FOCUS Magazin

FOCUS Magazin | Nr. 11 (2022)

Identität im Digitalen

Das digitale Ich in einer Hand

FOCUS-Autor Christoph Henn

Freitag, 18.03.2022, 10:43

Mithilfe digitaler Identitäten könnten Bürger:innen bald per Smartphone nachweisen, wer sie sind – aber auch, welchen Bildungsabschluss, Beruf, Grundbesitz oder Ehestand sie haben. Die neuen Möglichkeiten sollen den Alltag erleichtern und den Schutz der eigenen Identitätsmerkmale stärken

Wenn Jürgen Anke, Professor für Softwaretechnologie und Informationssysteme an der HTW **Dresden**, der Kita seines Sohnes etwas mitteilen möchte, ist das manchmal ein aufwendiger Prozess. Sollen andere Eltern den Kleinen direkt von der Kita zu einer **Geburtstagsfeier** mitnehmen, benötigen sie eine Abholberechtigung. »Diese Information ist wichtig, und die Kita muss sich darauf verlassen können, dass sie zweifelsfrei von mir stammt«, so Jürgen Anke. Streng genommen muss der Vaterdafür ein Formular ausfüllen, es unterschreiben und eindeutig nachweisen, dass die Mitteilung tatsächlich von ihm oder seiner Frau kommt. Ähnlich ist es bei vielen anderen typischen Einzelregelungen in Kitas, die sensible Themen betreffen, etwa bei Informationen zu Lebensmittelallergien.

Wenn es nach dem Dresdner geht, laufen solche Kita-Prozesse bald komplett digital ab, denn eines von Jürgen Ankes Spezialgebieten sind digitale Identitäten. »Viele verbinden mit Identität vor allem Name, Geburtsdatum, Wohnort«, sagt er, »aber zur Identität jeder und jedes Einzelnen gehören viel mehr Merkmale, als im Personalausweis stehen.«

Mit vielen anderen arbeitet der Wissenschaftler daran, dass künftig digitale Nachweise all jene Facetten einer Identität belegen, für die bislang zahllose Ausweise und Zertifikate aus Papier oder Plastik existieren: Schülerausweise, Hochschulzeugnisse, Schwerbehindertenausweise, Stadtpässe für sozial Benachteiligte, Grundbuchauszüge für Immobilienbesitzer:innen, Trauscheine für Verheiratete und so weiter.

Um zu erforschen, wie sich Identitätsmerkmale im Alltag nachweisen lassen, wurde in Sachsen »ID-Ideal« ins Leben gerufen. Dabei testen Wissenschaft, Behörden und Unternehmen gemeinsam, wie digitale Identitäten in unterschiedlichsten Lebensbereichen genutzt werden können. Das Kita-Szenario, bei dem Eltern rechtsverbindliche Meldungen übermitteln können, ist nur einer von mehreren Anwendungsfällen. Ein anderes Szenario dreht sich um Mobilität: »Wir wollen erreichen, dass sich in Dresden und Leipzig mit einem digitalen Fahrausweis alle Verkehrsmittel nutzen lassen, von Bussen und Bahnen bis hin zu Leihrädern, E-Scootern und Car-Sharing«, sagt Anke.

Nur die nötigsten Merkmale übertragen

Damit das funktioniert, will ID-Ideal alle notwendigen Nachweise wie persönliche Daten, Zahlungsinformationen, Ermäßigungsberechtigungen, bestehende Monatskarten und Fahrerlaubnisse in einer digitalen Wallet (deutsch: Brieftasche) speichern. Dort entsteht eine sogenannte selbstbestimmte Identität (Self-Sovereign Identity, kurz: SSI), über deren Verwaltung und Weitergabe die Person dahinter selbst entscheidet. Und im Gegensatz zu klassischen Ausweisen können datensparsam nur die relevanten Informationen übermittelt werden. Anstatt wie bisher beispielsweise einen kompletten **Führerschein** samt Foto, Geburtsdatum und allen erlaubten Fahrzeugklassen vorzulegen, lässt sich mit einer digitalen Identifizierung lediglich der Aspekt »Fahrerlaubnis für das gewünschte Auto« nachweisen – alle anderen Führerscheindaten bleiben dem Mobilitätsdienstleister verborgen.

ID-Ideal ist Teil einer größeren Initiative, mit der die Bundesregierung seit einiger Zeit digitale Identitäten voranbringen möchte. Im September 2021 trat das Smart-eID-Gesetz in Kraft. Es legt die Grundlage dafür, dass der

elektronische Personalausweis in einer Smartphone-Wallet gespeichert werden kann, sicher und binnen drei Minuten. Die Smart-eID soll 2022 für immer mehr Smartphones verfügbar werden, die die strengen Sicherheitsanforderungen erfüllen; für den geplanten Startschuss im Winter war nur ein Endgerät mit speziellem Chip vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert. »Das Smart-eID-Gesetz ist ein Quantensprung für Geschäftsmodelle im Internet und digitale Kommunikation mit der Verwaltung«, sagte der für die Einführung zuständige Bundes-CIO und Staatssekretär Markus Richter mit Blick auf die Erleichterungen, die die neue Technologie bringen soll. Zwar existiert bereits seit 2010 eine Online-Ausweisfunktion, doch ist sie bisher den meisten Menschen zu umständlich: Nur sechs Prozent der Deutschen nutzen das Verfahren, für das neben dem Ausweis eine PIN, eine Software auf dem Computer und ein Lesegerät oder NFC-fähiges Smartphone nötig sind.

» Zur Identität gehören viel mehr Merkmale, als im Personalausweis stehen «Jürgen Anke, Professor für Softwaretechnologie und Informationssysteme an der HTW Dresden

Im Gegensatz dazu soll die Smart-eID die Identifizierung gegenüber Behörden und Unternehmen einfacher machen; und die Anwendungsfälle zur Nutzung digitaler Identitäten sollen massiv anwachsen. Der Online-Personalausweis im Smartphone ist eng verbunden mit dem vom Bundeswirtschaftsministerium initiierten Innovationswettbewerb Schaufenster Sichere Digitale Identitäten. »Kommunen und Wirtschaftsunternehmen werden dabei unterstützt, digitale Identitäten in ihre Services zu integrieren«, erklärt Fabienne Eigner, die für den Wettbewerb verantwortliche Wissenschaftliche Referentin. »Im Mittelpunkt stehen aber die Bürgerinnen und Bürger, die in den Modellregionen sichere digitale Identitäten made in Germany erleben können.« ID-Ideal in Sachsen ist eines von vier ausgewählten Projekten; weitere laufen bis 2024 in **Köln**/**Berlin** (IDunion), Hessen/Bayern/Nordrhein-Westfalen (ONCE) sowie in Karlsruhe und der Metropolregion Rhein-Neckar (SDIKA).

»Insgesamt erproben wir 108 Anwendungsfälle«, erklärt Martin Schallbruch, Direktor des Digital Society Institute an der ESMT Berlin, der die Begleitforschung zum Innovationswettbewerb leitet. Digitale Identitäten beziehen sich dabei nicht zwangsläufig auf Menschen; sie können auch als rechtssichere Nachweise für Unternehmen oder Dinge – beispielsweise Verleih-Geräte – dienen. »Diese Identitäten sind der Schlüssel für alle digitalen Prozesse«, betont Schallbruch und zitiert eine Civey-Studie aus dem Jahr 2021, nach der ein Viertel der Deutschen 20 bis 100 digitale Identitäten nutzen – meist verteilt auf viele verschiedene Dienstleister und oft ineffizient und unsicher verwaltet: Nur jeweils 20 Prozent der Befragten verwenden einen Passwortmanager oder speichern ihre Passwörter im Browser.

Schaufenster Sichere Digitale Identitäten arbeitet daran, ein eID-Ökosystem zu schaffen, in dem einmal erfasste Identitätsnachweise für Anwendungsfälle aller Art nutzbar sind. »Eine wichtige Herausforderung ist es, diese Interoperabilität auch über Deutschland hinaus zu gewährleisten«, sagt Schallbruch und verweist auf Bestrebungen der EU-Kommission, eine einheitliche **europäische** digitale Identität einzuführen. Ebenso wichtig sind Datenschutz und Sicherheit, damit digitale Identitäten überhaupt das nötige Vertrauen genießen. »Die Echtheit eines Identitätsnachweises wird mit digitalen Signaturen der ausstellenden Instanz bestätigt«, erklärt dazu Professor Anke von der HTW Dresden. »Sie werden außerdem in einem geschützten Bereich auf dem jeweiligen Smartphone gespeichert und verschlüsselt zwischen der Wallet des Nutzers und den Systemen der Dienstleister übertragen.«

Dokumente aus Papier und Plastik können ersetzt werden

Auf dezentrale Speicherung digitaler Identitäten setzen auch die Entwicklerinnen und Entwickler von Helix ID aus Frankfurt. »Unsere Smart-Wallet-App bündelt persönliche Informationen sicher und dezentral, macht umständliches Anmelden auf verschiedenen Seiten überflüssig und sorgt gleichzeitig dafür, dass die Nutzerinnen und Nutzer die Hoheit über ihre Daten behalten«, erklärt Gründer Oliver Naegele. Wer relevante Nachweise verifiziert und hinterlegt hat, kann sich damit bei verschiedenen Partnern

identifizieren, mit denen das Start-up zusammenarbeitet. Zudem ist Helix ID Initiator einer Frankfurter Smart-City-Initiative, die es Einheimischen und Gästen ermöglichen soll, mit einer einzigen App etliche digitale Angebote und Dienstleistungen in der Stadt zu nutzen.

Ob in Unternehmen, Politik oder Wissenschaft: Die Zuversicht, dass digitale Identitäten Dokumente aus Papier und Plastik nach und nach ersetzen, scheint groß. »Ich denke, dass digitale Identitäten in drei bis fünf Jahren Teil unseres Alltags sind«, sagt Professor Anke. Der entscheidende Erfolgsfaktor für ihn ist die regelmäßige Anwendung für unterschiedlichste Zwecke: »Eine Identität, die ich nur ein-bis zweimal im Jahr für Behördengänge brauche, wird sich nicht durchsetzen.«

Allianzen für sichere Smartphone-Identitäten

Heutige und vor allem künftige Smartphones übernehmen immer mehr Aufgaben, die eng mit der Identität ihrer Besitzer:innen zusammenhängen: Kreditkartenzahlungen vornehmen, Autos aufschließen oder sich identifizieren. Um die dahinterliegenden Daten optimal zu schützen, hat Google bereits 2018 mit dem Smartphone Pixel 3 den speziellen Sicherheitschip Titan M eingeführt und ist aktiv an der Standardisierung und Implementierung von datensparsamen mobilen Führerscheinen nach dem internationalen Standard ISO 18013-5 beteiligt.

Im März 2021 startete Google gemeinsam mit verschiedenen Partnern, darunter dem Münchner Bezahl-und Identitätsspezialisten Giesecke+Devrient, die Android Ready SE Alliance. SE steht dabei für Secure Element (»sicheres Element«). Die Allianz soll Open-Source-Programme entwickeln, die direkt auf dem separaten Sicherheitschip ausgeführt werden. So können beispielsweise digitale Identitäten höchster Sicherheitsklassen ermöglicht werden, etwa die nächste Generation der Führerscheine. »Mit diesen frei verfügbaren sogenannten Secure Applets können Gerätehersteller digitale Identitäten einfach und mit zertifizierter Sicherheit umsetzen«, sagt René Mayrhofer vom Team der Android Platform Security.