parameter sind über folgende Endpunkte im Container zu erhalten ("Swagger"):

- `/redoc`
- `/docs`
- `/openapi.json`

API-Dokumentation: `POST /send-document/`

Dieser Endpunkt dient zum Senden eines medizinischen Dokuments (MIO) an die ePA. Die Anfrage enthält die KVNR (`insurent_id`) der versicherten Person, einen `SubmissionSet`-Eintrag, einen Dokumenteneintrag sowie die XML-Daten des Dokuments.

```
POST http://localhost:8000/send-document/
```

Request Body

Der Request muss im JSON-Format gesendet werden. Die Felder im Payload sind wie folgt:

Feldname	Typ	Beschreibung
<code>metadata.insurantId</code>	string	KVNR der versicherten Person
<code>metadata.submissionSet</code>	object	Objekt mit Metadaten zum Submission Set
<code>metadata.submissionSet.entryUUID</code>	string	Eindeutige UUID des Submission Sets
<code>metadata.documentEntry</code>	object	Objekt mit Metadaten zum eigentlichen Dokument
<code>metadata.documentEntry.creationTime</code>	string	Erstellungszeitpunkt des Dokuments im Format <code>"%Y%m%d%H%M%S"</code> (UTC) (z.B: 20250327165707)
<code>metadata.documentEntry.title</code>	string	Titel des Dokuments
<code>metadata.documentEntry.URI</code>	string	Speicherort oder Name der Datei (z. B. <code>testmio.xml</code>)
<code>metadata.documentEntry.entryUUID</code>	string	Eindeutige UUID für das Dokument Diese UUID sollte von der DiGA gespeichert werden um ggf. eine "replace"-Operation durchzuführen.
<code>metadata.documentEntry.oldEntryUUID</code>	string (optional)	Eindeutige UUID für das Dokument,

D		welches ausgetauscht werden soll (optional)
file	string /bytes	Als Bytes gelesener Inhalt des Dokuments

Beispiel Request in Python:

```

1 import json
2 import os
3 import requests
4 import uuid
5 import time
6
7 # Define the path to the file to be uploaded
8 xml_path = os.path.join(os.path.dirname(__file__), '..', 'data', 'REAL_
9
10 # Generate UUIDs - They should also be safed
11 document_uuid = str(uuid.uuid4())
12 submission_set_uuid = str(uuid.uuid4())
13
14 # Get file creation time from metadata
15 file_creation_time = os.path.getctime(xml_path)
16 # Transform into UTC-Time
17 adjusted_time = time.gmtime(file_creation_time)
18 creation_time = time.strftime("%Y%m%d%H%M%S", adjusted_time)
19
20 url = "http://localhost:8000/send-document/"
21 payload = {
22     "insurantId": "X110580673", # Insert a valid KVNR here
23     # See: https://gemspec.gematik.de/docs/gemSpec/gemSpec_Aktensystem_
24     "providerId": 2, # Insert the assigned number of the ePA provider o
25     "submissionSet": {
26         "entryUUID": submission_set_uuid
27     },
28     "documentEntry": {
29         # UTC
30         "creationTime": creation_time,
31         "title": "Testdokument",
32         "URI": "REAL_EXAMPLE_1_KBV_PR_MIO_DIGA_Bundle.xml",
33         "entryUUID": document_uuid,
34         # OPTIONAL - If you want to replace a document
35         # "oldEntryUUID": "929850b6-a5f2-46ca-b742-1abb754cfd45"
36     },
37 }
38
39 print("Payload:", json.dumps(payload, indent=4))
40
41 # Send the request with 120 seconds timeout
42 response = requests.post(url,
43     data={
44         "metadata": json.dumps(payload),
45     },
46     files={
47         "file": open(xml_path, "rb"),
48     },
49     timeout=120
50 )
51
52 response_dict = json.loads(response.text)

```

Rückgabewerte /send-document

Code	Bedeutung	Response-Body (JSON)
200	OK – Dokument erfolgreich verarbeitet und verschickt	<ul style="list-style-type: none"> • <code>success</code> : <i>Boolean</i>. Gibt an, ob der Upload erfolgreich war oder nicht. • <code>message</code> : <i>String</i>. Zusammenfassung der Antwort der Patientenakte auf den Upload-Versuch. • <code>details</code> : <i>Objekt</i>. Die genaue Antwort der Patientenakte auf den Uploadversuch. • <code>submissionSetEntryUUID</code> : <i>String</i>. Die <code>entryUUID</code> des Upload-Versuchs (SubmissionSet). • <code>documentEntryEntryUUID</code> : <i>String</i>. Die <code>entryUUID</code> des verschickten Dokuments (DocumentEntry).
422	Unprocessable Content – Falsche oder fehlende Request-Parameter im JSON-Payload	<ul style="list-style-type: none"> • <code>detail</code> : <i>Liste an Objekten</i>. Enthält Hinweise zu fehlenden oder falsch verwendeten Feldern in der Anfrage. <ul style="list-style-type: none"> ◦ <code>type</code> : <i>String</i>. ◦ <code>loc</code> : <i>Objekt</i>. ◦ <code>msg</code> : <i>String</i>. ◦ <code>input</code> : <i>Any</i>.
400+	Bad Request – Ungültiger Payload oder fehlende Felder	<ul style="list-style-type: none"> • <code>detail</code> : <ul style="list-style-type: none"> ◦ <code>error</code> : <i>String</i>. Kurze Beschreibung des Fehlers. ◦ <code>code</code> : <i>String</i>. Der Name des ErrorCodes. ◦ <code>type</code> : <i>String</i>. Der Name der Komponente, in dem der Fehler aufgetreten ist.

500+	Internal Server Error – Fehler bei der Verarbeitung auf Serverseite	<ul style="list-style-type: none"> ◦ <code>entryUUID</code> : <i>String</i>. Die <code>submissionSet.EntryUUID</code> des Upload-Versuchs (zu debugging Zwecken). ◦ <code>*detail</code> : <i>Dict<String></i>. Ist ein Fehler auf eine nicht erfolgreiche Antwort des Aktensystems zurückzuführen, wird der konkrete Response des Aktensystems an dieser Stelle angezeigt. <p>Diese Informationen dienen ausschließlich der Unterstützung beim Troubleshooting und haben keinen programmatischen Nutzen.</p>
------	--	---

ErrorCodes /send-document

Tritt ein Fehler auf, bevor das Dokument an die Patientenakte gesendet werden kann, antwortet der Service mit einem der folgenden ErrorCodes:

ErrorCode	Bedeutung	Verantwortung / Lösung
VAU_INIT_FAILED	Initialisierung des VAU-Kanals zwischen Client und Server fehlgeschlagen	<ul style="list-style-type: none"> • DiGA: <ul style="list-style-type: none"> ◦ Verbindung zwischen ePA-API und Konnektor fehlerhaft. ◦ SMC-B nicht über Konnektor abrufbar/ SMC-B nicht verifiziert • Aktensystembetreiber/ Gematik: Störungen in der TI oder am Aktensystem

VAU_CERT_VALIDATION_FAILED	Validierung des VAU-Server-Zertifikats nicht möglich	<ul style="list-style-type: none"> • Aktensystembetreiber/ Gematik: Störungen in der TI oder am Aktensystem
VAU_AUTH_FAILED	Authentifizierung über den VAU-Kanal fehlgeschlagen (ungültiges oder abgelaufenes Token)	<ul style="list-style-type: none"> • DiGA: Fehler im Redis, Token wird nicht aktualisiert. • Aktensystembetreiber/ Gematik: Störungen in der TI oder am Aktensystem
VAU_COMMUNICATION_ERROR	Allgemeiner Fehler beim Senden oder Verarbeiten von VAU-Nachrichten	<ul style="list-style-type: none"> • DiGA: <ul style="list-style-type: none"> ◦ Verbindung zwischen ePA-API und Konnektor fehlerhaft. ◦ SMC-B nicht über Konnektor abrufbar/ SMC-B nicht verifiziert • Aktensystembetreiber/ Gematik: Störungen in der TI oder am Aktensystem
EPA_GETNONCE_ERROR	Fehler beim Abrufen eines Nonce vom ePA-Autorisierungsservice	<ul style="list-style-type: none"> • DiGA: <ul style="list-style-type: none"> ◦ Verbindung zwischen ePA-API und Konnektor fehlerhaft. ◦ SMC-B nicht über Konnektor

		<p>abrufbar/ SMC-B nicht verifiziert</p> <ul style="list-style-type: none"> • Aktensystembetreiber/ Gematik: Störungen in der TI oder am Aktensystem
EPA_AUTHZ_ERROR	Autorisierung mit dem ePA-Dienst fehlgeschlagen	<ul style="list-style-type: none"> • DiGA: <ul style="list-style-type: none"> ◦ Verbindung zwischen ePA-API und Konnektor fehlerhaft. ◦ SMC-B nicht über Konnektor abrufbar/ SMC-B nicht verifiziert • Aktensystembetreiber/ Gematik: Störungen in der TI oder am Aktensystem
EPA_NOT_ENTITLED	Benutzer hat den Zugriff auf die ePA nicht über die FdV-App freigegeben	User: muss die DiGA in der FdV-App zum schreiben auf die ePA freigeben.
EPA_SEND_ERROR	Fehler beim Senden eines Dokuments an das ePA-System	
KONNEKTOR_INIT_FAILED	Initialisierung der Verbindung zum Konnektor fehlgeschlagen	<ul style="list-style-type: none"> • DiGA: <ul style="list-style-type: none"> ◦ Verbindung zwischen ePA-API und Konnektor fehlerhaft.

KONNEKTOR_REQUEST_FAILED	Anfrage an den Konnektor fehlgeschlagen	<ul style="list-style-type: none"> • DiGA: <ul style="list-style-type: none"> ◦ Verbindung zwischen ePA-API und Konnektor fehlerhaft.
KONNEKTOR_MALFORMED_REQUEST	An den Konnektor gesendete Anfrage war fehlerhaft	<ul style="list-style-type: none"> • DiGA: <ul style="list-style-type: none"> ◦ Fehlerhafte Eingabeparameter
CARD_NOT_FOUND	Die SMC-B-Karte wurde nicht im Kartenterminal gefunden	<ul style="list-style-type: none"> • DiGA: <ul style="list-style-type: none"> ◦ SMC-B nicht über Konnektor abrufbar
CARD_CERTIFICATE_ERROR	Fehler beim Abrufen oder Verarbeiten des Karten-Zertifikats	<ul style="list-style-type: none"> • DiGA: <ul style="list-style-type: none"> ◦ SMC-B nicht über Konnektor abrufbar/ SMC-B nicht verifiziert
CARD_PIN_NOT_VERIFIED	Die PIN der SMC-B-Karte ist nicht verifiziert/aktiviert	<ul style="list-style-type: none"> • DiGA: <ul style="list-style-type: none"> ◦ SMC-B nicht verifiziert
CARD_OPERATION_ERROR	Während einer Kartenoperation ist ein Fehler im Konnektor aufgetreten	<ul style="list-style-type: none"> • DiGA: <ul style="list-style-type: none"> ◦ SMC-B händisch prüfen <ul style="list-style-type: none"> ▪ Steckt SMC-B ▪ Wird SMC-B über GetCards richtig gelesen ▪ Wird SMC-B über getPINStatus als verifiziert angezeigt. • Konnektorbetreiber: Störung in der TI

		oder am Konnektor
DOC_DECODE_ERROR	Fehler beim Dekodieren der Dokumentdaten	<ul style="list-style-type: none"> • Aktensystembetreiber/ Gematik: Störungen in der TI oder am Aktensystem
DOC_MISSING_DATA	Erforderliche Daten für das Dokument fehlen	<ul style="list-style-type: none"> • DiGA: Erforderliche Daten für das Dokument fehlen (URI).
DOC_UPLOAD_DUPLICATE	Dokument besteht bereits in der elektronischen Patientenakte der KVNR. (File-Hash bereits im Aktensystem)	<ul style="list-style-type: none"> • DiGA: MIO oder PDF-A wurde seit dem letzten Upload nicht angepasst, bzw. es wird versehentlich erneut hochgeladen.
DOC_UPLOAD_ERROR	Fehler beim Hochladen des Dokuments in das ePA-System	<ul style="list-style-type: none"> • DiGA: <ul style="list-style-type: none"> ◦ Verbindung zwischen ePA-API und Konnektor fehlerhaft. ◦ SMC-B nicht über Konnektor abrufbar/ SMC-B nicht verifiziert ◦ Fehler im Datenformats des Uploaddokuments. • Aktensystembetreiber/ Gematik: Störungen in der TI oder am Aktensystem

DOC_REPLACE_UUID_ERROR	Das Dokument konnte nicht überschrieben bzw. ersetzt werden, da die angegebene oldEntryUUID keiner im Aktensystem der betreffenden KVNR vorhandenen entryUUID entspricht.	<ul style="list-style-type: none"> • DiGA: <ul style="list-style-type: none"> ◦ entryUUID des zu ersetzenden Dokuments wurde nicht korrekt gesichert, wiedergeholt oder gesetzt.
IDP_VERIFICATION_ERROR	Fehler bei der Verifizierung von Tokens oder Signaturen vom Identity Provider	<ul style="list-style-type: none"> • Gematik: Störungen in der TI oder am zentralen IDP
IDP_REQUEST_ERROR	Anfrage an den Identity Provider fehlgeschlagen	<ul style="list-style-type: none"> • DiGA: Verbindung zwischen ePA-API und IDP fehlerhaft. • Gematik: Störungen in der TI oder am zentralen IDP
SSL_ERROR	Bei einer Zertifikatsprüfung ist ein Fehler aufgetreten.	<ul style="list-style-type: none"> • DiGA: <ul style="list-style-type: none"> ◦ Fehler beim beziehen der Zertifikate. (In Logs schauen) ◦ Falsche URL in KONNEKTOR_JWS_URL
UNEXPECTED_ERROR	Ein unerwarteter Fehler, der nicht in andere Kategorien fällt	-

API-Dokumentation: POST /localize-record/

Der Endpunkt durchsucht systematisch alle konfigurierten Aktensystem-Provider (z.B. die verschiedenen Krankenkassen-Systeme), um herauszufinden, bei welchem Anbieter die elektronische Patientenakte eines bestimmten Versicherten gespeichert ist. Das Ergebnis wird cached, um wiederholte Anfragen zu optimieren.

POST http://localhost:8000/localize-record/

Request Body

Der Request muss im JSON-Format gesendet werden. Die Felder im Payload sind wie folgt:

Feldname	Type	Beschreibung
insurantId	string	Die Versichertennummer (KVNR) des Patienten, dessen Akte lokalisiert werden soll
ignoreCache	bool	Boolean-Flag, ob der Cache ignoriert werden soll (optional, Default: false)

Beispiel Request in Python

```
1 url = "http://localhost:8000/localize-record/"
2
3 # Send the request with 120 seconds timeout
4 payload = {
5     "insurantId": "Z987654321",
6     # "ignoreCache": True
7 }
8 response = requests.post(url, json=payload, timeout=120)
```

ErrorCodes /localize-record:

ErrorCodes	Bedeutung	Verantwortung / Lösung
RECORD_EXISTS_AND_ACTIVATED	KVNR ist bei einem der Aktensystembetreiber	-

	registriert und aktiviert	
RECORD_NOT_FOUND	KVNR wurde in keinen der Aktensystembetreiber gefunden.	User: muss sich mit KVNR bei einem Aktensystembetreiber registrieren.
RECORD_STATUS_CONFLICT	KVNR wurde zwar bei einem Aktensystembetreiber gefunden, scheint aber nicht aktiviert zu sein (ePA ist deaktiviert)	User: muss sich bei dem angemeldeten Aktensystembetreiber wieder freischalten lassen.

API-Dokumentation: GET /info

Dieser Endpunkt liefert technische Laufzeit-Metadaten zur laufenden Service-Instanz.

GET <http://localhost:8000/info >

Response-Body (JSON):

- service : Name des Services
- status : Laufzeitstatus
- apiVersion : API-Version
- deploymentVersion : Image-Version