[English Version] TI Guide for manufacturers of DiGA

This guide will be iteratively developed. If relevant aspects and/or questions are missing, please provide us feedback via the following e-mail address: diga@gematik.de

Update on 06.09.2023: Information was added on testoptions, which are now available for integrating the Health ID resp. the IDP-Federation.

Update on 22.11.2023: Information on the next steps after the successful testing of the Health ID has been added.

Update on 21.02.2024: Information on the confirmation process of the gematik, the 'ePA for all', and data submission to the BfArM has been added.

Update on 27.03.2024: Information regarding the HealthID logo has been provided.

Outline

- The TI Ecosystem in the Context of Digital Health Applications
- Writing a DiGA-MIO/PDF into the User's ePA
  - Implementation of the use case
  - About the ePA
    - Authorization of data transfer by the user
    - Data Upload
  - Implementation options for TI-access
    - Addressing Connector Interfaces
    - SMC-B Issuance
  - Testing Opportunities/Offers
    - RU-as-a-Service (Enabler)
  - DiGA MIO Toolkit
- Registration at DiGA with the HealthID
  - Implementation of the Use Case

Manufacturers of digital health applications (DiGA) have to comply with various obligations in the context of telematics infrastructure (TI). The present guide aims to assist DiGA manufacturers in implementing the TI use cases by providing all necessary information in a consolidated and clear manner. In particular, it is intended to:

- Describe the TI use cases and their implementation by DiGA manufacturers,
- inform about DiGA-relevant specification documents from the gematik,
- inform about existing possibilities for setting up access to the telematics infrastructure, and
- clarify existing possibilities/offers to test the TI use cases.

Following a comprehensive review of all the TI use cases in the context of DiGA, this document will particularly emphasize two mandatory use cases. The first one is the uploading of DiGA data into the Electronic Patient Record (ePA) by the DiGA manufacturer. The second focuses on the integration of digital identities (HealthID) provided by the health insurance companies for the insured individuals.

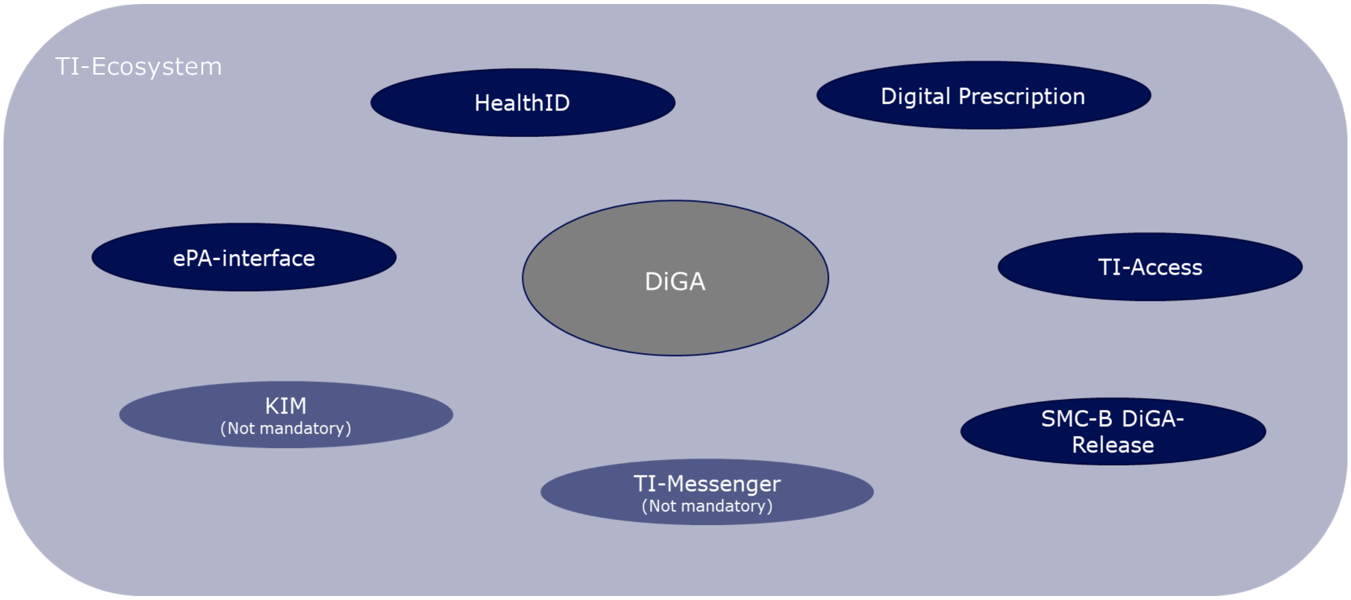
The TI Ecosystem in the Context of Digital Health Applications

Under the Digital Health Applications Regulation (DiGAV), DiGA manufacturers are mandated to transfer **data from the DiGA** into the **ePA** at the user's behest. If the user gives authorization, treating healthcare providers can view the relevant DiGA data from their familiar primary system without needing to operate an additional, DiGA-specific interface. The data should ideally be entered into the ePA in the form of a DiGA-MIO, as specified by mio42 GmbH, although it can technically also be stored as a PDF. Given that the current protocol only allows data entry into the ePA from the DiGA backend via access to the closed network of the TI – essentially, via a connector used in conjunction with a unique SMC-B DiGA smart card (smart card that uniquely identifies a participant of the TI) – DiGA manufacturers must equip themselves with the necessary components to implement this use case.

DiGA manufacturers are also obliged to enable **registration to the DiGA** via the **digital identities of the insured people (HealthID)** provided by the health insurance companies. The HealthID is intended to become a central access point to applications in the healthcare system, with so-called identity providers of the health insurances taking over the secure authentication of users for the application. DiGA manufacturers are required by the DiGA regulation to meet high security requirements in relation to user authentication and to prove this in the future by presenting a data security certificate. The identity providers of the health insurances meet the highest security requirements in relation to the identification and authentication of users and provide DiGA manufacturers with the health insurance number (KVNR) necessary for writing into the ePA in a secure manner. However, creating a HealthID is voluntary for insured people, so DiGA manufacturers must also implement their own authentication procedures (see chapter 3.4.4 "Identification and Authentication" of the DiPA guide (link)).

In addition, the gematik, in cooperation with the GKV-Spitzenverband and DiGA manufacturer associations, specifies the **digital DiGA prescription**. Currently, DiGA prescriptions must be submitted by the patient to their health insurance company to receive an activation code, which then must be entered into the DiGA. According to data from the GKV-Spitzenverband from 2022, almost 80% of prescriptions were redeemed in the period from September 2020 to September 30, 2022. The digital DiGA prescription aims to make the prescription and redemption process free of disruptions and quick. Currently, the regulation is still in conception and is therefore not part of this guide.

Considering that DiGA manufacturers must connect to the TI with the appropriate components for writing data into the ePA, the technical prerequisite for using a **TI messenger**, as well as the secure communication procedure **KIM**, is certainly met. However, the DiGAV currently does not mandate this, and therefore, these use cases are not part of this guide.



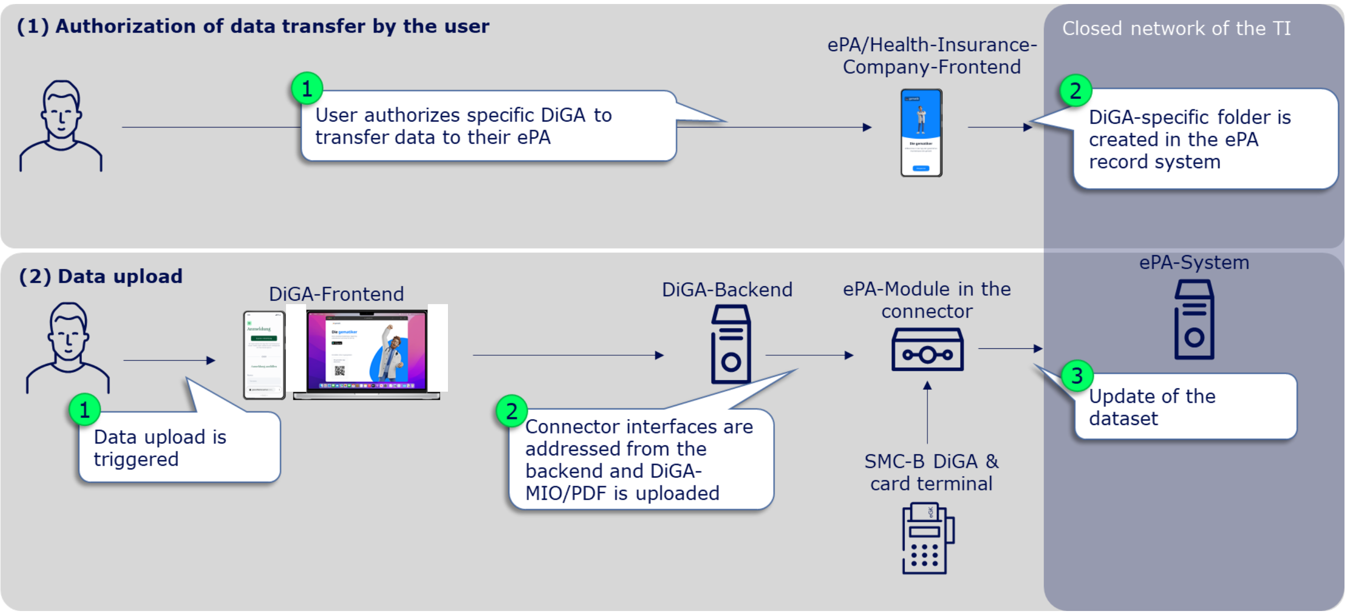
Writing a DiGA-MIO/PDF into the User's ePA

According to the DiGAV (§6 Abs. 1), manufacturers of DiGAs are obligated to transfer data from the DiGA to the ePA upon the user's request. If the user consents, treating healthcare providers can view the relevant DiGA data from their usual primary system without having to operate an additional, DiGA-specific interface. Ideally, the data should be entered into the ePA in the form of a DiGA-MIO, as specified by mio42 GmbH, although technically it can also be stored as a PDF. The ePA record systems provided by statutory health insurance providers and in the future also private health insurance companies are located in the closed network of the TI. To access this network, DiGA manufacturers need an institution card (SMC-B DiGA) that uniquely identifies the DiGA manufacturer to the telematics infrastructure and initially grants them writing rights in accordance with § 341 paragraph 2 no. 9 SGB V. This SMC-B must be connected to a connector via a card terminal, only then can the DiGA manufacturer write data into the user's ePA via defined interfaces of the connector. The challenge for DiGA manufacturers is to integrate the TI components into their IT infrastructure. This chapter is intended to support the implementation of the use case.

Implementation of the use case

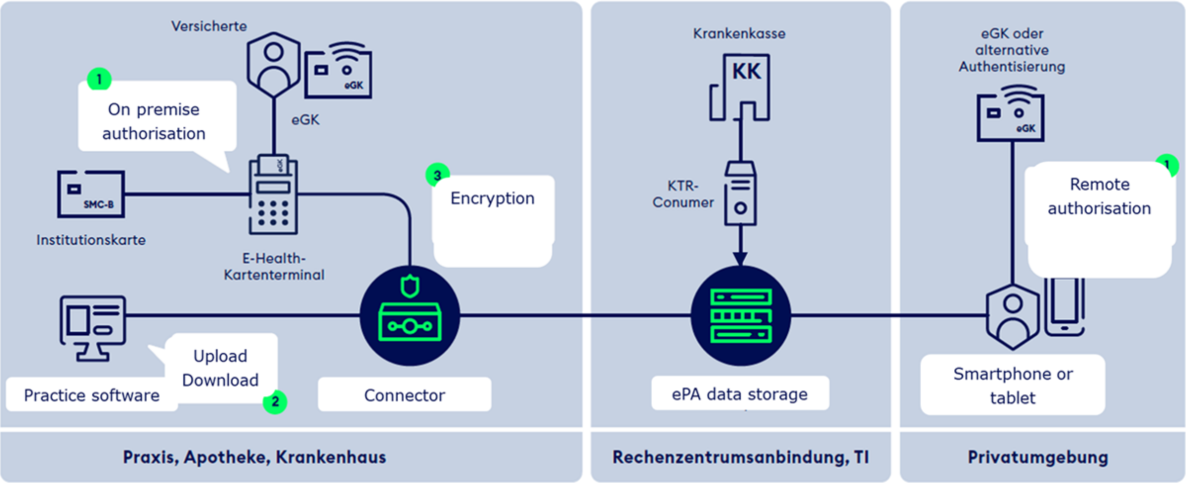
For the implementation of the use case, two basic steps are necessary:

1. The user must authorize the DiGA in their ePA frontend for data transfer. For this step, no adjustments to the systems of the DiGA manufacturers are necessary.
2. The DiGA manufacturer cyclically or event-based inserts the supply-relevant DiGA data in the form of a MIO or PDF into the user's ePA. For this step, adjustments to the systems of the DiGA manufacturers are necessary.


(1) Authorization of data transfer by the user
1
User authorizes specific DiGA to transfer data to their ePA
ePA/Health-Insurance-Company-Frontend
Closed network of the TI
2
DiGA-specific folder is created in the ePA record system
(2) Data upload
DiGA-Frontend
1
Data upload is triggered
DiGA-Backend
2
Connector interfaces are addressed from the backend and DiGA-MIO/PDF is uploaded
ePA-Module in the connector
SMC-B DiGA & card terminal
ePA-System
3
Update of the dataset

About the ePA

The electronic health record ePA is a service provided by every statutory health insurance company in Germany. This service is free of charge and it is up to the insurant whether or not to make use of it. It enables that medical documents and data are made available to the patient as well as to healthcare professionals who are involved in the treatment process. This leads to a broader knowledge base to all parties involved and which in turns is meant to improve diagnostics and the identification of more targeted care plans and interventions. Furthermore, ePA aims at strengthening patient empowerment as patients become increasingly involved in decision-making processes and in complying to agreed care plans. Given that the ePA service is build on gematik specifications and all ePA products are tested and accredited by gematik, APIs and functionalities are standardised and, thus, interoperable. The service can be used nationwide, across healthcare sectors and supports cross-institutional, asynchronous, non-directed communication. The ePA architecture in simplest terms is depicted in the illustration below. The current version of ePA that is productive is 2.6.



Under current legislation, ePA is provided as an opt-in model. This implies: 1) an insurant has to contact his insurance company to apply for an ePA, 2) an insurant has to actively register his smartphone for his ePA in order to activate it OR visit a HCP and have him activate the record system after the electronic healthcare card (eGK) has been read and its six digit PIN enterd, and 3) an insurant has to actively provide an HCP (document-specific) access to his ePA in order to read and write documents. With the Act for Accelerating the Digitalisation in Healthcare (Digital-Gesetz, DigiG), the provisioning model will be changed to an opt-out version. This change will come into effect by 15 January 2025. The conceptual model will lead to a number of changes: 1) insurants automatically receive an ePA, 2) HCPs are automatically authorised to interact with ePA once the patient has provided their electronic healthcare card when visiting the practice (without entering a six digit PIN), and 3) a selected number of documents that are legally pre-defined will have to be uploaded by the HCP to ePA. All of this applies, unless the insurant has opted-out to any of those steps. The future version of ePA will be release 3.0. With it come a number of changes that affect the architecture.

This document will be updated in the course of the year 2024 to reflect those changes and to detail what implications arise the perspective of a DiGA provider. For further updates and information regarding ePA 3.0, please visit our resources on GitHub at: https://github.com/gematik/ePA-Basic/tree/ePA-3.0

Authorization of data transfer by the user

ⓘ The following references published specification documents, implementation guides, and other documents from the gematik. The sections relevant to DiGA manufacturers are each mentioned. The documents can be retrieved in the latest version via the document search in the gematik professional portal. For this, the product type 'ePA-Aktensystem' in the latest version must be selected and the documents referenced here can be found among the search results (Link).

In mid-February 2024, an online reader was published that greatly simplifies the search and readability of the requirements: https://gemspec.gematik.de/

Before DiGA manufacturers can even place data in the user's ePA, it is absolutely necessary for the user to authorize the DiGA to write in their ePA. Without prior authorization from the user, no data upload is possible and the corresponding request will result in an error. The authorization can be granted by the user specifically for DiGA in the ePA frontend or ad hoc for DiGA in general at a card terminal in the service provider institution (document category "DiGA" in the ePA, see gemSpec_Dokumentenverwaltung Chap. 5.4 Zugriffsregeln).

The user can only authorize the DiGA when the gematik, as the issuer of the SMC-B DiGA *(see chapter Implementation options for TI access)*, has entered the DiGA manufacturer in the gematik directory. This happens immediately after the SMC-B DiGA has been delivered to the DiGA manufacturer. Only then can the user find the corresponding DiGA in his ePA-Frontend and grant the corresponding authorization. When the user grants authorization, a DiGA-specific folder is created in the user's ePA record system, into which the supply-relevant DiGA data can subsequently be stored.

The described functionalities/mechanisms have already been implemented by the record system providers and health insurances, so no technical adjustments are necessary on the part of the DiGA manufacturers for this partial step.

Data Upload

Provided that the user has authorized the DiGA to write to his ePA and thus the DiGA-specific folder in the ePA record system has been created, the DiGA manufacturer can place and/or replace care-relevant DiGA data in the user's ePA. This requires 3 or 4 steps:

(1) Calling up the ePA-specialist-module in the connector

Connectors have so-called specialist modules for various products of the telematics infrastructure, which encapsulate specific functionalities of these TI products. The first step to upload a document in the ePA is therefore to call up the ePA specialist module in the connector. For this, the corresponding endpoint must be determined. *(see ePA-Implementierungsleitfaden für Primärsysteme (gemILF_PS_ePA) chapter 4.2 Dienstverzeichnisdienst).*

(2) Find the user's file

It then needs to be determined which file provider the user's file is with. For this, a request with the health insurance number (KVNR) of the user must be made to the connector, which returns the file provider in the form of the so-called HomeCommunityID. The HomeCommunityID should - as long as the user wants to write data into the ePA - be stored together with the KVNR, which simultaneously represents the file ID, to save the (time-consuming) determination of the HomeCommunityID for a new data upload. *(see Implementierungsleitfaden Primärsysteme ePA (gemILF_PS_ePA) chapter 5.1.1 Aktenanbieter ermitteln, reference request on GitHub: link)*

(3) Post document

With the KVNR (= file-ID) and the HomeCommunityID as well as the authorization granted by the user, documents can now be uploaded into the ePA. To place a DiGA-MIO or a PDF document in the identified ePA of the user, a request according to IHE standard according to chapter 5.2.1 of the implementation guide primary systems ePA *(gemILF_PS_ePA)* must be made to the connector. General metadata requirements can be found in the ePA data model *(gemSpec_DM_ePA)* chapter 2.1.4 usage guidelines for IHE ITI XDS metadata. Here, the same general requirements for primary systems apply to DiGA. Metadata requirements to identify a DiGA-MIO can be found as a reference on GitHub (link). Likewise, a reference request for posting a DiGA-MIO (link) as well as a U-Heft-MIO is available on GitHub (link).

(4) Update/replace document

A previously posted ePA document can be replaced by adding the existing DocumentID (DocumentEntry.entryUUID) to the request required under (3). This must be persisted by the DiGA manufacturer, as currently no read access is possible *(see A_23131 in gemILF_PS_ePA chapter 6.4.4 Daten digitaler Gesundheitsanwendungen).*

If no DocumentID is provided, a new document is stored in the DiGA folder of the user's ePA and the responsibility to open the relevant or most recent document lies in the primary system.

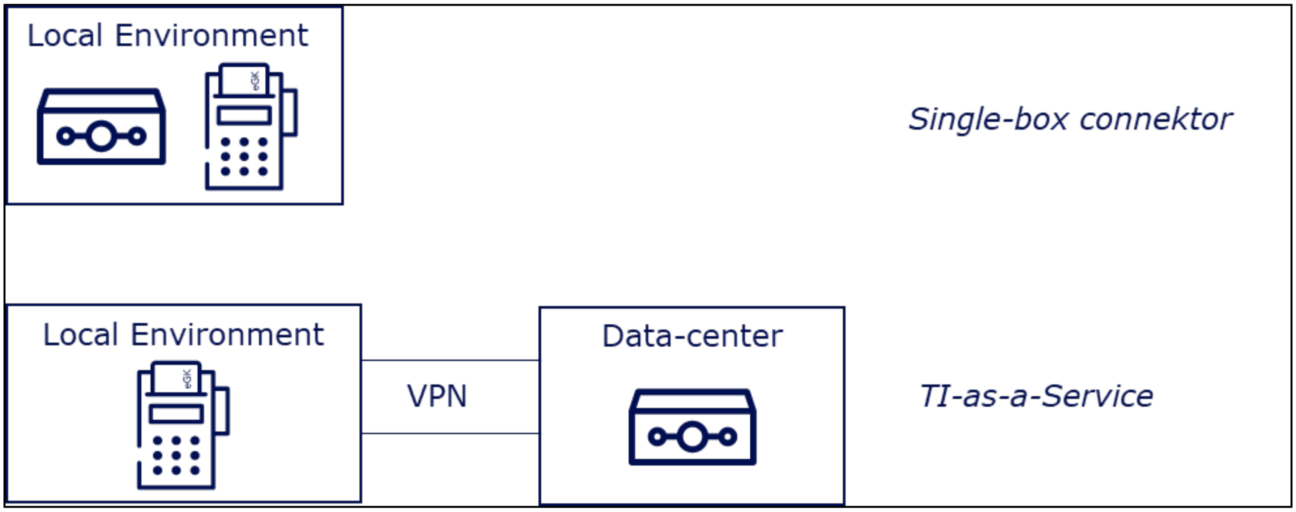
Implementation options for TI-access

As described earlier, it is necessary for the ePA use case that DiGA manufacturers equip themselves with TI access components. Specifically, the following components need to work together for TI access:

- SMC-B DiGA: Physical institution card, which identifies the DiGA manufacturer against the TI and authorizes this to write into the ePA
- Card terminal: Carrier of the SMC-B
- Connector: Physical component that encapsulates access and ePA functionalities in interaction with card terminal and SMC-B

Addressing Connector Interfaces

Currently, there are two ways to implement a TI access in the market. Firstly, a manufacturer can operate a single-box connector in an environment for which they are responsible, which communicates with an SMC-B in a card terminal. The other, and usually more comfortable option for DiGA manufacturers due to their IT infrastructure, is to realize the TI connection via a TI-as-a-Service provider.



TI-as-a-Service providers host connectors and secure operations for the DiGA manufacturer. They address the necessary connector interfaces for the TI use cases via a secure VPN connection. In this model, manufacturers usually pay a one-time connection fee and a monthly flat rate. The integration of the SMC-B in this model should be individually coordinated with the TI-as-a-Service provider, depending on the individual IT infrastructure of the DiGA manufacturer.

SMC-B Issuance

Applying for the SMC-B DiGA is only possible after the DiGA has been successfully listed in the DiGA directory. According to § 351 Abs. 3 SGB V, the gematik is the card issuer for SMC-B DiGA. DiGA manufacturers can apply for SMC-Bs via the application portal of d-trust, the card provider of gematik (link). The BfArM will confirm to the gematik that the applicant is authorized to receive an SMC-B.

ⓘ **Important:** As part of the SMC-B order, it is necessary for the DiGA manufacturer to undergo an identity verification process. **It is imperative that the person listed as the contact person in the BfArM application portal goes through the appropriate identity verification process.** Please ensure this before applying for the SMC-B according to the following document:

Änderung der Kontaktdaten für DiGA.pdf

It's important to note that a separate SMC-B must be ordered for each DiGA listed in the directory for the following reasons:

- The user must be able to grant ePA writing access (and prospectively reading access) for each DiGA individually.
- If a DiGA from the manufacturer is removed from the directory, each SMC-B associated with a DiGA must be able to be blocked separately.

For testing purposes, however, the gematik provides special test cards that can be ordered through the professional portal of the gematik or through your enabler – even before an official listing as a DiGA in the directory (link).

Testing Opportunities/Offers

DiGA manufacturers currently have the opportunity to test data upload to an ePA in the so-called TI reference environment (RU). There are basically 2 different ways to access the RU:

1. Hiring an "enabler" who provides you with all the necessary components and services, as well as further (individual) services for accessing the RU "from a single source"
2. Procurement of all the necessary components and services for accessing the RU (connector, card terminal with SMC-KT, test cards, VPN access to the RU)

It is recommended for DiGA manufacturers to obtain RU access via an "enabler" as a service, as the procurement and integration of the TI access components is much more complex to implement due to the IT infrastructure of the DiGA manufacturers.

RU-as-a-Service (Enabler)

For the ePA tests in the RU, a test insurance card (eGK) and a test institution card (SMC-B) are needed, among other components. Both test cards can be obtained via an enabler. The enabler can also have a file account set up for the insurance card and have permission granted for the institution card. Further information on RU-as-a-Service providers can be found here.

DiGA MIO Toolkit

The mio42 GmbH has specified a DiGA MIO Toolkit. All relevant information on this can be found here.

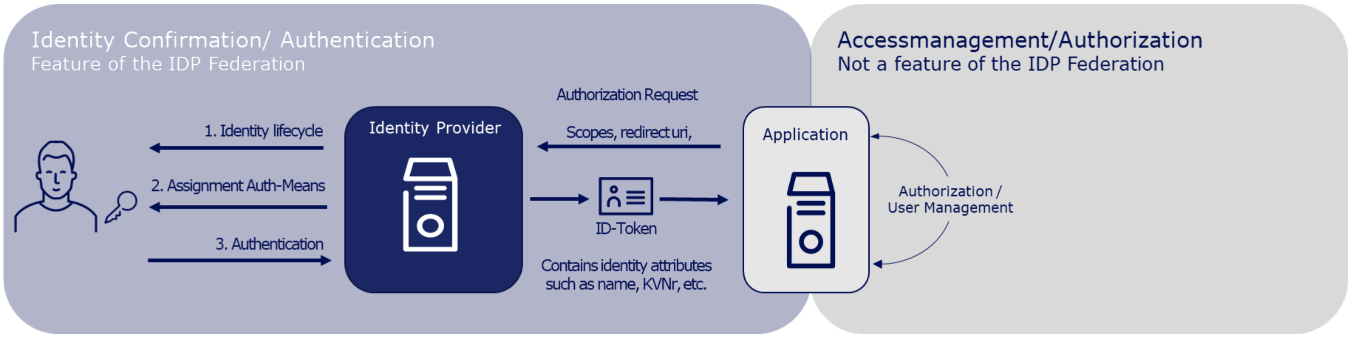
Registration at DiGA with the HealthID

From January 2024, DiGAs must offer a registration via the digital identities (HealthID) provided by the health insurance companies. This is stipulated in Annex 1 to the DiGAV in the data security category as item 15a. Since mid-2023, a so-called federation of sectoral Identity Providers (IDP) was gradually established according to the OpenID Connect standard. The sectoral IDPs manage the entire life cycle of the insured individuals' identities and, after successful authentication of the insured individual, provide identity confirmations to applications like a DiGA. Therefore, DiGA manufacturers can delegate user authentication to the IDP federation. After the authentication, they receive a DiGA- and user-specific pseudonym or, exclusively for writing care-relevant DiGA data into the user's ePA, the KVNR.

User management and authorization is not a feature of the IDP federation and remains the responsibility of the DiGA manufacturer.

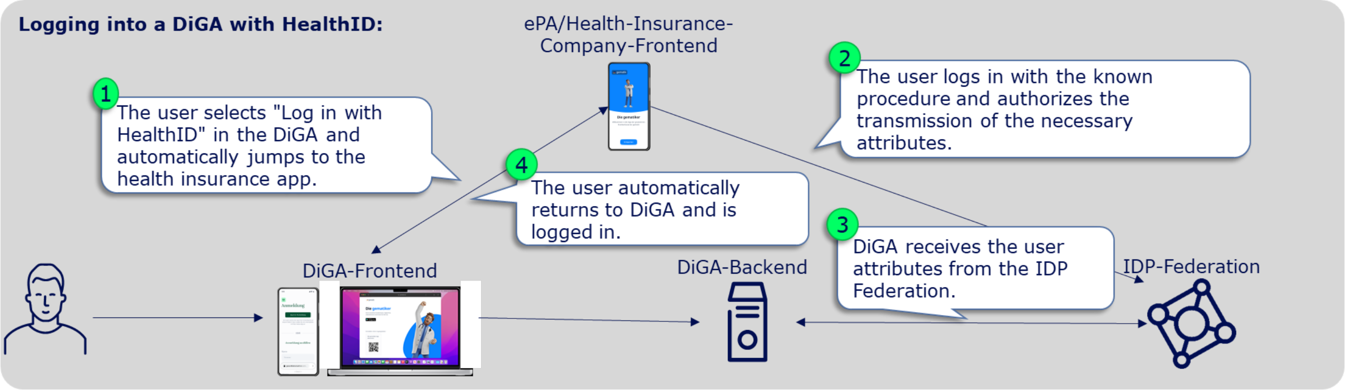
Further information on the IDP federation can be found in the IDP Knowledge Database of the gematik (Link).

Important: The logo for the HealthID is already available through the following link. It is designed for use in the frontend of your DiGAs to ensure a uniform identification and referencing of the HealthID.



Identity Confirmation/ Authentication
Feature of the IDP Federation
Accessmanagement/Authorization
Not a feature of the IDP Federation
1. Identity lifecycle
2. Assignment Auth-Means
3. Authentication
Identity Provider
Authorization Request
Scopes, redirect uri,
ID-Token
Contains identity attributes such as name, KVNr, etc.
Application
Authorization / User Management

Implementation of the Use Case



Logging into a DiGA with HealthID:
ePA/Health-Insurance-Company-Frontend
1
The user selects "Log in with HealthID" in the DiGA and automatically jumps to the health insurance app.
2
The user logs in with the known procedure and authorizes the transmission of the necessary attributes.
3
DiGA receives the user attributes from the IDP Federation.
4
The user automatically returns to DiGA and is logged in.
DiGA-Frontend
DiGA-Backend
IDP-Federation

DiGA are "Fachanwnedungen" (Relying Parties) in the sense of the IDP-Federation. All relevant information for "Fachanwendungen" in the IDP-Federation is bundled in the IDP knowledge base: Fachanwendungen der TI-Föderation

To integrate the HealthID/TI-Federation, the following specific steps are necessary:

1. Implementation of the HealthID in the test/reference environment:

First, the Health ID/TI-Federation must be integrated into the test/reference environment. TI-Federation professional services can use reference implementations and environments provided by the gematik for interoperability testing of their application. Information on this can be found in the IDP knowledge database: Fachdienste Test-Umgebungen.

As shown on the linked page, for some integration tests, it is necessary to register the Authorization Server of the DiGA in the TI-Federation. Only then will the professional service be recognized as a participant in the federation by all sectoral IDPs in the federation. Details on registration in the test/reference environment can also be found in the IDP knowledge database: Registrierung eines Fachdienstes in der TI-Föderation (für die Testumgebung (TU) und /oder Referenzumgebung (RU)).

As also described on Fachdienste Test-Umgebungen, the reference implementation of the gematik sectoral IDP is located in a restricted access network of the gematik. For this reason, the outbound IP of the DiGA manufacturer must be on the gematik's allowlist, or alternatively, the DiGA manufacturer must use an X-Auth header in their requests. This will be communicated by the gematik upon request at diga@gematik.de.

If an ID token issued by a sectoral IDP can be successfully decrypted, then the authentication process in the test environment has also been successfully completed. The final tests should not be conducted against the gematik sectoral IDP with its GSIA app but against a sectoral IDP approved by the gematik and its Authenticator app in the test environment. Currently, it is not yet possible to gain access to the Authenticator apps of the IDP providers. Further information will follow.

2. Confirmation as DiGA in the TI-Federation by the gematik

Once DiGA manufacturers have successfully tested the HealthID and retrieved an ID token, they must be confirmed by the gematik as a DiGA in the TI Federation. According to § 327 SGB V, confirmation by the gematik is required when components or products of the telematics infrastructure are used by further applications. The aim is to ensure in this way that the manufacturers meet the requirements specified by the gematik and maintain them during the confirmation period. The entire confirmation process from application to issuance of the confirmation notice can be found in detail at the following link, under "*Digitale Gesundheitsanwendungen (DiGA) Verfahrensbeschreibung Bestätigung Digitale Gesundheitsanwendungen*".

The requirements that a DiGA manufacturer must meet are summarized in an application profile (Anwendungssteckbrief). This can be found at the following link. DiGA manufacturers must provide evidence of meeting these requirements through self-declarations as part of the confirmation process. The gematik itself will not test the implementations of DiGA manufacturers. Applications for confirmation can now be made via the digital application portal of the gematik. A fee of €500 per DiGA for the confirmation process has been set (see "Gebührenübersicht Bestätigungsverfahren DiGA").

3. Proof of successful integration of the HealthID to the BfArM

The confirmation issued by the gematik in step 2 serves as proof to the BfArM for the HealthID implementation. By April 30, 2024, DiGA manufacturers must have successfully completed the gematik confirmation procedure for the use of components or products of the telematics infrastructure and submit the confirmation to the BfArM (see link). This also applies to DiGAs that are already listed.

4. Registration of the DiGA in the productive TI-Federation after successful listing in the DiGA directory

After DiGA manufacturers have demonstrated to the BfArM the successful integration of the HealthID through the confirmation issued by the gematik, they will be listed in the DiGA directory - provided all other requirements of the BfArM are met. After successful listing, the DiGA manufacturer can be registered in the productive TI Federation. The manufacturer must inform the BfArM within 6 weeks of receipt of the approval notice about the activation of the SMC-B and the successful IDP registration. If the DiGA is already listed, this must be done within 6 weeks after submitting the gematik confirmation (see link). Further information on the registration of DiGAs in the PU will be provided in due course.