

#5

Digitalisierung
von
Identitäten

Digitalisierung von Identitäten im Gesundheitswesen

eIDAS-Mittel zur Weiterentwicklung der
Telematikinfrastruktur

Werkzeuge für die TI 2.0. Ein Plädoyer für die Verwendung von eID, EUDI-Wallet, qualifizierten Vertrauensdiensten und anderen etablierten Mitteln zur Weiterentwicklung der Telematikinfrastruktur

Einleitung

Die eID und IDP als „das Identifizierungs- und Authentisierungsmittel“ in der TI

Beim Digitalgipfel 2023 stieß die Präsentation eines Demonstrators für den eID-basierten Identitätsprovider (IDP) auf großes Interesse. Dort wurden verschiedene Anwendungsfälle des eID-basierten IDPs im Gesundheitssektor vorgestellt. Auch das Bundesministerium für Gesundheit (BMG), betonte jüngst die Bedeutung des eID-basierten IDP für die Telematikinfrastruktur (TI) und den Trend weg vom Identifizierungsmittel der elektronischen Gesundheitskarte (eGK) hin zur eID. Ab Januar 2024 sind Krankenkassen gesetzlich dazu verpflichtet, digitale Identitäten basierend auf der eID-Funktion für den Zugang zu elektronischer Patientenakte oder E-Rezept zur Verfügung zu stellen. Das ist eine begrüßenswerte Entwicklung. Die eID setzt sich in immer mehr Bereichen als sicheres und stetig nutzerfreundlicheres Identifizierungsmittel durch und verzeichnet mittlerweile siebenstellige Nutzungszahlen pro Jahr. Die TI setzte in der Vergangenheit zu oft auf eigene Insellösungen und Standards, wie zB bei der eGK als primäres Identifizierungsmittel der Versicherten für die TI, anstatt vollumfänglich auf bereits etablierte und erfolgreiche Mittel und Werkzeuge auf nationaler oder europäischer Ebene, wie die eID, zu setzen. Der nun eingeschlagene Weg trägt dazu bei, die eID bald als das vorrangige Identifizierungs- und Authentisierungsmittel im Gesundheitssektor zu etablieren. Der Aufbau der TI 2.0, basierend auf dem Zero-Trust-Konzept, ist die Chance in der Entwicklung auf Standards aufzubauen und ein hochsicheres nationales- wie europäisch interoperables Gesundheitssystem zu etablieren. Ziel sollte es sein, dass alle Nutzer der TI, dort wo es möglich ist auf zusätzliche Hardware verzichten bzw. wenn nötig, auf bereits vorhandene Mittel und vorhandene Standardhardware

zurückgreifen können, und somit die Anschaffung eigener spezieller TI-Hardware, wie Konnektoren, entfallen kann.

EU-konforme Weiterentwicklungen der bestehenden TI

Aber auch in der Zwischenzeit könnten bereits mehr etablierte Werkzeuge, Mittel und Standards Berücksichtigung in der Weiterentwicklung der bestehenden TI finden. So ist die Verpflichtung der Einbindung eines IDP für Leistungserbringer erst für das Jahr 2025 geplant. Um auch hier Anwendern einen Vorteil bieten zu können, müssen eID, etablierte eIDAS-Mittel (beispielsweise elektronische Signaturen, Siegel und Zeitstempel) und allgemeine Standards Berücksichtigung finden und eine entsprechende Spezifikation der gematik zeitnah erfolgen.

Weiterhin ist es beispielsweise wichtig von der eHBA-(elektronischer Heilberufsausweis)- kartenbasierten qualifizierten elektronischen Signatur (QES) hin zur Zulässigkeit von qualifizierten Fernsignaturen zu kommen. Gemäß der eIDAS-Verordnung sind bereits seit 2016 Fernsignaturen in Deutschland zulässig. Bei einer Fernsignatur wird das Schlüsselmaterial nicht mehr auf einer Smart-Card gespeichert, sondern auf einem Hardware-Security-Module (HSM), das vom qualifizierten Vertrauensdiensteanbieter verwaltet wird. Hierdurch ist der Anwender hardwareunabhängig und braucht kein Kartenlesegerät, sondern kann von jedem Gerät aus der Ferne eine QES auslösen. So steigert sich der Nutzungskomfort der QES für Leistungserbringer signifikant, vor allem im mobilen Kontext. Ohne Weiteres könnten Zertifikate für Fernsignaturen inzident bei der Ausstellung eines eHBA oder auf Grundlage eines bestehenden eHBA erstellt werden. Ferner könnten qualifizierte elektronische Siegel für juristische Personen der QES mit Vertretungsattribut gleichgestellt werden und ausdrücklich in den Gematik-Spezifikationen verankert werden, um die Nutzungsfreundlichkeit weiter zu steigern. Es fehlen eigentlich nur noch die entsprechenden Spezifikationen der gematik. Daher bleibt zu hoffen, dass die anstehende Umstrukturierung der gematik hier nicht zu einer Verzögerung der Weiterentwicklung und Transformation der TI führen, sondern im Gegenteil als Chance einer Neuaufstellung mit einem breiteren Fokus der Regulierung wahrgenommen wird.

Die EUDI-Wallet als „Schweizer Taschenmesser“ für die TI

Im November 2023 einigten sich EU-Parlament, Kommission und Rat mit der revidierten eIDAS-Verordnung, welche im Frühjahr 2024 verabschiedet werden soll, auf einen neuen Meilenstein der europäischen Digitalpolitik. Die EUDI-Wallet wird die Infrastruktur der digitalen Identifizierung in Deutschland grundlegend verändern – und damit auch die Abbildung digitaler Identitäten im Gesundheitswesen. Dabei bietet die eIDAS 2.0, insbesondere mit der EUDI-Wallet und dem neuen Vertrauensdienst der qualifizierten Bestätigung elektronischer Attribute (QEAA), wichtige europäisch harmonisierte Werkzeuge zur Weiterentwicklung der TI. Da die EUDIW das Vertrauensniveau „hoch“ erfüllt, ist sie prädestiniert für den Einsatz im Gesundheitsbereich, inklusive der Verarbeitung und dem Zugang zu den besonders sensiblen Gesundheitsdaten. Dabei kann sie viele Funktionalitäten in der TI abdecken und ist für spezielle Use-Cases konfigurierbar. So lassen sich EUDI-Wallets für verschiedene Rollen, beispielsweise für Ärzte, Apotheker, Krankenhäuser oder Versicherte einrichten und in diesem Kontext periodisch und anlassbezogen einsetzen.

Es ist jedoch zu fordern die EUDIW explizit auch für juristische Personen nutzbar zu machen, um einen hohen Nutzungskomfort für Nutzer zu erreichen. Viele Akteure des Gesundheitsbereichs, beispielsweise Krankenhäuser und Apotheken sind regelmäßig juristische Personen. Diese werden bisher häufig nur als angehängte Attribute für die Vertretung durch eine natürliche Person, beispielsweise Arzt oder Apotheker abgebildet, was die Prozesse verkompliziert und die Nutzerfreundlichkeit für Standardprozesse, zB die Abrechnung, senkt. Bei der Abbildung der juristischen Person in der EUDIW gibt es nur wenige Vorgaben von Seiten der EU, sodass die genaue konzeptionelle Umsetzung der Wallet für juristische Personen (Gesellschaftsattribut für eine natürliche Person oder eine eigene Organisationswallet mit einer eigenen Grundidentität) von den Mitgliedsstaaten abhängig macht. Die einfache Nutzbarkeit für juristische Personen ist jedoch essentiell für den Erfolg der EUDI im Gesundheitsbereich. Etwaig verbliebene Lücken der EUDI-Standardisierung kann ferner die Gematik durch eigene Spezifikationen füllen.

Grundlage der EUDIW ist die Personal Identification Data (PID) eine Ableitung der eID auf dem Vertrauensniveau „hoch“. Ferner bietet die EUDI ein Authentifizierungselement mit zwei Faktoren. Diese Komponente kann in der TI überall dort genutzt werden, wo bereits heute eine Zweifaktorauthentifizierung eingesetzt wird. Außerdem kann mit dieser Funktion auch der Zugriff auf die TI erfolgen, sodass die umstrittenen Konnektoren vollumfänglich ersetzt werden können. Weiterhin eignet sich die Funktionalität als Authenticator um im Rahmen des avisierten Zero Trust Ansatzes der TI 2.0 künftig als Authentifizierungswerkzeug Anwendung zu finden, um dort Transaktionen und Zugriffe freizugeben. Zusätzlich hat die EUDI eine mandatorische Funktionalität der QES für natürliche Personen und dem QSeal für juristische Personen zur Signatur/Siegelung von elektronischen Dokumenten und Datensätzen. Weiterhin ist die EUDI auch als Applikation zur Verwaltung und Weitergabe von e-Rezepten und Impfberechtigungen konzipiert. Bereits jetzt ist auf europäischer Ebene die EUDI als Identifizierungs- und Authentifizierungsmittel für den europäischen Gesundheitsdatenraum (EHDS) samt elektronischer Patientenakte als Primärnutzung gesetzt.

Digitalisierung von eGK, eHBA und SMC-B mittels QEAA

Eine weitere bedeutende Funktionalität der EUDIW ist die Ausstellung, Speicherung und Weitergabe von QEAA und nicht qualifizierten elektronischen Attributen (EAA). Hiermit lassen sich alle hoheitlichen Nachweise, Registereinträge und Attribute, wie Berufsattribute oder Gesundheitskarte digitalisieren. Die QEAA sind selective-disclosure-fähig, können also einzeln und unabhängig voneinander weitergegeben werden. Außerdem können grundsätzlich auch nicht hoheitliche Nachweise als EAA von ausgebenden Stellen, wie Ärzten oder Krankenkassen, über die EUDI ausgegeben und gespeichert werden. Somit kann die EUDI als Austauschplattform für Attribute jeglicher Art in die TI hinein und aus der TI heraus genutzt werden. Mittels QEAA ist es außerdem möglich die eGK vollständig zu digitalisieren und hardwareunabhängig zu machen.

Auf Seite der Leistungserbringer bieten QEAA auch weitreichende Möglichkeiten. So lassen sich Berufsattribute und Organisationen mittels hoheitlicher Register (authentic sources) bestätigen. Hierdurch lassen sich sowohl der eHBA als auch der Praxis- und Institutionenausweis (SMC-B) innerhalb der EUDI samt allen Funktionalitäten in der Regel ohne die Hardwarekarten digital abbilden. Durch die Bereitstellungspflicht von

Schnittstellen zu den authentic sources, damit qualifizierte Vertrauensdienste die Attribute verifizieren können, vereinfachen sich zudem die Prozesse und die Antragsstellung für Leistungserbringer. Durch die Verbindung der Signaturfunktion der EUDIW lässt sich zudem die Signaturfunktion des eHBA vollständig abbilden und so die Fernsignatur in der TI, z.B. in der Anwendung bei e-Rezepten medienbruchfrei weiterentwickeln. Auch der Versicherte kann die Signaturfunktion seiner EUDI nutzen um damit einfach und medienbruchfrei Dokumente zu signieren. Auf diese Weise lassen sich die Praktikabilität der Signatur steigern und sich sämtlichen Dokumentenaustausch und alle Prozesse zwischen Versicherten, Leistungserbringer und Krankenversicherung digitalisieren.

Ausblick

Es kann davon ausgegangen werden, dass die Bereitstellung zentraler Attribute wie z.B. die Versicherungsnummer durch einen Kostenträger unabhängig von der Weiterentwicklung der TI 2.0 ein Bestandteil der ID-Infrastruktur in Deutschland und Europa sein wird und damit über eIDAS 2.0 Prinzipien unabhängig von der TI umgesetzt werden. Gleichzeitig sind die Anwendungsfälle in der Telematikinfrastruktur vielfältig und bedürfen in Zukunft einer flexiblen Gestaltung von Attributen und Sicherheitsmerkmalen. Daher ist davon auszugehen, dass die Weiterentwicklung digitaler Identitäten im deutschen Gesundheitsmarkt und damit auch die Migration der Föderation in dezentrale Identitäten in den kommenden Jahren parallel zur Etablierung von eIDAS 2.0 geschehen wird. So werden die IDP weiterhin bestehen bleiben und erst schrittweise durch die EUDI ergänzt werden. Es wird daher darauf ankommen, die Erkenntnisse aus der eIDAS 2.0 Entwicklung und insbesondere die Ergebnisse der LSP Projekte und somit auch des Architectural Reference Frameworks (ARF) mit in die Weiterentwicklung der TI 2.0 und damit auch in die standardisierte und europakonforme Gestaltung digitaler Identitäten im Gesundheitsmarkt einzubeziehen.

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

Franca Löwenstein, Bundesruckerei GmbH
Dominik Deimel, comuny GmbH

Ansprechpartner

Clemens Schlepner | Referent Vertrauensdienste & Digitale Identitäten
T 030 27576-424 | c.schlepner@bitkom.org

Verantwortliches Bitkom-Gremium

AK Digitale Identitäten

Copyright

Bitkom 2023

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität,

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.