

Telematikinfrastruktur 2.0

Spezifikation: TI-Flow-Fachdienst

Version:	1.0.0
Revision:	1742796
Stand:	02.10.2026
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_FD_TI-Flow

Dokumentinformationen

Gender-Hinweis

Aus Gründen der besseren Lesbarkeit wird in diesem Dokument überwiegend die männliche Form verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Änderungen zur Vorversion

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

Es handelt sich um die Erstversion des Dokumentes.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	02.10.2026		Erstellung der Spezifikation: TI-Flow-Fachdienst	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments.....	5
1.1 Zielsetzung.....	5
1.2 Zielgruppe.....	5
1.3 Geltungsbereich.....	5
1.4 Abgrenzungen.....	5
1.5 Methodik.....	6
2 Systemüberblick.....	7
3 Systemkontext.....	10
3.1 Nachbarsysteme.....	10
3.2 Akteure und Rollen.....	11
3.2.1 Herstellung und Betrieb.....	11
3.2.1.1 Hersteller des TI-Flow-Fachdienst.....	11
3.2.1.2 Anbieter TI-Flow-Fachdienst.....	12
3.2.1.3 Anbieter HCC-Plattform (HCC-Provider).....	12
3.2.1.4 gematik.....	12
3.2.1.5 Clientsystem-Hersteller.....	12
3.2.2 Nutzer des Dienstes.....	12
3.2.2.1 Akteure der Workflows.....	12
3.2.2.2 Versicherte.....	12
4 Datenschutz und Informationssicherheit.....	14
5 Übergreifende Festlegungen.....	18
5.1 Sicherheit.....	18
5.1.1 Allgemeine Sicherheitsanforderungen.....	18
5.1.2 Identifikation eines Clientsystems.....	18
5.1.3 Sicherheit der Netzübergänge.....	19
5.1.4 Nutzung Vertrauenswürdige Ausführungsumgebung.....	20
5.1.5 Speicherung Schlüsselmaterial.....	21
5.1.6 gematik-Logdaten zum Zwecke der gesetzlichen Kontrollpflichten der gematik.....	21
5.2 Integration in HCC-Plattform.....	22
5.3 Systemprotokolle.....	22
5.4 Zertifikatsprüfung.....	23
5.5 ZETA Guard im TI-Flow-Fachdienst.....	24
5.5.1 Konfiguration Ingress.....	25
5.5.2 Konfiguration PEP HTTP-Proxy.....	25
5.5.3 Konfiguration Authorization-Server.....	25
5.5.4 Konfiguration Telemetriedaten Service.....	26
5.5.5 Konfiguration Notification Service.....	26
5.6 Exporter.....	27

5.7 Vertrauenswürdige Uhrzeit im TI-Flow-Fachdienst.....	27
5.8 FHIR Validierung im TI-Flow-Fachdienst.....	28
5.8.1 Validierung bei Versionsübergängen.....	28
5.8.2 Architektur der Validierungskomponente.....	28
5.8.3 Konfiguration der Validierungskomponente des TI-Flow-Fachdienst.....	31
5.8.4 REST-Schnittstelle der Validierungskomponente des TI-Flow-Fachdienst.....	32
5.9 Konfiguration von Fachdienst-Instanzen.....	33
5.9.1 Konfiguration von Flowtypes.....	33
5.9.2 Konfiguration von Features.....	34
5.9.3 Konfiguration des Referenzzeitpunkts für die FHIR-Validierung.....	34
6 Anhang - Verzeichnisse.....	35
6.1 Abkürzungen.....	35
6.2 Glossar.....	38
6.3 Abbildungsverzeichnis.....	38
6.4 Tabellenverzeichnis.....	38
6.5 Referenzierte Dokumente.....	38
6.5.1 Dokumente der gematik.....	38
6.5.2 Weitere Dokumente.....	39

1 Einordnung des Dokuments

1.1 Zielsetzung

Die vorliegende Spezifikation definiert Anforderungen zu Herstellung und Betrieb des Produkttyps TI-Flow-Fachdienst.

Die Spezifikation wird ergänzt durch den Implementation Guide TI-Flow, in dem insbesondere die durch den TI-Flow-Fachdienst für Clientsysteme bereitgestellten Schnittstellen beschrieben sind.

1.2 Zielgruppe

Das Dokument richtet sich an den Hersteller des TI-Flow-Fachdienstes sowie an Hersteller und Anbieter von Clientsystemen des TI-Flow-Fachdienstes.

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 bekannt gegeben.

Wichtiger 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

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zum Themenbereich:

- Bereitgestellte Schnittstellen für Clientsysteme des TI-Flow-Fachdienstes
- Integration des TI-Flow-Fachdienstes als HCC-Dienst in die HCC-Plattform

Die Spezifikation TI-Flow-Fachdienst basiert im fachlichen Umfang auf der mit den Gesellschaftern abgestimmten Spezifikation des E-Rezept-Fachdienst. Für die geplanten Featureerweiterungen wie bspw. Verordnungen für Häusliche Krankenpflege (HKP), Betäubungsmittel (eBtM), Hilfsmittel und E-Überweisung (eÜ) sind die Abstimmungen mit

den Gesellschaftern noch nicht abgeschlossen. Die Spezifikation wird nach Freigabe der Featurespezifikationen durch die Gesellschafter erweitert.

1.5 Methodik

Anforderungen / Anwendungsfälle

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

Anforderungen und Anwendungsfälle werden im Dokument wie folgt dargestellt:

<ID> - <Titel der Anforderung / Titel des Anwendungsfalles>

Text / Beschreibung

[<=]

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

Hinweise auf offene Punkte

Themen, die noch intern geklärt werden müssen oder eine Entscheidung seitens der Gesellschafter erfordern, sind wie folgt im Dokument gekennzeichnet:

Beispiel für einen offenen Punkt.

2 Systemüberblick

Der **TI-Flow-Fachdienst** verwaltet verschiedene Workflows von Anwendungen der Telematikinfrastruktur als ein zentraler Ressourcenserver auf Basis des FHIR-Standards mit einer RESTful API.

Die Workflows werden dabei über eine eindeutige Ressourcen-ID (Task-ID) adressiert. Für jeden Workflow ist ein Statusmodell spezifiziert. Der TI-Flow-Fachdienst verwaltet die Statusübergänge und stellt die Zulässigkeit der durch Nutzer initiierten Statusübergänge sicher.

Der TI-Flow-Fachdienst protokolliert alle Zugriffe auf einen Workflow für den dem Workflow zugeordneten Versicherten.

Der TI-Flow-Fachdienst stellt sicher, dass die Daten nur entsprechend der gesetzlich zulässigen Speicherdauer vorgehalten werden.

Der TI-Flow-Fachdienst bietet seine Außenschnittstellen im Internet an und setzt für die Authentisierung und Autorisierung von Clientsystemen Zero Trust Access (ZETA) Mechanismen um.

Der TI-Flow-Fachdienst unterstützt eine asynchrone Übermittlung von Daten an Drittsysteme (bspw. ePA Medication Service).

Der TI-Flow-Fachdienst realisiert die Vertraulichkeit und Integrität der verarbeiteten Daten über das Konzept der vertrauenswürdigen Ausführungsumgebung (VAU), die eine durchgängige Verschlüsselung der Verordnungen und der dazu gehörigen Daten aus einer Kombination kryptographischer Verfahren während des Transports, der vertrauenswürdigen Verarbeitung und in der verschlüsselten Persistierung der Daten sicherstellt. Dabei realisiert der TI-Flow-Fachdienst die VAU nicht selbst, sondern dadurch, dass der TI-Flow-Fachdienst auf einer durch einen **Healthcare Confidential Computing** (HCC)-Provider betriebenen HCC-Plattform läuft, welche auch für weitere Anwendungen der TI genutzt werden kann.

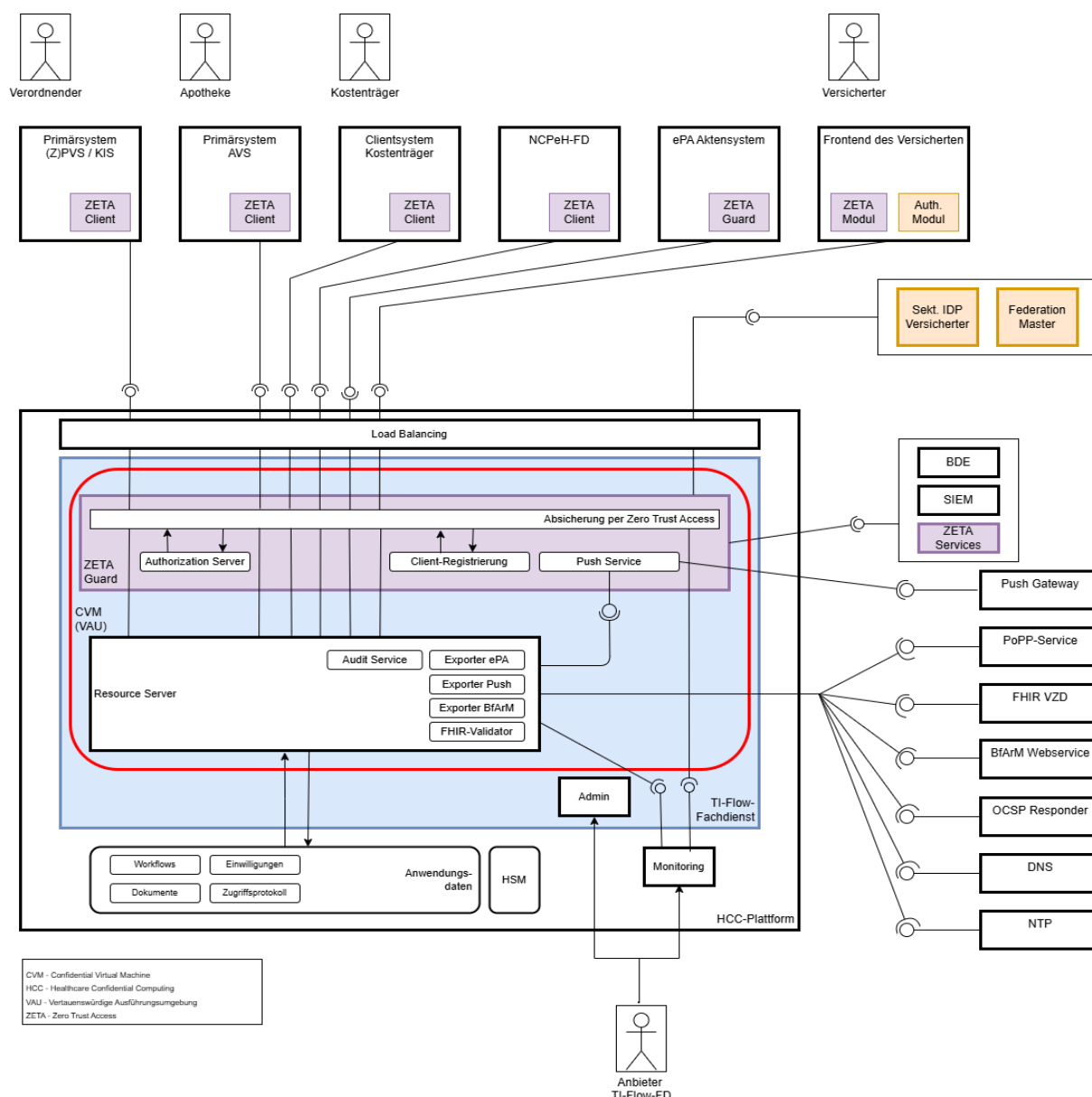


Abbildung 1: Systemüberblick TI-Flow-Fachdienst

Hinweis: Die Anbindung des TI-Flow-Fachdienstes an die ePA-Aktensysteme soll, wie in der Abbildung dargestellt, ab der Implementierung des ZETA Guards durch die ePA-Aktensysteme über den ZETA Guard erfolgen. Vor dieser Implementierung wird der TI-Flow-Fachdienst sich direkt über das Internet mit dem ePA-Aktensystem verbinden. Hierbei wird die mit dem E-Rezept-Fachdienst etablierte Authentisierung auch für den TI-Flow-Fachdienst genutzt.

Die durch den TI-Flow-Fachdienst unterstützten Workflow-Typen sind in Implementation Guides beschrieben. Der zur initialen Umsetzung des TI-Flow-Fachdienstes spezifizierte Umfang wird schrittweise um weitere Workflowtypen erweitert. Hierbei wird angestrebt, die fachlichen Anforderungen mit bereits bekannten Pattern umzusetzen. Dazu zählen bspw.

- FHIR-Validierung
- Übergangszeiten bei FHIR-Profilübergängen
- asynchrone Übermittlung zu Backendsystemen (bspw. zur ePA und zum BfArM)
- Anfrage-Workflow

- workflow-begleitende Dokumente

Diese Vorgehensweise soll die Umsetzung im TI-Flow-Fachdienst als auch bei den Clientsystemen beschleunigen.

3 Systemkontext

3.1 Nachbarsysteme

Betriebsdatenerfassung BDE

Managementsystem der gematik für Betriebsdaten von TI-Diensten

BfArM Webservice

Backend-System für den TI-Flow-Fachdienst. Der TI-Flow-Fachdienst übermittelt Daten zu eingelösten T-Rezepten an das BfArM.

Clientsystem des Kostenträgers

Das Clientsystem des Kostenträgers setzt die Bereitstellung von Freischaltcodes für Digitale Gesundheitsanwendungen um.

Domain Name Server (DNS-Server)

Namensdienst im Internet

ePA-Aktensystem

Der TI-Flow-Fachdienst übermittelt Verordnungsdaten und Dispensierinformationen von E-Rezepten an den ePA Medicationservice der Aktensysteme.

Federation Master

Federation Master des Identity Management der Telematikinfrastruktur

FHIR-VZD

Der TI-Flow-Fachdienst ermittelt am FHIR-VZD bspw. Informationen zu europäischen Ländern, welche ermöglichen, dass E-Rezepte im Szenario ePrescription/eDispensation Land A eingelöst werden können.

Frontend des Versicherten

Clientsystem des Versicherten zur Einsichtnahme seiner Daten am TI-Flow-Fachdienst und zur Kommunikation mit Leistungserbringern und Kostenträger im Rahmen der Workflow Anwendungsfälle.

HCC-Plattform

Die HCC-Plattform ist die Ausführungsumgebung des TI-Flow-Fachdienstes. Sie stellt dem TI-Flow-Fachdienst Mechanismen zur Umsetzung der Datenverarbeitung in einer VAU sowie Services wie bspw. Datenbankservices und HSM zur Verfügung.

NCPeH-FD

Der NCPeH-FD ist ein Clientsystem des TI-Flow-Fachdienst. Er übermittelt Anfragen zum Einlösen von E-Rezepten im Szenario ePrescription/eDispensation Land A.

Network Time Protocol NTP

Zeitdienst im Internet.

OCSP-Responder

OCSP-Responder im Internet, welche Informationen zur Gültigkeit von Zertifikaten bereitstellen.

PoPP-Service

Der TI-Flow-Fachdienst prüft von Clientsystemen übermittelte PoPP-Token. Hierfür bezieht der TI-Flow-Fachdienst Informationen zum Signaturzertifikat des Tokens vom PoPP-Service.

Primärsystem Apotheken

Primärsysteme (AVS) von Apotheken, welche die Verordnungen vom TI-Flow-Fachdienst abrufen, die verordnete Leistung erbringen und Dispensierinformationen im TI-Flow-Fachdienst bereitstellen.

Primärsystem verordnender Leistungserbringer

Primärsysteme (PVS/ZPVS/KIS) der Leistungserbringer, welche Verordnungen erstellen und in den TI-Flow-Fachdienst einstellen.

Push Gateway

Backend-System für den TI-Flow-Fachdienst. Der TI-Flow-Fachdienst übermittelt Informationen zu Notifications für das FdV des Versicherten an das für die FdV Instanz registrierten Push Gateway.

Security Information and Event Management SIEM

Security Information and Event Management Tool der gematik.

Sektoraler IDP Versicherter

Von den Kostenträgern betriebene sektorale IDPs für Versichertenidentitäten.

ZETA Service

Der ZETA Service stellt dem ZETA Guard regelmäßig Policy-Updates bereit, welche durch den Authorization Service im ZETA Guard angewandt werden.

3.2 Akteure und Rollen

Der TI-Flow-Fachdienst wird vom Anbieter TI-Flow-Fachdienst in der vom Anbieter HCC-Plattform bereitgestellten Infrastruktur im Internet betrieben. Es müssen für die verschiedenen Betriebsumgebungen (Produktivumgebung (PU), gemäß [gemKPT_Test] geforderten Test- und Referenzumgebungen (RU und RU-DEV)) in jeweils voneinander unabhängigen (virtuellen) Instanzen betrieben werden. Für die Absicherung gegenüber dem Internet wird der von der gematik beigestellte ZETA Guard verwendet.

3.2.1 Herstellung und Betrieb

3.2.1.1 Hersteller des TI-Flow-Fachdienst

Der Hersteller des TI-Flow-Fachdienstes implementiert und entwickelt den TI-Flow-Fachdienst gemäß [gemProdT_TI-Flow-FD].

Der Hersteller des TI-Flow-Fachdienstes übernimmt die Rolle HCC-Workload-Hersteller (siehe [gemSpec_HCC]).

3.2.1.2 Anbieter TI-Flow-Fachdienst

Der Anbieter TI-Flow-Fachdienst verantwortet und betreibt den TI-Flow-Fachdienst gemäß den Vorgaben der gematik. Der Anbieter TI-Flow-Fachdienst muss hierfür Dienste der HCC-Plattform nutzen.

Der Anbieter TI-Flow-Fachdienst übernimmt die Rolle des HCC-Dienstanbieters (siehe [gemSpec_HCC]).

Neben dem Betrieb von Instanzen für den Produktivbetrieb müssen weitere Instanzen für den Testbetrieb gemäß [gemAnbT_TI-Flow-FD] betrieben werden.

Der Anbieter TI-Flow-Fachdienst nimmt gemäß [gemAnbT_TI-Flow-FD] am TI-ITSM teil.

Der Anbieter TI-Flow-Fachdienst ist ein durch die gematik beauftragter Dienstleister.

3.2.1.3 Anbieter HCC-Plattform (HCC-Provider)

Der Anbieter HCC-Plattform verantwortet die HCC-Plattform gemäß den Vorgaben der gematik, auf der der TI-Flow-Fachdienst betrieben wird.

Der Anbieter HCC-Plattform stellt dem Anbieter TI-Flow-Fachdienst Dienste bereit, welche für das Deployment und den Betrieb des Fachdienstes genutzt werden.

3.2.1.4 gematik

Die gematik spezifiziert den TI-Flow-Fachdienst und schreibt die Entwicklung sowie den Produktivbetrieb des TI-Flow-Fachdienstes aus.

Die gematik unterstützt den Anbieter TI-Flow-Fachdienst durch die Beistellung des ZETA Guard. Darüber hinaus betreibt die gematik die Zero Trust Komponenten Policy Information Point (PIP) und Policy Administration Point (PAP): ZETA PIP und PAP-Service.

3.2.1.5 Clientsystem-Hersteller

Clientsystem-Hersteller setzen die TI-Flow-Client- inklusive ZETA Client/Modul-Funktionalität um. Sie nutzen die vom Anbieter TI-Flow-Fachdienst bereitgestellten Test- und Referenzumgebungen, um ihre jeweilige Umsetzung zu testen.

3.2.2 Nutzer des Dienstes

3.2.2.1 Akteure der Workflows

In der Spezifikation eines Workflow wird ein Statusmodell mit seinen Statusübergängen sowie die Akteure, welche diese Statusübergänge initiieren können, festgelegt.

Akteure sind bspw. (Zahn-)Arztpraxen, Krankenhäuser, Apotheken, Pflegeeinrichtungen, Kostenträger und Versicherte.

Die Akteure nutzen Clientsysteme, um auf die Daten des TI-Flow-Fachdienstes zuzugreifen. Der Datenzugriff von Akteuren im europäischen Ausland zum Einlösen von E-Rezepten wird über den NCPeH-FD geroutet.

Die deutschen institutionellen Akteure werden über ihre Telematik-ID identifiziert.

3.2.2.2 Versicherte

Ein Versicherter ist Begünstigter eines Workflows, bspw. als Empfänger der Leistung einer Verordnung. In der Spezifikation eines Workflows können Statusübergänge festgelegt werden, welche der Versicherte als Akteur durchführen kann.

Der TI-Flow-Fachdienst stellt dem Versicherten ein Zugriffsprotokoll bereit, welches die Zugriffe auf seine Daten dokumentiert.

Der Versicherte nutzt ein Frontend des Versicherten für den Zugriff auf den TI-Flow-Fachdienst.

Der Versicherte wird über seine Versicherten-ID (10-stelliger unveränderlicher Teil der Krankenversicherungsnummer (KVNR)) identifiziert.

Hinweis: Es ist geplant, die von der gematik zu erarbeitende anwendungsübergreifende Vertreterfunktionalität zu integrieren.

4 Datenschutz und Informationssicherheit

Der TI-Flow-Fachdienst zeichnet sich aus Datenschutz- und Informationssicherheitssicht insbesondere dadurch aus, dass er personenbezogene und personenbezogene medizinische Daten (Schutzbedarf Vertraulichkeit und Integrität „sehr hoch“) verarbeitet, ohne dass der Anbieter des TI-Flow-Fachdienstes eine Legitimation zum Zugriff auf diese Daten besitzt.

Da der TI-Flow-Fachdienst auf einer HCC-Plattform läuft, die von einem anderen Anbieter - dem HCC-Provider - betrieben wird, ergeben sich gegenseitige Abhängigkeiten bei der Realisierung von gesamtheitlich wirkenden Datenschutz- und Informationssicherheitsmaßnahmen.

Es müssen also technische und organisatorische Maßnahmen getroffen werden, um sowohl den Anbieter des TI-Flow-Fachdienstes als auch andere an der Zurverfügungstellung der TI-Flow-Fachdienst-Funktionalität beteiligte, vom Zugriff auf die im TI-Flow-Fachdienst verarbeiteten Daten auszuschließen.

Der TI-Flow-Fachdienst muss sich auf die für die Erbringung der Gesamtsicherheit erforderlichen Maßnahmen durch die HCC-Plattform verlassen können. Der Anbieter des TI-Flow-Fachdienstes erfüllt dabei seine Pflicht, wenn er den TI-Flow-Fachdienst ausschließlich auf einer HCC-Plattform zum Laufen bringt, die die gematik dafür als geeignet beurteilt hat. Zudem müssen sowohl der Hersteller als auch der Anbieter des TI-Flow-Fachdienstes die vom HCC-Provider bereitgestellten Leitlinien und Empfehlungen für die sichere Konfiguration, Installation und Nutzung der HCC-Plattform-Services für den TI-Flow-Fachdienst umsetzen.

Auf der anderen Seite darf ein HCC-Provider nur von der gematik als geeignet beurteilte Fachdienste auf seiner HCC-Plattform laufen lassen. Auf der technischen Seite wird dies durch eine Attestierung des TI-Flow-Fachdienstes beim Starten in der HCC-Plattform realisiert. Die dafür notwendigen Voraussetzungen werden in den Prozessen der Entwicklungs-Pipeline geschaffen.

Damit der TI-Flow-Fachdienst von der gematik als geeignet beurteilt werden kann, muss der Hersteller des TI-Flow-Fachdienstes (der zugleich auch der Anbieter des TI-Flow-Fachdienstes sein kann) die Qualität seines sicheren Entwicklungsprozesses durch ein Sicherheitsgutachten nachweisen und die Qualität des TI-Flow-Fachdienstes durch ein Produktgutachten.

Der Anbieter des TI-Flow-Fachdienstes (der zugleich auch der Hersteller des TI-Flow-Fachdienstes sein kann) weist seine Fähigkeit, den TI-Flow-Fachdienst sicher betreiben zu können, durch ein Sicherheitsgutachten und kontinuierlich durch die Integration in das Sicherheitsmanagement der gematik nach. Der Anbieter des TI-Flow-Fachdienstes ist aufgrund der Kritikalität des Dienstes und der Verantwortung der gematik für den Dienst dem Security Governance Level (SGL) 1 zugeordnet.

Der Anbieter TI-Flow-Fachdienst ist zusammen mit dem HCC-Provider gemeinsam datenschutzrechtlich Verantwortliche im Sinne Art. 26 DSGVO. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß der DSGVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. Die Vereinbarung muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung wird

der betroffenen Person zur Verfügung gestellt. Ungeachtet der Einzelheiten der Vereinbarung kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

Authentisierung und Autorisierung von Nutzern

Der TI-Flow-Fachdienst stellt sicher, dass ausschließlich die gesetzlich vorgesehenen Nutzer- bzw. Nutzergruppen auf die Daten zugreifen können, für die sie autorisiert sind. Umgesetzt wird dies einerseits durch die Zugriffsregeln im ZETA Guard und andererseits durch die statusabhängigen Zugriffsregeln im TI-Flow-Fachdienst. Die Authentisierungstärke ist für professionelle Nutzer (z.B. Leistungserbringer, Kostenträger) immer „gematik-ehealth-loa-high“. Versicherte können sich nach Einwilligung statt mit „gematik-ehealth-loa-high“ auch mit „gematik-ehealth-loa-substantial“ authentisieren. Die Zulässigkeit dieser Authentisierungsstärken wird von der gematik festgelegt und über die Policy im ZETA Guard durchgesetzt.

Authentisierung von Geräten

In Abhängigkeit vom Entwicklungsstand des ZETA Guard stellt dieser sicher, dass Nutzer nur mit registrierten und attestierten stationären und mobilen Clients auf den TI-Flow-Fachdienst zugreifen können. Die diesbezüglichen Policies sind anwendungsunabhängig und werden von der gematik festgelegt.

Ende-zu-Ende-Sicherheit

Zur Sicherstellung der Ende-zu-Ende-Sicherheit der Anwendungen, die den TI-Flow-Fachdienst nutzen, sind – neben der Maßgabe des Betreiberausschlusses bei der Verarbeitung der Daten (data in use) – alle Verbindungen zu Clients TLS- und ggf. (in Abhängigkeit des Schutzbedarfs der übertragenen Daten) zusätzlich ASL-verschlüsselt (data in transfer). Eine zusätzliche Verschlüsselung mittels ASL erfolgt in jedem Fall ausgehend von den Clients der Nutzer bis zum ZETA Guard im TI-Flow-Fachdienst. Dies ist dem hohen Angriffspotenzial des Internets geschuldet. Sollte der ZETA Guard und der Resource Server des TI-Flow-Fachdienstes in verschiedenen virtuellen Machines laufen, so erfolgt die Transportverschlüsselung zwischen den VMs mittels mTLS - also ohne zusätzlichen ASL. Damit wird der Betreiberausschluss gewährleistet und dem niedrigeren Angriffspotenzial der HCC-Provider-Betriebsumgebung Rechnung getragen. Perspektivisch erfolgt eine Migration auf Post-Quanten-TLS (PQC-TLS) sobald Implementierungen auf der Grundlage eines diesbezüglichen Standards verfügbar sind.

Die Speicherung von personenbezogenen medizinischen Daten erfolgt verschlüsselt, wobei die Verschlüsselung mit Schlüsseln erfolgt, auf die der Anbieter des TI-Flow-Fachdienstes selbst keinen Zugriff hat (data at rest).

Protokollierung und Monitoring

Der TI-Flow-Fachdienst protokolliert Daten für verschiedene Zwecke. Für Versicherte erfolgt eine Protokollierung der Zugriffe auf ihre Daten. Diese Protokolle können ausschließlich von den Versicherten selbst abgerufen werden (bzw. werden gemäß Referentenentwurf GDIG von der koordinierenden Stelle der gematik auf Anfrage eines Versicherten zur Verfügung gestellt). Zur Sicherstellung des Betriebs erfolgt einerseits eine Betriebsdatenerfassung (Telemetriedaten) für die gematik und andererseits führt der Anbieter des TI-Flow-Fachdienstes für seine betrieblichen Belange. In diesen Protokollen dürfen Identitäten natürlicher oder juristischer Personen ausschließlich pseudonymisiert erfasst werden. Der Anbieter des TI-Flow-Fachdienstes ist nicht in der Lage diese Pseudonyme aufzulösen. Die in den Daten der Betriebsdatenerfassung enthaltenen Pseudonyme können zweckgebunden durch die gematik aufgelöst werden. Der Zweck ist hierbei die Erkennung von Anomalien in der Verwendung der Anwendungen und ggf. die Möglichkeit für die gematik in Verdachtsfällen auf einzelne (professionelle) Nutzer zugehen zu können.

Neben der Protokollierung von Ereignissen, erfolgt eine sicherheitstechnische Überwachung des TI-Flow-Fachdienstes mittels Security Monitoring, das im ZETA Guard implementiert ist und Daten in Echtzeit an die gematik sendet, wo die Daten gesammelt und mit Security Monitoring Tools ausgewertet werden.

Drosselung bei Anomalie-Erkennung

Eine Anomalie-Erkennung findet auch im TI-Flow-Fachdienst selbst statt. Das Ausführen ausgewählter Anwendungsfälle wird sukzessive verzögert, wenn ein ungewöhnliches Nutzungsverhalten detektiert wird. DoS- bzw. DDoS-Angriffe werden an verschiedenen Stellen im Gesamtsystem (HCC-Plattform / ZETA Guard / TI-Flow-Fachdienst) abgewehrt.

Proof of Patient Presence (PoPP)

Der PoPP-Service erzeugt die Bestätigung eines Versorgungskontexts in Form eines kryptographisch gesicherten PoPP-Tokens. Dieses Token bestätigt, dass ein bestimmter Versicherter mit einer bestimmten LEI zusammengekommen ist. Im E-Rezept-Kontext wird der PoPP-Token im Anwendungsfall des Präsentierens der eGK in einer Apotheke zwecks Abrufs und Einlösung (vor Ort oder remote mit App) benötigt. Hierbei ist keine eGK-PIN-Eingabe durch den Versicherten erforderlich, um das Einlösen von E-Rezepten – auch durch Vertreter – möglichst niederschwellig zu gestalten. Das Verfahren kann zukünftig allgemein zum Einlösen elektronischer Verordnungen eingesetzt werden und auch mittels Gesundheits-ID genutzt werden.

Verifikations- und Prüfidentitäten

Die gematik besitzt eine Verifikationsidentität in Form einer SMC-B mit der sie sich in der Produktivumgebung ausweisen kann. Die Verwendung dieser Identität ist streng reglementiert. Mit dieser Identität kann die \$create-Operation ausführen und damit die Erreichbarkeit des TI-Flow-Fachdienstes auf der Ebene eines funktionalen Aufrufs verifizieren. Zur Ausführung anderer Operationen ist diese Identität nicht befugt.

Prüfidentitäten sind Identitäten fiktiver Versicherter, die insbesondere durch Dienstleister (vor Ort) zum Einsatz kommen, um das Funktionieren bestimmter Anwendungsfälle in der Produktivumgebung der TI aus Leistungserbringerinstitutionen heraus zu prüfen.

Der unveränderbare Teil der KVNR – die Versicherten-ID – der Prüfidentitäten entspricht einer bestimmten Bildungsregel, die von der gematik festgelegt ist. Die Versicherten-ID dient im TI-Flow-Fachdienst der Identifikation von Versicherten und der Zuordnung ihrer Daten. Dabei kann der TI-Flow-Fachdienst nicht feststellen, ob eine Versicherten-ID einer realen Person zugeordnet ist oder nicht. Er könnte zwar die Versicherten-ID einer Prüfidentität nach dem Muster der Bildungsregel identifizieren, aber bei von der Bildungsregel abweichenden fiktiven Versicherten-IDs könnte er diese nicht als Prüfidentität identifizieren.

Die aktuell spezifizierten Anwendungsfälle des TI-Flow-Fachdienstes lassen die Nutzung einer fiktiven Prüfidentität zu, ohne dass ein Schaden für Versicherte dabei entstehen kann.

Finanzielle Risiken entstehen u.U. für abgebende Leistungserbringer, falls für eine Prüfidentität ein E-Rezept eingestellt wurde, dass mit dieser Identität in einer Apotheke eingelöst wird.

Feature-Toggle

Feature-Toggle bieten eine Möglichkeit Funktionen vorzeitig in produktiven Code zu übernehmen, ohne diese direkt verfügbar zu machen. Sie bieten ebenso die Möglichkeit konfiguratив auf betriebliche Situationen durch An- oder Abschalten von Funktionen im laufenden Betrieb zu reagieren.

Sicherheitsrelevante Toggle dürfen nur nach Anweisung der gematik durch den Hersteller des TI-Flow-Fachdienstes umgestellt werden. Die dafür notwendigen Prozesse werden zwischen dem Hersteller des TI-Flow-Fachdienstes und der gematik vereinbart.

5 Übergreifende Festlegungen

5.1 Sicherheit

5.1.1 Allgemeine Sicherheitsanforderungen

A_29702 -TI-Flow-Fachdienst - Berücksichtigung OWASP-Top-10-Risiken

Der TI-Flow-Fachdienst MUSS Maßnahmen zum Schutz vor den OWASP-Top-10-Risiken in der aktuellen Version umsetzen.【<=】

Hinweis: Der Hersteller des TI-Flow-Fachdienstes muss die jeweils aktuellen OWASP Top 10 Risiken im TI-Flow-Fachdienst berücksichtigen, sobald diese veröffentlicht wurden.

Der TI-Flow-Fachdienst soll sich vor Anfragen, die nicht auf ein übliches Verhalten von Leistungserbringerinstitutionen und Versicherten während des Verordnungsprozesses schließen lassen, schützen. Diesen Anomalien wird mit einer Drosselung der Bearbeitungsgeschwindigkeit begegnet, um bspw. Brute-Force-Attacken auf das Erraten von AccessCodes für den Zugriff auf Verordnungsdaten unattraktiv zu machen.

A_29703 -TI-Flow-Fachdienst - Drosselung Brute-Force-Anfragen

Der TI-Flow-Fachdienst MUSS jede Antwort auf einen Funktionsaufruf, der einen nicht gültigen AccessCode oder ein nicht gültiges Secret enthält, um den http-Response-Header "Warning" (default "999 Throttling active") ergänzt und um ein konfigurierbares Zeitintervall (default: 500 Millisekunden) verzögert zurückschicken, um Brute-Force-Angriffe durch einen hohen Zeitaufwand unattraktiv zu machen.【<=】

A_29704 -TI-Flow-Fachdienst - Drosselung Fälschungen

Der TI-Flow-Fachdienst MUSS jede Antwort auf einen Funktionsaufruf, der einen Datensatz mit nicht gültig prüfbarer Signatur enthält, um den http-Response-Header "Warning" (default "999 Throttling active") ergänzt und um ein konfigurierbares Zeitintervall (default: 500 Millisekunden) verzögert zurückschicken, um Angriffe durch Fälschungen durch einen hohen Zeitaufwand unattraktiv zu machen.【<=】

Eine Anpassung der Konfigurationsparameter erfolgt in Absprache mit der gematik im Vorfeld des Build zu einem Release. Die Konfigurationsänderung erfolgt nicht zur Laufzeit.

A_29705 -TI-Flow-Fachdienst - Konfiguration und Deaktivierung Drosselung

Der Hersteller des TI-Flow-Fachdienstes MUSS die Funktion der Drosselung sowie die Konfiguration auf Weisung der gematik aktivieren oder deaktivieren bzw. die Konfigurationsparameter anpassen, um die Wirksamkeit des Mechanismus im Feld bei Bedarf zu verbessern.【<=】

5.1.2 Identifikation eines Clientsystems

Der TI-Flow-Fachdienst verwaltet und steuert den Einlöseprozess für elektronische Verordnungen. Damit kommt ihm eine Relevanz in der medizinischen Versorgung zu, die sich zum einen in einer hohen Verfügbarkeit und zum anderen in einem hohen Angriffspotential widerspiegelt. Zur Unterstützung der betrieblichen Überwachung des TI-Flow-Fachdienstes wird die Nutzung der im Feld befindlichen Clientsysteme protokolliert. Dabei ist der Zugriff auf die Schnittstellen des TI-Flow-Fachdienstes nur durch registrierte Clientsysteme zulässig. Der ZETA Guard stellt die Identifikation des Clientsystems sicher. Der Resource Server des TI-Flow-Fachdienst erkennt ein Clientsystem anhand der im

eingehender HTTP-Requests angegebenen product_id und product_version, die Attribute von zeta-client-data sind. Der TI-Flow-Fachdienst protokolliert diese Werte.

A_29706 -TI-Flow-Fachdienst - Erkennung und Protokollierung Clientsystem

Der TI-Flow-Fachdienst MUSS das vom aufrufenden Nutzer verwendete Clientsystem anhand des im Rahmen der Authentisierung übermittelten zeta-user-info und zeta-client-data erkennen und in den Einträgen zur Telemetriedatenerfassung gemäß [gemSpec_Perf] protokollieren.【<=】

5.1.3 Sicherheit der Netzübergänge

Der TI-Flow-Fachdienst wird für Clientsysteme über das Internet erreichbar gemacht. Die folgenden Anforderungen beschreiben die für diesen Netzübergang erforderlichen Sicherheitsmechanismen.

Alle Zugriffe von Clientsystemen erfolgen über den ZETA Guard, welcher u.a. die Authentisierung und Autorisierung für den Zugriff auf den Resource Server umsetzt.

Zugriffe des Resource Servers auf Dienste im Internet müssen ebenfalls abgesichert werden. Es kann bei Verfügbarkeit die Egress Komponente des ZETA Guard genutzt werden.

Für die Umsetzung sind Services des HCC-Providers entsprechend zu konfigurieren.

A_29707 -Anbieter TI-Flow-Fachdienst - Richtlinien für den Paketfilter zum Internet - Protokolle

Der Anbieter TI-Flow-Fachdienst MUSS sicherstellen, dass die Weiterleitung von IP-Paketen vom Resource Server an der Schnittstelle zum Internet auf die nachfolgenden Protokolle beschränkt wird:

1. HTTPS
2. OCSP
3. DNS
4. NTP

【<=】

A_29708 -Anbieter TI-Flow-Fachdienst - Richtlinien für den Paketfilter zum Internet - Anfragen im Internet

Der Anbieter TI-Flow-Fachdienst MUSS sicherstellen, dass die Weiterleitung von IP-Paketen vom Resource Server an der Schnittstelle zum Internet auf die Aktivitäten

1. OCSP-Responder und CRL-Download-Anfragen
2. DNS-Anfragen
3. NTP-Anfragen
4. FHIR-VZD-Suchanfragen
5. Anfragen an BfArM Webdienst
6. Anfragen an Push Gateways
7. Anfragen an PoPP-Service (Download des JWKS)
8. Anfragen an ePA-Aktensysteme

beschränkt sind und jeden anderen Verbindungsaufbau aus dem Resource Server in Richtung Internet unterbinden.【<=】

Für den ZETA Guard gibt es entsprechende Anforderungen für die Kommunikation ins Internet.

5.1.4 Nutzung Vertrauenswürdige Ausführungsumgebung

In diesem Abschnitt werden die Anforderungen an den TI-Flow-Fachdienst zur Umsetzung in einer Vertrauenswürdigen Ausführungsumgebung (VAU) dargestellt. Die VAU dient der datenschutzrechtlich zulässigen und sicheren Verarbeitung von schützenswerten Klartextdaten innerhalb des TI-Flow-Fachdienstes sowie dem technischen Ausschluss der Profilbildung durch den Anbieter bzw. Betreiber. Die VAU stellt dazu Verarbeitungskontexte (d. h. Instanzen der VAU) bereit, in denen die Verarbeitung sensibler Daten im Klartext erfolgen kann. Die VAU wird durch den HCC-Plattform-Provider für den Fachdienst bereitgestellt.

Verarbeitung von Daten

A_29709 -TI-Flow-Fachdienst - Umsetzung der fachlichen Operationen in einer VAU

Der TI-Flow-Fachdienst MUSS die Verarbeitung aller fachlichen Operationen des Fachdienstes in einer Vertrauenswürdigen Ausführungsumgebung umsetzen. [≤]

A_29710 -TI-Flow-Fachdienst - Nutzung HCC-Plattform für VAU

Der Anbieter TI-Flow-Fachdienst MUSS für die Umsetzung der VAU die durch einen durch die gematik beauftragten HCC-Plattform-Provider angebotenen Dienste nutzen. [≤]

Persistieren von Daten

A_29713 -TI-Flow-Fachdienst - Verschlüsselung von außerhalb der VAU zu speichernden Daten

Der TI-Flow-Fachdienst MUSS sicherstellen, dass sämtliche schützenswerten Daten vor einem Speichern außerhalb der VAU verschlüsselt werden. [≤]

A_29714 -TI-Flow-Fachdienst - Schlüssel für außerhalb der VAU zu speichernder Daten

Der TI-Flow-Fachdienst MUSS für das Verschlüsseln zu speichernder Daten den Schlüssel für nur jeweils einen individuellen Vorgang (bspw. Workflow zu einer Verordnung inkl. aller mit diesem Workflow verbundenen Daten) verwenden oder mindestens einmal pro Sekunde den verwendeten Schlüssel wechseln, so dass nur die innerhalb einer Sekunde neu angelegten Vorgänge mit demselben Schlüssel verschlüsselt werden. [≤]

Offener Punkt: Die gematik erarbeitet anwendungs-übergreifende Anforderungen für die Schlüsselableitung zur Persistierung der Daten (siehe offenen Punkt in [gemSpec_Krypt]). Nach dem Erarbeiten dieser Anforderungen wird bewertet, ob A_29714 dadurch ersetzt wird und entfallen kann.

A_29715 -TI-Flow-Fachdienst - Ableitung der Persistenzschlüssel durch ein HSM

Der TI-Flow-Fachdienst MUSS die zum Verschlüsseln der persistierten Vorgangsdaten verwendeten Schlüssel von einem HSM der HCC-Plattform abrufen. [≤]

Übermittlung von Daten

A_29716 -TI-Flow-Fachdienst - vertrauliche Kommunikation

Der TI-Flow-Fachdienst MUSS sicherstellen, dass er nur transportverschlüsselt mit Komponenten außerhalb des TI-Flow-Fachdienstes kommuniziert. [≤]

Diese Anforderung gilt insbesondere für die Clientsysteme des TI-Flow-Fachdienstes (u.a. PVS, AVS, TI-Flow-FdV, NCPeH-FD, ...)

Hinweis: Für die Qualität der Transportverschlüsselung gelten die Anforderungen aus [gemSpec_Krypt].

A_29717 -TI-Flow-Fachdienst - ZETA Guard als Eingangspunkt für Clientsysteme

Der TI-Flow-Fachdienst MUSS ausschliesslich den ZETA Guard als Eingangspunkt für Anfragen von Clientsystemen an den TI-Flow-Fachdienst erlauben. [≤]

5.1.5 Speicherung Schlüsselmaterial

A_29718 -TI-Flow-Fachdienst - Speicherung Schlüsselmaterial in HSM

Der TI-Flow-Fachdienst MUSS privates Schlüsselmaterial für kryptographische Verfahren (Entschlüsseln, Signieren) aus einem HSM nutzen. [≤]

Dies gilt insbesondere für die Identitäten des ZETA Guards.

A_29719 -Anbieter TI-Flow-Fachdienst - HSM der HCC-Plattform nutzen

Der Anbieter TI-Flow-Fachdienst MUSS für die Funktionen eines HSM einen Service der HCC-Plattform nutzen. [≤]

5.1.6 gematik-Logdaten zum Zwecke der gesetzlichen Kontrollpflichten der gematik

Für die Pseudonymisierung der gematik-Logdaten siehe [gemSpec_Krypt#Anomalie Erkennung].

A_29724 -TI-Flow-Fachdienst - Pseudonymisieren der gematik-Logdaten - Geheimer Schlüssel für Pseudonymisieren nur in VAU

Der TI-Flow-Fachdienst MUSS sicherstellen, dass der für das Pseudonymisieren der gematik-Logdaten benötigte geheime Schlüssel key_pn_log im Klartext ausschließlich innerhalb einer VAU verarbeitet wird. [≤]

A_29725 -Anbieter TI-Flow-Fachdienst - Pseudonymisieren der gematik-Logdaten - Möglichkeit zum Einbringen des Schlüssels im 4-Augen-Prinzip

Der Anbieter TI-Flow-Fachdienst MUSS sicherstellen, dass der für das Pseudonymisieren der gematik-Logdaten benötigte geheime Schlüssel key_pn_log ausschließlich im 4-Augen-Prinzip in den TI-Flow-Fachdienst eingebracht werden kann. [≤]

Hinweis: Der geheime Schlüssel für das Pseudonymisieren der gematik-Logdaten muss nicht im VAU-HSM gespeichert werden.

A_29726 -Anbieter TI-Flow-Fachdienst - Pseudonymisieren der gematik-Logdaten - Einbringen des Schlüssels im 4-Augen-Prinzip

Der Anbieter TI-Flow-Fachdienst MUSS den für das Pseudonymisieren der gematik-Logdaten benötigten geheimen Schlüssel key_pn_log ausschließlich im 4-Augen-Prinzip in den TI-Flow-Fachdienst einbringen. [≤]

A_29727 -Anbieter TI-Flow-Fachdienst - Pseudonymisieren der gematik-Logdaten - unverzüglicher Schlüsselwechsel

Der Anbieter TI-Flow-Fachdienst MUSS den für das Pseudonymisieren der gematik-Logdaten benötigten geheimen Schlüssel key_pn_log unverzüglich nach Bereitstellung durch die gematik wechseln. [≤]

Es ist ein jährlicher Schlüsselwechsel geplant.

5.2 Integration in HCC-Plattform

Die HCC-Plattform ist in [gemSpec_HCC] beschrieben.

Der Anbieter TI-Flow-Fachdienst übernimmt die Rolle des HCC-Dienstanbieters. Der Hersteller des TI-Flow-Fachdienstes übernimmt die Rolle HCC-Workload-Hersteller. Siehe [gemSpec_HCC#Rollen und Verantwortlichkeiten].

Der TI-Flow-Fachdienst ist in diesem Kontext ein HCC-Dienst.

Die Bereitstellung (der Komponenten) des TI-Flow-Fachdienstes erfolgt in Form von HCC-Workload-Images. Der HCC-Provider stellt dem Hersteller des HCC-Dienstes ein Template bereit.

Der HCC-Provider stellt dem Anbieter TI-Flow-Fachdienst die HCC-Infrastruktur zum Betrieb des Dienstes bereit. Siehe [gemSpec_HCC#HCC-Provider – Bereitstellung HCC-Infrastruktur] und [gemSpec_HCC#Weitere Dienste].

Der HCC-Provider stellt dem Anbieter TI-Flow-Fachdienst einen Mandantenkontext für die Administration des Dienstes in der Cloud zur Verfügung. Siehe [gemSpec_HCC#HCC-Provider – Mandanten für HCC-Dienstanbieter].

5.3 Systemprotokolle

Der TI-Flow-Fachdienst soll Protokolldateien schreiben, die eine Analyse technischer Vorgänge erlauben. Diese Protokolldateien sind dafür vorgesehen, aufgetretene Fehler zu identifizieren und die Performance zu analysieren. Für diese Zwecke führt der TI-Flow-Fachdienst ein Systemprotokoll, mit dem der Anbieter des Dienstes jederzeit den Betriebszustand des Systems kontrollieren kann.

A_29728 -TI-Flow-Fachdienst - Systemprotokoll für Betriebszustand

Der TI-Flow-Fachdienst MUSS ein Systemprotokoll über durchgeführte Operationen und deren Erfolg/Misserfolg führen, um dem Anbieter des Dienstes jederzeit eine Übersicht über den aktuellen Betriebszustand zu ermöglichen. [≤]

A_30134 -Anbieter TI-Flow-Fachdienst - Erlaubte Zwecke der Systemprotokolle

Der Anbieter TI-Flow-Fachdienst MUSS sicherstellen, dass Systemprotokolle ausschließlich zum Zwecke der Fehleranalyse und -behebung anlassbezogen sowie zum Zwecke des Security Monitorings verwendet werden. [≤]

A_30135 -Anbieter TI-Flow-Fachdienst - keine Profilbildung ausser für erlaubte Zwecke

Der Anbieter TI-Flow-Fachdienst DARF die im Rahmen von Logging und Monitoring erhobenen Informationen NICHT für eine Profilbildung nutzen, außer es besteht die Notwendigkeit im Rahmen der Fehleranalyse und -behebung oder des Security Monitorings. [≤]

A_29729 -TI-Flow-Fachdienst - Systemprotokoll ohne sensible Daten

Der TI-Flow-Fachdienst MUSS in jedem zu tätigenden Systemprotokolleintrag alle sensiblen Daten vor der Speicherung entfernen, damit vom administrativen Personal keine personenbezogenen Daten der Versicherten oder Leistungserbringer eingesehen werden können (z.B. personenbezogene, personenbeziehbare und medizinische Informationen sowie sicherheitsrelevante Daten, wie z.B. kryptographisches Material). [≤]

A_29730 -Anbieter TI-Flow-Fachdienst - Systemprotokoll Verfügbarkeit interner Logdaten

Der Anbieter TI-Flow-Fachdienst MUSS im Rahmen von Testmaßnahmen dem Testbetriebsverantwortlichen auf Anforderung die Log-Dateien des Systemprotokolls des TI-Flow-Fachdienstes übermitteln.【<=】

A_29731 -Anbieter TI-Flow-Fachdienst - Systemprotokoll Aufbewahrungsfristen

Der Anbieter TI-Flow-Fachdienst MUSS sicherstellen, dass die

- zum Zwecke der Fehleranalyse erhobenen Protokolle nach Behebung des Fehlers unverzüglich gelöscht werden,
- zum Zwecke des Security Monitorings erhobenen Protokolle nach 3 Monaten gelöscht werden.

【<=】

5.4 Zertifikatsprüfung

A_29732 -TI-Flow-Fachdienst - verpflichtende Zertifikatsprüfung

Der TI-Flow-Fachdienst MUSS alle Zertifikate, die er aktiv verwendet (bspw. TLS-Verbindungsaufbau), auf Integrität und Authentizität prüfen. Falls die Prüfung kein positives Ergebnis ("gültig") liefert, so MUSS es die von dem Zertifikat und den darin enthaltenen Attributen (bspw. öffentliche Schlüssel) abhängenden Arbeitsabläufe ablehnen.

Der TI-Flow-Fachdienst MUSS alle öffentlichen Schlüssel, die es verwenden will, auf eine positiv verlaufene Zertifikatsprüfung zurückführen können.【<=】

"Ein Zertifikat aktiv verwenden" bedeutet im obigen Sinne, dass der Fachdienst einen öffentlichen Schlüssel innerhalb einer kryptographischen Operation (Signaturprüfung, Verschlüsselung, Signaturprüfung von öffentlichen (EC)DH-Schlüsseln etc.) nutzt. Erhält der Fachdienst Daten, in dem Signaturen und Zertifikate enthalten sind und behandelt es dieses als opakes Datenobjekt, ohne die Zertifikate darin gesondert zu betrachten, dann verwendet der Fachdienst diese Zertifikate im obigen Sinne passiv.

Zertifikatsprüfung von Zertifikaten der TI-PKI

Der TI-Flow-Fachdienst prüft Zertifikate der TI-PKI gemäß den Vorgaben von [gemSpec_PKI], d.h. insbesondere X.509 nonQES Zertifikate gemäß "TUC_PKI_018 Zertifikatsprüfung in der TI" und X.509 QES Zertifikate gemäß "TUC_PKI_030 QES-Zertifikatsprüfung".

Zertifikatsprüfung von Zertifikaten der Internet-PKI

Der TI-Flow-Fachdienst prüft Internet TLS Zertifikate gemäß den Vorgaben von [gemSpec_Krypt].

5.5 ZETA Guard im TI-Flow-Fachdienst

Der ZETA Guard im TI-Flow-Fachdienst übernimmt wesentliche Sicherheitsleistungen für den Zugang von Clientsystemen zum TI-Flow-Fachdienst.

Der ZETA Guard erfüllt folgende Aufgaben:

- Die **Policy-basierte Zugriffskontrolle** stellt sicher, dass alle Zugriffe auf den TI-Flow-Fachdienst sicher und autorisiert sind, indem er kontinuierlich die Aktivitäten überwacht und analysiert.
- Clientsystem-Authentisierung Leistungserbringerinstitutionen
 - Die **Authentifizierung mittels SM(C)-B** erfolgt automatisch bei freigeschalteter SM(C)-B, indem der ZETA Client im Clientsystem ein ID Token erstellt und mit der SM(C)-B signiert. Dieses Token nutzt DPoP, um sicherzustellen, dass die Anfragen vom autorisierten Clientsystem stammen und Replay-Attacken verhindert werden.
- Das **Session Management** für den TI-Flow-Fachdienst im ZETA Guard verwendet OAuth2, wobei Access- und Refresh-Token sicher verwaltet und bei Bedarf erneuert werden. Die Token sind durch DPoP an spezifische Clientsystem-Instanzen gebunden, um sicherzustellen, dass nur autorisierte Clientsysteme Zugriff haben. Bei abgelaufenen Sessions ist eine erneute Authentifizierung erforderlich.

Der ZETA Guard wird dem Hersteller des TI-Flow-Fachdienstes durch die gematik bereitgestellt.

Dieses Kapitel beschränkt sich im Folgenden nur auf die ZETA Guard Komponenten mit TI-Flow-Fachdienst-spezifischen Konfigurationsanforderungen. Vorgaben zur operativen Umsetzung der folgenden Konfigurationsanforderungen sind [gemSpec_ZETA] zu entnehmen.

Tabelle 1: TAB_TI-Flow_Konfigurationsübersicht_ZETA_Guard

ZETA Guard Komponente	TI-Flow-spezifische Konfigurationsanforderungen auf Anwendungsebene
Ingress und Egress	nein
PEP HTTP-Proxy	ja
Authorization Server	ja
PDP Datenbank	nein
Policy Engine	nein
Telemetrie-Daten Service	ja
Notification Service	ja

Hinweis: Unabhängig von den folgenden Anforderungen muss der Hersteller des TI-Flow-Fachdienstes Konfigurationen für die Integration des ZETA Guards in die Runtime Umgebung vornehmen (bspw. für die Nutzung des Datenbankservices durch die Komponente PDP Datenbank).

A_29754 -TI-Flow-Fachdienst - Ausschließlich TLS-gesicherte Verbindungen mit Clientsystem

Der Hersteller des TI-Flow-Fachdienstes MUSS den ZETA Guard so konfigurieren, dass der ZETA Guard ausschließlich durch TLS gesicherte Verbindungen von Clientsystemen akzeptiert. [**<=**]

5.5.1 Konfiguration Ingress

Die Ingress Komponente bietet die Möglichkeit der Konfiguration von Ratelimits.

5.5.2 Konfiguration PEP HTTP-Proxy

Der HTTP-Proxy nimmt die Anfragen eines Clientsystems entgegen und prüft die Anfrage vor dem Weiterleiten an erlaubte Endpunkte des Resource Servers auf eine vorhandene sowie gültige Berechtigung auf Basis von DPoP- und Access-Token.

Antworten des Resource Servers nimmt der HTTP-Proxy entgegen und leitet diese an das Clientsystem weiter.

A_29761 -TI-Flow-Fachdienst - ZETA Guard - HTTP-Proxy - ZETA/ASL für Request an Resource Server

Der Hersteller des TI-Flow-Fachdienstes MUSS den HTTP-Proxy des ZETA Guard so konfigurieren, dass der ZETA Guard von Clientsystemen nur Anfragen an den Resource Server akzeptiert, welche mittels ZETA/ASL verschlüsselt sind. [≤]

A_29762 -TI-Flow-Fachdienst - ZETA Guard - HTTP-Proxy - ASL-Kanal terminieren

Der Hersteller des TI-Flow-Fachdienstes MUSS den HTTP-Proxy des ZETA Guard so konfigurieren, dass der ASL-Kanal vom Clientsystem terminiert wird. [≤]

A_29763 -TI-Flow-Fachdienst - ZETA Guard - HTTP-Proxy - ZETA/ASL für Responses des Resource Servers

Der Hersteller des TI-Flow-Fachdienstes MUSS den HTTP-Proxy des ZETA Guard so konfigurieren, dass die Response des Resource Servers durch ZETA/ASL gesichert an das anfragende Clientsystem übertragen wird. [≤]

A_29764 -TI-Flow-Fachdienst - ZETA Guard - HTTP-Proxy - HTTP-Header zeta-client-data

Der Hersteller des TI-Flow-Fachdienstes MUSS den HTTP-Proxy des ZETA Guard so konfigurieren, dass die Informationen des HTTP-Header zeta-client-data an den Resource Server weitergeleitet wird. [≤]

5.5.3 Konfiguration Authorization-Server

A_29765 -Anbieter TI-Flow-Fachdienst - ZETA Guard - AuthZ-Server - Authentifizierung von Institutionen mit SM(C)-B

Der Hersteller des TI-Flow-Fachdienstes MUSS den Authorization-Server des ZETA Guard so konfigurieren, dass die Authentifizierung einer Leistungserbringerinstitution oder Kostenträger nur auf Basis einer SM(C)-B durchgeführt wird. [≤]

Die Gültigkeit des Refresh-Tokens wird mittels dem Policy-Dokument umgesetzt. Sie ist standardmäßig 24 Stunden. Dieser Standardwert kann aufgrund von Sicherheitsereignissen oder auf Basis der Sicherheitsbewertung des Clientsystems (Client-Attestation) im Betrieb mittels ZT-Policy geändert werden

Die Gültigkeit des Access-Tokens wird mittels dem Policy-Dokument umgesetzt. Sie ist standardmäßig 5 Minuten. Dieser Standardwert kann bspw. aufgrund von Sicherheitsereignissen oder auf Basis der Sicherheitsbewertung des Clientsystems (Client-Attestation) im Betrieb mittels ZT-Policy geändert werden.

A_29766 -TI-Flow-Fachdienst - ZETA Guard - AuthZ-Server - Authentifizierung mit SM(C)-B einmal am Tag

Der Hersteller des TI-Flow-Fachdienstes MUSS den Authorization-Server so konfigurieren, dass - unabhängig von einem möglicherweise noch gültigem Refresh-Token - einmal

täglich die Authentifizierung von Institutionen auf Basis einer SM(C)-B durchgeführt wird.
[<=]

Hinweis: Die tägliche Authentifizierung ist ein Standardwert, der bspw. aufgrund von Sicherheitsereignissen oder auf Basis der Sicherheitsbewertung des Clientsystems (Client-Attestation) im Betrieb mittels ZT-Policy geändert werden kann. Zukünftig und bei Verfügbarkeit der TI-Flow-Fachdienst-Policy wird dieser Standardwert über die TI-Flow-Fachdienst-Policy festgelegt und nicht mehr innerhalb dieser Spezifikation. Die Authentifizierung der LEI erfolgt automatisiert über ZETA ohne deren manuelle Mitwirkung.

5.5.4 Konfiguration Telemetriedaten Service

Der TI-Flow-Fachdienst übermittelt Betriebsdaten, Selbstauskunft und Metriken zu Bestandsdaten unter Verwendung des OpenTelemetry-Frameworks an die gematik. Aus den Telemetriedaten können Informationen zur Performance, Last und Fehlersituationen sowie Daten über den Status und Versionsständen von Clientsystemen abgeleitet werden.

Die Schnittstelle ist in [gemSpec_Perf] beschrieben.

Die Kommunikation vom TI-Flow-Fachdienst zum gematik Telemetriedaten Service und SIEM übernimmt der ZETA Guard.

Für alle zu reportenden Aktivitäten, welche durch Clientsysteme getriggert werden und somit durch den ZETA Guard geroutet werden, erstellt der ZETA Guard den Trace und der Resource Server liefert die anwendungsspezifischen Daten im Span an den ZETA Guard.

Für den TI-Flow-Fachdienst muss die Konfiguration des OTEL Collectors (siehe Betriebshandbuch ZETA Guard) so angepasst werden, dass auch Traces zu Aktivitäten, welche durch den Resource Server gegenüber Backendsystemen getriggert werden, weitergeleitet werden.

5.5.5 Konfiguration Notification Service

A_30360 -TI-Flow-Fachdienst - ZETA Guard - Notification Service - Channels konfigurieren

Der Hersteller des TI-Flow-Fachdienstes MUSS den Notification Service des ZETA Guard so konfigurieren, dass die durch den TI-Flow-Fachdienst definierten Channels zulässig sind.
[<=]

Die definierten Channels sind im FHIR-IG für die verschiedenen Module beschrieben.

A_30361 -TI-Flow-Fachdienst - ZETA Guard - Notification Service - Verschlüsselten Versand konfigurieren

Der Hersteller des TI-Flow-Fachdienstes MUSS den Notification Service des ZETA Guard so konfigurieren, dass der Notification Service verschlüsselt versendet.[<=]

5.6 Exporter

Der TI-Flow-Fachdienst unterstützt eine asynchrone Übermittlung von Daten an Drittsysteme (bspw. ePA Medication Service und BfArM Webservice). Die dafür eingesetzte Exporter Komponente nutzt eine Queue für Übermittlungsaufträge inklusive eines Mechanismus für nicht abarbeitbare Aufträge (Dead Letter Queue (DLQ)).

A_29767 -TI-Flow-Fachdienst - Asynchrone Übermittlung an Backendsysteme (Exporter)

Der TI-Flow-Fachdienst MUSS es ermöglichen, Daten zu Backendsystemen asynchron zum initiiierenden Operationsaufruf eines Clientsystems zu übermitteln. [≤]

A_29768 -TI-Flow-Fachdienst - Exporter - Wiederholte Übermittlung an Backendsysteme (Retry)

Der TI-Flow-Fachdienst MUSS es ermöglichen, dass bei Nichtverfügbarkeit des Zielsystems oder Fehler bei der Übertragung der Daten, die Daten nach einem definierten und konfigurierbaren Verhalten erneut gesendet werden können. [≤]

A_29769 -TI-Flow-Fachdienst - Exporter - Dead Letter Queue

Der TI-Flow-Fachdienst MUSS es ermöglichen, dass im Falle von wiederholten nicht-erfolgreichen Übermittlungsversuchen die Übermittlung pausiert wird. [≤]

A_29770 -Anbieter TI-Flow-Fachdienst - Exporter - Dead Letter Queue bereinigen

Der Anbieter TI-Flow-Fachdienst MUSS es in Absprache mit der gematik ermöglichen, pausierte Übermittlungsaufträge zu löschen. [≤]

A_30109 -TI-Flow-Fachdienst - Exporter - Dead Letter Queue - Löschfrist

Der TI-Flow-Fachdienst MUSS Events, die nach wiederholten nicht-erfolgreichen Übermittlungsversuchen nicht zugestellt werden konnten, 100 Tage nach Eintritt in die Dead Letter Queue aus der Dead Letter Queue löschen. [≤]

5.7 Vertrauenswürdige Uhrzeit im TI-Flow-Fachdienst

Der TI-Flow-Fachdienst erstellt Signaturen für Abrechnungsinformationen und prüft den Zeitstempel des PoPP-Token. Für das Erstellen der Signatur und das Prüfen der Gültigkeit des PoPP-Token ist es notwendig, mit einer vertrauenswürdigen Uhrzeit zu arbeiten.

A_29734 -TI-Flow-Fachdienst - Vertrauenswürdige Uhrzeit

Der TI-Flow-Fachdienst MUSS seine lokale Systemzeit mindestens einmal täglich mit einem qualifizierten Zeitstempel eines eIDAS-Vertrauensdiensteanbieters synchronisieren, um sicherzustellen, dass die lokale, mittels NTP synchronisierte Systemzeit nie mehr als 10 Sekunden vom Wert des aktuell eingeholten qualifizierten Zeitstempels abweicht. [≤]

A_29735 -Anbieter TI-Flow-Fachdienst - Vertrauenswürdige Uhrzeit

Der Anbieter TI-Flow-Fachdienst MUSS, wenn die Systemzeit mehr als 10 Sekunden vom Wert des aktuell eingeholten qualifizierten Zeitstempels abweicht, einen Security Incident entsprechend [TI-SEC-Standard] eröffnen. [≤]

Hinweis: Die Bundesnetzagentur listet unter [AnbieterVZeitD] verschiedene Anbieter für qualifizierte Zeitstempel.

5.8 FHIR Validierung im TI-Flow-Fachdienst

Der TI-Flow-Fachdienst muss als zentraler Dienst für FHIR Artefakte in der TI eine umfassende Validierung der eingehenden FHIR-Ressourcen vornehmen, um die Weiterverarbeitung in Systemen auch außerhalb der TI sicherzustellen. Weiterhin ist auch die Unterstützung von Clients im Übergang zwischen verschiedenen Versionen von FHIR-Artefakten ein wesentlicher Aspekt.

Die gematik veröffentlicht und maintained den [gematik Referenzvalidator]. Dieser ist eine Erweiterung des [HL7 Java Validator]. Der Referenzvalidator liefert autoritative

Antworten zur Validität von übertragenen Datensätzen und ist somit eine Referenz für im Rahmen einer TI-Anwendung eingesetzten FHIR-Validatoren.

Der Referenzvalidator ist konfigurierbar und mit verschiedenen FHIR-Paketen ausführbar. Die FHIR-Pakete für die Anwendung TI-Flow werden dem Hersteller des TI-Flow-Fachdienst durch die gematik bereitgestellt.

Der TI-Flow-Fachdienst muss für eine korrekte Aussage zur Validität von FHIR Artefakten sicherstellen, dass die Ausgaben der Validierung des Fachdienstes exakt derer des gematik Referenzvalidators entsprechen. Es ist dem Anbieter des TI-Flow-Fachdienst freigestellt, ob dafür der Referenzvalidator eingebettet oder ein proprietärer Validator genutzt wird. Falls ein proprietärer Validator genutzt wird, muss der die gleichen Validierungsergebnisse wie der gematik Referenzvalidator liefern.

Für die weitere Beschreibung wird der Begriff "Validierungskomponente des TI-Flow-Fachdienst" eingeführt, die als eigenständiges Modul innerhalb des TI-Flow-Fachdienstes betrachtet wird.

5.8.1 Validierung bei Versionsübergängen

Im Verlauf der Weiterentwicklung von Anwendungsfällen kommt es fachlich oder technisch motiviert zu neuen Versionen von FHIR-Packages, welche durch den TI-Flow-Fachdienst verarbeitet werden. Den Clientsystemen des TI-Flow-Fachdienst werden für die Umsetzung von Major und Minor Updates von FHIR-Packages "Übergangszeiten" angeboten, in denen mehrere Versionen eines FHIR-Profils gültig sind. Der TI-Flow-Fachdienst muss für eine performante und flexible Realisierung dieser Übergänge, Validierungen gegen mehrere Versionen eines Profils gleichzeitig unterstützen.

5.8.2 Architektur der Validierungskomponente

Der TI-Flow-Fachdienst betreibt die FHIR-Validierung als eigenständiges, containerisiertes Modul. Die Architektur trennt zwischen dem unveränderlichen Validierungskern (CoreImage) und dem konfigurationsgebundenen Einsatzartefakt (ValidatorImage).

Der Hersteller des TI-Flow-Fachdienstes stellt das CoreImage bereit. Dieses CoreImage kann in Kombination mit einer FHIR-Konfiguration, die durch die gematik bereitgestellt wird, dann das ValidatorImage erzeugen. Die FHIR-Konfiguration bildet dabei die Kombination aus zulässigen Versionen von FHIR-Packages im Validierungskontext in einem Zeitraum ab. Als Beispiel dient [API-ERP: FHIR-Transition].

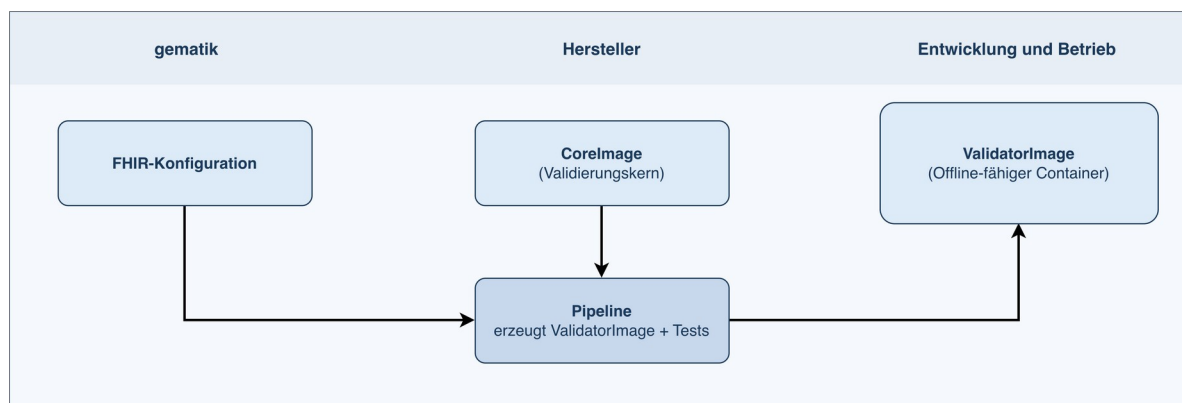


Abbildung 2: Entstehung FHIR-ValidatorImage für TI-Flow-Fachdienst

Ein ValidatorImage wird in einer Pipeline aus der Kombination des CoreImage mit einer FHIR-Konfiguration erzeugt. Ein erzeugtes ValidatorImage ist in der Lage eine FHIR-Konfiguration zu validieren.

Der TI-Flow-Fachdienst muss für die Realisierung der Übergangszeiten in der Lage sein mehrere verschiedene ValidatorImages gleichzeitig im Betrieb zu nutzen.

Damit das ValidatorImage für die Entwicklungsbegleitung der Industrie nach Abschluss der Spezifikation bereitgestellt werden kann, muss es möglich sein das ValidatorImage nach Abschluss der Spezifikation und Erstellung eines FHIR-Packages zu erzeugen und zu veröffentlichen.

Aufgrund der containerisierten Bereitstellung des ValidatorImages ist es möglich, dass dieses Artefakt in Testumgebungen und bei Bedarf auch in der Produktionsumgebung eingesetzt werden kann.

A_29821 -TI-Flow-Fachdienst - Validierungskomponente - Bereitstellung als OCI-Container

Der Hersteller des TI-Flow-Fachdienstes MUSS die Validierungskomponente als OCI-konformes Container-Image bereitstellen, das in einer Container-Laufzeitumgebung (z.B. Kubernetes, Docker) deploybar ist. [$\leq$]

Ein FHIR-Package kann ValueSets enthalten, welche Inhalte (Filter) definieren, die aus externen Quellen (bspw. Terminologieservern) bezogen werden müssen. Das ValidatorImage muss offline in der Lage sein; auch diese Terminologien zu validieren.

A_29822 -TI-Flow-Fachdienst - Validierungskomponente - Offline-Fähigkeit des ValidatorImage

Die Validierungskomponente des TI-Flow-Fachdienstes MUSS zur Build-Zeit des ValidatorImage alle notwendigen FHIR-Packages, Terminologien (ValueSets, CodeSystems) und Validierungsregeln herunterladen, alle referenzierten ValueSets gegen einen konfigurierten Terminologieserver expandieren und die expandierten Terminologieartefakte im Image persistieren. [$\leq$]

A_29823 -TI-Flow-Fachdienst - Validierungskomponente - Verbindungen des ValidatorImage zur Lauf-Zeit

Die Validierungskomponente des TI-Flow-Fachdienstes DARF NICHT erlauben, dass das Image zur Laufzeit ausgehenden Verbindungen zu externen Paket-Registries oder Terminologie-Servern aufbaut. [$\leq$]

A_29824 -TI-Flow-Fachdienst - Validierungskomponente - Snapshot Generierung zur Build-Zeit

Die Validierungskomponente des TI-Flow-Fachdienstes MUSS in der Lage sein, zur Build-Zeit des ValidatorImage Snapshots aus FHIR-Packages zu generieren, um diese für die Validierung zu nutzen. [$\leq$]

FHIR-Packages enthalten teilweise selbst generierte Snapshots. Diese sind beim Erstellen des ValidatorImage zu ignorieren. Das ValidatorImage soll für die Validierung eigen generierte Snapshots nutzen.

A_30098 -TI-Flow-Fachdienst - Validierungskomponente - Snapshot Generierung mit differential

Die Validierungskomponente des TI-Flow-Fachdienstes MUSS für die Snapshot Generierung die Differential Angaben in einem FHIR-Package nutzen, ohne dabei die im FHIR-Package angegebene Snapshotdefinitionen zu verwenden. [$\leq$]

A_29825 -TI-Flow-Fachdienst - Validierungskomponente - Bereitstellen von Snapshots zur Build-Zeit

Die Validierungskomponente des TI-Flow-Fachdienstes MUSS in der Lage sein, zur Build-Zeit des ValidatorImage Snapshots als paketierte Datei bereitzustellen, um den erzeugten Validierungskontext nachprüfbar zu machen. [≤]

Das ValidatorImage stellt eine REST-API zur Verfügung.

Der Hersteller des TI-Flow-Fachdienstes kann entscheiden, ob die Validierungskomponente für das Deployment des TI-Flow-Fachdienstes via REST-Schnittstelle oder über ein internes Protokoll angesprochen wird.

A_29827 -TI-Flow-Fachdienst - Validierungskomponente - Erweiterbarkeit des CoreImage

Der Hersteller des TI-Flow-Fachdienstes MUSS das CoreImage der Validierungskomponente des TI-Flow-Fachdienstes so entwerfen, dass es durch Konfiguration oder durch definierte Erweiterungsschnittstellen um weitere Validierungsmodule ergänzt werden kann (z.B. für CDA-Dokumente oder PDF/A-Validierung), ohne die bestehende FHIR-Validierungslogik zu verändern. [≤]

A_29828 -TI-Flow-Fachdienst - Validierungskomponente - Validierungsergebnisse wie gematik Referenzvalidator

Die Validierungskomponente des TI-Flow-Fachdienstes MUSS die gleichen Validierungsergebnisse wie der gematik Referenzvalidator erzeugen. [≤]

A_30169 -TI-Flow-Fachdienst - Validierungskomponente - Technische Isolation

Der TI-Flow-Fachdienst MUSS die Validierungskomponente technisch so isoliert ausführen, dass weder andere Komponenten noch andere Verarbeitungsvorgänge der Anwendung Schaden nehmen können.

[≤]

5.8.3 Konfiguration der Validierungskomponente des TI-Flow-Fachdienst

Wie in der Architektur der Validierungskomponente beschrieben, muss die Validierungskomponente des TI-Flow-Fachdienstes konfigurierbar sein.

A_29829 -TI-Flow-Fachdienst - Validierungskomponente - Ausgabe der Konfiguration

Die Validierungskomponente des TI-Flow-Fachdienstes MUSS die im ValidatorImage umgesetzte Konfiguration über die REST-Schnittstelle GET/fhir-configuration ausgeben. [≤]

A_29830 -TI-Flow-Fachdienst - Validierungskomponente - FHIR-Package-basierte Konfiguration

Die Validierungskomponente des TI-Flow-Fachdienstes MUSS für die Ausgabe der Konfiguration mindestens die folgenden Angaben enthalten:

- Eine Auflistung von FHIR-Konfigurationen:
 - Zeitlich begrenzte Gültigkeit einer FHIR-Konfiguration
 - Name und Versionen der FHIR-Packages einer Konfiguration
- Optionale Validierungsparameter (z.B. Aktivierung/Deaktivierung von Terminologie-Validierung)

[≤]

A_29831 -TI-Flow-Fachdienst - Validierungskomponente - Validierung der Konfiguration von FHIR-Packages

Die Validierungskomponente des TI-Flow-Fachdienstes MUSS in der Lage sein, zur Build-Zeit die bereitgestellte Konfiguration auf Plausibilität und Konsistenz hin zu prüfen und bei negativen Bescheid den Build-Prozess abbrechen. [$\leq$]

A_29832 -TI-Flow-Fachdienst - Validierungskomponente - Konfiguration von FHIR-Packages

Die Validierungskomponente des TI-Flow-Fachdienstes MUSS in der Lage sein, zur Build-Zeit eine Konfiguration von FHIR-Packages mit definierter Gültigkeit zu konsumieren und für die Validierung zu nutzen. [$\leq$]

Als fachliche Anforderung ist es notwendig, dass für einzelne Profile ein Datum (bspw. MedicationRequest.authoredOn) als zeitliche Referenz ausgewählt werden kann, wonach eine Zuordnung zu einer FHIR-Profilversion erfolgt.

A_29833 -TI-Flow-Fachdienst - Validierungskomponente - Konfiguration von datumsbezogenen Parametern

Die Validierungskomponente des TI-Flow-Fachdienstes MUSS in der Lage sein, für ein Datumsfeld mit Datentypen date, dateTime oder instant eines FHIR-Profiles die zeitliche Gültigkeit zu konfigurieren und für die Validierung zu verwenden. [$\leq$]

A_29845 -TI-Flow-Fachdienst - Validierungskomponente - Validierung von datumsbezogenen Parametern

Die Validierungskomponente des TI-Flow-Fachdienstes MUSS in der Lage sein konfigurierte Datumsfelder entsprechend der in der FHIR-Konfiguration angegebenen Datumsgrenzen zu validieren. [$\leq$]

A_30097 -TI-Flow-Fachdienst - Validierungskomponente - Validierung von datumsbezogenen Parametern - Referenz Zeitzone

Die Validierungskomponente des TI-Flow-Fachdienst MUSS sicherstellen, dass bei der Auswertung von Datums- und Zeitangaben ohne Zeitzoneneinformationen, die entsprechend dem Datum gültige deutsche Zeitzone (CET/CEST) angewendet wird. [$\leq$]

A_29834 -TI-Flow-Fachdienst - Validierungskomponente - Reproduzierbarkeit des Build-Prozesses

Der Hersteller des TI-Flow-Fachdienstes MUSS einen dokumentierten Build-Prozess für die Validierungskomponente des TI-Flow-Fachdienstes bereitstellen, durch den die gematik aus einer Konfigurationsdatei und dem CoreImage eigenständig ein ValidatorImage erzeugen kann. [$\leq$]

A_29835 -TI-Flow-Fachdienst - Validierungskomponente - Terminologieserver-Konfiguration im Build-Prozess

Der Hersteller des TI-Flow-Fachdienstes MUSS sicherstellen, dass der Build-Prozess für die Validierungskomponente des TI-Flow-Fachdienstes einen konfigurierbaren Terminologieserver-Endpoint unterstützt, gegen den alle in den FHIR-Packages referenzierten ValueSets und CodeSystems während des Builds expandiert werden. [$\leq$]

A_29836 -TI-Flow-Fachdienst - Validierungskomponente - Dokumentation Terminologieserver-Expansion im Build-Prozess

Der Hersteller des TI-Flow-Fachdienstes MUSS sicherstellen, dass der Build-Prozess für die Validierungskomponente des TI-Flow-Fachdienstes das Ergebnis der Terminologie-Expansion versioniert und im ValidatorImage eingefroren abrufbar macht, sodass spätere Builds mit demselben Terminologieserver und denselben Packages zu identischen Validierungsergebnissen führen. [$\leq$]

A_29837 -TI-Flow-Fachdienst - Validierungskomponente - Bereitstellung eines ValidatorImage bei Profilveröffentlichung

Der Hersteller des TI-Flow-Fachdienstes MUSS den Build-Mechanismus der Validierungskomponente des TI-Flow-Fachdienstes so gestalten, dass die gematik zum Zeitpunkt der Veröffentlichung einer neuen FHIR-Package-Version eigenständig und ohne

Mitwirkung des Anbieters ein ValidatorImage erzeugen und bereitstellen kann, das funktional identisch mit dem ValidatorImage der Produktivumgebung sein ist. [≤]

5.8.4 REST-Schnittstelle der Validierungskomponente des TI-Flow-Fachdienst

A_29838 -TI-Flow-Fachdienst - Validierungskomponente - FHIR-\$validate-Operation

Die Validierungskomponente des TI-Flow-Fachdienstes MUSS eine \$validate-Operation nach <https://gematik.de/fhir/tiflow/OperationDefinition/tiflow-core-validate-opbereitstellen>. [≤]

A_29839 -TI-Flow-Fachdienst - Validierungskomponente - Fehlerausgabe bei Validierung

Die Validierungskomponente des TI-Flow-Fachdienstes MUSS das Ergebnis der Validierungsoperation als FHIR OperationOutcome-Ressource zurückgeben. [≤]

A_30096 -TI-Flow-Fachdienst - Validierungskomponente - Fehlerausgabe bei Validierung - Flag für boolsche Ausgabe

Die Validierungskomponente des TI-Flow-Fachdienstes MUSS für den Aufruf der Validierungsoperation ein Flag unterstützen, womit das Ergebnis der Validierung mit true oder false bewertet wird. [≤]

Hinweis: Das Ergebnis der FHIR-Validierung ist als true zu bewerten, falls es keine Operation Outcomes im Validierungsergebnis gibt, die den Fehlerstatus (.severity) "fatal" oder "error" haben.

A_29840 -TI-Flow-Fachdienst - Validierungskomponente - Fehlerausgabe in Logs ohne Nutzdaten

Die Validierungskomponente des TI-Flow-Fachdienstes DARF zu Vorgängen von Validierungsoperation in betrieblichen Logs NICHT Inhalte der validierten Ressource (z.B. Patientennamen, Versicherungsnummer, Medikamentenbezeichnung) aufnehmen. [≤]

Hinweis: In den OperationOutcomes, die an den anfragenden Client ausgegeben werden, können Inhalte der Instanz enthalten sein, um eine bessere Fehleranalyse zu ermöglichen.

A_29841 -TI-Flow-Fachdienst - Keine FHIR-\$validate-Operation

Der TI-Flow-Fachdienst DARF NICHT die \$validate-Operation gegenüber Clientsystemen exponieren. [≤]

5.9 Konfiguration von Fachdienst-Instanzen

Der TI-Flow-Fachdienst unterstützt verschiedene Workflows. Er wird kontinuierlich weiterentwickelt und um neue Workflows ergänzt. Um Pilotierungsphasen eines Workflows zu begleiten und Entwicklungsumgebungen gezielt zu konfigurieren, muss der TI-Flow-Fachdienst in der Lage sein, Workflows und Features per Deployment-Konfiguration zu steuern. Damit ist es möglich, Funktionalität bereits im Code auszuliefern, ohne dass diese in der entsprechenden Umgebung aktiv ist. Dies ermöglicht eine bessere Release-Steuerung.

Die Konfiguration umfasst drei Bereiche: die Steuerung der Operationalisierung einzelner Flowtypes, die Steuerung der Verfügbarkeit von Features sowie die Festlegung des Referenzzeitpunkts für die FHIR-Validierung. Die jeweils aktive Konfiguration einer Instanz

wird im CapabilityStatement des TI-Flow-Fachdienstes ausgegeben, sodass Clientsysteme die Konfiguration abrufen und ihr Verhalten entsprechend anpassen können.

Die konkrete Darstellung und Ausgabe von Konfigurationsparametern im CapabilityStatement sowie die Struktur der Daten im Fehlerfall wird im FHIR-IG beschrieben.

A_29771 -TI-Flow-Fachdienst - Konfiguration je Instanz

Der TI-Flow-Fachdienst MUSS für jede Betriebsumgebung eine Konfiguration unterstützen und anwenden.[<=]

A_29772 -Anbieter TI-Flow-Fachdienst - Abstimmung zur Konfiguration

Der Anbieter TI-Flow-Fachdienst MUSS die Konfigurationen der Instanzen in Abstimmung mit der gematik umsetzen.[<=]

5.9.1 Konfiguration von Flowtypes

Die Operationalisierung einzelner Flowtypes kann per Konfiguration gesteuert werden. Das Deaktivieren eines Flowtypes verhindert den Abruf neuer Task-IDs für den entsprechenden Flowtype über die \$create-Operation. Bereits erzeugte Tasks mit einem deaktivierten Flowtype bleiben vollständig bearbeitbar, um die Versorgung sicherzustellen. Grundlage für die möglichen Konfigurationsparameter ist das CodeSystem (CS) der Flowtypes. Mit der Definition neuer Flowtypes im Codesystem wird die Menge der konfigurierbaren Parameter automatisch erweitert.

Anforderungen und Spezifikationen hierzu sind im Implementation Guide TI-Flow - Kernfunktionalitäten zu finden.

5.9.2 Konfiguration von Features

Neben Flowtypes können auch Features konfiguriert werden, die nicht über einen Flowtype abbildbar sind (bspw. Einlösen von E-Rezepten im europäischen Ausland oder der Übertrag des digitalen Durchschlags für T-Rezepte an den BfArM-Webservice). Features werden im FHIR-IG beschrieben und müssen bei der Konzeption so abgekapselt werden, dass eine Deaktivierung technisch umsetzbar ist. Das Deaktivieren eines Features verhindert die Ausführung der zugehörigen Operationsaufrufe bzw. Prozessschritte.

Die Definition eines Features wird im jeweiligen FHIR-IG beschrieben und als FeatureDefinition Ressource bereitgestellt.

5.9.3 Konfiguration des Referenzzeitpunkts für die FHIR-Validierung

Der TI-Flow-Fachdienst verwendet für die FHIR-Validierung jeweils eine definierte Kombination aus FHIR-Packages (FHIR-Konfiguration). Da der TI-Flow-Fachdienst auch externe FHIR-Pakete (bspw. kbv.ita.erp) unterstützt, die sich außerhalb des IG-Release-Zyklus ändern können, publiziert die gematik die FHIR-Konfigurationen außerhalb des FHIR-IGs (bspw. auf GitHub oder [RUaaS]). In einer Instanz ist jeweils genau eine FHIR-Konfiguration aktiv. Der Bezeichner der aktiven Konfiguration wird im CapabilityStatement ausgegeben (bspw. "fhir_config": "tif_fhir_2028_01").

Zur Unterstützung von Testumgebungen existiert ein optionaler Konfigurationsparameter, der einen zeitlichen Versatz (Offset) des Referenzzeitpunkts für die FHIR-Validierung ermöglicht. Dieser Parameter darf ausschließlich in Test- und Referenzumgebungen

gesetzt werden und erlaubt es, eine vorgelagerte FHIR-Validierung zu erzielen, ohne andere Systemkomponenten anpassen zu müssen. In der Produktivumgebung darf dieser Parameter nicht gesetzt sein.

A_29773 -Anbieter TI-Flow-Fachdienst - Übernahme der FHIR-Konfiguration

Der Anbieter TI-Flow-Fachdienst MUSS die von der gematik veröffentlichte FHIR-Konfiguration übernehmen und im TI-Flow-Fachdienst bereitstellen.【<=】

Ein Beispiel für eine FHIR Konfiguration kann in der API-ERP angesehen werden:

https://github.com/gematik/api-erp/blob/master/resources/configuration/2026-07-01_fhir-transition.json

6 Anhang - Verzeichnisse

6.1 Abkürzungen

Kürzel	Erläuterung
API	Application Programming Interface
ASL	Application Security Layer
AuthZ	Authorization
AVS	Apothekenverwaltungssystem
BDE	Betriebsdatenerfassung
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
CDA	Clinical Document Architecture
CEK	Content-Encryption-Key
CET	Central European Time
CEST	Central European Summer Time
CN	Common Name
CRL	Certificate Revocation List
CS	CodeSystem
cVM	Confidential Virtual Machine
DDoS	Distributed Denial of Service
DLQ	Dead Letter Queue
DNS	Domain Name System
DPoP	Demonstrating Proof-of-Possession
DoS	Denial of Service
DSGVO	Datenschutz-Grundverordnung

eBtM	elektronisches Betäubungsmittel Rezept
eGK	elektronische Gesundheitskarte
eIDAS	Electronic Identification, Authentication and Trust Services
ePA	elektronische Patientenakte
eÜ	elektronische Überweisung
FD	Fachdienst
FdV	Frontend des Versicherten
FHIR	Fast Healthcare Interoperability Resources
HCC	Healthcare Confidential Computing
HKP	Häusliche Krankenpflege
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDP	Identity Provider
IG	Implementation Guide
JWKS	JSON Web Key Set
KIS	Krankenhausinformationssystem
KVNR	Krankenversichertennummer
LEI	Leistungserbringerinstitution
mTLS	Mutual Transport Layer Security
NCPeH	National Contact Point for eHealth
NTP	Network Time Protocol
OCI	Open Container Initiative
OCSP	Online Certificate Status Protocol
OTEL	OpenTelemetry

OWASP	Open Worldwide Application Security Project
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
PKI	Public Key Infrastructure
PoPP	Proof of Patient Presence
PQC	Post-Quantum Cryptography
PU	Produktivumgebung
PVS	Praxisverwaltungssystem
QES	Representational State Transfer
REST	Representational State Transfer
RFC	Request for Comments
RU	Referenzumgebung
SAN	Subject Alternative Name
SGL	Security Governance Level
SIEM	Security Information and Event Management
SKI	Subject Key Identifier
SM(C)	Secure Module (Card)
SMC-B	Security Module Card Typ B
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TU	Testumgebung
VAU	vertrauenswürdige Ausführungsumgebung
ZETA	Zero Trust Access

ZPVS	Zahnärztliches Praxisverwaltungssystem
------	--

6.2 Glossar

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.
Versicherten-ID	10-stelliger unveränderlicher Teil der Krankenversichertennummer (KVNR)

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

6.3 Abbildungsverzeichnis

Abbildung 1: Systemüberblick TI-Flow-Fachdienst.....	8
Abbildung 2: Entstehung FHIR-ValidatorImage für TI-Flow-Fachdienst.....	29

6.4 Tabellenverzeichnis

Tabelle 1: TAB_TI-Flow_Konfigurationsübersicht_ZETA_Guard.....	24
--	----

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.

[Quelle]	Herausgeber: Titel
[API-ERP: FHIR-Transition]	gematik: E-Rezept API Dokumentation / Konfiguration https://github.com/gematik/api-erp/blob/master/resources/configuration/2026-07-01_fhir-transition.json
[gemAnbT_TI-Flow-FD]	gematik: Anbietertypsteckbrief TI-Flow-Fachdienst https://gemspec.gematik.de/docs/gemAnbT/gemAnbT_TI-Flow-FD/latest/

[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar https://fachportal.gematik.de/glossar
[gemProdT_TI-Flow-FD]	gematik: Produkttypsteckbrief TI-Flow-Fachdienst https://gemspec.gematik.de/docs/gemProdT/gemProdT_TI-Flow-FD/latest/
[gemSpec_HCC]	gematik: Spezifikation Healthcare Confidential Computing (HCC) https://gemspec.gematik.de/docs/gemSpec/gemSpec_HCC/latest/
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur https://gemspec.gematik.de/docs/gemSpec/gemSpec_Krypt/latest/
[gemSpec_Perf]	gematik: Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform https://gemspec.gematik.de/docs/gemSpec/gemSpec_Perf/latest/
[gemSpec_PKI]	gematik: Übergreifende Spezifikation PKI https://gemspec.gematik.de/docs/gemSpec/gemSpec_PKI/latest/
[gemSpec_ZETA]	gematik: Spezifikation Zero Trust Access (ZETA) https://gemspec.gematik.de/docs/gemSpec/gemSpec_ZETA/latest/
[gematik Referenzvalidator]	gematik: Gematik Referenzvalidator https://github.com/gematik/app-referencevalidator
[RUaaS]	gematik: RU as a Service https://wiki.gematik.de/spaces/RUAAS/pages/444109897/E-Rezept+RU

6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[AnbieterV ZeitD]	Die Bundesnetzagentur listet unter https://www.elektronische-vertrauensdienste.de/EVD/DE/Uebersicht_eVD/Dienste/5_Zeitstempel.html?nn=691392 verschiedene Anbieter für qualifizierte Zeitstempel.
[HL7 Java Validator]	https://github.com/hapifhir/org.hl7.fhir.core