Kartenungebundene digitale Identitäten des Gesundheitswesens (GesundheitsID)

Hier geht es um **kartenungebundene** digitale Identitäten. Bei den kartengebundenen digitalen Identitäten des deutschen Gesundheitswesens handelt es sich um die Smartcards des Gesundheitswesens.

Gesetzliche Rahmenbedingungen

Stellt die Einführung der al.vi mit der elektronischen Patientenakte (ePA) bereits den ersten Schritt hin zu kartenunabhängigen Identitäten für die Versicherten dar, so fordert das DVPMG die Einführung von schutzbedarfsgerechten kartenunabhängigen digitalen Identitäten für alle Personen und Organisationen, die als Akteure an der TI teilnehmen. Das KHPflEG hat die Termine nochmals nach hinten verschoben. So erhält die gematik über § 312 Abs. 1 S. 1 Nr. 8 SGB V den Auftrag, bis 1.4.2023 die erforderlichen Voraussetzungen zu schaffen, damit die jeweiligen Kartenherausgeber für Versicherte und Leistungserbringer digitale, kartenunabhängige Identitäten zur Verfügung stellen können. § 291 Abs. 8 SGB V verpflichtet die Krankenkassen ab 1.1.2024 für gesetzlich Versicherte, § 340 Abs. 6 SGB V die Herausgeber der Leistungserbringerkarten ab 1.1.2024 für Leistungserbringer solche digitalen Identitäten auszugeben.[1)] Medizinische Einrichtungen sollen gem. § 340 Abs. 7 SGB V zum 1.1.2025 eine kartenungebundene Institutionsidentität erhalten. Die digitale Versichertenidentität soll ab 1.1.2026 in gleicher Weise wie die eGK als Versicherungsnachweis dienen.[2)] Eine Abschaffung der eGK geht damit nicht einher, da die kartenunabhängige digitale Identität „ergänzend zur digitalen Identität, die mit der elektronischen Gesundheitskarte verbunden ist“[3)] Damit ist grds. gewährleistet, dass die relevanten Sicherheitsanforderungen auch für die Nutzung digitaler Identitäten für Anwendungen außerhalb der TI Berücksichtigung finden. Die konkrete Umsetzung eines Authentifizierungsmechanismus mittels kartenunabhängiger Identitäten ist nicht gesetzlich verankert. Eine digitale Identität kann explizit verschiedene Ausprägungen mit unterschiedlichem Sicherheits- und Vertrauensniveau haben, es muss jedoch das jeweilige für die Nutzung einer Anwendung benötigte Niveau erreicht werden, um Zugriff zu erhalten.[4)]

Synopsis

- Einführung im DVPMG, Terminverschiebungen im KHPflEG
- Spezifikationstermin für gematik: 1.4.2023
- Einführungstermin für
  - Versichertenidentitäten: 1.1.2024
  - Leistungserbringeridentitäten: 1.1.2024 (Korrektur im DigiG: 1.1.2025)
  - Identitäten für Leistungserbringerinstitutionen: 1.1.2025
- eGK als Versichertennachweis ab 1.1.2026

Grundsätzliche Konzeption

Die Bereitstellung kartenungebundener digitaler Identitäten im Gesundheitswesen erfolgt über den Ansatz eines föderierten Identitätsmanagements, eine wesentliche Säule der Telematikinfrastruktur (TI) 2.0.

Zu unterscheiden sind - auch gem. der gesetzlichen Vorgaben - somit:

- kartenungebundene digitale Identitäten für Versicherte
- kartenungebundene Identitäten für Leistungserbringende
- kartenungebundene Identitäten für Leistungserbringerinstitutionen.

Spezifikation

Finale Spezifikation für die (kartenlosen) digitalen Identitäten für Versicherte veröffentlicht die gematik am 10.02.2023.

Allerdings gab es kein Einvernehmen mit dem BfDI und BSI zum Thema **Biometrie** und **Single Sign On**[5], so dass ein Versicherter - je nach Smartphone-Klasse abhängig vom Secure Element - die Identität beim Login in regelmäßigen Abständen – von ‚alle 24 Stunden' bis ‚alle sechs Monate' – mit der Online-Ausweisfunktion oder der eGK mit PIN erneut bestätigen muss. Soviel zum Thema **kartenlose** Identität.[6]

Einzelne Spezifikationen

- Spezifikation Federation Master, V. 1.0.0, 06.02.2023
- Spezifikation Sektoraler Identity Provider, V. 2.0.1, 20.02.2023
- Spezifikation Signaturdienst, V. 1.5.0, 06.02.2023
- Spezifikation Identity Provider - Frontend V 1.4.0, 6.2.2023
- Spezifikation Identity Provider-Dienst V 1.4.0, 17.12.2021
- Spezifikation Identity Provider – Nutzungsspezifikation für Fachdienste V 1.5.0, 6.2.2023

Die obigen Spezifikationen stellen den Kern des Basis-Release für die GesundheitsID für Versicherte dar und haben den Stand des **IDP Maintenance_Release 22.2** (20.2.2023).

Anfang April (6.4.2023) ist ein **IDP Maintenance Release 23.1** veröffentlicht worden.

In den Spezifikationen werden Festlegungen ergänzt, die dem Nutzer die volle Kontrolle darüber geben, welche Authentisierungsverfahren für die Anmeldung an Anwendungen zulässig sind. Werden neben den geforderten Verfahren elektronischer Identitätsnachweis (A_22713) bzw. eGK+PIN (A_22712) verpflichtend weitere Authentifizierungsverfahren für einen Nutzer eingerichtet, so muss dem Nutzer die Möglichkeit gegeben werden, auszuwählen, welche Verfahren für die Authentisierung bei TI-Fachanwendungen verwendet werden dürfen.

Zudem ist ein weiteres **IDP Maintenance Release 23.2** in Abstimmung, das folgendes enthalten wird:

- Anforderungen an eine verbesserte Benutzerfreundlichkeit („**Komfortfeatures**“)
- Nutzung der GesundheitsID auch mit **niederschwelligeren Authentifizierungsverfahren** (§ 291 Abs. 8 S. 7 SGB V, angepasst durch KHPflEG)
- Das Featuredokument zur „Anbindung des eRezeptes an die Gesundheits-ID“ trifft notwendige Festlegungen, damit der zentrale IDP-Dienst auch innerhalb der Föderation als alleiniger Authorization-Server für den E-Rezept-Fachdienst agieren kann. Dieser wird in einem Parallelbetrieb bis zum Ende des Jahres 2023 sowohl diese Vorgehensweise sowie die bisherige Integration von sektoralen Identity Providern unterstützen. Dies macht zusätzlich minimale Anpassungen an E-Rezept Frontend des Versicherten sowie dem E-Rezept Fachdienst notwendig. Für die Identity Provider erfolgt die Anbindung entsprechend der bereits definierten Prozesse. **Falls die Komfortfeatures nicht umgesetzt werden, bedeutet dies aber auch einen Rückschritt in der Nutzerfreundlichkeit für das E-Rezept!**
- Zudem werden weitere Verfahren definiert zur Identifizierung (Apotheken-Ident) und eine Liste der zulässigen Verfahren veröffentlicht.

Aufgrund fehlender Einigung mit dem BfDI/BSI ist zunächst ein abgespecktes **IDP Maintenance Release 23.3** abgestimmt und veröffentlicht worden.

IDP Maintenance Release 23.4 ist seit September veröffentlicht. Das Release beinhaltet die notwendigen Änderungen für die Nutzung der GesundheitsID für das E-Rezept in der TI-Föderation. Die Umstellungen betreffen den operativen Betrieb des IDP-Dienstes als Authorization-Server für das E-Rezept sowie die zusätzliche Information in der Liste der registrierten sektorale IDP, ob es sich um einen sektoralen IDP einer gesetzlichen oder privaten Krankenkasse handelt.

Für gesetzlich Versicherte

- Im Frühjahr 2022 hat die BARMER den Auftrag an T-Systems und Verimi vergeben.[7)]

Für Privatversicherte

- PKV plant Einführung digitaler Identitäten zu Mitte 2023. Beauftragung von RISE und IBM. Abstimmung mit BfDI und BSI erfolgt[8)]

Strittige Komfort-/Akzeptanzfeatures

- Single Sign On (SSO)
- Biometrische Authentifizierung

- langfristige Gerätebindung

Mit dem DigiG wird nun die Grundlage für eine Einwilligung der Versicherten in niederschwelligere Authentifizierungsverfahren geschaffen, sodass diese Features sich aktuell in Vorbereitung für eine Spezifikation befinden.

Materialien

- BSI TR-03166 Technical Guideline for Biometric Authentication Components in Devices for Authentication

GesundheitsID und DiGAs

Gem. § 6a Abs. 1 der Digitale Gesundheitsanwendungen-Verordnung (DiGAV) sind DiGAs ab 1.1.2024 gesetzlich verpflichtet eine Möglichkeit anzubieten Daten der DiGAs in die ePA zu übernehmen. Das bedeutet, Sie müssen faktisch eine Anmeldung über die ePA-Apps der Krankenkassen mittels GesundheitsID anbieten. Ziel ist es , über diesen Weg dann Daten aus den DiGAs auf Wunsch der Versicherten in die EAP einstellen zu können. Das BfArM hat eine Übergangsfrist bis zum 30.04.2024 festgelegt, bis zu deren Ablauf DiGA-Hersteller eine erfolgreiche Implementierung durch Vorlage eines Bestätigungsbescheids der gematik nachweisen müssen. Das **Bestätigungsverfahren** der gematik soll zeitnah veröffentlicht werden. Ein entsprechender TI-Leitfaden für DiGA-Hersteller ist bereits veröffentlicht.

European Digital Identity Wallet (EUDI-Wallet)

Die EUDI-Wallet ist eine persönliche, digitale Brieftasche, mit der sich zukünftig EU-Bürger*innen (und Organisationen) digital ausweisen können. Sie ist in der Lage die zugehörigen Identitätsdaten und amtliche Dokumente darin zu speichern.[9)]

Die Notwendigkeit der Bereitstellung und gegenseitigen Anerkennung einer solchen Wallet bis Mitte 2027 durch und zwischen den europäischen Mitgliedstaaten ergibt sich aus der Revision der eIDAS-Verordnung (eIDAS 2.0), die voraussichtlich im April 2024 in Kraft treten wird, nachdem der Europäische Rat ihr im Februar 2024 zugestimmt hat.

Die genaue Umsetzung der eIDAS2.0-VO und damit der EUDI-Wallet in Deutschland ist noch offen.[10)]. Mit nationalen Durchführungsrechtsakten wird zu Mitte 2025 gerechnet.

Die technischen und europäisch verbindlichen Vorgaben werden im European Digital Identity Framework veröffentlicht:

- Outline: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline
- Spezifikation: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

Die eingesetzte Technologie im Rahmen der EUDI-Wallet ist OpenID for Verifiable Credentials (OpenID4VCI), während im Rahmen der GesundheitsID OpenID Connect (OICD) zum Einsatz kommt.

Im Rahmen des GovLabDE arbeiten gematik und BMG an der Ausgestaltung der nationalen Interpretation der EU-Vorgaben

Weitere Infos

- IDP-Wissensdatenbank der gematik

Umsetzungen

IdP-Dienstbetreiber

- RISE
- IBM
- T-Systems mit verimi

- Techniker bringt Gesundheits-ID-App raus, Wallet ist geplant[11)]

1)
Es ist davon auszugehen, dass eine Terminanpassung auf den 1.1.2025 - in Analogie zur Anpassung für die Institutionenidentitäten in § 340 Abs. 7 - im Gesetzgebungsverfahren für das KHPflEG übersehen wurde und mit dem nächsten Digitalisierungsgesetz angepasst wird.
2)
§ 291 Abs. 8 S. 2 SGB V.
3)
BT-Drs. 19/27652, 113).) ausgegeben wird. Zudem erlaubt § 336 Abs. 5 SGB V zwar den Zugriff auf Anwendungen nach § 334 Abs. 1 S 2 Nr. 1, 4, 6 und 7 SGB V, auf die der Versicherte bisher nur „mittels“ der eGK zugreifen konnte, auch über die kartenunabhängigen digitalen Identitäten, bindet diesen aber gleichzeitig an die vorherige sichere Ausgabe der eGK (→ Rn. 77). Die Festlegung der Sicherheitsanforderungen für die digitalen Identitäten muss dabei im Einvernehmen mit dem BSI auf Basis der einschlägigen, gültigen technischen Richtlinien des BSI erfolgen und das notwendige Vertrauensniveau der unterstützten Anwendungen berücksichtigen.((§ 291 Abs. 8 S. 3 u. 4 bzw. § 340 Abs. 8 S. 2 SGB V.
4)
§ 291 Abs. 8 S. 5 u. 6 bzw. § 340 Abs. 8 S. 4 SGB V.
5)
s. gemSpec_IDP_SeK_V2.0.0, S. 21f.
6)
Der c't-Artikel „Mit PIN oder ohne?“ fasst das ganz plastisch zusammen.
7)
s. https://www.pharmazeutische-zeitung.de/barmer-verschiebt-gesundheitskarte-in-die-virtuelle-welt-134037/
8)
vgl. https://www.heise.de/news/eID-Private-Krankenkassen-planen-Umsetzung-digitaler-Identitaeten-Mitte-2023-7443358.html.
9)

https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2023/11/digitale-brieftasche.html.
10)

Zum aktuellen Stand zu eIDAS2.0 in D vgl. https://dserver.bundestag.de/btd/20/082/2008201.pdf.
11)

https://www.heise.de/news/E-Patientenakte-E-Rezept-und-weitere-Techniker-bringt-Gesundheits-ID-App-raus-9534068.html.