Matthias Fuhrland, Jürgen Anke, HTW Dresden, 2023

Digitale Identitäten, Identifizierungsmittel und Identitätsmerkmale

Worin besteht der Unterschied?

Die Identität einer natürlichen Person wird durch eine Vielzahl von Identitätsmerkmalen beschrieben. Dies gilt prinzipiell auch im Digitalen, allerdings sind die technisch, philosophisch und politisch geprägten Darstellungen dazu in der Literatur teilweise sehr widersprüchlich. Für das bessere Verständnis ist eine klare begriffliche Unterscheidung wichtig. Daher versuchen wir nachfolgend eine konsistente Begriffserklärung, die auch Anwendungen außerhalb regulierter Anwendungsbereiche integriert:

Digitale Identitäten repräsentieren Personen, Organisationen und auch Objekte der Realwelt im digitalen Raum. Eine reale Person kann mehrere digitale Identitäten haben. Dies kann ein Avatar sein, ein vorgegebener Benutzername oder ein selbstgewähltes Pseudonym, wie im Darknet oder im WWW üblich, es kann aber auch eine sogenannte ***sichere digitale Identität*** sein. Die digitale Identität ist in jedem Fall die Summe aller in einem IT-System einer Entität zuzuordnenden digitalen Identitätsmerkmale (Attribute). Bei einer sicheren digitalen Identität stimmen diese Merkmale nachweislich mit der Realität überein. Die selbst verwaltete digitale Identität ist nicht zu verwechseln mit dem üblicherweise von anderen Akteuren ausgewerteten digitalen Fußabdruck einer Person, der die Spuren beinhaltet, die diese Person im Internet hinterlässt. Solche fremdverwalteten Profile (z.B. Suchverhalten auf Amazon) repräsentieren aber nicht die Person, sondern bilden nur deren Verhalten im Internet ab.

Identitätsmerkmale (**Attribute)** sind Merkmale, die die Identität von Personen, Organisationen bzw. Objekten beschreiben und anhand derer sie identifiziert werden können. Bei natürlichen Personen gehören dazu die im amtlichen Melderegister geführten Meldedaten (Basisidentität), biometrische Daten, Angaben in Nachweisen und Urkunden, aber auch Rechte/Berechtigungen und die Beziehungen gegenüber anderen natürlichen Personen, Organisationen sowie Objekten. Solche Identitätsmerkmale der realen Person können durch autorisierte Akteure in Form überprüfbarer digitaler Nachweise (***Verifiable Credentials***) ausgegeben und bei Bedarf von einem Dritten überprüft werden. Ein Attribut, das eine digitale Identität eindeutig identifiziert bezeichnet man als ***Identifikator***. Dies kann z.B. eine Email-Adresse, die Steuer-ID, eine Kundennummer oder auch die Wirtschaftsidentifikationsnummer eines Unternehmens sein.

Identifizierungsmittel sind Dokumente/Nachweise, die die Zuordnung i.d.R. mehrerer Identitätsmerkmale zu einer Person eindeutig belegen. In der Realwelt sind dies Ausweisdokumente mit Foto, wie Personalausweis, Betriebsausweis oder Krankenkassenkarte. Der Chip auf der Krankenkassenkarte dient der digitalen Übermittlung der darauf gespeicherten Identitätsmerkmale bei physischem Kontakt, die Authentifizierung erfolgt anhand des Fotos auf der Karte. In der digitalen Welt sind hingegen rein elektronische Identifizierungsmittel gefragt, wie die hoheitliche eID, die kommunale Datenkarte oder der digitale Betriebsausweis auf dem Smartphone.

Zur besseren Unterscheidbarkeit soll folgendes **Beispiel** dienen: Alle Daten, die ich einem Internet-Versandhandel bei Einrichtung meines Accounts mitteile, bilden für diesen Versandhandel in Summe

meine *digitale Identität*. Dazu gehört ein selbstgewählter Benutzername (z.B. Rotkäppchen23), der auf der Versandhandelsplattform als *Identifikator* dient. Aber ich übergebe bei der Account-Erstellung auch eine Reihe weiterer *Identitätsmerkmale*, wie Name, Geburtsdatum, Anschrift, Lieferadresse oder ggf. auch eine Kreditkartennummer. Solange diese Identitätsmerkmale nicht überprüft wurden, kann mir der Versandhandel nicht ohne Risiko vertrauen und muss je nach Schadenspotential ggf. viel Rechercheaufwand zu meiner Person betreiben, um sein Risiko zu minimieren. Zeige ich bei der Account-Erstellung aber ein *Identifizierungsmittel* vor, das der Versandhandel vertrauenswürdig findet, z.B. weil sie von einem vertrauenswürdigen Dritten bestätigt wurde, der wiederum anhand seiner eigenen digitalen Signatur oder seines digitalen Siegels eindeutig identifizierbar ist, so bildet die darin enthaltene Auswahl an Identitätsmerkmalen für den Versandhandel eine *sichere digitale Identität*. Alle zusätzlichen Daten, die der Versandhandel über meine Aktivitäten sammelt (Käuferprofil), sind mein *digitaler Fußabdruck* in diesem IT-System.

Status Quo bei den digitalen Identitäten

Zur Nutzung eines Onlinedienstes ist in der Regel die Erstellung eines Benutzerkontos erforderlich, auf das danach per Benutzername (Identifizierungsmittel) und Passwort zugegriffen wird. Dieses Modell der **isolierten Identität** wird aus der Perspektive der Organisation bereitgestellt, da nur der Zugang zu einem Benutzerprofil oder Kundenkonto verfügbar gemacht wird. Die Speicherung der Daten erfolgt bei der Organisation und kann von den Nutzern nur bedingt nachvollzogen werden. So entsteht ein unübersichtliches Nebeneinander an Benutzerkonten, welche die Bedürfnisse der Serviceanbieter erfüllen, für Nutzer aber eine hohe Komplexität verursachen. Im Schnitt hat jeder Mensch ca. 70 verschiedene Benutzerkonten, jeweils mit eigenem Login und Passwort. Tendenz steigend. Hand aufs Herz: Sehen Sie da selbst noch durch? Ein weiteres Problem aus Nutzersicht ist, dass man seine persönlichen Daten den Plattformen kostenlos zur Verfügung stellt, diese aber mit Aufbereitung und Verkauf dieser Daten viel Geld verdienen. Für Serviceanbieter entsteht das Problem, dass die Nutzerdaten immer auf Aktualität geprüft und datenschutzkonform verwaltet werden müssen. Durch mangelhafte Absicherung dieser Daten kommt es zu Diebstählen von Identitäts- und Kreditkarten-daten.

Als Alternative zu den isolierten Identitätslösungen haben sich **„föderierte“ ID-Systeme** entwickelt. Hierbei tritt ein Akteur als Identity Provider auf, der den Nutzern zentral die Anmeldung bei anderen Diensten sowie den Zugriff auf die von ihm verwalteten Identitäten (Nutzerkonten) ermöglicht. Für den Bürger bedeuten diese Systeme eine Vereinfachung, da man sich nur noch die Zugangsdaten zum Identity Provider merken muss. Organisationen können Identity Provider in ihre Services einbinden und erhalten so einen vereinfachten Zugang zu ihren Nutzern, ohne selbst eine digitale Identität anbieten zu müssen. Beispiele für Identity Provider sind Google, Facebook, Microsoft und Verimi. Da die Social-Logins von Google, Facebook & Co nicht für die deutsche Verwaltung einsetzbar sind, u.a. weil sie nicht dem EU-Datenschutz unterliegen, entstanden auf Landes- und Kommunalebene eigene Bürgerkonten. Diese wiederum werden nicht von Onlinediensten außerhalb der Verwaltung akzeptiert, weswegen sie keine intensive Nutzung erfahren. Eine Vereinheitlichung auf Bundesebene wird mit der BundID angestrebt. Trotz der Vereinfachung für Nutzer sind mit föderierten Identitäten vor allem Datenschutzprobleme verbunden, da jeder Login-Vorgang vom Identity Provider festgestellt wird und somit das Potenzial für die Erzeugung von Verhaltensprofilen besteht.

Digitale Identifizierungsmittel

Für die digitale Identifizierung natürlicher Personen gemäß der europäischen eIDAS-Verordnung gibt es prinzipiell als Identifizierungsmittel bereits die Online-Ausweisfunktion des Personalausweises, eine Bürgerkarte oder zukünftig auch eine Lösung mit Hardware Secure Element. Die eIDAS-Verordnung regelt die rechtlichen Rahmenbedingungen für die gegenseitige Anerkennung und Interoperabilität bei grenzüberschreitenden Identifizierungsverfahren. Sie sieht insbesondere vor, dass sich die Wahl der Identifizierungsmittel nach dem jeweils benötigten Vertrauensniveau der Verwaltungsdienstleistung richtet. Besonders sichere Identifizierungsmittel (eID) sind in Verwaltungsdienstleistungen mit hohem Vertrauensniveau einzusetzen. Zusätzliche Sicherheitsmechanismen erfordern zusätzliche Interaktionen und nötiges Hintergrundwissen, wodurch die Alltagstauglichkeit (Usability) beeinträchtigt wird. Der Einsatz der eID in Deutschland ist bislang mit hohem organisatorischem Aufwand für die Akzeptanzstellen (Datenschutzkonzept, Berechtigungszertifikat vom Bundesverwaltungsamt, ISO 27001 Zertifizierung, Lesegerät für den Personalausweis oder Hardware Secure Element fürs Smartphone, technische Integration …) und hohen Kosten verbunden (0,50€ bis 5€ Prüfgebühr pro Vorgang). In anderen europäischen Ländern gibt es abweichende Lösungen für die eID und eine Harmonisierung ist noch in Diskussion. Wenn Lisa z.B. ihren Hauptwohnsitz auf digitalem Weg ummelden und damit den Melderegistereintrag ändern möchte, dann rechtfertigt dies die Forderung nach hohem Vertrauensniveau, also den Einsatz der eID.

Bei Verwaltungsdienstleistungen mit substanziellem oder niedrigem Vertrauensniveau werden geringere Anforderungen an das Identifizierungsmittel gestellt. Hier reicht z.B. ein digitaler Auszug aus dem Melderegister (=> Kommunale Datenkarte) mit der überprüfbaren Signatur bzw. dem überprüfbaren Siegel der ausstellenden Kommune. Der Umfang der darin ausgewiesenen Identitätsmerkmale kann deutlich höher sein als bei der eID und somit auch viel mehr Anwendungen bedienen. Das Pendant für Unternehmensidentitäten wäre ein signierter digitaler Auszug aus dem Handelsregister (=> Unternehmens-ID). Aktuell erhält man den digitalen Auszug als unsigniertes PDF. Werden diese digitalen Registerauszüge als Verifiable Credentials ausgestellt und in die Wallet des ID-Inhabers übertragen, dann werden diese digitalen Nachweise zu Identifizierungsmitteln im Kontext der selbstsouveränen Identität. Was das ist, erklärt der nächste Artikel.