Anke, Jürgen; Knoll, Matthias

Digitale Identitäten

HMD Praxis der Wirtschaftsinformatik

Provided in Cooperation with:
Springer Nature

Suggested Citation: Anke, Jürgen; Knoll, Matthias (2023) : Digitale Identitäten, HMD Praxis der Wirtschaftsinformatik, ISSN 2198-2775, Springer Fachmedien Wiesbaden GmbH, Wiesbaden, Vol. 60, Iss. 2, pp. 251-254, https://doi.org/10.1365/s40702-023-00968-y

This Version is available at:
https://hdl.handle.net/10419/307958

HMD Praxis der Wirtschaftsinformatik (2023) 60:251–254
https://doi.org/10.1365/s40702-023-00968-y

EDITORIAL

Digitale Identitäten

Jürgen Anke · Matthias Knoll

Angenommen: 7. März 2023 / Online publiziert: 20. März 2023

Auf den ersten Blick scheint uns das Themengebiet Digitale Identitäten bereits gut vertraut. Wir nutzen in unserem immer stärker von Technologie durchdrungenen Alltag eine Vielzahl digitaler Identitäten, ohne länger darüber nachzudenken. Überall dort, wo wir uns – mehr oder weniger gut überprüfbar – identifizieren und authentifizieren müssen, besitzen wir auch eine digitale Identität. Eine Anmeldung zu Social Media hier, ein Bezahlvorgang im stationären Handel oder im Webshop dort und nicht zuletzt die elektronische Steuererklärung beim Finanzamt suggerieren, dass das Thema digitale Identitäten leicht zu überblicken ist.

Weit gefehlt! Zwar ist eine „Digitale Identität“ gemäß ISO/IEC 24760-1:2019 scheinbar leicht als Datensatz beschreibbar. Doch mit dem Verständnis dieses Datensatzes ist das Thema nicht ansatzweise erschlossen und verstanden. Im Gegenteil: Die Norm selbst beschreibt einen „kleinsten gemeinsamen Nenner“ aus technischer Sicht. Zahlreiche weitere Regelungen sowie technische und fachliche Anforderungen müssen beachtet werden, um alltagstaugliche und rechtskonforme Verfahren zu realisieren. Allerdings können viele Dienste und Anwendungen nicht auf bereits bestehende digitale Identitäten zurückgreifen, sondern erfordern eine erneute Registrierung, Identifizierung und Datenverifikation. Damit entstehen viele digitale Identitäten, die jeweils nur für sehr begrenzte Zwecke einsetzbar sind. So kommt es zu einer großen Fragmentierung von Diensten, Benutzerkonten, Apps und Sicherheitsprozeduren, die wir im digitalen Alltag oft als Hindernisse empfinden.

✉ Jürgen Anke
Arbeitsgruppe Digitale Dienstleistungssysteme, HTW Dresden, Dresden, Deutschland
E-Mail: juergen.anke@htw-dresden.de

Matthias Knoll
Hochschule Darmstadt, Darmstadt, Deutschland
E-Mail: matthias.knoll@h-da.de

Der Umgang mit digitalen Identitäten ist ein Thema, das aus sehr unterschiedlichen Perspektiven betrachtet werden muss: Nutzung, Angebot, Sicherheit und Vertrauen, gesellschaftliche und politische Akzeptanz, Rechtsrahmen und Ethik – all das beeinflusst die Diskussion. Das erschwert einerseits den Überblick, andererseits einen Konsens. Denn die Beteiligten in Politik, Wirtschaft, Verwaltung und Zivilgesellschaft besitzen ihre jeweiligen Präferenzen und verfolgen – das ist vollkommen normal – zunächst ihre eigenen Interessen. Gleichzeitig nähern sie sich der Diskussion von unterschiedlichen Seiten an. Dies hat zur Folge, dass das verwendete Vokabular im Idealfall zwar ähnlich, semantisch aber vollkommen unterschiedlich ist – oder umgekehrt. Das alles zusammen begünstigt „Silodenken" und „Insellösungen", die sich in der erwähnten Fragmentierung widerspiegeln.

Eine solche Situation führt zu Unmut und Frustration, zu Nicht-Nutzung und Nicht-Angebot oder dazu, dass eine mächtige Industrie Quasi-Standards nach eigenen Vorstellungen setzt, wie wir sie aktuell mit der Präsenz bekannter Identifikations- und Authentifizierungsdiensten auf einer Vielzahl von Websites kennen – und praktisch nutzen müssen, wollen wir dabei sein. Gleichzeitig verhindert eine fehlende gemeinsame, international standardisierte und akzeptierte Lösung eine rasche Digitalisierung zentraler, gesellschaftlich relevanter Leistungen. Die Tatsache, dass es andere Länder vermeintlich besser machen, ist auch nur bedingt ein Argument, denn jede Lösung hat ihre charakteristischen Stärken und Schwächen – nicht zuletzt im Kontext der jeweiligen Länder und deren rechtlichen und kulturellen Besonderheiten. Und zugegeben: Einfach ist das Thema nicht. Schon die Frage, wer in der Position sein darf, digitale Identitäten zu erstellen und zu verwalten, die über den Zugang zu einfachen Dienstleistungen ohne nennenswertes Schadenspotential hinausgehen, ist nicht leicht zu beantworten – staatliche Stellen, private Unternehmen oder eine Kombination daraus? Denn digitale Identitäten sind eng mit den Menschen verbunden, denen sie „gehören". Besonders herausfordernd wird es, wenn biometrische Informationen für die Authentifizierung verwendet werden sollen.

Was also tun? Den Finger in die Wunde legen und gleichzeitig Handlungsempfehlungen aufzeigen ist eine gute Möglichkeit, für die Dringlichkeit zu sensibilisieren. Skierka & Parycek gelingt dies in ihrem Einwurf zu diesem Schwerpunktheft mit sprachlicher Leichtigkeit und auf den Punkt gebrachter fachlicher Präzision.

Der Grundlagenbeitrag von Anke & Richter stellt anschließend zentrale Zusammenhänge, Begriffe und Ansätze vor und gibt einen Überblick über den Status Quo. Ein derzeit intensiv diskutiertes Konzept sind selbstbestimmte Identitäten (Self-Sovereign Identity, SSI), bei denen Nutzerinnen und Nutzer digital signierte Nachweise in digitalen Brieftaschen (Wallets) verwalten. SSI hat das Potenzial, einen einheitlichen Mechanismus für digitale Identitäten in diversen Einsatzgebieten mit ihren jeweiligen Anforderungen zu realisieren. Aus diesem Grund greifen die folgenden Schwerpunktbeiträge dieses Konzept aus unterschiedlichen Blickwinkeln immer wieder auf.

Die ersten beiden Beiträge nehmen eine Anwendungsperspektive ein und zeigen, wie Systeme für den Umgang mit digitalen Identitäten gestaltet werden können. Als Einstieg zeigen Roland, Höller & Mayrhofer in ihrem Beitrag, wie der Einsatz von digitalen Identitäten mit Hilfe von Biometrie an physischen Kontaktpunkten unter Berücksichtigung der Privatsphäre der Nutzerinnen und Nutzer aussehen kann.

Das Thema Datenschutz ist auch im Kontext der Einwilligung für Cookies relevant, anhand derer Websites Profile über das Surfverhalten und damit verbundene Interessen erstellen können. Bernemann & Kneuper behandeln in ihrem Beitrag Personal Information Management Systeme, die künftig als Erweiterungen für Browser die Verwaltung von Einwilligungen unterstützen sollen.

Eine häufige Kritik an Technik für den Umgang mit digitalen Identitäten ist die mangelhafte Fokussierung auf die Bedürfnisse von Nutzenden, insbesondere technisch weniger versierten Menschen. Dies wird durch die folgenden beiden Beiträge adressiert. Zunächst stellen Kostic & Poikela Ergebnisse aus zwei Nutzerstudien vor, die u. a. die wahrgenommene Vertrauenswürdigkeit von digitalen Identity Wallets untersuchen. Usability steht auch im Fokus des Beitrags von Krauß, Sellung & Kostic, die einen Vorschlag für die nutzerfreundliche Gestaltung künftiger Wallets präsentieren.

Mit der zugrundeliegenden Technik und Verfahren befassen sich die folgenden drei Beiträge. Das Autorenteam um Jahnke geht auf die Nutzung biometrischer Authentifizierungsverfahren ein, die hohe Benutzerfreundlichkeit aber auch besondere Sicherheitsherausforderungen aufweisen. Die Verwaltung digitaler Nachweise stellt hohe Anforderungen an die Sicherheit von Wallets, die künftig auch Gegenstand von Zertifizierungen sein werden. Bastian, Kraus & Fischer systematisieren in ihrem Beitrag die relevanten Angriffsvektoren und diskutieren Lösungsoptionen auf Basis aktueller technischer Möglichkeiten in mobilen Geräten. Da in Zukunft eine Vielfalt von Wallet- und Dienstanbietern sowie Herausgebern von Nachweisen zu erwarten ist, spielt die Frage nach der Interoperabilität eine wichtige Rolle. Yildiz et al. zeigen anhand der im Schaufensterprogramm „Sichere digitale Identitäten“ verwendeten Technologien, wie Interoperabilitätsprobleme auf verschiedenen Ebenen adressiert werden können.

Die Rahmenbedingungen und Auswirkungen digitaler Identitäten werden in den folgenden drei Beiträgen thematisiert. Für die Nutzung interoperabler digitaler Identitäten ist das Zusammenspiel verschiedener Dienste erforderlich. Damit solche Identitäts-Ökosysteme ökonomisch tragfähig sind, werden geeignete Geschäftsmodelle gebraucht, deren Gestaltungsoptionen Kubach & Roßnagel in ihrem Beitrag diskutieren. Für die Zahlungsbereitschaft der beteiligten Akteure sind die Einsatzmöglichkeiten und damit verbundenen Nutzenpotenzialen maßgeblich. Wie diese im Kontext von Verwaltung und öffentlichen Institutionen aussehen können, wird im Beitrag von Biedermann et al. diskutiert. Dabei gehen die Autorinnen und Autoren auch auf Skalierungs- und Transferpotenziale ein. Einen Aspekt der Regulierung für den Einsatz digitaler Identitäten in der Verwaltung greift der Beitrag von Dorenbusch, Auth & Pflüger auf. Sie schlagen ein Modell für die systematische Bestimmung von erforderlichen Vertrauensniveaus im Kontext des Onlinezugangsgesetzes vor.

Die letzten beiden Beiträge in diesem Heft geben einen Ausblick auf die Einsatzpotenziale jenseits von Personenidentitäten. Babel et al. stellen einen Ansatz vor, mit dem vernetzte Kleingeräte wie Photovoltaikanlagen und Wärmepumpen mittels SSI-basierter Identitäten als vertrauenswürdige Datenquellen in Informationssysteme eingebunden werden können. Schließlich ist auch die Absicherung von kritischen Infrastrukturen eine wichtige Anwendung. Der Beitrag von Buck et al. zeigt auf Ba-

sis einer Zero-Trust-Architektur, wie Zugriffe auf Energieanlagen gesteuert werden können und leiten dazu Handlungsempfehlungen für deren Gestaltung ab.

Zwei Rezensionen runden diese Schwerpunktausgabe ab. Die erste Rezension widmet sich dem Lehrbuch „Cyber-Sicherheit“ von Norbert Pohlmann. In mehreren Kapiteln wird dort das Thema Digitale Identitäten aufgegriffen und in den Gesamtkontext der Sicherheit eingebunden – nicht die einzige, aber eine wichtige Perspektive im Kontext Digitaler Identitäten.

Die zweite Rezension, ein Herausgeberband von Alex Preukschat und Drummond Reed, geht ins Detail. Unter dem Titel „Self-Sovereign Identity – Decentralized Digital Identity and Verifiable Credentials“ wird das aktuell diskutierte Paradigma der selbstbestimmten Identitäten aus verschiedenen Perspektiven im Detail vorgestellt und kritisch diskutiert.

Unser herzlicher Dank gilt allen Autorinnen und Autoren sowie den Gutachterinnen und Gutachtern aus Wissenschaft und Praxis, die mit ihrer Expertise und Ihren Erfahrungen das anspruchsvolle Gebiet der Digitalen Identitäten erschließen helfen.

Liebe Leserinnen und Leser, wir wünschen Ihnen eine spannende Lektüre, aus der Sie viel Wissen mitnehmen können! Wir freuen uns über Ihr Lob, aber auch über Ihre Fragen, Anregungen und Kritik.

Jürgen Anke und Matthias Knoll

Funding Open Access funding enabled and organized by Projekt DEAL.