Fachliche & technische Grundlagen

- Fachliche Grundlagen
  - Begriffsbestimmungen
- Technische Grundlagen
- Identifikationsmittel und -systeme
- Die Ausgangslage im deutschen Gesundheitswesen
  - Identitätsherausgeber, Identitätsträger und Trust Service Provider
    - Elektronische Gesundheitskarte (eGK)
    - Elektronischer Heilberufsausweis (HBA)
    - Institutionsbezogene Identität SM(C)-B
  - Der Weg zur TI 2.0
  - Gesetzliche Rahmenbedingungen
- Fachliche Einordnung der sektoralen Identity Provider
  - Rahmenbedingungen des Authentisierungs-Flows
    - Relevante Anwendungen der IDP-Nutzung
    - Vertrauensniveaus
    - Bereitstellung von claims
    - Zugriffsmedien
  - Ablauf der Authentisierung

Fachliche Grundlagen

Begriffsbestimmungen

Zum weiteren Verständnis ist notwendig zunächst die wesentlichen Begrifflichkeiten zu klären.

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 oder anderer übermittelter Daten mit Metadaten, die es einer vertrauenden Entität ermöglichen, die Herkunft, Echtheit und Gültigkeit der Identität oder der Daten zu überprüfen. Der Überprüfungsvorgang durch die vertrauende Entität ist die Authentifizierung der Identität/der Daten. (BSI TR-03107)

Authentisierungsmittel: Authentisierungsmittel sind technische Mittel, die es dem Inhaber erlauben, eine Identität (das heißt eine Menge von Identitätsattributen) oder andere 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.

Enrolment: Das Enrolment 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)

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 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 Zusammenfassungen 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.

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 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 entweder kontaktbehaftet oder mit NFC Funktionalität und einem auf ihr enthaltenen Lichtbild für Vor-Ort-Identifizierung bzw. eine PIN für eine Identifizierung online und vor Ort eingesetzt werden. Des Weiteren stellt der neue Personalausweis bzw. der elektronische Aufenthaltstitel bzw. die ID-Karte für EU/EWR-Bürger/innen 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.

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.

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 und sonstige Kostenträger 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. 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 Gesundheitsberufsregister (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 Kassenärztlichen Vereinigungen, Kassenzahnärztliche Vereinigungen, Apothekerkammern, DKTIG, gematik, Gesundheitsberufsregister und Handwerkskammern. Hier agieren in Summe rund 70 Identitätsherausgeber für den Identitätsträger der SMC-B-Karte.

Mit der Bereitstellung der Identitätsträger werden bei Bedarf sog. Trust Service Provider beauftragt. 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.

Elektronische Gesundheitskarte (eGK)

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 abhängig des Ausgabezeitpunktes auch als dezentraler Speicher für die Datensätze Notfalldaten-Management, Datensatz Persönliche Erklärung, Organspendeerklärung, E-Medikationsplan und den Versichertenstammdaten (gemäß §291 Absatz 2 Nummer 3 SGB V ermöglicht die eGK - sofern sie nach dem 1. Januar 2023 ausgestellt wird, nur noch die Speicherung von Daten nach § 291a Absatz 2 Nummer 1 bis 3 und 6). 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.

Elektronischer Heilberufsausweis (HBA)

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.

Institutionsbezogene Identität SM(C)-B

Die Security Module (Card) Typ B ist eine institutionsbezogene Identität, welche an eine Smartcard oder als Zertifikatsbundle gekoppelt herausgegeben wird. Sie repräsentiert eine Institution innerhalb der TI und sie stellt Zertifikate für Authentisierung, Ver-, Ent- und Umschlüsselung sowie elektronische Signaturen zur Verfügung.

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 eine 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 Konzeption der digitalen Identitäten 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.

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.

Gesetzliche Rahmenbedingungen

In diesem Kapitel folgt eine Übersicht über die relevantesten rechtlichen Grundlagen der vorliegenden Konzeption. Sie erhebt keinen Anspruch auf Vollständigkeit. Zum 01.01.2023 trat das Krankenhauspflegeentlastungsgesetz (KHPflEG) in Kraft, welches zu einer Änderung der §§291 und 340 SGB V führte. Die Neuerungen finden bereits Berücksichtigung in diesem Kapitel.

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

„Spätestens ab dem 1. Januar 2024 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 SGB 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 SGB V)**.

„(7) Spätestens ab dem 1. Januar 2025 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 SGB 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 SGB V** bzw. sinngemäß **§340 Absatz 8 Satz 1 und 2 SGB V).**

Sowohl für digitale Identitäten für Versicherte nach § 291 Abs. 8 SGB V als auch für Leistungserbringende und Leistungserbringerinstitutionen nach § 340 Abs. 8 SGB V muss das '[...] Sicherheits- und Vertrauensniveau der Ausprägung einer digitalen Identität [...] mindestens dem Schutzbedarf der Anwendung entsprechen, bei der diese eingesetzt wird (§ 291 Absatz 8 Satz 6 bzw. § 340 Absatz 8 Satz 4 SGB V, gleichlautend).

Mit den Änderungen des KHPflEG wurde des Weiteren Satz 7 in §291 SGB V aufgenommen: "Abweichend von Satz 6 kann der Versicherte nach umfassender Information durch die Krankenkasse über die Besonderheiten des Verfahrens in die Nutzung einer digitalen Identität einwilligen, die einem anderen angemessenen Sicherheitsniveau entspricht." (**§291 Absatz 8 Satz 7 SGB V**)

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

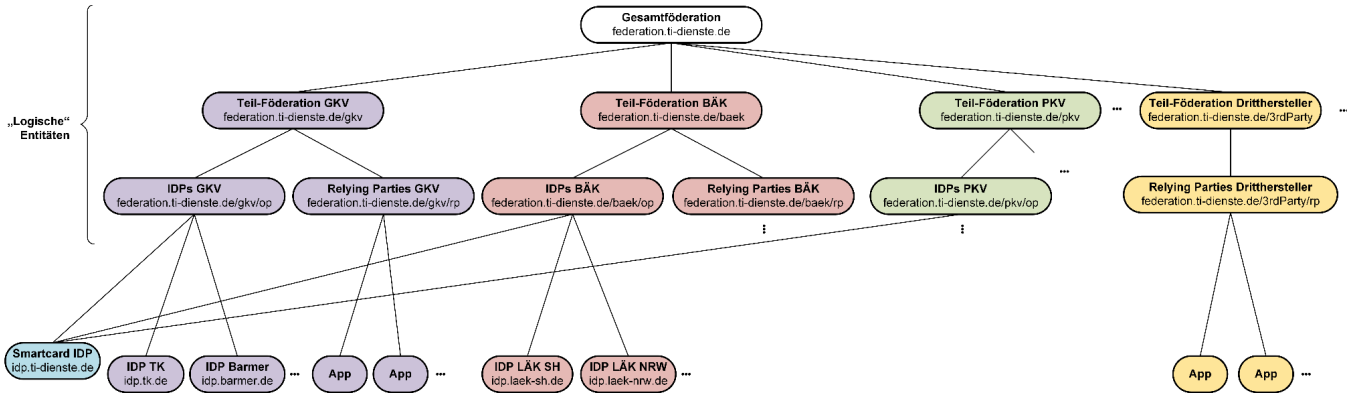
- **BSI TR-03107-1** Elektronische Identitäten und Vertrauensdienste im E-Government
- **BSI TR-03147** Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen.

Allgemein gilt nach EU-DSGVO, dass Gesundheitsdaten von besonders schützenswertem Charakter sind. Entsprechend ist das Vertrauensniveau nach TR-03107-1 mit einem hohen Vertrauensniveau zu bewerten.

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.

Fachliche Einordnung der sektoralen Identity Provider

Aufbau, Funktionsumfang und Schnittstellen der Identity Provider, sollen im Rahmen einer Föderation den Zugang zur Telematikinfrastruktur alternativ der kartengebundenen Identitäten ermöglichen.



Unter Föderation versteht sich, dass jeder Sektor, und innerhalb der Sektoren die jeweiligen Identitätsherausgeber einen eigenen Identity Provider für dessen Mitglieder bereitstellt. Bei den digitalen Identitäten für den Sektor „Versicherte“ 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. Die Anforderungen an die Identity Provider der unterschiedlichen Sektoren unterscheiden sich. Dies liegt vor allem darin begründet, dass die Anwendungsfälle und Anwendungen, welche eine Authentifizierung eines Nutzers über einen IDP erfordern für Versicherte andere sind als z.B. für Ärzte in Praxen und Krankenhäusern oder für andere medizinische Berufe wie Hebammen und Pflegedienste.

Die Orchestrierung der unterschiedlichen Identity Provider in der Föderation erfolgt über den sog. Federation Master. 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.

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 im Februar 2023 veröffentlichte 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 Spezifikation der gematik 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.

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.

Hieraus ergibt sich der Bedarf an unterschiedlichen Flows, welche durch die IDPs zu unterstützen sind.

- **App-App-Flow:** Der App-App-Flow beschreibt die Einzelschritte für die Authentifizierung eines Nutzers im Rahmen einer Fachanwendung, bei der die Fachanwendung eine 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.

Ablauf der Authentisierung

Der genaue Ablauf der Authentisierung hängt von den 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* einsc hließlich 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.