bitkom

#2
Digitalisierung von Identitäten

Digitalisierung von Identitäten im Gesundheitswesen

Umbruch und Herausforderungen im Gesundheitswesen

Digitalisierung von Identitäten im Gesundheitswesen

Einleitung

Von Kartentechnologie zu digitalen Identitäten

Mit der Telematikinfrastruktur (TI) in ihrer ersten Version entstand durch die gematik als hoheitliche Instanz der Gesundheitstelematik in den letzten 20 Jahren ein in sich geschlossenes Branchennetzwerk für alle Akteure im Gesundheitswesen (Versicherte, Ärzte, Apotheker, Krankenhäuser und sonstige Leistungserbringer). Der Zugang zu Diensten der TI erfolgt bis heute weitgehend über hochsichere Karten- und andere Hardwaretechnologie. Mit der elektronischen Gesundheitskarte (eGK) für gesetzlich Versicherte sowie den Heilberufsausweis für Ärzte bzw. die HSMC-B-Karte für Organisationen als Leistungserbringer ist der Rollout seit 2022 abgeschlossen und in der TI etabliert. Der große Unmut über die Telematikinfrastruktur macht sich allerdings nicht an der Nutzung von Karten als Zugangsmittel, sondern vielmehr an den fehlenden echten Mehrwertanwendungen für Versicherte und Leistungserbringer fest.

Mit der Einführung der elektronischen Patientenakte (ePA) als Versicherten-geführter Gesundheitsakte, des elektronischen Rezeptes (eRezept) sowie Kommunikations-diensten zwischen den Leistungserbringern mit KIM (sichere E-Mail) und TI-Messenger (sichere Chat-Kommunikation) stehen seit 2022/23 Anwendungen zur Verfügung, die eine einfache, aber auch sichere Identifizierung und Authentifizierung mit dem Mobilgerät als Ergänzung der eGK ermöglichen.

Parallel zu dieser Entwicklung hat die gematik ihre Strategie für eine Telematikinfrastruktur 2.0 und damit den Umbau des geschlossenen Branchen-netzwerks in ein offenes und sicheres Zero-Trust-Framework im Internet verkündet und die Umsetzung gestartet. Mit dieser Strategie geht die Nutzung digitaler Gesundheits-anwendungen als Teil eines größeren und auch europäisch gedachten Ökosystems einher. Das ebnet den Weg für die Nutzung europaweit etablierter Technologie und Interoperabilitätsstandards in einer harmonisierten Public-Key-Infrastruktur.

Die gematik positioniert digitale Identitäten als erste relevante Anwendung der TI 2.0. Gleichzeitig sie sich stärker den Entwicklungen rund um die eIDAS-Verordnung, den etablierten Vertrauensdiensten, aber auch den zukünftigen Prinzipien einer ID-Infrastruktur in Deutschland nach den Vorgaben von eIDAS 2.0.

Etablierung einer Föderation aus dezentralen Identitätsprovidern von Krankenkassen, Krankenversicherungen und Leistungserbringern

Bereits 2022 wurde über einen zentralen Identitätsprovider (IDP) zum eRezept auf Basis von OpenID Connect (OIDC) ein Token-basierter Zugang als erste Lösung für digitale Identitäten im Gesundheitssektor über die mobile eRezept-App in der Telematikinfrastruktur realisiert.

Für den weiteren Ausbau digitaler Identitäten insbesondere im Kontext eines Single Sign On auf viele verschiedene Fachanwendungen in und außerhalb der TI hat sich die gematik für den Aufbau einer Föderation entschieden und die hierfür notwendige Spezifikation entwickelt. Gesetzliche Krankenkassen und neu in die gematik eingetretene privaten Krankenversicherungen wurden verpflichtet, bis zum 01. Januar 2023 für die Bereitstellung einer digitalen Versicherten-Identität (im weiteren als Gesundheits-ID bezeichnet) einen sektoralen IDP bereitzustellen und bei der gematik zuzulassen. Auf dem Markt haben sich Anbieter einer Identity-as-a-Service in Ausschreibungen der Kostenträger durchgesetzt. Sie realisieren 2023 die Bereitstellung der Infrastruktur sowie die Anpassung der notwendigen User-Flows in den mobilen Apps für die Versicherten.

Mit diesem Schritt richtet die gematik ihre Spezifikation sehr eng an den OIDC-Vorgaben aus und fordert den Betrieb der Identitätslösung in einer abgesicherten, vertrauenswürdigen Ausführungsumgebung (VAU). Der wichtigste Grund hierfür ist die Verhinderung der Profilbildung zu Nutzern durch den Betreiber der Identitätslösung. Gleichzeitig wurden die Verfahren zur Personenidentifizierung auf den elektronischen Personalausweis (eID-Verfahren) oder alternativ eine Vor-Ort-Identifizierung (in einer Postfiliale, der Geschäftsstelle des Kostenträgers oder zukünftig auch der Apotheke) beschränkt. Um ein eIDAS-Vertrauensniveau „hoch“ zu erreichen, wurden zusätzlich Einschränkungen in der Authentifizierung durch das BSI und BfDI durchgesetzt, die je nach Mobilgerät eine Wiederholung der sicheren Authentifizierung nach 12 Stunden bis 6 Monaten vorsieht. Die Einschränkung der Usability und damit die Gefahr, dass ein solches Vorgehen keine Nutzerakzeptanz findet, führen weiterhin zu einem zähen Ringen zwischen gematik und BSI und BfDI bei der finalen Ausgestaltung der Richtlinien (Stand Juli 2023).

In einem nächsten Schritt steht die Entwicklung und Spezifikation einer Identitätslösung für die Leistungserbringer (Ärzte, Apotheker, Therapeuten, Pflege, u.a. Gesundheitsberufe) sowie der Leistungserbringer-Organisationen an. Hierbei besteht die Herausforderung in den dynamischen Attributen für die zum Zeitpunkt der Nutzung für den Leistungserbringer relevante Funktion bzw. Standort (Arzt im Krankenhaus oder im MVZ). Hierzu sondiert die gematik aktuell auch flexiblere Konzepte wie z. B. OpenID für Verifiable Credentials und macht damit den Weg zu neuen Standards frei, die auch später für eine eIDAS-2.0-Umsetzung relevant werden.

Die Herausforderungen auf dem Weg hin zu einem dezentral organisierten Ökosystem digitaler Identitäten

Die Migration von der Telematikinfrastruktur 1.0 als geschlossenes Branchennetzwerk auf eine Zero-Trust-Architektur der TI 2.0 ist nicht nur herausfordernd bei der Auswahl

geeigneter technischer Komponenten und Standards. Der Wechsel wird nicht zu einem definierten Stichtag für die gesamte TI erfolgen, sondern schrittweise über die Umsetzung einzelner Komponenten. Digitale Identitäten sind dabei ein erster und wichtiger Baustein in der Realisierung der TI 2.0. Die Roadmap der gematik wird einen Parallelbetrieb der bestehenden, etablierten Komponenten (z. B. Karten- und Konnektorentechnologie) und der neuen Möglichkeiten, die z. B. die Nutzung des Mobilgerätes oder auch die eIDAS-2.0-Verordnung mit sich bringt, berücksichtigen.

Die noch im Aufbau befindliche Föderation digitaler Identitäten wird in den kommenden Jahren dabei weiterhin das Zusammenspiel zwischen Fachdiensten als Relying Party und sektoral gestalteten Identitätsprovidern bestimmen. Eine Änderung dieser Strategie ist nur zu erwarten, wenn durch neue technische Möglichkeiten und Standards die Fragen zu Nutzerkomfort, Kosten oder Sicherheit bzw. Datenschutz optimiert werden können. Parallel wird sich die Gestaltung der EUDI-Infrastruktur in Deutschland im Kontext der eIDAS-2.0-Verordnung und hierbei insbesondere die Entscheidung zur Wallet-Strategie auf die Umsetzung digitaler Identitäten im Gesundheitsmarkt auswirken – allerdings verbunden mit der Frage, ab wann und in welcher Form die Möglichkeiten der EUDI-Infrastruktur die teilweise komplexen Anwendungsfälle der deutschen Gesundheitstelematik unterstützen können.

Daher wird die gematik die Erkenntnisse aus der eIDAS-2.0-Entwicklung – insbesondere die Ergebnisse der LSP-Projekte und somit auch des Architectual Reference Frameworks (ARF) – mit in die Weiterentwicklung der TI 2.0 und damit auch in die standardisierte und Europa-konforme Gestaltung digitaler Identitäten im Gesundheitsmarkt einbeziehen müssen. Der Wechsel vom aktuellen, föderierten Ansatz hin zu dezentral organisierten Identitätsattributen wird schrittweise und nicht mit einer Rip-and-Replace-Strategie erfolgen können. Fachanwendungen wie ePA, eRezept, TI Messenger und digitaler Gesundheitsanwendungen (DiGa) können bei der Umstellung auf Wallet-basierte Ansätze sowie die Integration der eIDAS-2.0-Verordnung schrittweise profitieren, wenn der Fokus auf dem Nutzen für den Anwender bzw. die Verbesserung von Sicherheit und Datenschutz liegt. In dem Kontext passen z. B. die im ARF mit hinterlegten neuen Möglichkeiten der OpenID-Connect-Erweiterung im Verifiable Credentials (OI4VC-Standard), da sie einen deutlich flexibleren Umgang mit Attributen im Vergleich zu den heute etablierten klassischen OIDC-Prozessen erlauben.

Unabhängig von der Weiterentwicklung der TI 2.0 wird es eine Aufgabe sein, den Versicherten wichtige Attribute wie z. B. seine Versicherungsnummer in ihrer EUDI-Wallet zur Verfügung zu stellen, damit er diese europaweit digital verwenden kann. Auch werden Initiativen wie der EU Health Data Space einen eIDAS-2.0-konformen Zugang des Versicherten fordern. Da davon auszugehen ist, dass die Weiterentwicklung digitaler Identitäten in der TI 2.0 aufgrund der Migration des föderierten Ansatzes hin zu dezentralen Identitäten länger dauern wird, muss parallel zur Etablierung der EUDI-Wallet-Infrastruktur eine separate Nutzung wichtiger Attribute für Versicherte und Leistungserbringer ermöglicht werden. Sicher ist, dass Wallet-basierte, dezentrale Identitäten zu einer wichtigen Komponente in der Gesundheitstelematik werden, die in fünf bis zehn Jahren die etablierte Karten- und Konnektorentechnologie sowie die Nachteile eines föderierten Identitätsmanagements komplett ersetzen.

Unabhängig von der Diskussion der technischen Roadmap digitaler Identitäten in der deutschen Gesundheitstelematik wird die erwartete Verbesserung durch die

Digitalisierung nur eintreten, wenn die Nutzerperspektive zukünftig deutlich mehr in den Vordergrund gerückt wird.

Die bisherige Einführung von Komponenten in der TI hat sowohl bei leistungserbringenden Krankenhäusern, Ärzten, Apothekern u. a. sowie den Versicherten den Eindruck hinterlassen, dass diese nicht ausreichend getestet und im Design kaum Mehrwerte für den Nutzer mit sich bringen. Die Etablierung neuer Dienste in der TI (wie z. B. ePA, eRezept, eAU, TI Messenger u.a.) geht immer mit der Gefahr einher, dass schlecht designte Nutzerflows oder hohe regulatorische Hürden keine Akzeptanz bei Versicherten und Leistungserbringern finden. Gerade hier ist das für die Nutzung digitaler Fachanwendungen der TI notwendige Onboarding und die sichere Nutzung digitaler Identitäten eine Schlüsselfaktor: Gelingt es nicht, dass Versicherte und Leistungserbringer die Umsetzung der auferlegten Sicherheitsprozesse beim Onboarding und der Anmeldung bei digitalen Services akzeptieren, werden sie auch ePA oder eRezept nicht – wie von der Politik erhofft – nutzen.

Daher wird die größte Herausforderung für die gematik als neue Digitalagentur der deutschen Gesundheitstelematik darin bestehen, das Anwendungsdesign für die Nutzung digitaler Identitäten komfortabel und auf die Lebensrealität der Nutzer (Versicherte und Leistungserbringer) abgestimmt zu gestalten – und es nicht Krankenkassen und -versicherungen bzw. Leistungserbringer-Organisationen zu überlassen. Dazu muss das Design digitaler Identitäten im Gesundheitsmarkt aus Sicht des Nutzers als Versicherter, Arzt oder Pfleger betrachtet werden.

Damit kommt auf die gematik zusätzlich zur weiterhin notwendigen Erstellung von Spezifikationen sowie der Zulassung der Lösungen die Verantwortung zu, das Prozess- und Anwendungsdesign sowie ihre technische Umsetzung mitzugestalten. Diese Aufgabe kann gemeinsam mit Industrie und Anwendern z. B. in einem Co-Creation-Prozess angegangen werden und dann auch Nutzertests bzw. -befragungen umfassen. Damit lassen sich die notwendigen funktionalen Anforderungen mit dem Anspruch der gematik an Sicherheit und Interoperabilität mit den Bedürfnissen der Nutzer verbinden. Notwendige Investitionen der Politik in Co-Creation und Anwendungsdesign werden helfen, das Potenzial digitaler Identitäten für die Gesundheitstelematik mit deutlich geringen Risiken in die Umsetzung zu bringen.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Autoren
Dominik Deimel, comuny GmbH
Franca Löwenstein, Bundesruckerei GmbH

Ansprechpartner
Clemens Schleupner | Referent Digitale Identitäten & Vertrauensdienste
T 030 27576-424 | v.name@bitkom.org

Verantwortliches Bitkom-Gremium
AK Digitale Identitäten