gematik

A warm welcome

to the world of digital healthcare systems – communication using TI Messenger

This **Welcome Package** is intended to be used as 'step-by-step' guide to help you with onboarding the TI Messenger.

Overview

This document is intended to be a guide for potential manufacturers and providers of a TI Messenger (abbreviated to TI-M).

The TI Messenger is a secure, interoperable and trustworthy method of communication for instant messaging within the healthcare system.

This document first provides a basic overview of the process steps, from the orientation stage through to the accreditation procedure and successful commissioning. It also sets out a list of relevant documents that will provide you with additional information, as well as the forms you will need for the requests. Furthermore, it provides the names of the relevant contact persons for the individual process steps.

The information listed here is provided as a supplement to the informative and normative documents that have been published or provided by gematik on this topic.[1]

Note: The informative and normative documents are currently only available in German.

Nine steps to being approved as a manufacturer or provider of a TI Messenger

This Welcome Package will guide you through the process of onboarding a TI Messenger in the nine steps below:
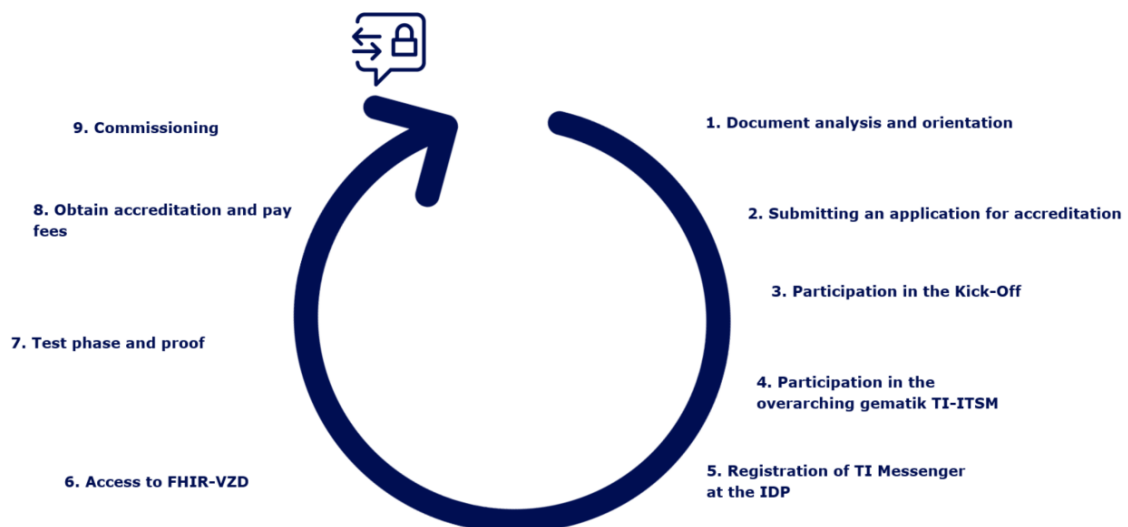
The steps are described in detail below, along with the names of the relevant documents, forms and contact people and the answers to some of the questions that are most often asked.

---

[1] This document (Welcome Package) is not normative.

Step 1: Document analysis and orientation

Before you contact gematik as a new manufacturer or a new provider of a TI Messenger, you can download various documents from the gematik Fachportal (professional portal)and discover the general terms and conditions applicable to you as a manufacturer or provider of a TI Messenger.

This document (Welcome Package) can be used as an introduction to the topic as it provides an initial overview of the key processes and useful sources of information on connecting your TI Messenger, putting them into the context of a time frame. Further information can also be found on the gematik Fachportal.

Procedure:

- ☐ View the initial documents in the Fachportal
- ☐ Learn about the onboarding process
- ☐ Clarify requirements
- ☐ Determine framework for costs and time

During the orientation phase, gematik will help you to further understand the framework conditions and the individual steps for onboarding a TI Messenger and will guide you through the onboarding process.

As part of the consultation your questions will be answered, any requirements discussed, the cost framework clarified and the procedure will be determined.

In order to be approved as a manufacturer or provider of a TI Messenger, a number of requirements must be met. These requirements are described in documents and also summarised in Step 2 'Submitting an application for accreditation.

Consideration of costs

The following cost item must be taken into account when connecting a TI Messenger.

Accreditation fees
gematik charges fees and expenses for carrying out the accreditation procedure in accordance with the 'Telematics Fee Ordinance' (Telematikgebührenverordnung). The specific fee is listed in the charge rate table, which can also be found in the product and provider accreditation application.

Relevant documents and corresponding links for Step 1:

Sozialgesetzbuch V (SGB V)
contains legal information about social security
regulationshttps://www.bmas.de/DE/Service/Gesetze-und-
Gesetzesvorhaben/sozialgesetzbuch-5-gesetzliche-krankenversicherung.html

TI Messenger procedure descriptions & overview of costs
▸ Procedure description Accreditation Product Type Backend and Client TI Messenger
  [gemZUL_Prod-TI-M]
▸ Procedure description Accreditation Provider Backend and Client TI Messenger
  [gemZUL_Anbieter]
https://fachportal.gematik.de/schnelleinstieg/downloadcenter/zulassungs-
bestaetigungsantraege-verfahrensbeschreibungen

Product type and provider requirements including performance & operational
specifications
▸ Product requirements TI Messenger Client [gemProdT_TIM_Client _PTV]
▸ Product requirements TI Messenger Backend [gemProdT_TIM_FD_PTV]
▸ Product requirements VZD-FHIR [gemProdT_VZD_FHIR_PTV]
▸ Provider requirements TI Messenger [gemAnbT_TIM_ATV]
▸ Specification performance [gemSpec_Perf]
▸ Operating concept Online productive operation [gemKPT_Betr]
▸ General guidelines for the operation of the TI [gemRL_Betr_TI]
https://fachportal.gematik.de/schnelleinstieg/downloadcenter/releases#c6503

Fees
▸ Overview of fees in the Fachportal:
https://fachportal.gematik.de/schnelleinstieg/downloadcenter/zulassungs-
bestaetigungsantraege-verfahrensbeschreibungen/kosten
▸ Telematics fees ordinance (Telematikgebührenverordnung) [TeleGebV]
https://www.gesetze-im-internet.de/telegebv/BJNR338200017.html

Frequently asked questions about Step 1:

Where can I find the gematik Fachportal and the relevant documents?
▸ You can find the Fachportal online at:
https://fachportal.gematik.de/

How can I search for specific documents in the Fachportal?
▸ Please use the document search to do this:
https://fachportal.gematik.de/dokumentensuche
▸ You can also make use of the download centre:
https://fachportal.gematik.de/schnelleinstieg/downloadcenter
▸ Or use the general search in the Fachportal via the search button at the top right.

Where can I find general information about TI Messenger?
▸ Comprehensive information about the TI Messenger can be found on the Fachportal at:
https://fachportal.gematik.de/anwendungen/ti-messenger#

Who is my contact person for advice about onboarding the TI Messenger?
▸ During the orientation phase, your contact person will be gematik's Transition Management department (transition@gematik.de).

What requirements do I have to fulfil as an applicant?
▸ Fundamentally, all requirements must be met. If you, as the applicant, recognise any requirements that you will only be able to fulfil at a later date, then you must inform us of this during the approval procedure. In each individual case, gematik will carefully examine whether a later check will be possible in this instance. gematik has the right to attach ancillary provisions to approvals, which then permit the corresponding requirement(s) to be fulfilled at a later date.

How long does the accreditation process take?
▸ The duration of the accreditation procedure will depend on the complexity of the documents to be checked, the number of other applications being made at the same time and the resources that are available. Experience tells us that an error-free accreditation process takes between 4 and 6 weeks after the test report of the independent testing has been made available.

Step 2: Submitting an application for accreditation

If you have decided to make your TI Messenger usable in the TI, submit an application to gematik for product or provider accreditation. gematik will check the information provided as part of the application for accreditation and will send you a confirmation, including a unique approval key, if it is complete.

Based on the fulfilment of the requirements, gematik assesses whether approval for the product or to be a provider of a 'TI Messenger' can be granted. The manufacturer or provider will provide the necessary proof to the gematik accreditation department as part of the accreditation procedure.

> *Procedure:*
>
> ☐ Fill out, sign and submit the product or provider accreditation application
> ☐ Submit supporting documents for the application for accreditation

Requirements for product accreditation of TI Messenger

As a manufacturer of a TI Messenger, you need the following for accreditation:

- Product accreditation application
- Manufacturer's declaration of functional and security suitability (implicitly completed with the application for product accreditation)
- Security assessment (procedure number as reference in the product accreditation application)
- signed root user confirmation and agreement to the TI-ITSM user agreement, signed service contract for the TI service portal
- Establishment of raw data delivery
- Test concept, test AFO matrix and test case specification
- Test protocols and test report of independent testing (EvT)

Requirements for TI Messenger provider accreditation

As a provider of a TI Messenger, you need the following for accreditation:

- Provider accreditation application
- Provider declaration of operational and security suitability (implicitly completed with the application for provider accreditation)
- Proof of an approved product by providing the procedure key (the product type version must be able to be approved or valid at the time of the provider accreditation application[2])
- Security assessment (procedure number as reference in the provider accreditation application)
- Contact person list in accordance with requirement GS-A_4088-01

---

[2] A possible update of the product to a higher, approved version is carried out independently of the accreditation as a provider, per operational change, and within an approved maintenance window. In this case, the product requires a new accreditation.

- Signed root user confirmation and agreement to the TI-ITSM user agreement, signed service contract for the TI service portal
- Provision of the operations manual
- Successful completion of the process testing
- Establishment of raw data and inventory data delivery
- Support for probing facility

Relevant documents and corresponding links for Step 2:

Accreditation, confirmation applications & procedural descriptions ('General Regulations' section)
  ‣ Superordinate procedure description for accreditation and confirmation procedures [gemZul_übergrVerf]
  https://fachportal.gematik.de/schnelleinstieg/downloadcenter/zulassungs-bestaetigungsantraege-verfahrensbeschreibungen

Procedure descriptions and applications for accreditation for the TI Messenger ('Applications' section and 'Backend & Client TI Messenger (V1.0.0)' subsection)
  ‣ Procedure description Accreditation Product Type Backend and Client TI Messenger [gemZUL_Prod-TI-M]
  ‣ Procedure description Accreditation Provider Backend and Client TI Messenger [gemZUL_Anbieter]
  ‣ Application for accreditation Product Type Backend and Client TI Messenger [gemZUL_Antrag_Prod_TI-M_FD_CM]
  ‣ Application for Accreditation Provider of a TI Messenger [gemZUL_Antrag_Anbieter_TI-M]
  https://fachportal.gematik.de/schnelleinstieg/downloadcenter/zulassungs-bestaetigungsantraege-verfahrensbeschreibungen

---

Frequently asked questions about Step 2:

Who is my contact person for product or provider accreditation?
  ‣ For accreditation your contact will be the gematik Accreditations department (zulassung@gematik.de).

Who is my contact for further information on the requirements?
  ‣ For further information on the requirements, please contact gematik's Transition Management department (transition@gematik.de).

What do I have to take into account as a manufacturer or provider regarding the security assessment?
  ‣ The security assessment confirmation is a separate, upstream procedure with a separate application. Without this confirmation it is not possible to grant product or provider accreditation.
  ‣ Security assessors need lead time! – Please commission in good time!
  ‣ The security assessor must provide proof of training conducted by gematik.
  ‣ An overview of TI safety assessors can be found in the 'List of confirmed security assessors' in the Fachportal under 'Security assessors' (https://fachportal.gematik.de/sicherheitsgutachter-1).

Step 3: Participation in the Kick-Off

gematik will be happy to support you during a preliminary meeting ('Kick-Off'). As part of this the procedure, key documents and processes are presented and any outstanding issues will be clarified. If required, gematik can also help you fill out the application for product or provider accreditation and answer other detailed questions. gematik will coordinate the kick-off date and invite you to attend in your role as the applicant. Participating parties on the part of gematik are:

> *Procedure:*
>
> ☐ Clarify outstanding issues
> ☐ Get to know contact persons and detailed processes
> ☐ Talk through project planning

- an accreditation manager for questions regarding the overall process and the product or provider accreditation procedure,
- a Transition Manager (TRM) to support the onboarding process as well as integration into the overarching gematik TI-ITSM and into operations (see also Step 4: Participation in the overarching gematik TI-ITSM),
- a Test Manager (TM),
- a security expert (SI),
- an operational architect (BA) for issues relating to operational framework conditions and aspects, and
- other gematik experts, if neccessary.

The contents of the Kick-off include:

- Presentation or status of the product or provider accreditation procedure and clarification of the basis for accreditation by the Accreditations department
  - Application (product or provider accreditation application)
  - Security assessment
- Documents to be submitted and proof to be provided by the applicant
  - Application for product or provider accreditation
  - Proof of approved product (for provider accreditation)
  - Current security assessment
  - Operations manual (for provider accreditation)
  - Contact person list (in accordance with GS-A_4088-01)
  - Signed root-user confirmation for TI-ITSM
  - Proof of successful process testing
  - Raw data and inventory data delivery (initially reference environment [RU])
  - Naming of the provider's subcontractors (according to A_23411)

- Outline project planning by the applicant (time frame, infrastructure, resources)
- Agreement on the mode of working and coordination and type of document exchanges
- Planning for the Production Environment (PU) after successful provider accreditation

> *Relevant documents for Step 3:*
>
> ‣ Your project planning and your outstanding issues
> ‣ Your list of contact persons for the accreditation process

> *Frequently asked questions about Step 3:*
>
> **Is participation in the Kick-Off compulsory?**
> ‣ Participation is not compulsory but is recommended, especially for new participants in the TI.

Step 4: Participation in the overarching gematik TI-ITSM

gematik has established a TI-IT Service Management (TI-ITSM) to report and eliminate faults. All general faults, including local faults, which have overarching effects must be recorded in this TI-ITSM.

In most cases this is used to report faults that you report to other service providers. This is mostly necessary if the provision of your own service is dependent on this/these fault(s).

Depending on the priority of the fault report, response times have been agreed with the TI-ITSM participants within the Service Level Agreement (SLA). In the TI-ITSM system, response times are therefore measured automatically in order to assess compliance with the agreed service levels and make a comparison

> *Procedure:*
>
> ☐ Download gematik e-mail certificate
> ☐ Request participation in the TI-ITSM
> ☐ Conclude the TI-ITSM systems user agreement
> ☐ Provide email certificates for secure communication
> ☐ Make an appointment for advice on use
> ☐ Make your own e-mail certificate available in the knowledge base

with the agreed response times. You will be assessed on the values that are determined by this and specifically with regard to your compliance with the reaction times.

Access to the TI-ITSM tool is also linked to access to the TI knowledge base. This is where, in addition to information pertaining to your business, you can also retrieve further certificates for secure e-mail communications that you need to participate in the TI-ITSM.

In the TI knowledge base you can also find numerous training videos on how to use the TI-ITSM system. If you have any further questions, please contact Transition Management.

Encrypted e-mail communication

The exchange of information with gematik via e-mail must be encrypted and signed (via S/MIME – Secure/Multipurpose Internet Mail Extensions). This ensures that no unauthorised people are able to gain knowledge of any faults in the TI, especially in the event of security incidents. Furthermore, this prevents the manipulation of e-mails. The authenticity of the sender can therefore be proven.

Upon receipt of the TI-ITSM information package, you should immediately download the mail certificate for the address transition@gematik.de from here: https://www.globaltrustpoint.com/. After correctly importing the certificate, you will be able to verify the authenticity of e-mails from this sender.

In return you must apply for S/MIME certificates for all of the e-mail addresses that you designate and then make them available at https://www.globaltrustpoint.com/ and in the TI knowledge base. Transition management will be able to support you with this.

Setup of TI-ITSM

In order to participate in the TI-ITSM, service requests must be made for the organisation, the assignment group, the product and logical product instances (reference environment

(RU), test environment (TU), production environment (PU)). After creating the organisation and assignment group, the users that you have designated in the root user confirmation are assigned and configured with the corresponding rights. This is completed for you by Transition Management. You can then make further service requests for the product, the logical product instances, access to the FHIR-VZD and an order for the reference implementations (Backend, Clients) in the TI-ITSM itself. gematik Transition Management will be able to provide you with support regarding the set-up and configuration.

Relevant documents for Step 4:

‣ User agreement TI-ITSM systems
‣ Service contract for the TI service portal
‣ Root user confirmation

Frequently asked questions about Step 4:

Who is my contact person for the TI-ITSM and can they advise me on use?
‣ For the TI-ITSM, your contact person is the Transition Manager (transition@gematik.de) who was appointed to you at the Kick-Off.

Where can I find the ITSM Systems User Agreement, the Service Contract for the TI Service Portal and the Root User Confirmation?
‣ You will receive the user agreement from gematik after you have applied for TI-ITSM access.

How do I get an account for the TI-ITSM system?
‣ Your contact at Transition Management will apply for a root user account for your organisation with the responsible service provider. This user is then able to set up other users for your organisation. When applying for the root user account with the responsible service provider of the TI-ITSM system, gematik takes on the role of an advocate.
‣ You will receive information on usage from your Transition Management once you have set up your permissions.

How can I access the TI-ITSM system?
‣ Access to the system is online (https://www.ti-itsm.de/).
After entering the password you will receive an OTP code (one-time password code) by e-mail.
After entering the OTP code please select the option 'TI-ITSM-System (Production)' or Arvato TI-Serviceportal Frontend (Production) (which is required for VZD [Directory] registration).

Where can I find the TI knowledge base?
‣ The TI knowledge base can be accessed at: https://gematikde.sharepoint.com/sites/Wissensdatenbank-TI. For this you will need a user account (applied for with TI-ITSM access).

Step 5: Registration of TI Messenger at the IDP

If you would like to provide the TI Messenger, then the TI Messenger backend must be enabled to redeem tokens (id_token) at the IDP so that registration of TI Messenger users can be performed (application case 1 from [gemSpec_TI-Messenger-Service]).

A completed Scope registration already exists for this purpose, which is why you might still need to apply for a Client ID. In this regard, the registration form for TI Messenger already focuses on the key information.

> **Procedure:**
>
> ☐ Registration information
> ☐ Request registration
> ☐ Registration data implemented

Registration TI Messenger at the IDP – Application

Service environment	RU
Request type	New installation
For which application do you need the backend registration? (short description of the application case)	n-Messenger
	The Registration Service as a subcomponent of a TI-M backend of a TI Messenger manufacturer (reference Environment – RU) or TI Messenger provider (Production Environment – PU) requires confirmation from the customer that they are ordering the Messenger service for a healthcare organisation within the framework of the ordering process for a Messenger service. Confirmation shall be provided by the healthcare system through OIDC authentication using the SMC-B.
expected enquiries (per 5 minutes)	10
Applicant	*Name Surname of applicant*
	Organisation name
	Street Building number
	Postcode City
	E-mail address of applicant
URI of the backend (redirect_uri; for the redirect from the IDP to the backend)	*Redirect_URI_ED*

Applicant:

We will need the name, address and e-mail address of the applicant in order to be able to assign requests, for getting in touch, for queries, etc.

Reply URL (redirect_uri; for the redirect from the IDP to the backend):

The Redirect URI is the endpoint to which the IDP service sends its response. The authenticator sends the authorisation code generated by the IDP service to this address, i.e., the application front end for the backend has to be able to accept the authorisation code at this address. You must therefore specify a valid URI here.

The Client ID is registered to this redirect_uri. The Client ID is assigned by gematik and will be provided to you in an overview once this registration has been completed.

redirect_uri: For each application front end that needs to be registered, 1-* (one to many) redirect_uris shall be specified. The IDP service uses the registered 'redirect_uri' to perform a redirection. In doing so the 'AUTHORIZATION_CODE' that has been issued is forwarded from the Authenticator module to the application front end that is using this URI. The IDP checks the redirect_uris that have been supplied by the Client against the registered redirect_uris. The format MUST be a valid URI in accordance with RFC 3986 and must start with 'http' or 'https' accordingly.

The TI Messenger data that has already been registered on the IDP service is as follows:

TI Messenger registration in the reference environment (RU)	
URI_FD (aud)	https://gematik.tiin.ti-dienste.de
Scope	ti-messenger
Claims	o professionOID o Organisation name o ID number (TelematicsID)
Backend ID	ti-messenger-fd-tu
Duration of an issued Access Token	300 seconds

Please send the completed form by e-mail to idp-registrierung@gematik.de. You will receive the following TI Messenger registration information back after approx. 5 working days:

- Generated Client ID
- Redirect URI (as reported by the applicant)
- Download point of the Discovery document

Frequently asked questions about Step 5:

Who is my contact person for IDP registration?
‣ Your contact person is the Transition Manager (transition@gematik.de) who was appointed to you at the Kick-Off.
‣ You can also additionally contact idp-registrierung@gematik.de if you have any questions.

Where can I get the TI Messenger registration form?
‣ You can get the form through your designated Transition Manager or by sending an enquiry to idp-registrierung@gematik.de.

Step 6: Access to FHIR-VZD

To access the FHIR-VZD, the 'VZD token registration' service must be ordered in the TI-ITSM. By using this service the provider of a TI Messenger backend (TI-M Provider) receives access data for the maintenance interface of the Messenger service entries (domains). The necessary access data for the TI provider authentication interface of the Directory service (FHIR-VZD) is provided to you for this purpose.

Procedure:

- ☐ Access to TI-ITSM
- ☐ Submit service request for FHIR-VZD in TI-ITSM
- ☐ Access to PMS
- ☐ Retrieve signature certificate

The service includes the registration or de-registration of a participant as an authorised organisation with the FHIR-VZD of the service provider. The service request must be made on a per environment basis (reference environment, test environment, production environment – RU/TU/PU) and has an SLA [Service Level Agreement] of 5 working days.

You additionally need a signature certificate that has been issued by a registration service for an actor assigned the role of 'Org-Admin'. This should be retrieved in the PKI Management System (PMS). In order to be able to retrieve the signature certificate, a user account and authorisations first need to be requested via additional service requests for the organisation and the user (root user only) in TI-ITSM.

- Information in the PMS: OID (TI-M: oid_tim) and FQDN as Common Name (CN)
- Provision in PMS: certificate is provided as a download

The CA certificate for the gematik telematics infrastructure that is associated with the signature certificate can be downloaded from public download points.

RU: https://download-ref.tsl.ti-dienste.de/ and https://download-ref.tsl.ti-dienste.de/ECC/
TU: https://download-test.tsl.ti-dienste.de/ and https://download-test.tsl.ti-dienste.de/ECC/
PU: https://download.tsl.ti-dienste.de/ and https://download.tsl.ti-dienste.de/ECC/

Frequently asked questions about Step 6:

Who is my contact person for the use of TI-ITSM and PMS?
▸ For TI-ITSM and PMS, your contact person is the Transition Manager (transition@gematik.de) who was appointed to you at the Kick-Off.

How can I access the TI-ITSM system?
▸ Access to the system is online (https://www.ti-itsm.de/).
  After entering the password, you will receive an OTP code (one-time password code) by e-mail.
  After entering the OTP code, please select the option 'TI-ITSM-System (Production)' or Arvato TI-Serviceportal Frontend (Production) (which is required for FHIR-VZD registration).

How can I access PMS?
▸ Access is online at:
  RU/TU: https://www-testref.tms.ti-dienste.de/
  PU: https://www.tms.ti-dienste.de/

Step 7: Test phase and proof

Order test cards

TI Messenger Clients require test identities (SMC-B/HBA cards). Test cards for manufacturers can be ordered via the webshop on the Fachportal. When ordering, manufacturers will receive an order reference that can be used in the event that they have any queries.

<div style="border:1px solid #000; padding:10px;">

Procedure:

- ☐ Order test cards
- ☐ Carry out independent testing in the reference environment (RU)
- ☐ Deliver raw data
- ☐ Use of the test suite
- ☐ Designation of a reference authority
- ☐ Submit a security assessment

</div>

Independent testing

The functional tests of the TI Messenger are carried out by the manufacturer in the reference environment (RU) as part of the product accreditation process. By this phase the raw data must be delivered to the Operating Data Recording (BDE). The relevant manufacturer is responsible for this as at this point in time, i.e., in the RU, the provider is not yet active. The applicant shall draw up a summary of the successful testing in the signed test report for the independent testing, which shall be submitted to the test manager along with test protocols. It is mandatory for the applicant to use an instance of the TI Messenger reference implementation when carrying out the independent testing.

Raw data delivery

Each provider usually operates several physical product instances (real or virtual). The combination of a provider's product instances form a logical product instance. With regard to TI Messenger raw data delivery, each provider delivers the raw data under its logical product instance (a CI-ID, assigned by gematik in the TI-ITSM) and aggregated across all physical instances. In principle, raw data is reported every 5 minutes.

The manufacturer is responsible for ensuring that the product is able to provide correct raw data. The provider must configure the product so that this raw data is delivered to the Operating Data Recording at the correct intervals.

Since experience has shown that initial start-up difficulties can happen with the delivery and formatting of the raw data files, gematik recommends starting with the delivery of raw data at an early stage. Tests are only started when raw data delivery is activated.

Use of the gematik test suite

gematik provides a test suite for automated tests of the TI Messenger. The TI Messenger Test Suite is used to test instances of TI messengers against each other via the test driver interface. The focus of the test suite is on interoperability tests of different TI Messenger instances.

The use of the test suite is not mandatory. However, it is recommended that you test your TI Messenger using the test suite before the gematik accreditation tests are carried out. For the accreditation tests gematik will also use the test suite for automated tests, i.e., by using the

test suite you will be given an opportunity to personally check in advance the quality of your TI Messenger in accordance with the accreditation tests.

The test-suite requires a certain number of clients to run the tests, especially for the group chat. Fundamentally, at least three devices must be available at each interface (e.g. 3x IOS clients, 3x Android clients, 3x Windows clients, etc.). The Org-Admin is an exception to this rule; in this instance, one device is sufficient.

On the gematik GitHub pages [(https://github.com/gematik/TI-Messenger-Testsuite)](https://github.com/gematik/TI-Messenger-Testsuite) the test suite is described in detail and available for download.

Tests using the reference implementation

gematik provides a TI Messenger service reference implementation. To ensure interoperability between different TI Messenger backends within the TI Messenger service, the TI Messenger service (TI Messenger Client and TI Messenger backend) of a TI Messenger manufacturer must be tested against the reference implementation (TI Messenger Client and TI Messenger backend).

In TI-ITSM you can execute the following orders for the reference instances via a service request:

- TI Messenger backend with quantity and runtime
- TI Messenger Client (different types: Windows, Web, Android, iOS) with quantity and runtime
- Change of order for quantity and runtime (backend and Client)

Once the order has been processed, you will be contacted directly for delivery of the order. gematik will invoice you accordingly for the duration of use.

Security assessment for the product and the provider

Security assessments must be submitted to the gematik accreditations department for proof of suitability in terms of security. A security assessment must be prepared for the product and for the provider in each instance. The security assessments are reviewed by gematik's Data Protection & Information Security department and the respective result will be summarised and provided in a test report. In the event that the result is positive, a confirmation based on the test report is issued in a separate procedure.

Further details on the security assessment are regulated in the relevant normative documents and guidelines (product or provider requirements and normative body text in the TI Messenger specification, 'Confirmation of security assessment', 'Guideline for testing security suitability'), in which the requirements for the testing process and for the security assessment are laid out. The security assessments to be submitted must be prepared by security assessors that have been accredited by gematik and who have been specifically named on the list on the gematik Fachportal.

Operations manual for the provider

For proof of operational suitability, the provider must submit an operations manual to the gematik accreditations department. The requirements that are assigned in the provider

requirements to the operational suitability of the 'operational manual' must be demonstrated in the operational manual that is to be submitted. The requirements are taken from the general documents (reference in Source column) and included in the TI Messenger provider requirements and are described in more detail in the source documents. The scope and content of the Operations Manual is as defined in the Operations Directive.

The Operations Manual is audited by gematik's Operations & Information Security department and the respective result is summarised in a test report.

Process testing for the provider

For proof of operational suitability, the provider must carry out a process test with gematik. The requirements that are assigned in the provider requirements to the operational suitability of the 'process test' must be proven in a gematik process test. The requirements are taken from the general documents (reference in Source column) and included in the TI Messenger provider requirements and are described in more detail in the source documents.

The process testing is audited by gematik's Operations & Information Security department and the respective result is summarised in a test report. For the preparation and organisation of the process test, please contact Transition Management.

Relevant documents and corresponding links for Step 7:

Accreditations and confirmations
‣ Confirmation of security assessments for accreditations [gemZul_Best_SiGu]
https://fachportal.gematik.de/schnelleinstieg/downloadcenter/zulassungs-bestaetigungsantraege-verfahrensbeschreibungen

Guidelines on testing security suitability
‣ Guidelines on testing security suitability [gemRL_PruefSichEig_DS]
https://fachportal.gematik.de/sicherheitsgutachter-1

Provider requirements including performance & operational specifications
‣ Provider requirements [gemAnbT_TIM_ATV]
‣ General operation documents [gemKPT_Betr], [gemRL_Betr_TI], [gemSpec_Perf]
https://fachportal.gematik.de/schnelleinstieg/downloadcenter/releases#c6503

Frequently asked questions about Step 7:

Who is my contact person during the test phase and the use of the test-suite and reference instance?
- During the tests your contact person is the gematik test manager that has been assigned to you (testmanagement@gematik.de).
- You can send subject-specific test topics to a group mailbox: VL_Test_TI_Messenger@gematik.de

How do I access the webshop on the Fachportal?
- Access to the webshop is online at: https://fachportal.gematik.de/gematik-onlineshop.

How can I receive detailed information on the subject of test cards?
- The information can be found online at: https://fachportal.gematik.de/toolkit/testkarten.

Which test cards need to be ordered?
- 1. 'TestCard SMC-B G2.1 Hospital' or 'TestCard SMC-B G2.1 Doctor's office' (1x for OrgAdmin interface)
- 2. 'TestCard HBA G2.1 Doctor' (3x per interface)

Are digital certificates (PEM files) also available for the test cards?
- If required, please send a request for the test cards that were ordered along with the order number by e-mail to transition@gematik.de.

How can I access gematik's GitHub regarding the test suite?
- The system is accessed online: https://github.com/gematik/TI-Messenger-Testsuite.

How can I access the TI-ITSM system for ordering a reference instance?
- Access to the system is online (https://www.ti-itsm.de/). After entering the password you will receive an OTP code (one-time password code) by e-mail. After entering the OTP code please select the option 'TI-ITSM system (production)' and go to Service catalogue/Direct catalogue request/TI-ISTM provider/TI-ITSM provider Akquinet, where you will find the service for ordering the reference instance.

Where can I find information on the topic of security assessments?
- You can find general information on the security assessment and on certified security assessors in the Fachportal at: https://fachportal.gematik.de/informationen-fuer/sicherheitsgutachter.

Where can I find information on the scope and content of the operations manual?
- You will find information about this in the Operations guideline [gemRL_Betr_TI], which can be accessed in the Fachportal and is also delivered with the provider requirements.

How can I prepare for process testing?
- You can find training videos on the subject of TI-ITSM (CIS) processes in the TI knowledge base at: https://gematikde.sharepoint.com/sites/Wissensdatenbank-TI.

Step 8: Obtain accreditation and pay fees

gematik grants product or provider accreditation when all requirements have been met by the manufacturer or provider and the necessary proof has been provided.

As a manufacturer or provider, you will receive a product or provider accreditation notice from gematik. Should there be a need to put restrictions with regard to the accreditation in place, which shall be done within the framework of ancillary provisions.

gematik charges fees to implement the accreditation procedures. The amount of the fees can be found in the applications for accreditation.

Procedure:

☐ Obtain product or provider accreditation
☐ Take note of any potential ancillary provisions
☐ Pay fees
☐ Plan TI Messenger commissioning for production environment (PU)

Relevant documents for Step 8:

▸ Product accreditation notice
▸ Provider accreditation notice
▸ Potential ancillary provisions
▸ Notice of fees

Step 9: Commissioning of TI Messenger

The commissioning of your TI Messenger in the Production Environment (PU) must be carried out according to the concept of 'Controlled Commissioning' (KIB). This sets out the scope that an applicant must demonstrate in order to be granted accreditation for online productive operation, as well as the reporting obligations that they have in regard to gematik so that they can demonstrate the implementation and results of this commissioning.

Procedure:

- ☐ Check KIB concept
- ☐ Prepare and submit implementation description
- ☐ Carry out KIB

While the accreditation tests demonstrate the functionality of the TI Messenger Client and the TI Messenger backend in the reference environment (RU), the intention of the KIB is to ensure that the functionality and interoperability of the TI Messenger Client and the TI Messenger backend are also provided after a change has been made to the production environment (PU). The aim of the KIB is therefore to verify the functionality and interoperability of the TI Messenger Client and the TI Messenger backend within a real healthcare environment, i.e., in the productive environment of the participating healthcare provider institutions (LEI) and hospitals. The defined use cases are carried out to verify the objectives.

Only once the KIB has been successfully passed will the KIB ancillary provision no longer apply and you may begin with regular PU operation of your TI Messenger.

Relevant documents and corresponding links for Step 9:

Concept for controlled commissioning of TI Messenger
▸ KIB [gemKPT_Commissioning_TI-Messenger]
https://fachportal.gematik.de/schnelleinstieg/downloadcenter/zulassungs-bestaetigungsantraege-verfahrensbeschreibungen#c3419

https://fachportal.gematik.de/fileadmin/Fachportal/Downloadcenter/Antraege_Verfahrensbeschreibungen/Anwendungen/gemKPT_Inbetriebnahme_TI-Messenger_V1.0.0.pdf

---

Frequently asked questions about Step 9:

Who is my contact person for commissioning?
▸ For commissioning, your contact person is gematik's Transition Management (transition@gematik.de).

Abbreviations

Abbreviation	Explanation
TI	Telematics infrastructure
TI-M	TI Messenger
TI-ITSM	IT Service Management of TI
PU	Production environment
TU	Test environment
RU	Reference environment
SMC-B	Type B security module
HBA	Health Professional Card
EvT	Independent testing
IDP	Identity provider
VZD	Directory service
FHIR	Interoperability standard for the exchange of public health data
CI-ID	Configuration item ID in TI-ITSM
LEI	Healthcare provider institutions
KIB	Controlled commissioning
PMS	PKI management system