Elektronische Gesundheitskarte und Telematikinfrastruktur

Feature:
IDP Föderation

Version:	1.0.0 CC
Revision:	477820
Stand:	11.07.2022
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemF_IDP_Federation

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0 CC	11.07.22		initiale Erstellung des Dokuments	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments

1.1 Motivation und Zielsetzung

Eine zentrale Herausforderung im deutschen Gesundheitswesen stellt die Zusammenarbeit zwischen unterschiedlichen Versorgungsbereichen über deren eigene Grenzen hinweg dar. Der weitreichende und globale Megatrend der Digitalisierung macht auch vor den über Jahre gewachsenen Strukturen des Gesundheitswesens keinen Halt. Er bildet dabei gleichzeitig die elementare Grundvoraussetzung für einen effizienten und sektorübergreifenden Datenaustausch. Die TI 2.0 als Arena für digitale Medizin trägt hierbei zur Qualitäts- und Effizienzverbesserung in der Patientenversorgung bei und stellt die Basisplattform für das digitale Ökosystem der Gesundheitsdaten von morgen. Zur Realisierung der Ziele fußt die TI 2.0 auf sechs architektonischen Säulen. Die erste Säule stellt das föderierte Identitätsmanagement dar. Auch auf Ebene der Gesetzgebung wurde der Bedarf an digitalen Identitäten erkannt und in einschlägigen Paragrafen entsprechend gefordert. Grundlegend geht es bei deren Einführung, die heutigen Identitäten, welche über die elektronische Gesundheitskarte, den elektronischen Heilberufsausweis und die Institutionskarte SMC-B an eine physische Chipkarte gebunden sind, um kartenunabhängige Identitätsträger zu ergänzen. Dabei kommt sowohl den Kostenträgern als auch den Leistungserbringerorganisationen als Identitätsherausgeber eine zentrale Rolle zu: Zur Bereitstellung der digitalen Identität sind diese in der Verantwortung, für ihre Versicherten bzw. Mitglieder einen sog. Identity Provider (IDP) aufzubauen, welcher die Authentifizierung zur Nutzung der Anwendungen übernimmt.

Unter dem Identity Provider versteht man ein zentrales Zugangssystem, an welchem sich ein Nutzer authentisieren kann, um im Anschluss die angebundenen Fachanwendungen unmittelbar nutzen zu können. Die Kommunikation zwischen IDP und Fachanwendung läuft über den sog. OpenID Connect Standard. In diesem Kontext kommt dem IDP eine kritische Rolle zu, da dieser das Eingangstor zur Nutzung sämtlicher Fachanwendungen bereitstellt und somit maßgeblich zur gesamtheitlichen Nutzerakzeptanz der Dienste beiträgt.

Neben der Backend-Komponente zur Verwaltung der Nutzeridentitäten gehört ein Authenticator-Modul zum Gesamtumfang eines sektoralen IDP. Dieses kann entweder in eine App integriert sein oder als eigenstehende App bereitgestellt werden, um gemeinsam mit dem Backend die Authentisierung des Nutzers durchzuführen.

Das vorliegende Feature-Dokument verfolgt das Ziel, die Ausgangslage und den Kontext der Bereitstellung der digitalen Identitäten zu erläutern und aufbauend auf den User Stories, eine Übersicht über relevante Anforderungen (Afos) und weitergehende Spezifikationen zu liefern.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter von Produkten zur Realisierung der IDP-Föderation mit dem Fokus auf den Versichertenkontext. Es beschreibt die Änderungen, welche sich an Komponenten ergeben, um die Integration von sektoralen IDP zu ermöglichen.

1.3 Abgrenzungen

Das Dokument umfasst in Kapitel 4 Änderungen an bestehenden Spezifikationen bzw. Steckbriefen der gematik und ist daher als Ergänzung zur entsprechenden Spezifikation der gematik zu verstehen und zu lesen. Der als Teil dieses Features vollständig überarbeitete Produkttyp des sektoralen Identity Provider wird detailliert im neuen Dokument [gemSpec_IDP_Sek] spezifiziert und hier nur referenziert. Der neue Produkttyp des Federation Master wird detailliert im neuen Dokument [gemSpec_IDP _FedMaster] spezifiziert und ebenfalls nur referenziert. Die neuen Dokumente für die Produkttypen sowie die entsprechenden Steckbriefe werden ergänzend zur Feature-Spezifikation veröffentlicht.

Das vorliegende Dokument behandelt in erster Linie die Bereitstellung und Nutzung der digitalen Identitäten für die Nutzergruppe der Versicherten. Technisch bildet die Spezifikation auch die Grundlage für die IDPs im Leistungserbringer- und Leistungserbringerorganisationskontext. Die fachlichen Use Cases und weiteren technischen Anforderungen werden jedoch erst in einer weiteren Spezifikationsstufe beschrieben. Des Weiteren ist die Spezifikation nicht als Information für den Endnutzer, sprich den Versicherten gedacht. Diese werden durch die Kostenträger informiert. Auch PVS-Hersteller sind durch die Inhalte der Spezifikation nicht betroffen. Ebenfalls ist klar abzugrenzen, dass die Einführung der digitalen Identitäten nicht die Anwendung VSDM (weder in der aktuellen noch in einer zukünftigen Ausbaustufe) ersetzen soll. Schließlich ist der Produkttyp der sektoralen IDPs in Föderation klar abzugrenzen von den Spezifikationsdokumenten des Fasttracks, welche vordergründig auf die Authentisierung am E-Rezept fokussiert sind.

1.4 Methodik

Die Spezifikation ist im Stil einer RFC-Spezifikation verfasst. Dies bedeutet:

- **Der gesamte Text in der Spezifikation ist sowohl für den Hersteller des Produktes Federation Master als auch für den betreibenden Anbieter entsprechend [gemKPT_Betr] verbindlich zu betrachten und gilt als Zulassungskriterium beim Produkt und Anbieter.**
- Die Verbindlichkeit SOLL durch die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet werden.
- Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen." die Phrase „DARF NICHT" semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen „Eine leere Liste DARF KEIN Element besitzen." verwendet.
- Die Schlüsselworte KÖNNEN außerdem um Pronomen in Großbuchstaben ergänzt werden, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

1.4.1 Anforderungen

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in eckigen Klammern sowie die dem RFC 2119 [RFC2119] entsprechenden, in

Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:
<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

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

1.4.2 Anwendungsfälle und Akzeptanzkriterien

Anwendungsfälle und als Ausdruck normativer Festlegungen werden als Grundlage für Erlangung der Zulassung durch Tests geprüft und nachgewiesen. Sie besitzen eine eindeutige, permanente ID, welche als Referenz verwendet werden SOLL. Die Tests werden gegen eine von der gematik gestellte Referenz-Implementierung durchgeführt.

Anwendungsfälle und Akzeptanzkriterien werden im Dokument wie folgt dargestellt:
<ID> - <Titel des Anwendungsfalles / Akzeptanzkriteriums>
Text / Beschreibung
[<=]

Die einzelnen Elemente beschreiben:

- **ID**: einen eindeutigen Identifier.
  - Bei einem Anwendungsfall besteht der Identifier aus der Zeichenfolge 'AF_' gefolgt von einer Zahl,
  - Der Identifier eines Akzeptanzkriteriums wird von System vergeben, z. B. die Zeichenfolge 'ML_' gefolgt von einer Zahl
- **Titel des Anwendungsfalles / Akzeptanzkriteriums**: Ein Titel, welcher zusammenfassend den Inhalt beschreibt
- **Text / Beschreibung**: Ausführliche Beschreibung des Inhalts. Kann neben Text Tabellen, Abbildungen und Modelle enthalten

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

Der für die Erlangung einer Zulassung notwendige Nachweis der Erfüllung des Anwendungsfalls wird in den jeweiligen Steckbriefen festgelegt, in denen jeweils der Anwendungsfall gelistet ist. Akzeptanzkriterien werden in der Regel nicht im Steckbrief gelistet.

1.4.3 Hinweise

- Das Ursprungskapitel der jeweiligen Dokumente wird in Klammern () geschrieben im Titel der Unterkapitel geschrieben.
- Hinweise zu den Unterkapiteln werden wie Änderungen dargestellt.
- Hinweis auf offene Punkte: Themen, die noch intern geklärt werden müssen oder eine Entscheidung seitens der Gesellschafter erfordern, sind wie folgt im Dokument gekennzeichnet:

238

Offener Punkt: Das Kapitel wird in einer späteren Version des Dokumentes ergänzt.

239

2 Fachliche Grundlage der Spezifikation

2.1 Begriffsbestimmungen

Zum Verständnis des Dokumentes werden zunächst die wesentlichen Begrifflichkeiten geklärt. (Ein erweitertes Abkürzungsverzeichnis und Glossar findet sich im Anhang dieses Dokuments.)

Identität: Eine Identität ist eine Menge von Identitätsattributen, die einer [Person oder Organisation] zugeordnet sind. Eine eindeutige Identität ist eine Identität, die innerhalb eines bestimmten Anwendungskontextes die zugehörige Entität eindeutig repräsentiert, unterschiedliche Entitäten haben unterschiedliche eindeutige Identitäten. Eine Identität (das heißt eine Menge von Identitätsattributen), die innerhalb eines Anwendungskontextes eindeutig ist, ist dies nicht notwendigerweise auch in einem anderen Kontext. (BSI TR-03107)

Attribut: Ein Identitätsattribut oder ein Identitätsdatum ist eine Charakteristik oder eine Eigenschaft einer Entität. Beispiele für Identitätsattribute einer natürlichen Person sind Name, Geburtsdatum oder die Eigenschaft, ein bestimmtes Alter erreicht zu haben. Identitätsattribute von Behörden umfassen etwa Bezeichnung der Behörde oder deren Webadresse. (BSI TR-03107)

Authentisierung/Authentifizierung: „Authentifizierung" ist ein elektronischer Prozess, der die Bestätigung der elektronischen Identifizierung einer natürlichen oder juristischen Person oder die Bestätigung des Ursprungs und der Unversehrtheit von Daten in elektronischer Form ermöglicht. (eIDAS)

Eine Authentisierung ist das Versehen einer Identität […], die es einer vertrauenden Entität ermöglichen, die Herkunft, Echtheit und Gültigkeit der Identität […] zu überprüfen . Der Überprüfungsvorgang durch die vertrauende Entität ist die Authentifizierung der Identität […]. (BSI TR-03107)

Authentisierungsmittel: Authentisierungsmittel sind technische Mittel, die es dem Inhaber erlauben, eine Identität (das heißt eine Menge von Identitätsattributen) oder andere übermittelte Daten zu authentisieren. Beispiele für Authentisierungsmittel sind Passwörter, der Personalausweis oder kryptographische Token. Sind mehrere technische Mittel notwendig (etwa Chipkarte und PIN), so besteht das vollständige Authentisierungsmittel aus mehreren Authentisierungsfaktoren. (BSI TR-03107).

Multifaktor-Authentisierung: Multifaktor-Authentisierung ist eine Form der Authentisierung, bei welcher zur Identitätsbestätigung mehrere unabhängige Merkmale (Faktoren) überprüft werden. Üblicherweise werden für eine Zwei-Faktor-Authentisierung unterschiedliche Merkmale aus Wissen, Besitz, Biometrie, Standort miteinander kombiniert. Am häufigsten kommt im Bereich der mobilen Anwendungen die Kombination aus Faktor Besitz (repräsentiert durch das Smartphone) und Faktor Biometrie (z. B. durch FaceID oder TouchID) bzw. Faktor Wissen (z. B. eine PIN) zum Einsatz.

Enrolement: Das Enrolement ist die Registrierung einer Entität in einem Authentisierungssystem, meist verbunden mit einer Identitätsprüfung, die in der Ausgabe von Authentisierungsmitteln mündet. (BSI TR-03107)

Identifizierung: Eine Identifizierung ist die Übermittlung von anwendungsbezogen geeigneten Identitätsattributen (einer Identität), einschließlich authentisierender

Metadaten (Authentisierung), sowie die Überprüfung (Authentifizierung) dieser Identität durch die vertrauende Entität. (BSI TR-03107)

Identifizierungsdiensteanbieter: Diensteanbieter, deren Dienst darin besteht, für einen Dritten eine einzelfallbezogene Identifizierungsdienstleistung mittels des elektronischen Identitätsnachweises nach § 18 zu erbringen (§ 2 Abs. 3a PAuswG).

Autorisierung: Die Autorisierung einer Entität ist die Zuordnung und Überprüfung von Rechten zu einer Entität, zum Beispiel Zugriffsrechte oder das Recht, eine bestimmte Anwendung zu nutzen. Eine Autorisierung erfolgt immer anwendungsbezogen […]. (BSI TR-03107)

2.2 Technische Grundlagen

Für ein grundlegendes Verständnis des Konzeptes des föderierten Identitätsmanagements werden in diesem Kapitel zunächst die Grundlagen des eingesetzten Authentifizierungsprotokolls und die relevanten technischen Parameter kurz erläutert. Unter einem Authentifizierungsprotokoll versteht man im Allgemeinen eine Reihe an Befehlen, die zur Verifizierung einer Nutzeridentität zwischen zwei Entitäten verwendet werden. Für unterschiedliche Einsatzszenarien haben sich verschiedene Authentifizierungsprotokolle und De-Facto-Standards etabliert. Im Rahmen der Mensch-zu-Gerät Authentisierung in der Telematikinfrastruktur wird das sog. OpenID Connect Protokoll verwendet, welches auf dem sog. OAuth 2.0-Standard basiert und diesen um Informationen zur Identität über Attribute erweitert.

OAuth 2.0: Hinter dem Begriff verbirgt sich ein **Autorisierungsdienst**, welcher es einem registrierten Nutzer ermöglicht, die Kontrolle über die Art und den Umfang der von ihm erteilten Freigaben zu steuern. Der Benutzer kann mittels OAuth der anfragenden Drittanwendung (dem sog. „**Client**“) erlauben, auf Daten des Nutzers auf einem **Resource-Server** (z. B. Bilder, Dokumente, u.ä.) zuzugreifen. Dazu authentisiert ein **Authorization-Server** den Nutzer z. B. mit username + Passwort und fordert von ihm die Erlaubnis (**Consent**) für den Zugriff des Client auf die Resource ein. Für den Zugriff auf die Daten des Nutzers vom Resource-Server erhält der Client ein **`ACCESS_TOKEN`**, welches dieser bei jedem Aufruf des Resource-Server mit übertragen muss. Vor Herausgabe des der Daten prüft der Resource-Server durch eine Abfrage beim Authorization-Server, ob die Datenherausgabe an den Client legitim ist. OAuth 2.0 unterstützt `scopes` (Gruppe von Informationen), allerdings ohne diese weiter zu benennen. OAuth 2.0 kümmert sich ausschließlich um die Autorisierung von Zugriffen durch einen Nutzer, nicht aber um dessen Authentifizierung.

OpenID Connect (OIDC): Der OIDC-Standard erweitert OAuth 2.0 um die Fähigkeit der Nutzer-**Authentisierung**. Neben dem Zugriffstoken (`ACCESS_TOKEN`) liefert die Erweiterung OIDC nach erfolgreicher Nutzer-Authentisierung einen **`ID_TOKEN`,** welche Informationen (`claims`) zum Nutzer selbst enthält. `Claims` sind Eigenschaftsattribute (z. B. der Vorname oder die Mailadresse). Die Zusammenfassung von `claims` zu logischen Gruppen werden als `scopes` bezeichnet. Diese Identitätsdaten des Nutzers werden von einem **Identity Provider** in dem `ID_TOKEN` verpackt und als Json Web Token (**JWT**) einem anfragenden Client zur Verfügung gestellt.

2.3 Identifikationsmittel und -systeme

Es gibt je nach Schutzbedarf und Regulierungsniveau der zu verwendenden Anwendung unterschiedliche Möglichkeiten, eine Identifizierung des Nutzers durchzuführen. Gesundheitsdaten weisen nach DSGVO einen besonders schützenswerten Charakter auf. Folglich muss bei deren Zugriff absolut zweifelsfrei sichergestellt sein, dass dieser nur durch berechtigte Personen möglich ist. Hierfür gibt es in Deutschland unterschiedliche hoheitliche Identifikationssysteme mit einer jeweiligen Zweckbindung. Sie dienen dazu, eine Person oder ein Objekt eindeutig innerhalb eines Nutzungskontextes zu identifizieren. Im Kontext des Gesundheitswesens dient die Gesundheitskarte mit zugehöriger Krankenversichertennummer als Identifikationsmittel mit entsprechender Zweckbindung. Diese kann über einen Chip mit NFC Funktionalität und ein Lichtbild für Vor-Ort- bzw. eine PIN für eine Identifizierung online und vor Ort eingesetzt werden. Des Weiteren stellt der neue Personalausweis mit integrierter eID-Funktionalität ein universell einsetzbares Identifikationssystem dar. Zu dessen digitaler Verwendung muss die zugehörige PIN durch den Nutzer freigeschaltet werden. Auf Basis des Personalausweises existieren unterschiedliche Identifizierungsverfahren. Das sicherste Verfahren ist das Online-Ausweisident-Verfahren, bei welchem das Auslesen des Datensatzes mittels NFC-Schnittstelle über die Eingabe der PIN abgesichert wird.

2.4 Die Ausgangslage im deutschen Gesundheitswesen

Die Telematikinfrastruktur (TI) ist die Plattform für Gesundheitsanwendungen in Deutschland. Millionen Versicherte profitieren durch die digitalen Anwendungen der TI von einer verbesserten medizinischen Versorgung. Ziel und Aufgabe der gematik ist es, diese Infrastruktur auszubauen, zu modernisieren und so fit für das digitale Gesundheitswesen der Zukunft zu machen.

Im Jahr 2005 wurde mit dem Aufbau der Telematikinfrastruktur durch die gematik begonnen. Mit dem Whitepaper zur Telematikinfrastruktur 2.0 wurde 2020 von der gematik ein Impuls veröffentlicht, die TI als zukunftsfähige Arena für digitale Medizin voranzutreiben.

Die Architektur der TI 2.0 basiert demnach auf sechs fundamentalen Säulen:

1. Einem föderierten Identitätsmanagement, weil mit dieser "Brücke" mehr Flexibilität und Nutzerfreundlichkeit durch die einfache Nutzung von Identitätsbestätigungen der TI für eigene digitale Angebote der Nutzergruppen möglich ist.
2. Der universellen Erreichbarkeit der Dienste, weil der Wegfall proprietärer IT-Lösungen (z. B. Konnektor) Kosten senkt und den Betrieb stabilisiert.
3. Einer modernen Sicherheitsarchitektur, weil diese die eigenständige Bereitstellung von Diensten durch unterschiedliche Anbieter ermöglicht und sowohl sicherer als auch effizienter ist.
4. Verteilten Diensten, weil aus Sicht optimierter Versorgungsprozesse die Verknüpfung von Daten aus verschiedenen Quellen notwendig ist.
5. Interoperabilität und strukturierte Daten, weil die anwendungsfallbezogene Versorgung und Forschung eine Verbesserung der Datenqualität erfordert. Standardbasierte strukturierte Daten und Schnittstellen erhöhen die Verfügbarkeit bei Produkten und Services.

6. Einem automatisiert verarbeitbaren Regelwerk der TI, weil eine automatisierte Überprüfung der Sicherheit und des Datenschutzes sowie der Interoperabilität und Verfügbarkeit das Vertrauen in die TI stärken.

Das vorliegende Dokument stellt die spezifikatorische Grundlage für die erste Säule des föderierten Identitätsmanagements.

Zu deren Verständnis werden im weiteren Verlauf dieses Kapitels zunächst die elementaren Grundpfeiler des Identitätsmanagements im Gesundheitswesen vorgestellt und soweit notwendig erläutert.

2.4.1 Identitätsherausgeber, Identitätsträger und Trust Service Provider

Unter Identitätsherausgeber versteht man diejenigen Instanzen, welche die Datenhoheit über die (digitalen) Identitäten und deren zugehörige Attribute besitzen. Für unterschiedliche Sektoren gibt es unterschiedliche Identitätsherausgeber, welche im SGB V geregelt werden. Je Sektor existieren spezifische Identitätsträger, welche in der Telematikinfrastruktur 1.0 über Smartcards repräsentiert werden und in der TI 2.0 durch digitale Identitäten bereitgestellt werden sollen.

Im gesetzlichen Versichertensektor agieren die Krankenkassen als Identitätsherausgeber, welche für ihre Versicherten die elektronische Gesundheitskarte als Identitätsträger herausgeben. Die gesetzliche Grundlage hierfür bilden §291 SGB V. In Deutschland gibt es derzeit 97 gesetzliche Krankenkassen (Stand 01.01.2022). Jede Kasse ist selbst für die Ausgabe der Identitätsträger zuständig. Eine Ausgabe von elektronischen Gesundheitskarten als Identitätsträger durch private Krankenversicherer gibt es derzeit nicht.

Im Leistungserbringerbereich wird die Identitätsherausgabe, im engeren Sinne die Ausgabe von elektronischen Heilberufs- und Berufsausweisen sowie von Komponenten zur Authentifizierung von Leistungserbringerinstitutionen, in § 340 SGB V geregelt. Die Identitätsherausgeber werden demnach durch die Länder bestimmt. In der praktischen Umsetzung ergibt sich hieraus die Zuständigkeit für die Herausgabe der elektronischen Heilberufsausweise durch die Kammern auf Landesebene (z. B. Landesärztekammern, Landeszahnärztekammern, Psychotherapeutenkammern, Apothekerkammern, Handwerkskammern). Darüber hinaus übernehmen die gematik und das elektronische Gesundheitsberuferegister (eGBR) für ausgewählte Gruppen die Rolle des Identitätsherausgebers, sodass sich in Summe für den Identitätsträger eHBA rund 100 Identitätsherausgeber ergeben. Die Herausgabe der SMC-Karte als Identitätsträger für Leistungserbringerinstitutionen übernehmen je Sektor die Kassen(-zahn)ärztlichen Vereinigungen, Apothekerkammern, DKTIG, gematik, Gesundheitsberuferegister und Handwerkskammern. Hier agieren in Summe rund 70 Identitätsherausgeber für den Identitätsträger der SMC-B-Karte.

Die Identitätsherausgeber beauftragen in der Regel einen sog. Trust Service Provider mit der Bereitstellung der Identitätsträger als Authentisierungsmittel. Ein Trust Service Provider oder Vertrauensdiensteanbieter ist eine Organisation, welche digitale Zertifikate bereitstellt, um elektronische Signaturen zu erstellen und zu validieren und ihre Unterzeichner im Allgemeinen zu authentifizieren.

2.4.1.1 Elektronische Gesundheitskarte

Die elektronische Gesundheitskarte (eGK) ist eine personenbezogene Smartcard. Die eGK gilt seit Anfang 2015 als ausschließlicher Krankenversicherungsnachweis für gesetzlich Versicherte. Neben den kryptographischen Schlüsseln und dazugehörigen Zertifikaten zur

Authentisierung gegenüber der TI dient sie auch als dezentraler Speicher für die Anwendungen Notfalldaten-Management, Datensatz Persönliche Erklärung, Organspendeerklärung, E-Medikationsplan und dem Versichertenstammdaten-Management. Außerdem kann durch das Stecken der eGK in der Leistungserbringerumgebung (z. B. Arztpraxis oder Apotheke) eine Adhoc-Berechtigung für den Zugriff auf die elektronische Patientenakte (ePA) erteilt werden. Zukünftig sollen auch E-Rezepte durch Stecken der eGK in der Apotheke abgerufen werden können.

2.4.1.2 Elektronischer Heilberufsausweis

Der elektronische Heilberufsausweis ist eine personenbezogene Smartcard, welche an Leistungserbringer wie Ärzte, Zahnärzte oder Apotheker ausgegeben wird. Er enthält das kryptographische Schlüsselmaterial und die zugehörigen Zertifikate zur Authentisierung gegenüber der TI, zum Ausstellen einer qualifizierten elektronischen Signatur für die E-Rezept-Ausstellung, die Signatur von KIM-Nachrichten, Notfalldaten und dem elektronischen Arztbrief sowie der Verschlüsselung, Entschlüsselung und Umschlüsselung von Nachrichten.

2.4.1.3 SMC-B

Die Security Module Card Typ B ist eine institutionsbezogene Smartcard. Sie repräsentiert mit ihren Schlüsseln und Zertifikaten eine Institution innerhalb der TI und dient zur Authentisierung insbes. zum Zugriff der Daten der eGK, zur Signatur, Ver-, Ent- und Umschlüsselung von Nachrichten via KIM (Kommunikation im Medizinwesen). Darüber hinaus ist hierüber der ePA-Zugriff nach erteilter Freigabe durch den Nutzer möglich.

2.4.2 Der Weg zur TI 2.0

Die drei genannten Smartcard-Typen stellen in der Telematikinfrastruktur 1.0 die primären Identitätsträger dar. Jedoch bringt die Anwendung (ausschließlich) kartenbasierter Identitätsträger eine Reihe an Nachteilen und Einschränkungen mit sich. Als wesentliche Grenzen seien an dieser Stelle genannt:

- Smartcards schränkten die Usability ein, insbesondere im Einsatz mit mobilen Endgeräten
- In mobilen Szenarien ist die Einsetzbarkeit von Smartcards abhängig von der Gerätehardware (Vorhandensein und Platzierung des NFC-Moduls)
- Änderungen an Rollen oder Attributen in Zertifikaten auf Smartcards können nur schwer nachgerüstet werden. Für neue Nutzergruppen müssen neue Smartcards durch Herausgeber und TSPs bereitgestellt werden. Insbes. unter den aktuellen Lieferengpässen von Hardware und Chipkarten stellt dies seine große Einschränkung der Nutzeranbindung dar.
- Lange (Wieder-)beschaffungszeiten, insbesondere bedingt durch den aktuellen Engpass von Chipkarten.

Auch auf Seite des Gesetzgebers wurden diese Einschränkungen erkannt und die Einführung digitaler Identitäten vorgesehen. Die vorliegende Konzeption strebt an, die Gesamtheit der relevanten Use Cases in Bezug auf die Authentisierung zu betrachten, welche zuvor für den aktuellen Einsatz der Smartcards vorgestellt wurden. Diese sollen auch um die Einsatzszenarien der digitalen Identitäten erweitert werden. Weitere kartenbasierte Anwendungen wie beispielsweise der elektronische Medikationsplan oder

das Versichertenstammdaten-Management in deren jetziger Form werden in dieser Spezifikation nicht berücksichtigt.

Darüber hinaus kommen mit gSMC-K und gSMC-KT zwei gerätespezifische Sicherheitsmodulkarten in der TI zum Einsatz. Für das föderierte Identitätsmanagement finden diese jedoch keine Anwendung und werden deswegen nicht weiter betrachtet.

2.4.3 Gesetzliche Rahmenbedingungen

In diesem Kapitel folgt eine Übersicht über die relevantesten rechtlichen Grundlagen der vorliegenden Konzeption. Sie erhebt keinen Anspruch auf Vollständigkeit.

Die Begründung der verpflichtenden Einführung der digitalen Identitäten im Gesundheitswesen findet sich im fünften Sozialgesetzbuch. Hier heißt es:

„Spätestens ab dem 1. Januar 2023 stellen die Krankenkassen den Versicherten ergänzend zur elektronischen Gesundheitskarte auf Verlangen eine sichere digitale Identität für das Gesundheitswesen barrierefrei zur Verfügung, die die Vorgaben nach Absatz 2 Nummer 1 und 2 erfüllt und die Bereitstellung von Daten nach § 291a Absatz 2 und 3 durch die Krankenkassen ermöglicht" **(§291 Absatz 8 Satz 1 SGV V).**

Eine analoge Vorgabe für Leistungserbringer und deren Institutionen findet sich in Paragraph 340:

„(6) Spätestens ab dem 1. Januar 2024 haben die Stellen nach Absatz 1 Satz 1 Nummer 1 sowie den Absätzen 2 und 4 ergänzend zu den Heilberufs- und Berufsausweisen auf Verlangen des Leistungserbringers eine digitale Identität für das Gesundheitswesen zur Verfügung zu stellen, die nicht an eine Chipkarte gebunden ist" **(§340 Absatz 6 Satz 1 SGV V)**.

„(7) Spätestens ab dem 1. Januar 2024 haben die Stellen nach Absatz 1 Satz 1 Nummer 3 sowie den Absätzen 2 und 4 ergänzend zu den Komponenten zur Authentifizierung von Leistungserbringerinstitutionen auf Verlangen der Leistungserbringerinstitution eine digitale Identität für das Gesundheitswesen zur Verfügung zu stellen, die nicht an eine Chipkarte gebunden ist." **(§340 Absatz 7 Satz 1 SGV V).**

Des Weiteren definieren die jeweiligen Paragraphen die Rolle der Verantwortlichkeiten:

„Die Gesellschaft für Telematik legt die Anforderungen an die Sicherheit und Interoperabilität der digitalen Identitäten fest. Die Festlegung der Anforderungen an die Sicherheit und den Datenschutz erfolgt dabei im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragen für den Datenschutz und die Informationsfreiheit auf Basis der jeweils gültigen Technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik und unter Berücksichtigung der notwendigen Vertrauensniveaus der unterstützten Anwendungen." **(§291 Absatz 8 Satz 3 und 4 SGV V** bzw. sinngemäß **§340 Absatz 8 Satz 1 und 2 SGV V).**

Die entsprechenden Technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik beziehen sich auf:

- **BSI TR-03107** Elektronische Identitäten und Vertrauensdienste im E-Government
- **BSI TR-03147** Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen

Ferner beeinflussen Inhalte der Verordnung „über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt" (kurz: **eIDAS-Verordnung**, [eIDAS]) die Anforderungen an die Bereitstellung der digitalen Identitäten.

2.5 Fachliche Einordnung der Spezifikation gemSpec_IDP_Sek

Die Spezifikation [gemSpec_IDP_Sek] beschreibt Aufbau, Funktionsumfang und Schnittstellen der Identity Provider, welche im Rahmen einer Föderation den Zugang zur Telematikinfrastruktur alternativ der kartengebundenen Identitäten ermöglichen soll.

Unter Föderation versteht sich, dass jeder Sektor, und innerhalb der Sektoren die jeweiligen Identitätsherausgeber einen eigenen Identity Provider für dessen Mitglieder bereitstellt. Die vorliegende Spezifikation befasst sich hierbei vordergründig mit den digitalen Identitäten für den Sektor „Versicherte". Hierbei stellen die Kostenträger, sprich die gesetzlichen Krankenversicherungen und die privaten Versicherungsunternehmen jeweils eigene Identity Provider zur Verfügung, über welchen sich deren Versicherte gegenüber den Diensten der TI und kasseneigenen sowie Drittdiensten authentisieren können. Dabei ist es auch möglich, dass mehrere Institutionen auf freiwilliger Basis einen gemeinsamen IDP bereitstellen. Der Sektor der Leistungserbringer und deren Institutionen wird in einer weiteren Ausbaustufe der Spezifikation folgen.

Die Rahmenbedingungen können hierfür bereits als Grundlage angesehen werden. Die Orchestrierung der unterschiedlichen Identity Provider in der Föderation erfolgt über den sog. Federation Master [gemSpec_IDP_FedMaster]. Ziel der Föderation aus Versichertensicht ist es, dass sich jeder Nutzer an jedem relevanten Dienst der TI, der Kassen und an digitalen Gesundheitsanwendungen (DiGAs) mit einem zentralen Zugang über den IDP seiner Krankenversicherung authentisieren kann. Hierbei soll der IDP einen relevanten Basisdatensatz an Attributen, welcher zur Anwendungsnutzung benötigt wird, bereitstellen und in Form eines Tokens an die jeweilige Anwendung übergeben. Auf diese Weise soll den Versicherten über den zentralen Zugang eine komfortable und niederschwellige Nutzung ermöglicht sowie auf Seiten der Anwendungen eine Konzentration auf deren Kernprozesse vereinfacht werden.

2.5.1 Rahmenbedingungen des Authentisierungs-Flows

Relevante Anwendungen der IDP-Nutzung

Die Einführung digitaler Identitäten in Föderation beschreibt keinen Selbstzweck. Es geht dabei vordergründig darum, über einen zentralen Zugang die Nutzung sämtlicher Anwendungen des Gesundheitswesens sicher und komfortabel nutzen zu können. Dabei kommen Anwendungen zum Einsatz, welche kassenspezifisch und kassenübergreifend bereitgestellt werden.

Kassenübergreifende Anwendungen werden dadurch charakterisiert, dass die gleiche Anwendung für jeden Versicherten unabhängig seiner Krankenversicherung angeboten wird. Dabei müssen sich Versicherte unterschiedlicher Kassen über deren jeweiligen Kassen-IDP authentisieren können. Als kassenübergreifende Anwendungen sind insbesondere relevant:

- **E-Rezept**: Hierbei handelt es sich um eine kassenübergreifende Anwendung, welche zentral durch die gematik für alle Kassen bereitgestellt wird. Die entsprechenden Regelungen finden sich in §360 SGB V. Das E-Rezept ist eine zentrale Anwendung der Telematikinfrastruktur und somit eine der Kernnutzungsanwendung der digitalen Identitäten.
- **Digitale Gesundheitsanwendungen:** Der Leistungsanspruch auf digitale Gesundheitsanwendungen (kurz: DiGA) begründet sich auf das Digitale-

Versorgung-Gesetz. In der zugehörigen DiGA-Verordnung ist u.a. festgeschrieben, dass DiGA-Hersteller eine Authentisierung über die Kassen-IDPs ermöglichen müssen.

- **Drittanwendungen** mit Gesundheitsbezug: Des Weiteren soll es über die Kassen-IDPs auch ermöglicht werden, kassenübergreifende Dritt-Anwendungen, vordergründig mit einem Bezug zum Gesundheitswesen, nutzbar zu machen. Beispielsweise könnte dies eine kassenunabhängige App zur digitalen Terminbuchung von Arztterminen sein, an welcher sich ein Versicherter mit seinem Zugang des Kassen-IDPs authentisieren kann. Die Nutzung dieser Anwendungen ist nicht gesetzlich reguliert und obliegt der Hoheit der jeweiligen Kasse.

Darüber hinaus sollen über die digitalen Identitäten kasseneigene Anwendungen für Versicherte nutzbar gemacht werden. Diese müssen jeweils nur eine Authentisierung über den eigenen IDP ermöglichen. Versicherte anderer Kostenträger müssen an dieser Stelle nicht berücksichtigt werden. Es handelt sich insbesondere um folgende Anwendungen:

- **Elektronische Patientenakte:** Die Bereitstellung der elektronischen Patientenakte (kurz: ePA) durch die Kassen wird in §341 SGB V geregelt. Folglich ist diese Anwendung kassenspezifisch und muss entsprechend nur mit dem eigenen IDP kommunizieren können.
- **Kasseneigene Service-Anwendungen:** Dies können beispielsweise kasseneigene Service-Apps, Online-Geschäftsstellen oder Informations-Apps sein. Aus nutzerorientierten und wirtschaftlichen Gesichtspunkten heraus soll es den Kassen nach eigenem Ermessen möglich sein, auch für diese Anwendungen eine Nutzung mittels sektoralem Kassen-IDP zu implementieren.

Die Spezifikation der gematik richtet sich aufgrund der gesetzlichen Anforderungen vordergründig an den Anwendungen E-Rezept, DiGAs und ePA aus. Die Erweiterung des Funktionsumfangs eines Kassen-IDPs zur Nutzung weiterer, insbes. kasseneigener Anwendungen obliegt dem Kostenträger und ist außerhalb des Anwendungsbereichs der vorliegenden Spezifikation zu sehen, sofern sicherheitskritische Aspekte nicht beeinträchtigt werden.

Vertrauensniveaus

Das Vertrauensniveau einer Anwendung definiert sich aus dem Schutzbedarf der Daten, welche innerhalb der Anwendung verarbeitet werden. Die Zuordnung zu einem Vertrauensniveau berücksichtigt dabei u.a. die technische und organisatorische Sicherheit des Verfahrens sowie rechtliche Rahmenbedingungen. Die zugrundeliegende TR-03107 des BSI definiert hierbei 3 Vertrauensniveaus: normal, substantiell, hoch. Die zuvor beschriebenen Fokusanwendungen E-Rezept, DiGAs und ePA haben das Vertrauensniveau hoch inne. Folglich fokussiert sich die Spezifikation auf dieses Vertrauensniveau. Die Unterstützung von weiteren Vertrauensniveaus obliegt der Kasse und wird nicht durch die Spezifikation tangiert, sofern sicherheitskritische Aspekte nicht beeinträchtigt werden.

Bereitstellung von `claims`

Anwendungen fragen im Rahmen der Authentisierung spezifische `scopes` beim IDP an, welche sich aus vordefinierten `claims` zusammensetzen. Damit sichergestellt ist, dass der IDP für die Fokusanwendungen E-Rezept, DiGAs und ePA die erforderlichen

`scopes` bereitstellen kann, wird ein sog. Minimal `claims` Set definiert, welches ein IDP mindestens vorhalten muss, um an der Föderation teilzunehmen.

Offener Punkt: Genaue Zusammensetzung des Minimal `claims` Set

Zugriffsmedien

Die zuvor beschriebenen Anwendungen sollen über unterschiedliche Medien und Anwendungstypen ermöglicht werden. Im Grunde unterscheiden sich die Zugriffsmedien zwischen Smartphone (und hier weiter zwischen mobiler App und Browseranwendung) und zwischen Desktop-PCs. Sämtliche betrachteten Anwendungen können sowohl über eine App als auch über eine Browseranwendung bereitgestellt werden.

- **App-App-Flow:** Der App-App-Flow beschreibt die Einzelschritte für die Authentifizierung eines Nutzers im Rahmen einer Fachanwendung, bei der die Fachanwendung ein App ist, welche auf demselben Gerät wie die Authenticator-App installiert ist. Beispielsweise kommt dieser Flow zum Tragen, wenn ein Nutzer die E-Rezept-App auf seinem Smartphone benutzen möchte und sich mit der Kassen-App auf dem gleichen Gerät authentisiert.
- **Web-App-Flow auf einem Gerät:** Der Web-App-Flow beschreibt die Einzelschritte für die Authentifizierung eines Nutzers im Rahmen einer Web-Anwendung, welche im Browser desselben Geräts ausgeführt wird, auf dem auch die Authenticator-App installiert ist. Ein Beispiel hierfür ist eine DiGA als Webanwendung, für welche die Authentisierung per Kassen-App auf demselben Smartphone erfolgt.
- **Zwei-Geräte-Flow:** Der Zwei-Geräte-Flow beschreibt die Einzelschritte für die Authentifizierung eines Nutzers im Rahmen einer Fachanwendung, wobei die Fachanwendung eine App oder Web-Anwendung sein kann, welche auf einem anderen Gerät als die Authenticator-App ausgeführt wird. Als Beispiel ist hier ein Zugriff auf die ePA über einen Desktop-Browser zu nennen, für welche die Authentisierung per Kassen-App auf dem Smartphone erfolgt.

Hieraus ergibt sich der Bedarf an unterschiedlichen Flows, welche durch die IDPs zu unterstützen sind. Diese werden im Detail in [gemSpec_IDP_Sek] Anhang B detailliert beschrieben.

Offener Punkt: Definition der Kriterien und Prozesse, wie eine Drittanwendung in die Föderation aufgenommen wird.

2.5.1.1 Ablauf der Authentisierung

Der genaue Ablauf der Authentisierung hängt von den in diesem Kapitel beschriebenen Rahmenbedingungen ab. Diese entscheiden maßgeblich darüber, für welche Anwendung, über welches Medium und mit welchen Authentisierungsmitteln zugegriffen werden kann. Unabhängig der Rahmenbedingungen kommt der zuvor beschriebene Standard des OpenID Connect Protokolls zum Einsatz. In dessen Kontext wird nach erfolgreicher Authentifizierung des Nutzers beim IDP ein `ID_TOKEN` generiert und an die Fachanwendung übermittelt. Dieser Token enthält die durch den Client angefragten `scopes` einschl. weiterer relevanter Daten. Nach Erhalt des `ID_TOKEN` ist das eigentliche Zugriffsmanagement in der Verantwortung der Fachanwendung. Diese prüft, welche

Berechtigungen und ggf. Bevollmächtigungen für die Entität des `ID_TOKEN` vorliegen. Das Ergebnis dieser Prüfung äußert sich in der Ausstellung des `ACCESS_TOKEN` durch die Fachanwendung, über welchen der authentisierte Nutzer die Zugriffsberechtigung auf die Daten der Fachanwendung erhält.

2.6 Epic und User Stories

In diesem Abschnitt wird das Feature fachlich motiviert und der Mehrwert für Nutzer vorgestellt. Aus diesen Epics und User Stories wird anschließend unter Berücksichtigung der vorgestellten Ausgangslage im deutschen Gesundheitswesen ein technisches Konzept abgeleitet. Dabei wird sich in dieser Spezifikation auf die Versicherten- und Anwendungsanbietersicht beschränkt. Weitere Nutzergruppen wie z. B. Leistungserbringer werden in einer weiteren Stufe der Spezifikation behandelt.

2.6.1 Versichertensicht

2.6.1.1 Epic

Als Versicherter möchte ich jede Anwendung im Gesundheitswesen mit meiner digitalen Identität komfortabel, ortsunabhängig und jederzeit nutzen können, ohne dass eine Smartcard erforderlich ist.

2.6.1.2 User Stories

Die User Stories beschreiben die Erwartungen der Nutzer für die neuen digitalen Prozesse mit Bezug zur Abrechnung.

ID	User Story
	Als Versicherter möchte ich mich beim IDP meiner Kasse komfortabel, dauerhaft und sicher registrieren können, sodass eine Nutzung der angebundenen Dienste vollumfänglich möglich ist.

Akzeptanzkriterien:

„vollumfänglich“:

Mit meiner digitalen Identität kann ich mich auf dem höchsten Vertrauensniveau unmittelbar authentisieren

„komfortabel“:

- Die Identifizierung erfordert keine Bindung an Geschäftszeiten.
- Die Identifizierung kann ortsunabhängig erfolgen.
- Eine komfortable Registrierung ist für jeden Versicherten möglich.

„dauerhaft“:

- Die Identifizierung findet einmalig statt, sofern kein Ereignis eine begründete Neuidentifizierung* erfordert.

„sicher“:

- Die Identitätsfeststellung über einen Identifizierungsdiensteanbieter ist zweifelsfrei.

ID	User Story
	Als Versicherter möchte ich mit einem zentralen Zugang komfortablen Zugriff auf die TI-Anwendungen ePA, E-Rezept, sowie DiGAs und Drittanwendungen mit Gesundheitsbezug, die von meinem Kostenträger oder einem anderen Anbieter angeboten werden, erhalten.
	Als Versicherter möchte ich mich je nach Schutzbedarf der Anwendung mit unterschiedlichen Authentisierungsmitteln authentisieren können, sodass die Nutzung der Anwendung so komfortabel wie möglich und so sicher wie nötig ist.
	Als Versicherter möchte ich mich sowohl für die Nutzung einer mobilen App als auch für Browseranwendungen, welche auf meinem Smartphone oder einem Desktop-PC laufen authentisieren.
	Als Versicherter möchte ich mich an einer Anwendung einmalig authentisieren und im Anschluss alle Funktionen auf dem entsprechenden Vertrauensniveau unmittelbar ohne weitere Authentisierungsschritte nutzen können.

2.6.2 Anwendungsanbietersicht

2.6.2.1 Epic

Als Anbieter einer Anwendung möchte ich die sichere Authentifizierung meiner Nutzer an die IDP-Föderation delegieren, sodass ich mich auf die Mehrwertfunktionen meiner Anwendungen konzentrieren kann.

2.6.2.2 User Stories

ID	User Story
	Als Anbieter einer Anwendung möchte ich meine kassenübergreifende Anwendung über die digitale Identität der Versicherten jeder Kasse nutzbar machen.
	Als Anbieter einer Anwendung möchte ich meine kassenspezifische Anwendung über die digitale Identität der Versicherten dieser Kasse nutzbar machen.

668

Offener Punkt: Definition der Kriterien, welche eine Drittanwendung erfüllen muss, um in die Föderation aufgenommen zu werden

669

670

3 Einordnung in die Telematikinfrastruktur

Als sektoraler IDP wird ein Dienst zur Authentifizierung von Nutzern bezeichnet. Nach erfolgreichen Durchlaufen des Authentifizierungsprozesses stellt der sektorale IDP Identitätsinformationen für eine bestimmte Gruppe von Nutzern innerhalb der Telematikinfrastruktur des Gesundheitswesens bereitstellt. Diese werden anschließend durch den anfordernden Fachdienst verwendet, um auf dessen Fachdaten und -prozesse zuzugreifen. Insbesondere umfasst ein Sektor die Krankenkassen mit den Versicherten als Nutzer. Zukünftig werden allerdings auch andere Personengruppen wie z. B. Ärzte oder Pflegeinstitutionen über Identity Provider angebunden.

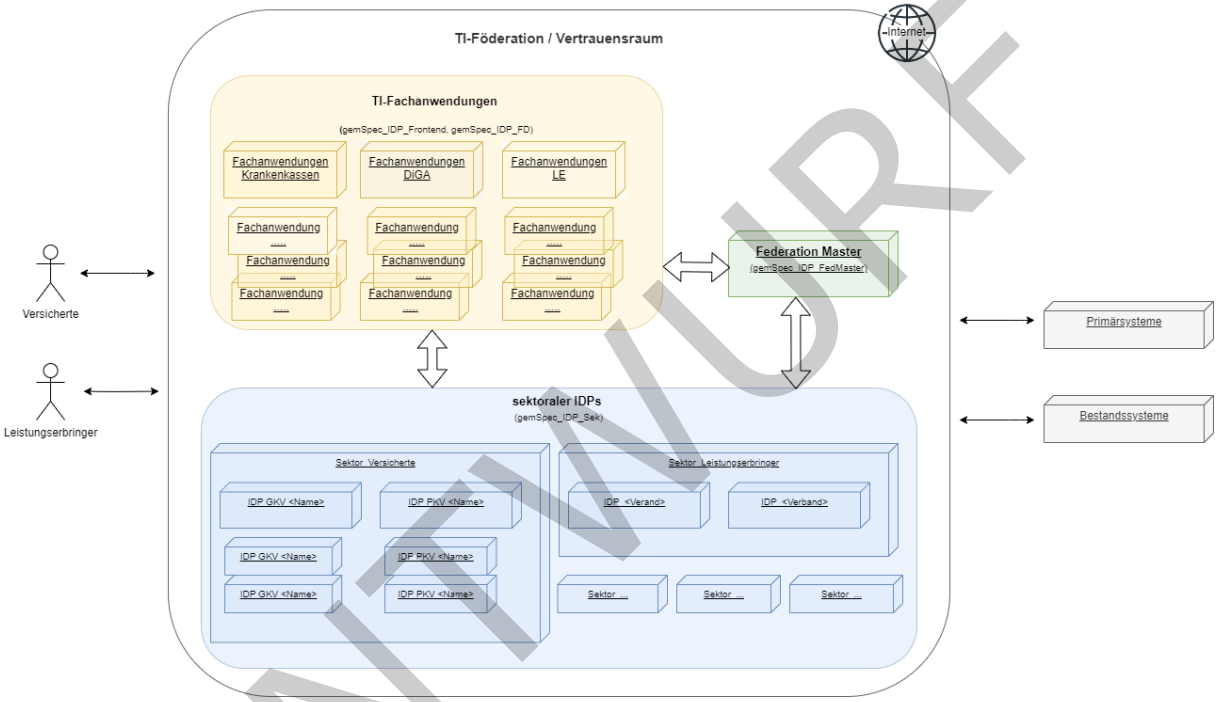

Abbildung 1 : Überblick TI-Föderation

Diese sektoralen Identity Provider werden durch dieses Featurerelease zusammen mit den Fachdiensten in einem gemeinsamen Vertrauensraum zusammengefasst.

Dieser Vertrauensraum wird durch den sogenannten Federation Master verwaltet. Der Federation Master basiert auf den Standards OpenID Connect (OIDC), Open Authorization 2.0 (OAuth 2) und JSON Web Token (JWT). Der Federation Master ist einerseits der Trust Anchor des Vertrauensbereichs der Föderation. Andererseits stellt der Federation Master Schnittstellen bereit, welche Auskunft über die in der Föderation registrierten sektoralen Identity Provider gibt.

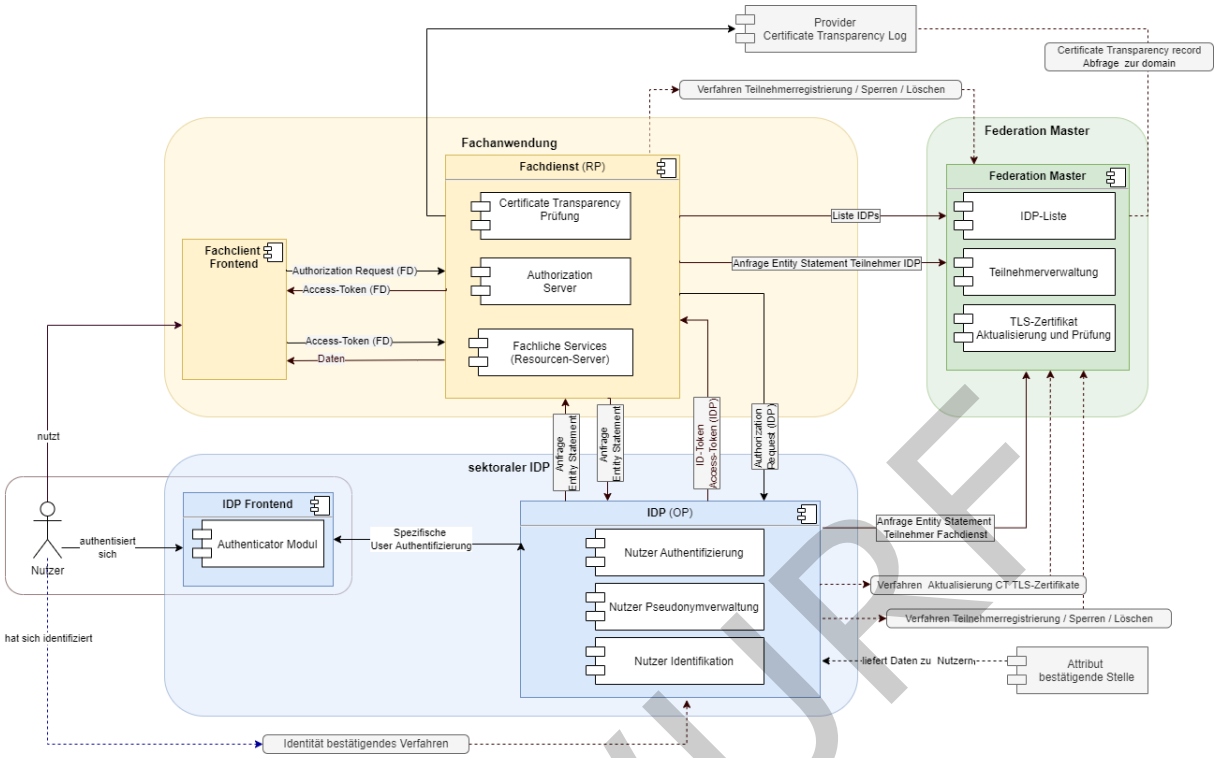

Abbildung 2 : Übersichtsschaubild OIDC Federation

Jeder Fachdienst verfügt über einen eigenen Authorization-Server, welcher basierend auf den Informationen der sektoralen Identity Provider über den jeweiligen Nutzer dessen Zugriffsrechte definiert.

Der zentralen IDP-Dienst welcher im Rahmen des sogenannten Fast-Track-E-Rezept als Mittler zwischen dem Anwendungsfrontend, den sektoralen Identity Providern und dem E-Rezept-Fachdienst eingesetzt wurde, übernimmt die Rolle des Authorization-Server für die Anwendung E-Rezept.

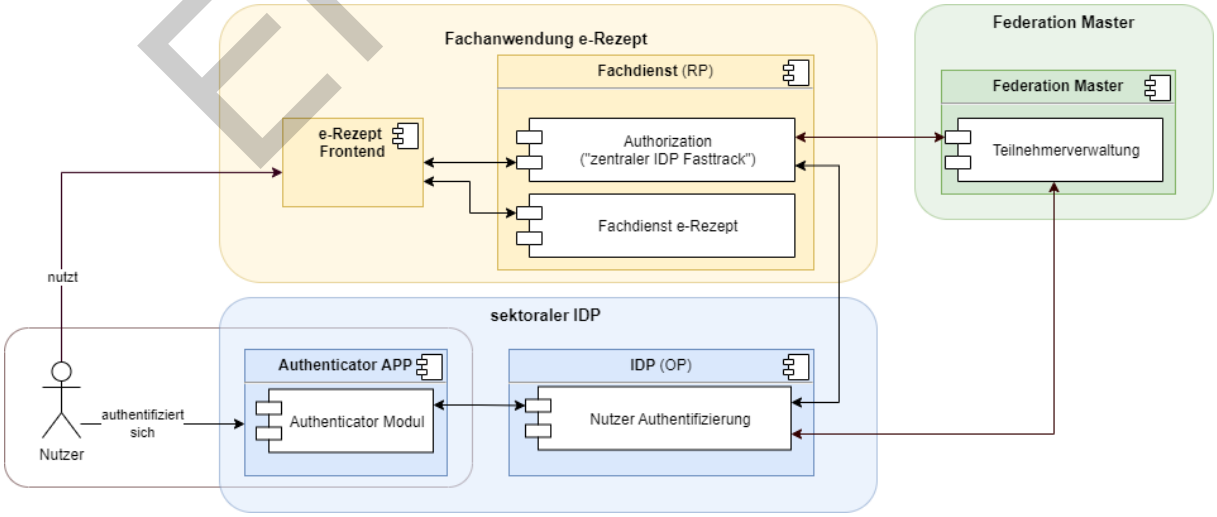

Abbildung 3 : e-Rezept in Föderation

4 Spezifikation

4.1 [gemSpec_IDP_FedMaster]

Hierbei handelt es sich um ein komplett neues Dokument. Es gehört zu diesem Feature-Release aber wird getrennt vom Feature Dokument behandelt.

4.2 [gemSpec_IDP-Sek]

Hierbei handelt es sich um ein umfangreich überarbeitetes Dokument. Es gehört zu diesem Feature-Release aber wird getrennt vom Feature Dokument behandelt.

4.3 [gemSpec_Perf]

neue Rohdaten-Use Cases ins Kap. 3.1.2.2 gemSpec_perf:

Ablösung der A_22226: (Entfernung IDP.UC_20 und IDP.UC_21)

Anpassung A_22013-01: (Entfernung IDP.UC_20 und IDP.UC_21)

Ergänzung der Tabelle Tab_gemSpec_Perf_Berichtsformat_sektoraler_IDP mit neuer zugehöriger AFO:

A_22825 - Performance - Rohdaten - Spezifika - Operation (Rohdatenerfassung v.02)
Der Produkttyp MUSS bei Rohdaten-Performance-Berichten bzgl. der "operation"-Felder die Angabe aus der Tabelle Tab_gemSpec_Perf_Berichtsformat_sektoraler_IDP in der Spalte"$IDP-Operation" berücksichtigen. **[<=]**

Tabelle 1: Tab_gemSpec_Perf_Berichtsformat_sektoraler_IDP

$IDP-Operation	Produkttyp	Operation	Schnittstelle zu
IDP.UC_30	sektoraler Identity Provider	Processing of Pushed Authorization Requests	Internet
IDP.UC_31	sektoraler Identity Provider	Processing of Authorization Requests (mit online Ausweisfunktion)	Internet

IDP.UC_32	sektoraler Identity Provider	Processing of Authorization Requests (mit eGK und PIN)	Internet
IDP.UC_33	sektoraler Identity Provider	Processing of Authorization Requests (mit kassenindividuellem Authentisierungsverfahren)	Internet
IDP.UC_39	sektoraler Identity Provider	Token Requests	Internet

Hinweise:
Die Duration für IDP.UC_30 beginnt mit der Annahme des Pushed Authorization Request (PAR) vom Authorization-Server des Fachdienstes und endet mit der Übermittlung der "URI-PAR" zum Authorization-Server des Fachdienstes. Zeiten zwischen der optionalen Anfrage "Get Entity Statement RP" des sektoralen IDP an den Fachdienst und der Antwort "Entity Statement" sowie der optionalen Anfrage "Fetch Entity Statement RP" des sektoralen IDP an den Federation Master und Antwort "Entity Statement" sind in der Berechnung für den IDP.UC_30 herauszurechnen.

Die Duration für IDP.UC_31 - IDP.UC_33 beginnen mit der Annahme des Authorization Request (URI-PAR) vom Authenticator-Modul und enden mit der Übermittlung der "Redirect to redirect url,`AUTH_CODE`" zum Authenticator-Modul. Zeiten zwischen der optionalen Anfrage "Login, User Consent" und der Antwort "Credentials, Consent" sind in der Berechnung für den IDP.UC_31 - IDP.UC_33 herauszurechnen.

Die Duration für IDP.UC_39 beginnt mit der Annahme des `AUTH_CODE` vom Authorization-Server des Fachdienstes und endet mit der Übermittlung des `ID_TOKEN` (`ACCESS_TOKEN`) zum Auth Server des Fachdienstes.

Neue AFO für Sektoralen IDP in Föderation: (Ablösung von A_22226 und A_22226-01 durch die A_22833)

A_22833 - Performance – Sektoraler Identity Provider in der Föderation – Bearbeitungszeiten unter Last
Der Anbieter des sektoralen Identity Provider MUSS die Bearbeitungszeitvorgaben unter Last aus Tab_gemSpec_Perf_sektoraler_IDP erfüllen.
Es wird davon ausgegangen, dass der sektorale Identity Provider eingeschwungen ist und z. B. Lokalisierungsanfragen lokal zwischengespeichert sind, sowie Verbindungen nicht neu ausgehandelt werden.
MA ist der Marktanteil des Anbieters gemäß [A_22225].
Im Fall der Authorization Requests zählt die Zeit von Anfrage des Authenticator-Moduls bis zum Eintreffen der Antwort nicht zur Bearbeitungszeit.

Tabelle 2: Tab_gemSpec_Perf_sektoraler_IDP: Bearbeitungszeitvorgaben

ID	Anwendungsfälle	Lastvorgaben	Bearbeitungszeitvorgaben
		Spitzenlast [1/sec]	Maximalwert [msec]

IDP.UC_30	Processing of Pushed Authorization Requests	10 + (450 x MA)	800
IDP.UC_31, IDP.UC_32, IDP.UC_33	Processing of Authorization Requests (mit online Ausweisfunktion) oder (mit eGK und PIN) oder (mit kassenindividuellem Authentisierungsverfahren)	10 + (450 x MA)	2000
IDP.UC_39	Token Requests	10 + (450 x MA)	800

[<=]

Einarbeitung in Kapitel 3.1.2.2 [gemSpec_Perf]

A_22828 - Performance - Rohdaten - Spezifika sektoraler IDP - Feldtrennzeichen im JSON (Rohdatenerfassung v.02)
Der Produkttyp MUSS, sofern vom Authenticator irrtümlicherweise im `authenticator_identifier` Wert oder im `authenticator_version` Wert das verbotene Feldtrennzeichen ";" übertragen wurde, dieses ";" gegen das Zeichen "┼" austauschen und in der Rohdatenlieferung senden.
(siehe: A_21981: Feldtrennzeichen ";"
Das Zeichen ┼ ist definiert gem. Unicode **U+253C** (9532) - BOX DRAWINGS LIGHT VERTICAL AND HORIZONTAL - ALT-Code 197)
[<=]

- referenzierte Tabelle in der gemSpec_Perf in Kapitel 2.5.2: PDT-Tabelle erweitern -

Tab_gemSpec_Perf_Produkte_Rohdatenerfassung_Version_v02 gibt einen Überblick über die Produkttypen, welche bereits Rohdaten-Performance-Berichte in der Version v.02 übermitteln, bzw. sich aktuell in der Umstellung befinden.

Tabelle 3 : Tab_gemSpec_Perf_Produkte_Rohdatenerfassung_Version_v02

PDT	Produkttyp
....	....
PDT70	Federation Master
.....	...

Zu ergänzen in Kapitel 3.1.1.3 Performancevorgaben IDP-Dienste

A_22950 - Performance – Federation Master – Bearbeitungszeit unter Last

Der Produkttyp Federation Master MUSS die Bearbeitungszeitvorgaben unter Last aus Tab_gemSpec_Perf_FedMaster erfüllen.

Es wird davon ausgegangen, dass der Federation Master eingeschwungen ist und z.B. Verbindungen nicht neu ausgehandelt werden.

Für die Zulassung ist je Anwendungsfall der Nachweis bei einer Last von 25 Anfragen pro Sekunde zu erbringen.

Tabelle 4: Tab_gemSpec_Perf_FedMaster: Bearbeitungszeitvorgaben

ID	Anwendungsfälle	Lastvorgaben	Bearbeitungszeitvorgaben
		Spitzenlast [1/sec]	Mittelwert [msec]
FEDM.UC_1	get_IDP_list (Internet)	25	5000
FEDM.UC_2	fetchEntityStatement (Internet)	25	5000

Hinweise:
Die Duration für FEDM.UC_1 beginnt mit der Annahme der getIDP_list-Anfrage und endet mit der Lieferung der IDP-Liste als Antwort zum Fachdienst.
Die Duration für FEDM.UC_2 beginnt mit der Annahme der fetchEntityStatement-Anfrage und endet mit der Lieferung der StatementResponse als Antwort zum IDP.

Es ist eine ausreichend großzügige Performance-Vorgabe von 5 Sekunden als Antwortzeit vorgegeben, jedoch darf diese in keinem Fall überschritten werden. Eine Quantil-Schranke wird nicht gewährt.

[<=]

A_22957 - Performance – FedMaster – Verfügbarkeit
Der Anbieter des Federation Master MUSS sein Produkttyp so betreiben, dass es zur Hauptzeit mindestens eine Verfügbarkeit von 99,99 % und zur Nebenzeit eine Verfügbarkeit von 99,97 % hat.
Genehmigte Wartungsfenster dürfen nur in der Nebenzeit liegen und werden nicht als Ausfallzeit gewertet.
Hauptzeit des Produkttyps ist Montag bis Sonntag von 6 bis 22 Uhr, ausgenommen bundeseinheitliche Feiertage. Alle übrigen Stunden der Woche sind Nebenzeit.
[<=]

zu Ergänzen im neuen Kapitel 3.1.1.4 Performance-relevante weitere Vorgaben IDP-Dienste

A_22252-01 - Erkennung Authenticator-Module im User-Agent (Rohdatenerfassung v.02)

Der sektorale Identity Provider MUSS das vom aufrufenden Nutzer verwendete Authenticator-Modul eindeutig erkennen und in den Einträgen zur Performance-Rohdatenerfassung gemäß [gemSpec_Perf# A_22944] protokollieren.
[<=]

Hinweis: Die Information über das Client System kann anhand des im HTTP-Request enthaltenen Header-Feld User-Agent gemäß [RFC7231] übermittelt werden.

AFO war für den zentralen IDP vorgesehen in der Föderation
Entscheidung für die dezentrale Zuständigkeit hat zur Folge, dass folgende beiden AFOs storniert werden:
1. A_22226 - storniert:

2. A_22226-01 storniert:

abzulösende AFO :

A_22357 - Verfügbarkeit sektoraler IDP
Der Produkttyp sektoraler Identity Provider MUSS zur Hauptzeit eine Verfügbarkeit von 99,9 % und zur Nebenzeit eine Verfügbarkeit von 99,0 % haben.
Wartungsfenster dürfen nur in der Nebenzeit liegen. Genehmigte Wartungsfenster werden nicht als Ausfallzeit gewertet.
Hauptzeit ist Montag bis Sonntag von 6 bis 22 Uhr, ausgenommen bundeseinheitliche Feiertage. Alle übrigen Stunden der Woche sind Nebenzeit.**[<=]**

neue, suffixierte Nachfolger-AFO:

A_22357-03 - Verfügbarkeit sektoraler IDP
Der Anbieter des sektoralen IDP MUSS sein Produkttyp so betreiben, dass es zur Hauptzeit mindestens eine Verfügbarkeit von 99,99 % und zur Nebenzeit eine Verfügbarkeit von 99,97 % hat.
Genehmigte Wartungsfenster dürfen nur in der Nebenzeit liegen und werden nicht als Ausfallzeit gewertet.
Hauptzeit des Produkttyps ist Montag bis Sonntag von 6 bis 22 Uhr, ausgenommen bundeseinheitliche Feiertage. Alle übrigen Stunden der Woche sind Nebenzeit.**[<=]**

Zuordnung zur Rohdatenlieferung v.02:

A_22230 wird abgelöst durch A_22826

A_22826 - Performance - Rohdaten - Spezifika - Status (Rohdatenerfassung v.02)
Wenn bei der Durchführung der Operation/des Use Case ein Fehler aufgetreten ist, MUSS der Produkttyp sektoraler IDP-Dienst - bei Rohdaten-Performance-Berichten bzgl. des "status"-Feldes - den Statuscode gem.
Tab_gemSpec_Perf_Fehlercodes_sektoraler_IdP festlegen, sofern ein spezifischer Fehlercode bestimmt werden kann. Ist dies nicht möglich, MUSS der definierte Standardcode für interne bzw. externe Fehler verwendet werden.

Tabelle 5: Tab_gemSpec_Perf_Fehlercodes_sektoraler_IDP

Statuscode	Definition	Beschreibung
79000	IDP_ERROR	alle internen Fehler des sektoralen IDP
79105	SEK_IDP_ERROR_NOT_ALLOWED_USER	Useragent/Version/ClientID-Kombination nicht erlaubt

[<=]

neue Afo unter 3.1.2.2

A_22944 - Performance - Rohdaten - Spezifika föderierter IDP - Message (Rohdatenerfassung v.02)
Der Produkttyp MUSS - bei Rohdaten-Performance-Berichten folgende Parameter im JSON-Format übermitteln:
{"HN": "$Herstellername", "PN": "$Produktname", "PV": "$Produktversion", "Client_ID": "$client_id"}

Für **"HN": "$Herstellername", "PN": "$Produktname", "PV": "$Produktversion"** ist der übermittelte user-agent zu verwenden, der vom Client übermittelt wird.
Für **$client_id** ist der entsprechende Wert zu verwenden, welcher vom Client im Verbindungsaufbau übermittelt werden. <=

*Hinweis: Die client_id ist dem IDP unabhängig vom user-agent im Verbindungsaufbau bekannt.***[<=]**

Erweiterung der Zuordnungen der Afos in Kapitel 2.5.2 "Rohdaten-Performance-Reporting (Rohdatenerfassung v.02)":

A_22057, A_22002, A_22000, A_22429, A_22004, A_22003-01, A_22005, A_21976, A_22047, A_22620, A_21978, A_21975, A_21979, A_21980, A_22001-01, A_21981-02, A_22500-01, A_21982-01, A_22513-01

neue Anforderung:

A_22996 - Performance - Rohdaten - Zeitpunkte der Übermittlungen (Rohdatenerfassung v.02)
Der Anbieter, der zur Rohdatenlieferung verpflichtet ist, MUSS jede Lieferung der Rohdaten unverzüglich - spätestens innerhalb der 10 auf das Berichtsintervall folgenden Minuten - beginnen.
[<=]

4.4 Spezifikation Identity Provider – Nutzungsspezifikation für Fachdienste [gemSpec_IDP_FD]

4.4.1 (1.1) Zielsetzung

Dies Kapitel definiert die Anforderungen zu Herstellung, Test und Betrieb der Schnittstellen von Fachdiensten, die am föderierten Identity Management der TI teilnehmen wollen, um dessen Benutzern darüber die Authentisierung zu ermöglichen. Die bisherigen Inhalte der gemSpec_IDP_FD beschreiben die Nutzung des IDP Dienstes und gelten weiterhin.

4.4.2 (2) Systemüberblick

Im Rahmen der Telematikinfrastruktur (TI) werden zahlreiche Fachdienste angeboten. Sektorale Identity Provider (IDPs) übernehmen für diese Fachdienste die Aufgabe der Authentisierung des Nutzers. Anwendungsfrontends können, über die Authentifizierung des Nutzers gegenüber sektoralen IDP, Zugriff zu den von den Fachdiensten für den jeweiligen Nutzer angebotenen Daten erhalten. Sektorale IDP stellen durch gesicherte JSON Web Token (JWT) attestierte Identitäten aus, sogenannten `ID_TOKEN`. Auf dieser Basis wird dem Anwendungsfrontends vom Authorization-Server des Fachdienstes ein `ACCESS_TOKEN` ausgestellt. Gegen Vorlage dieses `ACCESS_TOKEN` erhalten Anwendungsfrontends, entsprechend der im Token attestierten Informationen, Zugriff auf die Inhalte der Fachdienst API. Der Authorization-Server und die Fachdienst API sind Teile des Fachdienstes. Fachdienste müssen keine Überprüfung des Nutzers selbst implementieren, sondern können sich darauf verlassen, dass der Nutzer bereits identifiziert und authentisiert wurde und die im `ID_TOKEN` enthaltenen Attribute gültig sind. Zudem müssen im `ACCESS_TOKEN` keine persönlichen Informationen enthalten sein, sondern diese können, sofern benötigt von der Fachdienst API abgerufen werden.

Im Falle einer App als Anwendungsfrontend werden direkt dort die `ACCESS_TOKEN` gehandhabt und gespeichert. Im Falle eines Web-basierten Anwendungsfrontends kann diese Aufgabe das Web-Backend übernehmen.

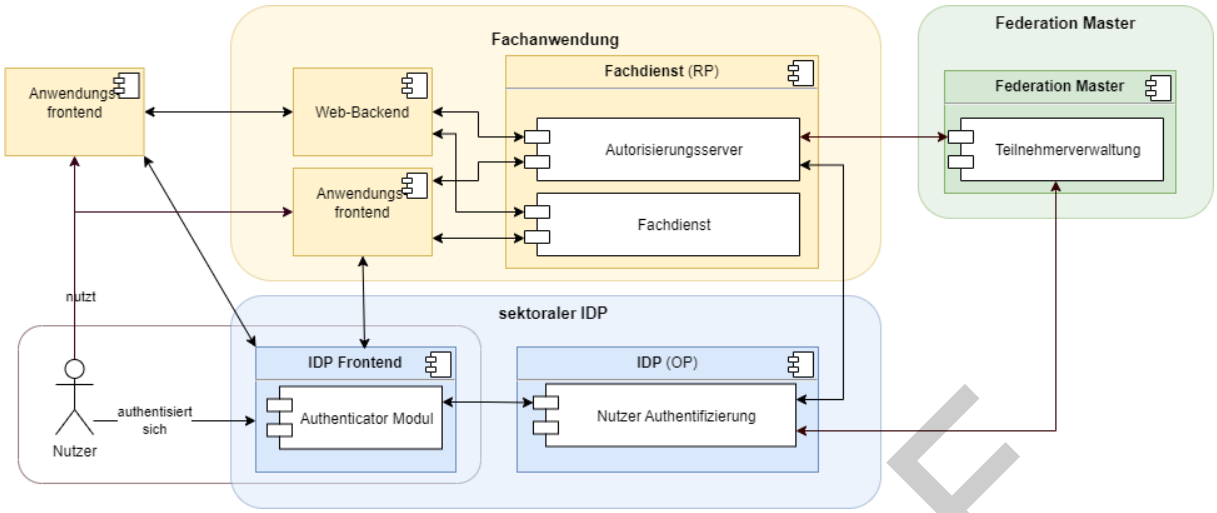

Abbildung 4 : Systemüberblick

Die Abbildung stellt den Systemüberblick dar. Der Authentifizierungsprozess, welcher mit der Ausstellung und Übergabe der Token an das Anwendungsfrontend endet, wird dabei zur besseren Übersicht vereinfacht dargestellt.

Fachdienste, welche sektorale IDPs der TI-Föderation zur Nutzer-Authentisierung nutzen möchten, müssen die folgenden Prozesse und Schnittstellen bedienen:

- Registrierung des Fachdienstes beim Federation Master (organisatorischer Prozess gemäß [gemSpec_IDP_FedMaster]), sowie der verwendeten öffentlichen Schlüssel für die Signatur von Entity Statements und Mitteilung der benötigten `scopes` (Key/Value-Paare im Payload eines JWT)
- Veröffentlichung ihres signierten Entity Statements (siehe 4.5).

Alle Fachdienste müssen zur Absicherung der JWT gegen Einsichtnahme und Profilbildung durch Dritte den Transportweg bis in die Vertrauenswürdige Ausführungsumgebung (siehe [gemSpec_IDP_Sek]) mit Transport Layer Security (TLS) gemäß [gemSpec_Krypt] absichern.

4.4.3 (3) Systemkontext

Der Systemkontext besteht für den Fachdienst aus einem sektoralen Identity Provider, dem Federation Master und einem Anwendungsfrontend.

Der Fachdienst muss beim Federation Master eine organisatorische Registrierung durchführen [gemSpec_IDP_FedMaster], bei welcher der vom Fachdienst verwendete kryptographische öffentlicher Schlüssel sowie dessen Adresse beim Federation Master hinterlegt werden.

Der Fachdienst besteht aus einem Authorization-Server, einer Fachdienst API und optional aus einem Web-Backend. Das Web-Backend kann im Falle einer Web-Anwendung zur Anwendung kommen. In diesem Fall besteht das Anwendungsfrontend aus einer Web-Anwendung die üblicherweise im Browser des Benutzers ausgeführt wird. Diese Web-Anwendung interagiert mit dem Web-Backend, der wiederum Teilaufgaben übernehmen kann und insb. mit dem Authorization-Server kommuniziert. Bei einer solchen Web-Lösung muss keine direkte Interaktion zwischen Anwendungsfrontend und Authorization-Server erfolgen.

Im Falle einer mobilen App stellt diese das Anwendungsfrontend dar und es ist kein Web-Backend nötig.

Das Anwendungsfrontend bzw. Web-Backend erlangt nach Vorlage des `ACCESS_TOKEN` und positiver Validierung der Inhalte des Tokens durch den Fachdienst Zugang zu den angeforderten Fachdaten.

Die folgende Abbildung stellt den Systemkontext aus Sicht eines Fachdienstes dar.

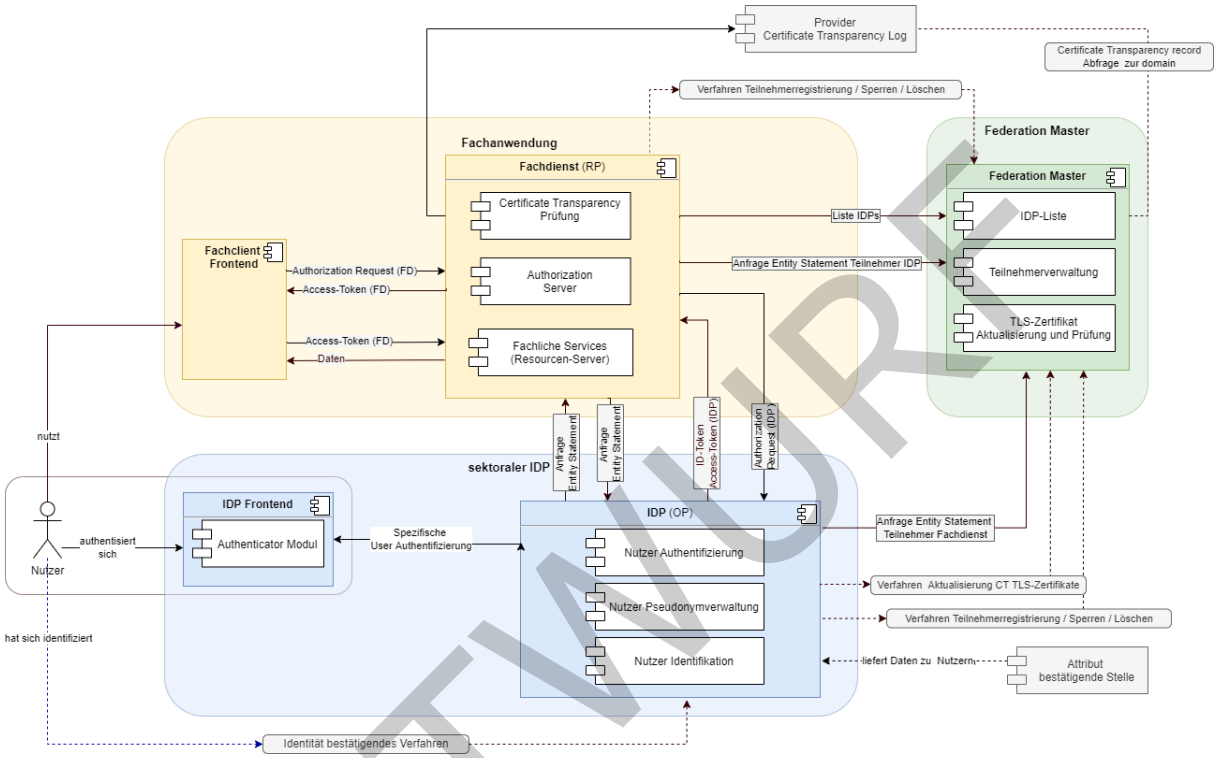

Abbildung 5 : Systemkontext

4.4.4 (4) Authorization-Server

4.4.4.1 (4.1) Registrierung des Fachdienstes beim Federation Master

Fachdienstbetreiber müssen ihren Authorization-Server beim Federation Master registrieren. Die Registrierung erfolgt als organisatorischer Prozess, bevor ein Fachdienst an den vom föderierten Identitätsmanagement (IDM) angebotenen Authentifizierungsprozessen teilnehmen kann. Erst nach erfolgter Registrierung, bei der die Adresse des Fachdienstes bzw. seines Authorization-Servers, seine öffentlichen Schlüssel sowie der verwendete `scope` angegeben wurden, können sektorale Identity Provider `ID_TOKEN` für den Fachdienst ausstellen.

Hinweis: `scopes` definieren konkrete Key/Value-Paare, die als Payload eines JWT codiert werden. Ein vereinbarter `scope` sagt aus, welche Key/Value-Paare im Payload erwartet werden. Die Vereinbarung wird zwischen dem Fachdienst und dem Federation Master während der Registrierung des Fachdienstes getroffen. Im Rahmen einer Authentifizierung fragen Authorization-Server den jeweils benötigten `scope` an, der im Rahmen des `ID_TOKEN` vom sektoralen Identity Provider bestätigt wird.

Offener Punkt: Definition der Kriterien, welche eine Drittanwendung erfüllen muss, um in die Föderation aufgenommen zu werden

Offener Punkt: Definition der Kriterien und Prozesse, wie eine Drittanwendung in die Föderation aufgenommen wird.

A_23045 - Registrierung des Fachdienstes
Anbieter von Fachdiensten MÜSSEN bei der Registrierung ihrer Authorization-Server am Federation Master die von ihnen erwarteten Attribute in `scopes` (siehe Abschnitt ML-128467 - (4.2) Inhalte der "scopes") beschreiben und dem Federation Master zur Verfügung stellen. Die Registrierung MUSS ebenso die absolute URI des Fachdienstes im Internet umfassen (seine Client-ID) sowie dessen Signaturschlüssel für das Entity_Statement.**[<=]**

A_23046 - öffentlicher Schlüssel des Federation Master
Anbieter von Fachdiensten MÜSSEN den öffentlichen Signaturschlüssel des Federation Master durch einen sicheren Registrierungsprozess im Authorization-Server einbringen und initial zur Signaturprüfung verwenden.**[<=]**

Hinweis: Weitere Signaturschlüssel des Federation Master können aus dessen Entity Statement importiert werden.

A_23042 - Verifikation der Certificate Transparency für TLS Verbindungen in die VAU
Die Hersteller der Fachdienste MÜSSEN prüfen ob die CA, welche die TLS Zertifikate für Verbindungen in den sicheren Verarbeitungskontext eines sektoralen Identity Provider erstellt hat, Certificate Transparency gemäß RFC 6962/RFC 9162 unterstützt. **[<=]**

Hinweis: Diese Funktionalität wird durch aktuelle Standard Bibliotheken für TLS Verbindungen unterstützt.

4.4.4.2 (4.2) Inhalte der "scopes"

Der Payload eines JWT beinhaltet Key/Value-Paare, welche in einem oder mehreren `scopes` definiert werden. Inhalte eines scopes sind mehrere Attribute, welche der sektorale IDP auf Basis der vorgetragenen Identität bestätigen kann.

Die `scopes` beinhalten die für diesen Fachdienst abgestimmten Attribute (die `scopes` werden pro Fachdienst in einem organisatorischen Prozess gesondert vom jeweiligen Fachdienst mit dem Federation Master abgestimmt) und den Wertebereich, welchen diese annehmen können.

Neben den im Standard vorgesehenen Attributen (siehe openid-connect-core-1_0.html#IDToken) erwarten Fachdienste in der Regel weitere Informationen, wie zum Beispiel Vorname, Name, Rolle und KVNR des Nutzers. Siehe hierzu auch [gemSpec_IDP_Sek] Kapitel: *"Token-Endpunkt Ausgangsdaten"*.

Das Attribut `iss` beschreibt, wer den `ID_TOKEN` ausgestellt hat.

Das Attribut `sub` beschreibt das Subjekt, mit welchem der Fachdienst kommuniziert. Anhand dieses Attributes lassen sich Vorgänge einer bestimmen Entität zuordnen.

Das Attribut `professionOID` beschreibt die Rolle der agierenden Entität und ist im Falle eines Versicherten immer mit der OID eines Versicherten "`oid_Versicherter`" befüllt.

A_23035 - pseudonymes Attribut "sub"
Fachdienste MÜSSEN das Attribut `sub` mit einem Pseudonym befüllen, welches nur durch den sektoralen IDP auflösbar ist. **[<=]**

A_23036 - Inhalte der "scopes" für Versicherte
Fachdienste MÜSSEN bei ihrer Registrierung am Federation Master sicherstellen, dass ausschließlich die fachlich benötigten Attribute aus der in [gemSpec_IDP_Sek] Kapitel: *"Token-Endpunkt Ausgangsdaten"* definierten Auswahl als `scopes` beantragt werden.**[<=]**

Hinweis: Der Aufbau von `ID_TOKEN` entspricht den Anforderungen gemäß [gemSpec_IDP_Sek] Kapitel: "Token-Endpunkt Ausgangsdaten".

A_23037 - Robustheit bei fehlenden Daten
Sind einzelne `claims` des angefragten `scopes` nicht im `ID_TOKEN` enthalten, weil beispielsweise der Nutzer die Herausgabe verweigert oder Daten nicht hinterlegt wurden, so MUSS der Fachdienste das `ID_TOKEN` trotzdem akzeptieren und innerhalb der Fachanwendung geeignet reagieren. **[<=]**

Hinweis: Geeignete Reaktion auf fehlenden `claims` könnten darin bestehen, dass nur fachliche Anwendungsfälle ausgeführt werden, für welche die Informationen zum Nutzer hinreichend vorhanden sind. Zulässig ist auch eine Ablehnung des Benutzers mit entsprechender Information für den Fall das eine ohne die notwendigen Angaben keine fachlichen UseCases möglich sind.

A_23004 - Anforderung eines Vertrauensniveaus
Fachdienste MÜSSEN eine Authentisierung auf dem für den Zugriff auf ihre Fachdaten notwendigen Vertrauensniveau im Parameter `acr_values` des Pushed Authorization-Request anfragen oder wenn nur ein Wert in Frage kommt diesen im Feld `default_acr_values` ihres Entity Statements nennen.**[<=]**

A_23005 - Verifikation des durchgeführten Vertrauensniveaus
Fachdienste MÜSSEN prüfen, ob das im `ID_Token` im Feld `acr` gelistete Vertrauensniveau der durchgeführten Authentisierung für den Zugriff auf die Fachdaten ausreicht.**[<=]**

A_23030 - Erzwingen einer Authentisierung des Nutzers
Fachdienste KÖNNEN eine Benutzerauthentisierung auch dann erzwingen wenn mögliche Single-Sign-On Mechanismen durch den sektoralen IDP unterstützt werden indem der Parameter `max_age` des Pushed Authorization-Request auf den Wert 0 gesetzt wird.**[<=]**

AF_10100 - Bereitstellung IDP-Liste

Tabelle 6 : Anwendungsfall "Bereitstellung Liste registrierte Identity Provider"

Attribute	Bemerkung

Beschreibung	Ein Anwender möchte einen in der TI registrierte Fachdienst nutzen. Der Fachdienst muss sicherstellen, dass der Anwender zur Nutzung des Dienstes berechtigt ist. Hierzu authentisiert sich der Anwender gegenüber einem sektoralen Identity Provider, bei dem er registriert ist. Diesen wählt er aus einer Liste aller in der TI zur Verfügung stehenden sektoralen Identity Provider aus. Der Authorization-Server MUSS dem Anwendungsfrontend oder dem Web-Backend eine Liste der in der TI registrierten sektoralen Identity Provider zur Verfügung stellen, oder selbst dem Benutzer eine Auswahlmöglichkeit bieten. Diese Liste MUSS sich der Authorization-Server vom Federation Master abfragen. Jeder Listeneintrag MUSS mindestens diese Informationen enthalten: • eindeutige issuer-id des sektoralen Identity Provider in der TI-Föderation • Name des sektoralen Identity Provider in lesbarer Form • Logo des sektoralen Identity Provider (wenn vorhanden). Der Anwender des Fachdienstes MUSS genau einen sektoralen Identity Provider aus der Liste auswählen. Das Anwendungsfrontend kann sich die Zuordnung eines Anwenders zu seinem sektoralen Identity Provider speichern, so dass die Abfrage der Liste nicht bei jeder Anmeldung des Anwenders wiederholt werden muss.
Akteur	Anwender der Fachanwendung
Auslöser	Ein Anwender möchte eine Gesundheitsanwendung der TI (Fachdienst) nutzen. Als Voraussetzung für die Authentifizierung des Anwenders muss dieser auswählen, bei welchem Identity Provider er registriert ist (bei Versicherten - Auswahl der Krankenkasse).
Komponenten	• Anwendungsfrontend (App oder Web) oder Web-Backend • Authorization-Server eines Fachdienstes • Federation Master
Vorbedingung	1. Es gibt eine Liste der in der TI-Föderation registrierten (sektoralen) Identity Provider, deren Schlüssel dem Federation Master bekannt sind. 2. Der Anwender ist durch einen der (sektoraler) Identity Provider identifiziert worden. 3. Das Entity Statement des Federation Master steht zur Verfügung und die unter dem Attribut idp_list_endpoint benannte URL ist aus dem Internet erreichbar.

Ablauf	1. Das Anwendungsfrontend oder Web-Backend (im Folgenden als aufrufende Instanz bezeichnet) schickt eine Anfrage zum Abruf der IDP-Liste an den Authorization-Server. 2. Sofern der Authorization-Server die IDP-Liste nicht zwischengespeichert hat, ruft er diese vom Federation Master ab. Hierbei greift er auf die entsprechende URL zu, die im Entity Statement des Federation Master angegeben ist. 3. Der Authorization-Server gibt die vom Federation Master erhaltene IDP-Liste an die aufrufende Instanz zurück. Der Inhalt der Liste ist hierbei nicht zu verändern. (Daher gelten an dieser Stelle keine weiteren Detailanforderungen an die Struktur und Inhalt der Liste. Eine Umschlüsselung der IDP-Liste ist zulässig.) 4. Die aufrufende Instanz überprüft die Integrität der erhaltenen IDP-Liste, die entweder vom Federation Master oder vom Authorization-Server signiert ist ([gemSpec_IDP_FedMaster] Kapitel: *"Anwendungsfall - IDP-Liste bereitstellen"*). 5. Die aufrufende Instanz kann die IDP-Liste für die Dauer ihrer Gültigkeit (Feld "exp") zwischenspeichern.
Ergebnis	Das Anwendungsfrontend zeigt dem Nutzer die Liste der registrierten Identity Provider an.
Akzeptanzkriterien	ML-133108 , ML-133109 , ML-128411
Alternativen	Das Anwendungsfrontend oder Web-Backend kennt (z. B. aus früheren Sitzungen) den sektoralen Identity Provider des Anwenders. In diesem Fall KANN auf den Abruf und Anzeige der IDP Liste verzichtet werden. Das Anwendungsfrontend oder Web-Backend hat die IDP-Liste bereits zwischengespeichert. In diesem Fall KANN auf den Abruf der IDP Liste verzichtet werden.

ML-133108 - AF_10100 - Abruf der IDP-Liste liefert signiertes JWS als Response
Der Request vom Anwendungsfrontend an den Authorization-Server zum Abruf der IDP-Liste wird entgegengenommen und gibt als Response ein signiertes JWS zurück.

ML-133109 - AF_10100 - Abruf der IDP-Liste liefert signiertes JWS als Response
Der Request vom Anwendungsfrontend an den Authorization-Server zum Abruf der IDP-Liste wird entgegengenommen und gibt als Response ein signiertes JWS zurück.

A_23033 - Integritätsschutz der IDP-Liste
Die Integrität der vom Anwendungsfrontend verarbeitete IDP-Liste MUSS gewährleistet werden (z. B. mittels Signaturprüfung).**[<=]**

Hinweis: Dabei kann das Anwendungsfrontend entweder gegen den bekannten öffentlichen Schlüssel des Federation Master prüfen, der Authorization-Server die Liste mit einem dem Anwendungsfrontend bekannten Schlüssel neu signieren oder aber die

Liste durch den Authorization-Server innerhalb einer gesicherten TLS Verbindung zum Anwendungsfrontend zur Anzeige gebracht werden.

4.4.4.3 (4.4) Entity Statements

A_23034 - Entity Statement veröffentlichen
Authorization-Server MÜSSEN über sich ein Entity Statement entsprechend AF_10101 und gemäß [OpenID Connect Federation 1.0#rfc.section.6] unter ".well-known/openid-federation" veröffentlichen.**[<=]**

A_23038 - Entity Statement abrufen
Authorization-Server MÜSSEN benötigte Schlüssel und Endpunkte des Federation Master und verwendeter sektoraler Identity Provider durch Abfrage ihrer Entity Statements entsprechend AF_10101 einholen. **[<=]**

A_23039 - Entity Statement vorhalten
Authorization-Server KÖNNEN einmal heruntergeladene fremde Entity Statements zwischenspeichern. Diese SOLLEN nach 12 Stunden erneut heruntergeladen werden und MÜSSEN nach maximal 24 Stunden verworfen werden. **[<=]**

A_23040 - Fachdienst: Prüfung der Signatur des Entity Statements
Authorization-Server MÜSSEN die Signatur der heruntergeladenen Entity Statement mathematisch prüfen und auf einen zeitlich gültigen Signaturschlüssel zurückführen, welcher von dem ihm bekannten Federation Master oder von einem durch den Federation Master beglaubigten sektoralen Identity Provider ausgestellt sein MUSS. Vor der weiteren Verwendung MUSS die Prüfung der Entity Statements erfolgreich abgeschlossen sein. **[<=]**

Hinweis: Der Abgleich des Signaturschlüssels muss gegen ein frisch abgerufenes Statement des Federation Master zu diesem sektoralen Identity Provider erfolgen.

4.4.4.4 (4.5) Anfrage von "ID_TOKEN" beim sektoralen Identity Provider

AF_10101 - OAuth 2.0 Pushed Authorization Request

Tabelle 7 : Anwendungsfall "OAuth 2.0 Pushed Authorization Request"

Attribute	Bemerkung
Beschreibung	Ein Anwender möchte einen in der TI registrierten Fachdienst nutzen. Der Fachdienst muss sicherstellen, dass der Anwender zur Nutzung des Dienstes berechtigt ist. Hierzu authentisiert sich der Anwender gegenüber einem sektoralen Identity Provider, bei dem er registriert ist. Der Authorization-Server MUSS bei Erhalt eines Autorisierungs Requests vom Anwendungsfrontend oder vom Web-Backend eine entsprechende Anfrage (Pushed Authorization Request) an den angegebenen sektoralen Identity Provider senden. Anschließend sendet der Authorization-Server die vom sektoralen Identity Provider erhaltene URI zurück an die aufrufende Instanz.

Akteur	Anwender der Fachanwendung
Auslöser	Ein Anwender möchte eine Gesundheitsanwendung der TI (Fachdienst) nutzen. Als Voraussetzung muss er sich bei einem sektoralen Identity Provider authentifizieren, bei welchem er registriert ist.
Komponenten	• Anwendungsfrontend oder Web-Backend • Authorization-Server eines Fachdienstes • sektoraler Identity Provider
Vorbedingung	1. Der Anwender ist durch einen der (sektoralen) Identity Provider identifiziert worden 2. Das Entity Statement des Federation Master steht zur Verfügung. 3. Der involvierte sektorale Identity Provider ist beim Federation Master registriert.
Ablauf	1. Das Anwendungsfrontend oder Web-Backend schickt einen OAUTH2 Authorization Request unter Angabe des zu verwendenden sektoralen Identity Providers an den Authorization Endpoint des Authorization-Servers. ([gemSpec_IDP_Sek] Tabelle: *"Authorization Request von Anwendungsfrontend zum Authorization-Servers"*) 2. (Falls nötig, lädt der Authorization-Server das Entity Statement vom angegebenen sektoralen Identity Provider entsprechend [gemSpec_IDP_Sek] Kapitel: *"Entity Statement des sektoralen IDP"*) 3. Der Authorization-Server sendet seinerseits einen Authentication Request an den Authentication Endpoint des angegebenen sektoralen Identity Providers ([gemSpec_IDP_Sek] Tabelle: *"Parameter HTTP-POST Request"*). 4. (Falls nötig, lädt der sektorale Identity Provider das Entity Statement vom Authorization-Server entsprechend A_23034.) 5. Der sektorale Identity Provider antwortet mit einer URI auf den Pushed Authorization Request ([gemSpec_IDP_Sek] Tabelle: *"Parameter der HTTP-Response"*) (https://www.rfc-editor.org/rfc/rfc9126.html). 6. Der Authorization-Server sendet die URI auf den Pushed Authorization Request zurück an die aufrufende Instanz. ([gemSpec_IDP_Sek] Tabelle: *"Request Parameter des Fachdienstes zum sektoralen IDP"*)
Ergebnis	Das Anwendungsfrontend oder Web-Backend hat die PAR URI erhalten, mittels derer er die Benutzerauthentifizierung initiieren kann.

Akzeptanzkriterien	ML-133233, ML-133234
Alternativen	keine

ML-133233 - AF_10101 - Antwort auf den Pushed Authorization Request
Das Anwendungsfrontend oder Web-Backend hat die Antwort auf den Pushed Authorization Request vom Authorization-Server erhalten.

ML-133234 - AF_10101 - PAR URI
Die gelieferte Antwort enthält die PAR URI, mittels derer das Anwendungsfrontend oder Web-Backend die Benutzerauthentifizierung initiieren kann.

A_23047 - Endpunkt für OAuth 2.0 Authorization Endpoint
Authorization-Server MÜSSEN einen OAuth 2.0 Authorization Endpunkt anbieten um Authorization Requests mit PKCE/Code Challenge entsprechend https://datatracker.ietf.org/doc/html/rfc6749#section-4.1.1 und https://datatracker.ietf.org/doc/html/rfc7636#section-4.3 zu akzeptieren und zu verarbeiten.**[<=]**

A_23048 - Response für OAuth 2.0 Pushed Authorization Requests
Authorization-Server MÜSSEN nach Erhalt eines Authorization Request entsprechend OAuth 2.0 Pushed Authorization Requests (PAR) https://datatracker.ietf.org/doc/html/rfc9126 mit sektoralen Identity Providern kommunizieren und eine entsprechende Antwort an die aufrufende Instanz zurück senden.**[<=]**

AF_10102 - Benutzerauthentifizierung und Erhalt des "ID_TOKEN"

Tabelle 8 : Anwendungsfall "Benutzerauthentifizierung und Erhalt des`ID_TOKEN`"

Attribute	Bemerkung
Beschreibung	Ein Anwender möchte einen in der TI registrierten Fachdienst nutzen. Der Fachdienst muss sicherstellen, dass der Anwender zur Nutzung des Dienstes berechtigt ist. Hierzu authentisiert sich der Anwender gegenüber einem sektoralen Identity Provider, bei dem er registriert ist. Nach Abschluss der Authentisierung des Nutzers gegenüber dem sektoralen Identity Provider, erhält der Authorization-Server den `AUTHORIZATION_CODE` mit dem er das `ID_TOKEN` abrufen kann.
Akteur	Anwender der Fachanwendung
Auslöser	Ein Anwender möchte eine Gesundheitsanwendung der TI (Fachdienst) nutzen. Als Voraussetzung muss er sich bei einem sektoralen Identity Provider authentifizieren, bei welchem er registriert ist. Das Anwendungsfrontend erhält vom Authorization-Server die Pushed Authorization Requests URI zurück ([gemSpec_IDP_Sek] Kapitel: ”PAR-Endpunkt Ausgangsdaten”).
Komponenten	• Anwendungsfrontend oder Web-Backend • Authorization-Server eines Fachdienstes

	• sektoraler Identity Provider
Vorbedingung	1. Der Anwender ist durch einen der (sektoraler) Identity Provider identifiziert worden 2. Das Entity Statement des Federation Master steht zur Verfügung. 3. Der involvierte sektorale Identity Provider ist beim Federation Master registriert. 4. Eine OAuth 2.0 Pushed Authorization Request URI wurde entsprechend [gemSpec_IDP_Sek] Kapitel: "PAR-Endpunkt Ausgangsdaten" zurück geliefert.
Ablauf	1. Das Anwendungsfrontend oder Web-Backend ruft den Authorization-Endpunkt des sektoralen Identity Providers auf und übergibt die OAuth 2.0 Pushed Authorization Requests URI. Diese leitet weiter auf das Web-Frontend des sektoralen Identity Providers oder direkt auf dessen Authenticator-Modul. (Die eigentliche Authentifizierung erfolgt Implementations-spezifisch und wird hier nicht weiter definiert.) 2. Nach erfolgreichem Abschluss der Authentisierung sendet der sektorale Identity Provider einen `AUTHORIZATION_CODE` an das aufrufende Anwendungsfrontend oder Web-Backend. 3. Das Anwendungsfrontend oder Web-Backend sendet den `AUTHORIZATION_CODE` an den Authorization-Server. 4. Der Authorization-Server sendet den `AUTHORIZATION_CODE` an den involvierten sektoralen Identity Provider. ([gemSpec_IDP_Sek] Kapitel: "Detailinformationen zum App-App-Flow" - Schritt 10) 5. Der sektorale Identity Provider überprüft die Gültigkeit des `AUTHORIZATION_CODE` entsprechend https://datatracker.ietf.org/doc/html/rfc7636#section-4.6 6. Der sektorale Identity Provider antwortet dem Authorization-Server nach erfolgreicher Überprüfung des `AUTHORIZATION_CODE` mit dem zugehörigen `ID_TOKEN`. ([gemSpec_IDP_Sek] Kapitel: "Detailinformationen zum App-App-Flow" - Schritt 11)
Ergebnis	Der Nutzer ist authentifiziert und der Authorization-Server hat den `ID_TOKEN` mit dem es den `ACCESS_TOKEN` zum Zugriff auf die Fachdienst API abrufen kann.
Akzeptanzkriterien	ML-133236, ML-133237
Alternativen	keine

ML-133236 - AF_10102 - `ID_TOKEN` erhalten

Der Authorization-Server hat einen `ID_TOKEN` vom sektoralen Identity Provider erhalten.

ML-133237 - AF_10102 - `ID_TOKEN` entspricht Vorgaben
Der erhaltene `ID_TOKEN` entspricht den Vorgaben in [gemSpec_IDP_Sek] Tabellen: *"Header-`claims` des ID_TOKEN des sektoralen IDP"*, *"Signature Header-`claims` des ID_TOKEN des sektoralen IDP"* und *"Body-`claims` für den ID_TOKEN des sektoralen IDP"*.

4.4.4.5 (4.6) Verifikation des "ID_TOKEN"

A_23049 - Überprüfung des "ID_TOKEN" durch Authorization-Server
Zugriffsgeschützte Fachdienste MÜSSEN vor Gewährung des Zugriffs, den erhaltenen `ID_TOKEN` wie folgt prüfen. Nur nach erfolgreicher Überprüfung darf der Zugriff gewährt werden.

1. Verschlüsselte `ID_TOKEN` müssen entschlüsselt werden.
2. Das `ID_TOKEN` muss valide signiert sein durch einen Schlüssel des ausstellenden sektoralen Identity Provider.
3. Das `ID_TOKEN` muss zeitlich gültig sein (Felder: `iat`, `exp`)
4. Das `ID_TOKEN` muss im Feld `aud` den jeweiligen Fachdienst eingetragen haben.
5. Falls es sich um eine pseudonyme Benutzeranmeldung handelt, muss die Kombination der Felder `iss` und `sub` auf den Benutzer zugeordnet werden.
6. Das Feld `nonce` MUSS mit der ausgelösten Authentisierungsanfrage übereinstimmen.

[<=]

A_22861 - Aktualisierung der bekannten Signaturschlüssel bei unbekannter "kid" der Signatur
Bei der Überprüfung eines `ID_TOKEN` MUSS der Fachdienst, wenn der vom sektoralen Identity Provider verwendete Signatur-Schlüssel ihm unbekannt ist, das Entity Statement des sektoralen Identity Provider sowie die Schlüssel hinter einer eventuell verwendeten `signed_jwks_uri` herunterladen und auf Vorhandensein der verwendeten `kid` prüfen.
[<=]

A_23050 - Löschen personenbezogener Daten
Authorization-Server MÜSSEN personenbezogene Daten wie z. B. `ID_TOKEN` alsbald möglich verwerfen und dürfen diese nicht dauerhaft speichern, sofern diese nicht anderweitig zu legitimen Zwecken vorgehalten werden müssen (z. B. Protokollierung).**[<=]**

A_22860 - Prüfung benötigter "scopes"
Fachdienste MÜSSEN erhaltene `ID_TOKEN` auf das Vorhandensein der benötigten `scopes` überprüfen.**[<=]**

Hinweis: Wenn dem Fachdienst im `ID_TOKEN` zwingend notwendige Daten nicht übermittelt werden, kann er die Anmeldung des Nutzers nicht durchführen. Gemäß A_22733 ist es für sektorale Identity Provider zulässig, bei fehlenden Daten oder nicht erteilter Zustimmung des Nutzers gewisse Werte in `ID_TOKEN` nicht zu liefern.

4.4.5 Blacklisting von Client-IP-Adressen

Die Anforderungen im entsprechenden Kapitel 5 der gemSpec_IDP_FD gelten unverändert auch für Fachdienste im Rahmen der Föderation.

4.4.6 ACCESS_TOKEN

A_23076 - OAuth 2.0 Token Endpunkt
Authorization-Server MÜSSEN einen OAuth 2.0 Token Endpunkt anbieten um dort das Abrufen von Zugriffstoken mittels OAuth Code Flow und PKCE entsprechend https://datatracker.ietf.org/doc/html/rfc7636 zu ermöglichen.
[<=]

A_23077 - OAuth "ACCESS_TOKEN"
Authorization-Server KÖNNEN Zugriffstoken entsprechend OAuth `ACCESS_TOKEN` anbieten.**[<=]**

A_23078 - Zugriffstoken ohne Personenbezogene Daten
Vom Authorization-Server bereitgestellte Zugriffstoken DÜRFEN NICHT personenbezogene Daten enthalten, es sei denn diese sind Ende-zu-Ende verschlüsselt.**[<=]**

A_23079 - Gültigkeitszeitraum von Zugriffstoken
Vom Authorization-Server bereitgestellte Zugriffstoken DÜRFEN NICHT länger als 10 Minuten gültig sein.**[<=]**

4.4.7 REFRESH_TOKEN

A_23080 - OAUTH 2.0 "REFRESH_TOKEN"
Authorization-Server KÖNNEN einen OAuth 2.0 Token Endpunkt anbieten um dort das Abrufen von `REFRESH_TOKEN` entsprechend https://datatracker.ietf.org/doc/html/rfc6749#section-1.5 zu ermöglichen.**[<=]**

4.5 Spezifikation sektoraler Identity Provider - Frontend [gemSpec_IDP_Frontend]

- gemSpec_IFP_Frontend#6 "Funktionsmerkmale Authenticator-Modul" wird umbenannt in "Funktionsmerkmale Authenticator-Modul des IDP-Dienstes".
- gemSpec_IFP_Frontend: Abgrenzung und Verweis zu gemSpec_IDP_Sek aufnehmen
- A_19908-01, A_21414, A_21431, und A_22296 bzgl. Discovery Document anpassen. A_20613 und A_20614 entfallen.
- gemSpec_IDP_Frontend#7 wird umbenannt in "Funktionsmerkmale Anwendungsfrontend des IDP Dienstes"

4.5.1 (7.3) Nutzung sektoraler Identity Provider

A_23082 - Abruf und Anzeige der IDP Liste

Anwendungsfrontends MÜSSEN, sofern nicht anderweitig ein sektoraler Identity Provider zuvor gemerkt oder festgelegt wurde, die IDP-Liste vom Authorization-Server herunter laden, auf Integrität prüfen und (bei erfolgreicher Prüfung) dem Benutzer zur Auswahl anzeigen.**[<=]**

A_23083 - Auslösung der Benutzerauthentifizierung
Anwendungsfrontends SOLL zur Auslösung der Benutzerauthentifizierung einen Oauth Authorization Request an den zugehörigen Authorization-Server schicken.**[<=]**

A_23084 - Aufruf des Authenticator-Moduls
Anwendungsfrontends MÜSSEN bei Erhalt einer URI-PAR nach https://www.rfc-editor.org/rfc/rfc9126.html#name-successful-response das Authenticator-Modul mittels der übergebenen Redirect-URL aufrufen und hierbei ggf. die Link-Technologie des jeweiligen Betriebssystems verwenden.**[<=]**

A_23085 - Registrierung des Anwendungsfrontends
Anwendungsfrontends MÜSSEN sich mittels Universal-Link bzw. App-Link unter der URL des Authorization-Servers im Betriebssystems registrieren.**[<=]**

A_23086 - Aufruf des Authorization-Servers
Anwendungsfrontends MÜSSEN `AUTHORIZATION_CODE` vom Authenticator-Modul annehmen und an den Authorization-Server weiterleiten.**[<=]**

A_23081 - Automatisches Löschen von Token bei Inaktivität
Anwendungsfrontends und Web-Backend MÜSSEN bei Inaktivität des Nutzers von 10 Minuten automatisch zwischengespeicherte ACCESS_TOKEN und REFRESH_TOKEN löschen. **[<=]**

A_23097 - Logout im Anwendungsfrontend
Anwendungsfrontends MÜSSEN Nutzenden die Möglichkeit zum Abmelden bieten, und in diesem Fall zwischengespeicherte ACESS_TOKEN und REFRESH_TOKEN verwerfen.**[<=]**

AF_10103 - Abruf des "ACCESS_TOKEN"
Das Authenticator Modul SOLL folgenden Anwendungsfall umsetzen.

Tabelle 9 : Anwendungsfall "Abruf des`ACCESS_TOKEN`"

Attribute	Bemerkung
Beschreibung	Ein Anwender möchte einen in der TI registrierte Fachdienst nutzen. Der Fachdienst muss sicherstellen, dass der Anwender zur Nutzung des Dienstes berechtigt ist. Hierzu authentisiert sich der Anwender gegenüber einem sektoralen Identity Provider, bei dem er registriert ist. Nach Abschluss der Authentisierung des Nutzers gegenüber dem sektoralen Identity Provider, erhält das Anwendungsfrontend oder Web-Backend vom Authorization-Server den `AUTHORIZATION_CODE` mit dem er das `ACCESS_TOKEN` abrufen kann.
Akteur	Anwender der Fachanwendung
Auslöser	Ein Anwender möchte eine Gesundheitsanwendung der TI (Fachdienst) nutzen. Als Voraussetzung muss er sich bei einem sektoralen Identity Provider authentifizieren, bei welchem er registriert ist. Nach Abschluss der Authentifizierung erhält der Authorization-Server vom sektoralen Identity Provider einen

	ID_TOKEN (entsprechend AF_10102 - "Benutzerauthentifizierung und Erhalt des ID_TOKEN").
Komponenten	• Anwendungsfrontend oder Web-Backend • Authorization-Server eines Fachdienstes • Fachdienst API
Vorbedingung	1. Der Authorization-Server hat entsprechend AF_10102 - "*Benutzerauthentifizierung und Erhalt des ID_TOKEN*" dasID_TOKEN erhalten.
Ablauf	1. Der Authorization-Server sendet einen AUTHORIZATION_CODE an das Anwendungsfrontend oder Web-Backend ([gemSpec_IDP_Sek] Tabelle: *"Parameter des Redirect-Request"*). 2. Das Anwendungsfrontend oder Web-Backend ruft mit diesem AUTHORIZATION_CODE den Token-Endpunkt des Authorization-Servers auf. 3. Der Authorization-Server sendet einen ACCESS_TOKEN und ggf. ein REFRESH_TOKEN zurück. 4. Das Anwendungsfrontend oder Web-Backend ruft mittels des ACCESS_TOKEN die Fachdienst-API auf.
Ergebnis	Das Anwendungsfrontend oder Web-Backend hat den ACCESS_TOKEN zum Zugriff auf die Fachdienst API.
Akzeptanzkriterien	ML-133246, ML-133244, ML-133245
Alternativen	1. Das Anwendungsfrontend oder Web-Backend hat bereits zuvor ein ACCESS_TOKEN erhalten, welches abgelaufen ist. 2. Um ein neues ACCESS_TOKEN zu erhalten ruft das Anwendungsfrontend oder Web-Backend den Authorization-Server mittels REFRESH_TOKEN auf (anstelle des AUTHORIZATION_CODE). 3. Der Authorization-Server antwortet mit einem gültigen ACCESS_TOKEN und ggf. einem neuen REFRESH_TOKEN. 4. Das Anwendungsfrontend oder Web-Backend ruft mittels des ACCESS_TOKEN die Fachdienst-API auf.

ML-133246 - AF_10103 - Nutzer wurde erfolgreich authentifiziert

Der Nutzer wurde erfolgreich authentifiziert.

ML.133244 - AF_10103 - "ACCESS_TOKEN" ausgestellt

Es wurde ein ACCESS_TOKEN und ggf. REFRESH_TOKEN für den Nutzer und den Authentisierungskontext ausgestellt.

ML-133245 - AF_10103 - OAuth 2.0 Security Best Current Practice eingehalten
Die OAuth 2.0 Security Best Current Practice https://datatracker.ietf.org/doc/html/draft-ietf-oauth-security-topics wurden eingehalten.

4.6 [gemSpec_SigD]

4.6.1 (2) Systemüberblick

Der Signaturdienst erzeugt elektronische Identifizierungsmittel für Versicherte in der Umgebung des Anbieters des Signaturdienstes. Ein elektronisches Identifizierungsmittel ist gemäß Verordnung (EU) Nr. 910/2014 [eIDAS] eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten verwendet wird. Die vom Signaturdienst ausgestellten elektronischen Identifizierungsmittel sind kryptographische Identitäten basierend auf asymmetrischer Kryptographie und Teil des Vertrauensraums für X.509 nonQES-Identitäten der Telematikinfrastruktur. Die vom Signaturdienst erstellten elektronischen Identifizierungsmittel (Zertifikate) nutzen Versicherte zur Authentisierung an den Diensten der elektronischen Patientenakte.

Versicherte können elektronische Signaturen, mittels Authentisierung durch einen sektoralen Identity Provider, in der vom Anbieter des Signaturdienstes geführten Umgebung. erstellen lassen. Die elektronischen Signaturen des Signaturdienstes sind eine Alternative zur elektronischen Signatur mittels der Identität ID.CH.AUT der eGK.

Der Signaturdienst erstellt elektronische Identifizierungsmittel für Versicherte ausschließlich über korrespondierende Identitäten bzw. Personenidentifizierungsdaten eines sektoralen Identity Provider gemäß [gemSpec_IDP_Sek] im Auftrag des Kartenherausgebers der eGK des Versicherten. Personenidentifizierungsdaten sind ein Datensatz, der es ermöglicht, die Identität des Versicherten mitsamt der Herkunft der erhobenen Daten abzubilden. Die von einem sektoralen Identity Provider bereitgestellten Personenidentifizierungsdaten entsprechen den Personenidentifizierungsdaten im Zertifikat C.CH.AUT der eGK des Versicherten. Das Zertifikatsprofil C.CH.AUT_ALT für die vom Signaturdienst ausgestellten elektronischen Identifizierungsmittel ist in [gemSpec_PKI] festgelegt.

4.6.2 (3) Systemkontext

4.6.2.1 (3.1) Akteure und Rollen

Im Kontext des Signaturdienstes treten folgende Akteure auf:

Anbieter des Signaturdienstes:
Anbieter eines Signaturdienstes setzen die in dieser Spezifikation beschriebenen Aufgaben des Signaturdienstes um.

Kartenherausgeber eGK
Kartenherausgeber der eGK beauftragen den Anbieter eines Signaturdienstes, um für ihre Versicherten auf deren Wunsch hin elektronische Identifizierungsmittel ausstellen zu lassen, die alternativ zur Identität ID.CH.AUT der eGK genutzt werden können. Falls sich ein Versicherter gegenüber dem Kartenherausgeber seiner eGK für ein elektronisches

Identifizierungsmittel entscheidet, beauftragt der Kartenherausgeber eGK für diesen Versicherten beim Anbieter des Signaturdienstes das elektronische Identifizierungsmittel. Der Kartenherausgeber eGK übermittelt hierzu die für das elektronische Identifizierungsmittel notwendigen Personenidentifikationsdaten des Versicherten (u.a. Name, KVNR) an den Anbieter des Signaturdienstes.
Der Kartenherausgeber eGK veranlasst die Sperrung von elektronischen Identifizierungsmitteln bzgl. seiner Versicherten beim TSP X.509 nonQES eGK, der das Zertifikat für das elektronische Identifizierungsmittel erstellt hat.

Versicherte
Versicherte nutzen mittels eigener Client-Systeme den Signaturdienst, um mittels der elektronischen Identifizierungsmittel anderen Diensten ihre Identität zu bestätigen. Versicherte richten sich an den Kartenherausgeber ihrer eGK, falls sie ihr elektronisches Identifizierungsmittel sperren lassen möchten.

Sektoraler Identity Provider

Ein sektoraler Identity Provider einer autoritativen Stelle (z. B. eine Krankenversicherung) gibt für ihre Versicherten eine digitale Identität aus. Diese Versicherten-ID wird über Standards der OpenID Foundation Anwendungen der TI zur Verfügung gestellt. Zu den Aufgaben einer autoritativen Stelle gehören:

- die Feststellung der Versichertenidentität auf geeigneter Basis (Identity Proofing),
- die Authentifizierung den Versicherten vor Zusicherung der Versicherten-ID,
- geben diese Versicherten-ID für digitale Anwendungen und Dienste heraus,
- und stellen die Verwaltung sicher.

Der sektorale Identity Provider übernimmt aus diesen Aufgaben die Identitätsfeststellung und Authentifizierung von Versicherten sowie die Bestätigung ihrer Attribute. Die verschiedenen Dienste und sektoralen Identity Provider sind über den Federation Master [gemSpec_IDP_FedMaster] in einem Vertrauensraum organisiert. Jedoch ist es aufgrund der direkten Beziehungen zwischen Karteherausgeber der eGK, sektoralem Identity Provider, Signaturdienst und ePA-FdV nicht notwendig, dass der Signaturdienst die Funktionen der Föderation verwendet. Es besteht im Fall einer Anmeldung für den Zugriff auf eine elektronische Patientenakte eine klare Verbindung zwischen ePA-FdV, Signaturdienst und sektoralem Identity Provider, sodass die Vertrauensbeziehungen hier nicht über die Mechanismen der Föderation aufgebaut werden müssen.

4.6.2.2 (3.2) Nachbarsysteme

Die folgende Abbildung zeigt die Beziehung zu benachbarten Systemen mit den vom Signaturdienst bereitgestellten und genutzten Schnittstellen.

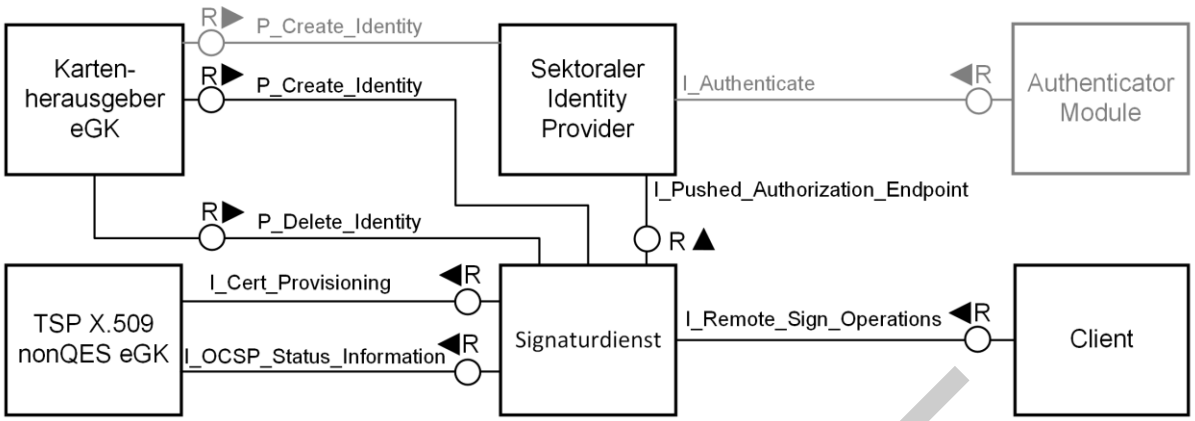

Abbildung 6: benachbarte Systeme des Signaturdienstes mit bereitgestellten und genutzten Schnittstellen

Der Signaturdienst wird als Provider einer technischen Schnittstelle zum Erstellen elektronischer Signaturen für Clients und einer Prozessschnittstelle für Kartenherausgeber eGK zum Beauftragen und Löschen von elektronischen Identifizierungsmitteln für Versicherte aufgerufen.

Der Signaturdienst nutzt die Schnittstellen des TSP X.509 nonQES - eGK zum Erstellen von Zertifikaten.

4.6.2.3 (3.3) Sicherheitsanforderungen für den operativen Betrieb

A_19041 wird wie folgt ersetzt

A_19041-01 - Umsetzung Signaturdienst für Zertifikate
Der Anbieter Signaturdienst MUSS nach erfolgreicher erster Authentifizierung des Antragstellers die erforderlichen Angaben zur Zertifikatserstellung an den Erstellungsdienst des TSP X.509 nonQES - eGK weiterleiten.**[<=]**

Alle anderen Anforderungen dieses Kapitels bleiben unverändert bestehen

4.6.3 (5) Übergreifende Festlegungen

Der Signaturdienst muss die folgenden übergreifenden Anforderungen erfüllen.

A_17373 wird ersetzt durch

A_17373-01 - Signaturdienst - Produkt erfordert Authentisierung auf dem Vertrauensniveau "hoch"
Der Hersteller des Signaturdienstes MUSS sein Produkt so implementieren, dass dieses die Freischaltung nach einer Authentisierung des Nutzers über einen sektoralen Identity Provider auf dem Vertrauensniveau "gematik-ehealth-loa-high" vorsieht.
[<=]

A_17336 wird ersetzt durch

A_17336-01 - Signaturdienst - Sicherheitsniveau der Authentisierung auf dem Vertrauensniveau "hoch"

Der Anbieter des Signaturdienstes MUSS für den angebotenen Signaturdienst sicherstellen dass die Nutzung nur nach Authentisierung des Nutzers über einen zugelassenen sektoralen Identity Provider auf dem Vertrauensniveau "gematik-ehealth-loa-high" erfolgt.**[<=]**

A_20240 "Signaturdienst - Entgegennahme von Sperrmeldungen" sowie der nachfolgende Text entfällt. - Sperrungen realisiert der sektorale Identity Provider.

Die Anforderungen A_17369, A_17370,A_17371, A_17339, A_18957 und A_18958 bleiben unverändert bestehen

A_17852 "Signaturdienst - Information des Versicherten über Änderungen an Authentifizierungsfaktoren" entfällt. - Die Verwaltung der Authentifizierungsfaktoren realisiert der sektorale Identity Provider.

A_17853 wird wie folgt geändert:

A_17853-01 - Signaturdienst - Auskunft an Versicherten
Der Anbieter des Signaturdienstes MUSS dem Versicherten auf dessen Verlangen Auskunft geben über erfolgte Zugriffe auf das elektronische Identifizierungsmittel des Versicherten.

Die Auskunft des Versicherten kann auch über den Kartenherausgeber erfolgen, der den Anbieter des Signaturdienstes mit der Erstellung des elektronischen Identifizierungsmittels beauftragt hat.
[<=]

4.6.4 (6) Funktionsmerkmale

Der Signaturdienst realisiert die Funktionsmerkmale zur Erstellung elektronischer Identifizierungsmittel und deren Nutzung für elektronische Signaturen. Das Funktionsmerkmal wird über die Implementierung der Schnittstellen `I_Remote_Sign_Operation`, `P_Create_Identity` und `P_Delete_Identity` realisiert.

4.6.4.1 (6.1) Schnittstelle I_Remote_Sign_Operations

Die Anforderung A_17583 entfällt, die anderen Anforderungen dieses Kapitels (**A_17383, A_17382 und A_17528)** bleiben unverändert bestehen.

4.6.4.1.1 (6.1.1) Operationsdefinition I_Remote_Sign_Operations::sign_Data

A_17238 Signaturdienst - Logische Schnittstelle I_Remote_Sign_Operations - wird wie folgt geändert zu

A_17238-01 - Signaturdienst - Logische Schnittstelle I_Remote_Sign_Operations

Der Signaturdienst MUSS die Schnittstelle `I_Remote_Sign_Operations::sign_Data` gemäß dem folgenden logischen Ablauf implementieren:

Tabelle 10: Tab_SigD_01 - I_Remote_Sign_Operations::sign_Data - Definition

Operation	**I_Remote_Sign_Operations::sign_Data**	
Beschreibung	Die Operation erzeugt eine ECDSA-Signatur unter Einhaltung der Vorgaben in [gemSpec_Krypt] des übergebenen Datum *(Data*) mittels des privaten Schlüssels des elektronischen Identifizierungsmittels ID.CH.AUT_ALT des aufrufenden Nutzers *(Identifier)*. Das signierte Datum (*SignedData*) und das Zertifikat des elektronischen Identifizierungsmittels C.CH.AUT_ALT der Identität, für die signiert wurde, werden als Ergebnis der Operation zurückgeliefert.	
Eingangsparameter		
Name	**Beschreibung**	**Typ**
`Data`	Die zu signierenden Daten.	Binary
`Identifier`	Identifiziert, welches elektronisches Identifizierungsmittel ID.CH.AUT_ALT zur Signatur des Datums genutzt werden soll. Der Identifier ergibt sich aus den Attributen nach Authentisierung des Nutzers an einem sektoralen Identity Provider.	String
Ausgangsparameter		
Name	**Beschreibung**	**Typ**
`SignedData`	Das mit dem privaten Schlüssel des elektronischen Identifizierungsmittels ID.CH.AUT_ALT signierte Datum.	Binary
`Certificate`	Zertifikat C.CH.AUT_ALT des elektronischen Identifizierungsmittels, mit dessen zugehörigem privaten Schlüssel signiert wurde.	**Certificate X.509**

[<=]

4.6.4.1.2 (6.1.2) Umsetzung I_Remote_Sign_Operations::sign_Data

Die Anforderungen A_17384, A_18172 und A_18173 entfallen, da der Signaturdienst selbst kein Authentisierungsverfahren mehr anbietet sondern stattdessen auf einen zugelassen sektoralen Identity Provider zurückgreift (A_17373-01 und A_17336-01). Aufgrund der direkten Beziehungen zwischen Karteherausgeber der eGK, sektoralem

Identity Provider, Signaturdienst und ePA-FdV ist es jedoch nicht notwendig, dass der Signaturdienst die Funktionen der Föderation verwendet.

Die anderen Anforderungen des Kapitels (A_17527, A_17741, A_18710 und A_18711) bleiben unverändert bestehen.

4.6.4.2 (6.2) Schnittstelle P_Create_Identity

A_17375 wird wie folgt geändert

A_17375-01 - Signaturdienst - P_Create_Identity
Der Anbieter des Signaturdienstes MUSS eine Prozess-Schnittstelle umsetzen, mittels derer Kartenherausgeber dem Signaturdienst einen Auftrag zur Ausstellung eines elektronischen Identifizierungsmittels für einen Versicherten erteilen können. Der Auftrag MUSS die für das elektronische Identifizierungsmittel notwendigen Personenidentifikationsdaten für das Zertifikat C.CH.AUT_ALT enthalten.
Die Zuordnung des elektronischen Identifizierungsmittels zu einem Nutzer erfolgt über die Identifikationsdaten des sektoralen Identity Provider.
[<=]

A_17372 und A_17379 bleiben bestehen.

A_17381 entfällt, da die Identifikation durch den sektoralen Identity Provider durchgeführt wird bevor dieser einen Versicherten in seinen Datenbestand aufnimmt.

4.6.4.3 (6.3) Schnittstelle P_Delete_Identity

A_17808 Signaturdienst - P_Delete_Identity bleibt unverändert bestehen.

4.7 [gemSpec_FD_eRp]

Offener Punkt: Der Produkttyp IDP-Dienst wird die bestehende Funktionalität der Third-Party-Authorization an die Vorgaben und Methoden der Föderation und als Authorization-Server des e-Rezept Fachdienstes agieren.

Der genaue Umfang der daraus resultierenden Änderungen zwischen IDP-Dienst, E-Rezept-FdV und ggf. minimal am E-Rezept-Fachdienst wird in einer späteren Version des Dokumentes konkretisiert.

4.8 [gemSpec_IDP_Dienst]

Offener Punkt: Der Produkttyp IDP-Dienst wird die bestehende Funktionalität der Third-Party-Authorization an die Vorgaben und Methoden der Föderation und als Authorization-Server des e-Rezept Fachdienstes agieren.

Der genaue Umfang der daraus resultierenden Änderungen zwischen IDP-Dienst, E-Rezept-FdV und ggf. minimal am E-Rezept-Fachdienst wird in einer späteren Version des Dokumentes konkretisiert.

Das E-Rezept-FdV wird parallel die zuvor etablierten Prozesse für die Third-Party-Authorization und die Methoden der Föderation unterstützen bis alle Versicherten über sektorale Identity Provider beauskunftet werden welche Teil der Föderation sind.

Kapitel 1.4

Folgende Aussage wird gestrichen, da Fachdienste, wie das E-Rezept, aktuell auch innerhalb der TI für TLS-Verbindungen dieselben EV-TLS-Zertifikate nutzen wie im Internet.

~~Es wird angenommen, dass Fachdienste ihre innerhalb der TI zu verwendenden Zertifikate für die Transport Layer Security (TLS)-Sicherung über zentrale Plattformdienste der TI beziehen und diese dort auch geprüft werden können.~~

4.9 [gemKPT_Betr]

Anbietererklärung zur Umsetzung der durch die gematik definierten notwendigen Major-Releases für die föderierten IDPs >> Kommt ins Kapitel 3.4.1.2

A_22954 - Umsetzung definierter Releases durch den Anbieter
Der Anbieter MUSS umsetzungspflichtige Release umsetzen, um weiterhin Mitglied des IDP-Vertrauensraumes zu sein.
Bei nicht rechtzeitiger Umsetzung der durch die gematik angekündigten und als solches gekennzeichneten Release wird die gematik den Anbieter aus der Vertrauensbeziehung (Trusted Party des IDP) der Föderation ausschließen. Die Umsetzung eines Releases durch den Anbieter setzt die rechtzeitige Verfügbarkeit des damit verbundenen zugelassenen Produktes voraus.
Die Zulassung bleibt davon unberührt.
[<=]

Hinweis: Die gematik kündigt mit sechsmonatiger Vorlaufzeit den Anbietern das umsetzungspflichtige Release an.

5 Anhang A – Verzeichnisse

5.1 Abkürzungen

Kürzel	Erläuterung

5.2 Referenzierte Dokumente

5.2.1 Dokumente der gematik

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

[Quelle]	**Herausgeber: Titel**
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur

5.2.2 Weitere Dokumente

[Quelle]	**Herausgeber (Erscheinungsdatum): Titel**
