eGK AUF DEM PRÜFSTAND: DIE ZUKUNFT GEHÖRT DIGITALEN IDENTITÄTEN

Ein Beitrag von Christian Hälker, Michael Hartmann und Dominik Deimel

Sonderdruck aus
E-HEALTH-COM 06/2021

eGK AUF DEM PRÜFSTAND: DIE ZUKUNFT GEHÖRT DIGITALEN IDENTITÄTEN

„Ohne eGK in die TI“: Mit dieser Herausforderung startete Ende 2020 der Verband der Privaten Krankenversicherung (PKV-Verband) ein Innovationsprojekt zu digitalen Identitäten. Es findet mittlerweile große Aufmerksamkeit und könnte die Zukunft der deutschen Telematikinfrastruktur entscheidend mitprägen.

TEXT: CHRISTIAN HÄLKER, MICHAEL HARTMANN, DOMINIK DEIMEL

Mit der Entscheidung der PKV-Branche, sich wieder in der gematik einzubringen und den Privatversicherten den Zugang zu Diensten in der Telematikinfrastruktur (TI) wie zum Beispiel dem E-Rezept oder der elektronischen Patientenakte (ePA) zu ermöglichen, stellte sich für die PKVen schnell die Frage nach dem Bedarf, die elektronische Gesundheitskarte (eGK) auszurollen oder direkt auf digitale Identitäten zu setzen – aufbauend auf der Verpflichtung des Gesetzgebers, ab dem 01.01.2023 den Versicherten digitale Identitäten bereitzustellen.

In einer Marktrecherche im zweiten Halbjahr 2020 hat sich der PKV-Verband mit unterschiedlichen Ansätzen bei der Realisierung digitaler Identitäten in der Branche beschäftigt und sich für eine Innovationspartnerschaft mit den Firmen msg systems ag und comuny entschieden. >

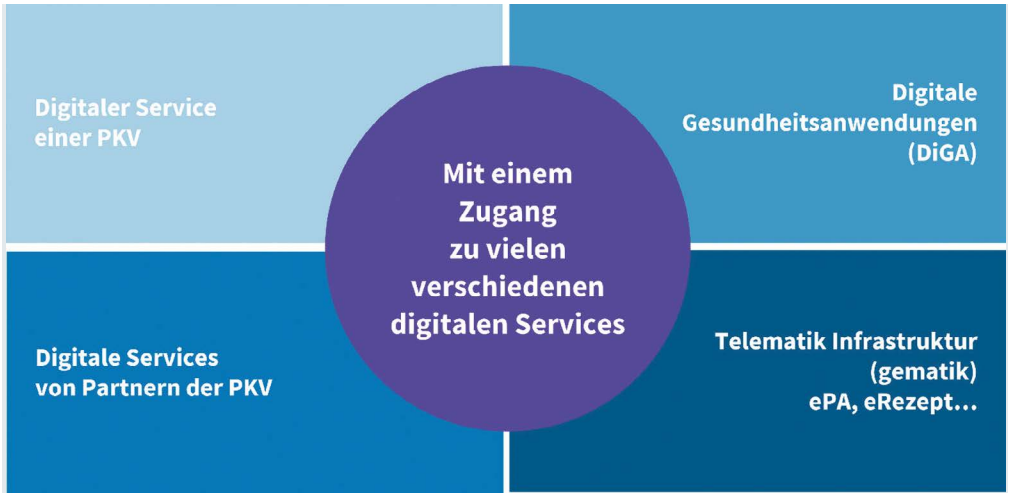

Abb. 1: PKV Zielbild digitale Identitäten

Seit Februar 2021 arbeiten diese beiden Unternehmen zusammen mit den privaten Krankenversicherungen Allianz, Debeka, Signal Iduna und mit Beteiligung der gematik unter der Koordination des PKV-Verbands an der technischen Realisierung der Lösung zum Zugang zur TI ohne eGK. Im August hat sich diesem Projekt auch die BARMER als erste gesetzliche Krankenversicherung angeschlossen und im September dann die ERGO/DKV als weitere PKV, um den Einsatz des Lösungsansatzes für ihre Versicherten zu eruieren.

Nach einer intensiven gemeinsamen Konzeptionsphase wurde auf Basis einer Demo-App und einer hierfür aufgebauten technischen Infrastruktur der Zugang zu beispielhaften Anwendungen (E-Rezept und ePA) ohne eGK realisiert. Konzept und technische Umsetzung wurden anschließend von der gematik sowie einem hinzugezogenen, akkreditierten Sicherheitsgutachter bewertet. Aufgrund des Innovationscharakters wurde auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie der Bundesbeauftragte für den Datenschutz und Informationsfreiheit (BfDI) hinzugezogen. Ergebnisse aus diesem Projekt können nun vorgestellt werden. Sie kommen gerade zur richtigen Zeit, denn in den kommenden sechs Monaten werden alle Krankenkassen und Krankenversicherungen vor der Entscheidung stehen, eine Identitätslösung für ihre Versicherten auszuwählen und aufzubauen.

ANSPRUCH DER PKV AN DIGITALE IDENTITÄTEN

Nach dem Motto „mit einem Zugang zu vielen digitalen Lösungen in der TI" startete die gematik die Konzeption eines föderierten Identitätsmanagements. Jeder Versicherer stellt zukünftig einen Identitätsprovider bereit, lässt diesen hierfür bei der gematik zu und betreibt ihn anschließend entkoppelt von eigenen Fachanwendungen wie zum Beispiel der ePA. Dafür setzt die gematik mit Vorgabe des OIDC-Standards auf die Konzepte der OpenID Foundation, um die Interoperabilität zwischen nutzenden Diensten und den unterschiedlichen Identitätsprovidern zu gewährleisten. Für die notwendige IT-Sicherheit wird ein eIDAS-Vertrauensniveau „hoch" angestrebt. Darüber hinaus soll aus Sicht des Datenschutzes sichergestellt werden, dass eine Krankenversicherung keine Profilbildung über die Nutzung digitaler Dienste bei ihren Versicherten durchführen kann. Zukünftig können diese Identitätsprovider von Fachanwendungen in der TI sowie von weiteren Diensten bzw. Anwendungen wie zum Beispiel digitalen Gesundheitsanwendungen (DiGA) verwendet werden.

Im Juni 2021 – also mitten im Projekt – gab die EU bekannt, dass sie mit der Novellierung der eIDAS-Verordnung (eIDAS 2.0) als europäischer Rechtsrahmen für digitale Vertrauensdienste und damit auch für digitale Identitäten alle Staaten verpflichten möchte, bis 2024 ihren Bürger:innen eine sichere Verwahrung digitaler Identitätsmerkmale wie die des Personalausweises oder auch der Versichertennummer auf dem Mobilgerät zu ermöglichen. Die Ausstellung digitaler Identitäten auf das Mobilgerät und die Nutzung dieser dezentral gespeicherten Informationen in vielen verschiedenen Anwendungsfällen sollten es Bürger:innen erlauben, selbstbestimmt und souverän mit den persönlichen Identitätsdaten zu agieren. Ein Anspruch, der sich auch über den Begriff Self Sovereign Identity, verkürzt SSI, beschreiben lässt.

Diese gesetzlichen Vorgaben und regulatorischen Rahmenbedingungen stehen parallel zum Wunsch der privaten Krankenversicherer, Prozesse und Services immer weiter zu digitalisieren und somit über ihre zukünftige Identitätslösung einen Zugangspunkt auf ihre eigenen Dienste und auf Anwendungen von Partnern aufzubauen (Abb. 1). Die PKV setzt dabei stark auf die Nutzung des Mobilgeräts, denn immer mehr Versicherte nutzen dieses alltäglich in ihren unterschiedlichen Lebensbereichen. Komfort und Einfachheit in der Anwendung werden über das Gerät ermöglicht und müssen auch bei der Anwendung hochsicherer Identitätslösungen im Vordergrund stehen, denn sonst werden sie vom Versicherten nicht angenommen.

IDENTITÄTEN AUF DEM MOBILGERÄT KOMFORTABEL ERZEUGEN UND NUTZEN

Der Anspruch an Datensouveränität des Versicherten und Komfort wird im Innovationsansatz der PKV erreicht, indem zentrale Funktionen eines Identitätsproviders vom Rechen-

zentrum bzw. der Cloud in die App auf dem Mobilgerät verlagert werden. Die Speicherung von Personendaten und Passwörtern in einem „Wallet“ und eine unverschlüsselte Datenverarbeitung ausschließlich innerhalb der App stellen keinen Widerspruch zum in Konzeption befindlichen Zielbild der gematik dar und bereiten die Unternehmen auf die Regelungen der neuen eIDAS-2.0-Verordnung vor (Abb. 2).

Mit dem White-Label-Ansatz werden die Funktionalitäten für die Authentifizierung des Versicherten und damit des Identitätsproviders über ein Software Development Kit (SDK) so bereitgestellt, dass eine Versicherung ihre eigene App und somit auch ihren eigenen Nutzerflow und Frontend für den Versicherten selbst bauen kann (Abb. 3). Die PKV setzt dabei auf eine Ein-App-Strategie, das heißt, alle Funktionen werden über das SDK in die heute schon vorhandenen Apps der Versicherer integriert. Das schafft die Voraussetzungen, dass der Versicherte für die Prozesse – zum Beispiel die digitale Verifizierung seiner Person über den Personalausweis – nicht in andere Apps wechseln muss. Ein Bespiel dafür ist das eID-Verfahren, bei dem der Versicherte seine Personendaten über den neuen Personalausweis über die Nutzung seiner PINs und der NFC Schnittstelle des Mobilgerätes verifiziert. Diese Funktion wird einfach in die Oberfläche der Versicherer-App eingebaut, ohne dass der Versicherte einen Medienbruch verspürt. Im Projekt wurden die Funktionen der AUTHADA GmbH und IDnow GmbH in die Demo-App hierfür integriert (Funktionen der Demo-App werden in einem YouTube-Video vorgestellt: https://youtu.be/NoZLakzeBCw).

Ähnlich verhält es sich mit der Krankenversichertennummer (KV-Nummer) als Nachweis für den Versichertenstatus, die den Status eines wichtigen Attributs für den Zugang zu TI-Anwendungen darstellt. Die Krankenversicherung als Aussteller dieser Daten agiert dabei nach den Prinzipien von SSI als sogenannter Issuer. Die Daten werden vor der Weitergabe auf das Mobilgerät von der Versicherung signiert und mit einem Gültigkeitsdatum versehen. Diese Informationen können im Login-Prozess auf dem Mobilgerät zur Erstellung des ID-Tokens verwendet und später dann auch vom Dienst geprüft werden. Die Lösung nutzt dabei heute noch eine zentrale Public Key Infrastruktur (PKI). Zukünftig können auch die im Aufbau befindlichen, dezentralen PKI-Strukturen, wie sie dann über Distributed Ledger Technology (DLT) bereitstehen, durch den Lösungsansatz unterstützt werden.

App-Sicherheit, Umsetzung der 2-Faktor-Authentifizierung ohne zentrale Passwortspeicherung und Absicherung des Wallet werden über eine mobile Komponente der Build38 GmbH, ein Spin Off der Giesecke + Devrient, erreicht. In Kombination mit einem Cloud-Dienst der Build38 ist in Prüfung, ob hierdurch das eIDAS-Vertrauensniveau „hoch“ erreicht werden kann, ohne dass Software im eigenen Rechenzentrum betrieben werden müsste.

Für die Weitergabe der auf dem Mobilgerät erzeugten und gespeicherten Daten an Dienste nach dem OIDC-Standard nach gematik-Vorgabe braucht es heute noch ein Backend, welches von Versicherungen selbst oder ihren Dienstleistern betrieben wird. Im Unterschied zu aktuellen Identitätsprovider-Lösungen werden in diesem Backend keine Daten gespeichert oder unverschlüsselt verarbeitet. Das Backend dient lediglich dazu, die Kommunikation zwischen Fachanwendung und App auf dem Mobilgerät aufzubauen und verschlüsselte ID- >

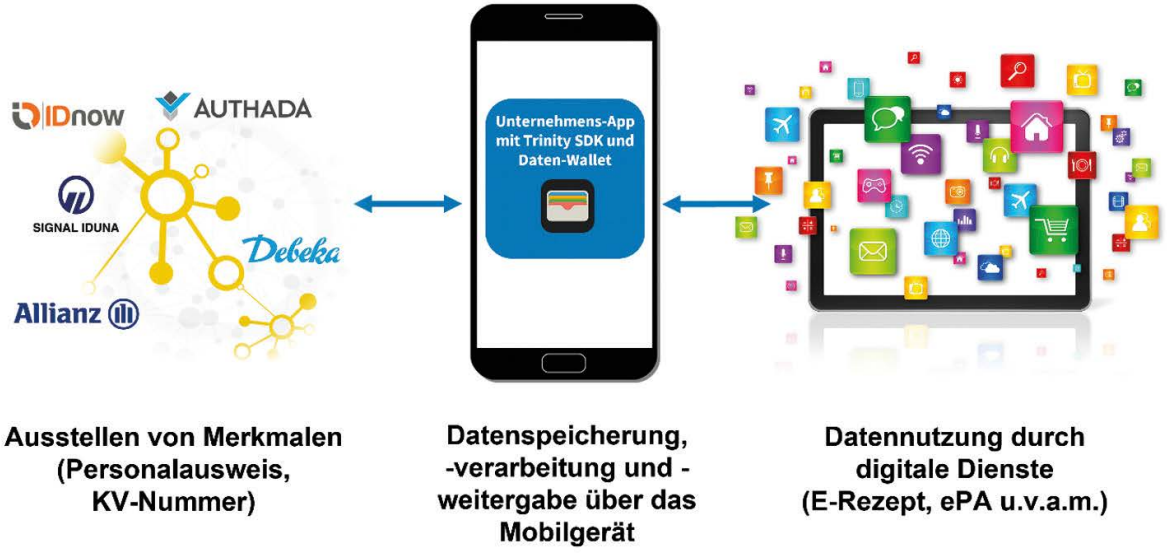

Abb. 2: PKV Lösungsansatz – mobil, standardisiert, zukunftsfähig

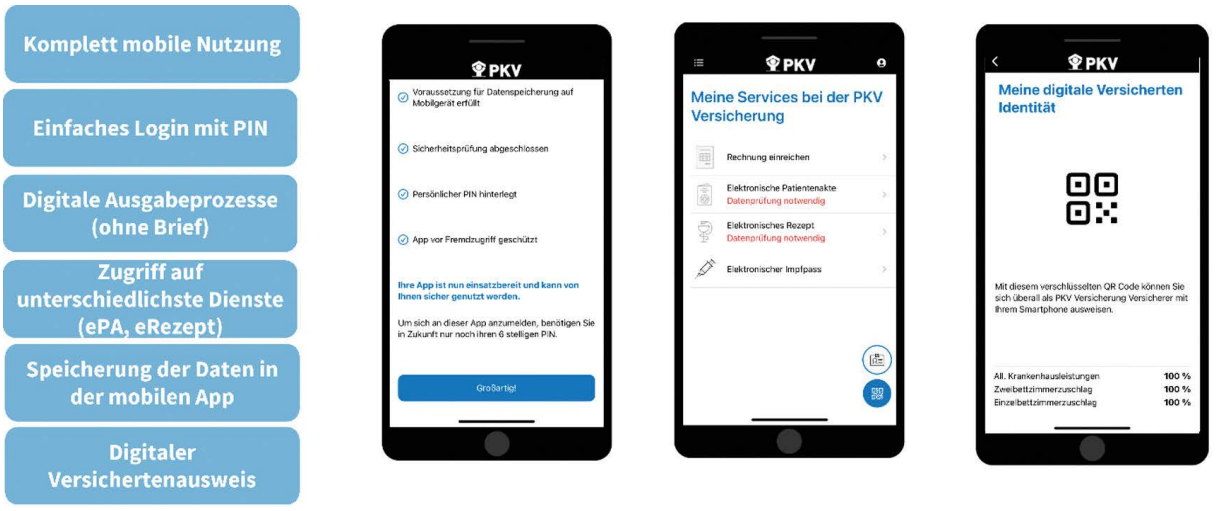

Abb. 3: Prozesse in der Demo-App – Komfortable Perspektive für Krankenversicherte (PKV und GKV)

Daten an die Fachanwendung weiterzugeben. Damit hat die Versicherung keinen Zugriff auf die Versichertendaten und erfüllt automatisch die Forderung des Datenschutzes nach Verhinderung von Profilbildungen.

PROJEKTERKENNTNISSE UND KONSEQUENZEN FÜR VERSICHERER

Das Innovationsprojekt konnte aufzeigen, dass die Einführung von physischen eGK-Diensten wie E-Rezept und ePA für private Krankenversicherer nicht zwangsläufig notwendig sein wird. PKVen können auf dieser Basis selbst entscheiden, ob sie trotzdem einen Rollout der eGK für ihre Versicherten vorsehen. Der vom PKV-Verband favorisierte Lösungsansatz mit seiner Perspektive hin zu eIDAS 2.0 und SSI erfordert allerdings ein starkes Umdenken bei den Versicherern, denn persönliche Informationen, wie Personalausweisdaten oder zukünftig auch andere Attribute, liegen nun in der Datenhoheit des Versicherten. Gleichzeitig gibt es die Chance, dass Versicherungen das Teilen von Daten über das Mobilgerät nicht nur einfacher für ihre Kund:innen gestalten, sondern auch eine Vertrauensstellung mit dem Versicherten aufbauen, um zukünftig mehr persönliche Daten von ihm freiwillig über diesen Weg zu erhalten.

Mit dem gewählten technischen Design lassen sich die Anforderungen an die eIDAS-2.0-Verordnung (s. o.) grundsätzlich heute schon realisieren, auch wenn Anpassungen aufgrund der finalen Veröffentlichung der zugrunde liegenden Standards, z.B. für das Wallet oder die Ausstellung von Signaturen, notwendig sein können. Das schützt die Unternehmen davor, bereits zwölf Monate nach Einführung alternativer Technologieansätze eine komplette Migration, verbunden mit einer neuen Investition, durchführen zu müssen. Die Umsetzung über eine White-Label-Lösung, die viel Flexibilität bei der individuellen Gestaltung des Frontends des Versicherten zulässt, ist sehr positiv bei den Versicherungen aufgenommen worden, die am Ende auch über einen spartenübergreifenden Einsatz der Lösung nachdenken.

Mit der Demo-App und der Ende-zu-Ende-Realisierung der technischen Prozesse konnte die Umsetzung eines sehr komfortablen und einfachen Nutzerflows aufgezeigt werden, insbesondere wenn es darum geht, alle Prozesse in einer Versicherer-App abzubilden und diese ohne Medienbruch zu bedienen. Die Projektteilnehmer:innen gehen davon aus, dass auch gerade die Bereitstellung persönlicher Daten über die mobile App und somit in der Hand des Nutzers das Vertrauen beim Umgang mit digitalen Anwendungen bei den Versicherten erhöht.

In der Diskussion mit der gematik werden aber auch die Herausforderungen für einen solchen Innovationsansatz deutlich, da die Gesamtlösung komponentenbasiert und nicht monolithisch aufgebaut ist. Die Trennung von mobilem SDK und Backend, die Einbeziehung von Cloud-Diensten und Sicherheitsfeatures, die außerhalb der TI platziert sind, das alles ist neu in der Betrachtung der gematik. Gleichzeitig orientiert sich dieser Ansatz schon an der Neuausrichtung hin zur TI 2.0 und bedarf daher auch neuer Formen der Begutachtung und Zulassung.

Die mit der TI 2.0 geplante Einführung von international anerkannten Sicherheitsniveaus wie z. B. das eIDAS-Vertrauensniveau „hoch“, stellt alle Akteure vor große Herausforderungen, insbesondere wenn es um die Nutzung des Mobilgeräts als Authentisierungsmittel geht. Das notwendige Schlüsselmanagement bzw. auch die Speicherung von personenbezogenen Daten auf dem Mobilgerät sind durch die noch fehlende Zertifizierung von Hardware-Komponenten (Secure Elements) auf den Geräten unterschiedlicher Mobilgeräte-Hersteller durch das BSI, wie bisher nur im Rahmen des OPTIMOS-Projekts erfolgt, aktuell in der Diskussion. Eines der Ziele des PKV-Verbands ist es, mit dem hier vorgestellten Ansatz und technischen Maßnahmen zur Erhöhung der IT-Sicherheit auf dem Mobilgerät das BSI vom Einsatz bei weiteren Smartphones mit heute noch nicht zertifizierten Se-

cure Elements zu überzeugen, um in einer Übergangsphase bis zur Zertifizierung weiterer Geräte bereits 2022 eine 90-prozentige Abdeckung bei den Mobilgeräten der Versicherten zu erreichen.

INNOVATION WEITERTREIBEN UND IMMER MEHR DAVON BEGEISTERN

Die Ende September abgeschlossene Konzeptions- und technische Umsetzungsphase konnte allen Beteiligten die Machbarkeit und die Vorteile eines IDP-Lösungsansatzes mit Datenhaltung und Prozesssteuerung auf dem Mobilgerät aufzeigen. Die Zeit bis zur Veröffentlichung der Zulassungsvoraussetzungen durch die gematik bis spätestens 01. April 2022 und die sich daran anschließende Zulassung von Identitätsprovider-Lösungen auf Basis des vorgestellten dezentralen Technologieansatzes gilt es nun zu nutzen, um die oben beschriebenen Herausforderungen zu lösen. Hierzu werden nun die Voraussetzungen geschaffen, über technische „Proof of Concept"-Projekte bei ausgewählten Versicherern weitere Erfahrungen im Einsatz der Technologie und deren Integration in die Bestandssysteme zu sammeln. Dies geschieht mit dem Bewusstsein, dass bisher seitens gematik, Sicherheitsgutachtern und weiteren relevanten Stakeholdern noch keine Show-Stopper aufgedeckt wurden. Das starke Umdenken der gematik mit einer hohen Dialogbereitschaft, auch innovative Lösungen mitzugestalten, fördert die Etablierung zukunftsfähiger Lösungen am Markt. Die PKV-Branche sieht sich hierbei in der Rolle des Innovationstreibers, der die Voraussetzungen und die Rahmenbedingungen für das Entstehen von Innovationen fördert.

Das laufende Innovationsprojekt steht für Transparenz und Offenheit und lädt alle Akteure ein, sich aktiv zu beteiligen. So wurde der Innovationsansatz z. B. auch in einer Arbeitsgruppe des GKV-Spitzenverbandes und Vertreter:innen der Bundesärztekammer sowie dem Verband Sichere Digitale Identität vorgestellt. Aus dem Projekt soll eine Bewegung für dezentrale Lösungsansätze und selbstbestimmtes Datenmanagement entstehen, der sich Versicherungen, Kostenträger der Beihilfe, Leistungserbringer, Industriepartner, gematik und Politik anschließen. Denn nur, wenn wir aktiv an der Telematikinfrastruktur 2.0 mitarbeiten, können wir sie auch zukunftsfähig und nach unseren Vorstellungen – insbesondere der Versicherten – gestalten und eine Vorreiterrolle auch in Europa einnehmen. ■

■ **CHRISTIAN HÄLKER**
Geschäftsführer
Verband der Privaten Krankenversicherung
Kontakt: christian.haelker@pkv.de

■ **MICHAEL HARTMANN**
Lead Business Consultant
Geschäftsbereich Healthcare
msg systems ag
Kontakt: michael.hartmann@msg.group

■ **DOMINIK DEIMEL**
CEO, Gründer
comuny GmbH
Kontakt: dominik.deimel@comuny.de