cottonbro / Pexels

Self-Sovereign Identity – Herzlich willkommen im Zeitalter der Datensouveränität

von Marlene Hoffmann, Fabiane Völter und Tobias Guggenberger

Digitale Identitäten für die öffentliche Verwaltung

Die anhaltende technische Entwicklung und wachsende Anzahl von Bürger:innen, die das Internet benutzen, erfordern, dass Verwaltungs- und Behördenprozesse auch online angeboten werden. In vielen europäischen Ländern ist dies bereits Teil des Alltags: die Anmeldung einer neuen Wohnung oder die Ummeldung des Kfz kann vom Smartphone aus getätigt werden. Die digitale Transformation des öffentlichen Sektors kann zu verbesserten Zugangsmöglichkeiten zu Leistungen und Informationen sowie einer effizienteren und damit kosteneffektiven öffentlichen Hand führen.

Für die elektronische Bereitstellung von Verwaltungsservices muss allerdings auf eine entsprechende Infrastruktur zur eindeutigen Identifizierung von Nutzer:innen zurückgegriffen werden können. In der analogen Welt ist es möglich, sich gegenüber Behörden mit physischen Urkunden, wie Personalausweisen oder beglaubigten Dokumenten auszuweisen. Dem digitalen Raum fehlt es momentan allerdings an einem universellen, elektronischen und nutzerfreundlichen Identifizierungsmittel, welches von einer Mehrheit der Bürger:innen genutzt werden kann.

Zwar können mit der Einführung der elektronischen Ausweisfunktion im Personalausweis erste Erfolge verzeichnet werden, allerdings bleibt die Adoption des elektronischen Personalausweises insgesamt sehr gering – einer **aktuellen Umfrage** zufolge nutzen lediglich 7% der Befragten diese Funktion. Zudem ist für viele Verwaltungsservices nicht lediglich die Identifizierung von Personen und Organisationen notwendig, sondern auch die Bereitstellung von weiteren Nachweisen und Bescheinigungen, wie beispielsweise Vollmachten. Dieser Umstand zwingt das öffentliche Verwaltungswesen bisher, an der physischen Bereitstellung von Leistungen festzuhalten.

Was ist Self-Sovereign Identity?

Das Konzept Self-Sovereign Identity, also der »selbstbestimmten Identität«, beschreibt das nutzergesteuerte Management der digitalen Identität. Einen Überblick über die Rollen und Bausteine verschafft Abbildung eins. Dabei werden digitale Identitätsnachweise entsprechend zu analogen Identitätsnachweisen wie dem Personalausweis durch Issuer (Aussteller:in) erstellt und signiert. Diese Identitätsnachweise werden Verifiable Credentials genannt. Mithilfe von Decentralized Identifiers kann eine Verbindung zu den Nutzer:innen hergestellt und die Verifiable Credentials übertragen werden. Nutzer:innen speichern und verwalten die Verifiable Credentials sowie ihr kryptografisches Schlüsselmaterial in Wallets, welche digitale Geldbörsen darstellen.

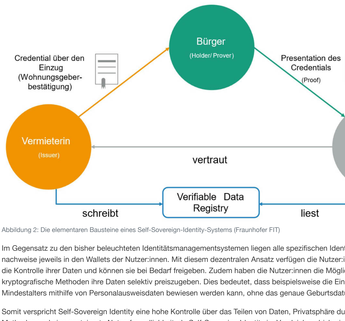

Abbildung 1: Die elementaren Bausteine eines Self-Sovereign-Identity-Systems (Fraunhofer FIT)

Anschließend kann aus Verifiable Credentials eine Verifiable Presentation abgeleitet und einem Dritten, dem sogenannten Verifier, vorgezeigt werden. Dieser überprüft die digitale Signatur des Ausstellers und kann so Rückschlüsse auf die Echtheit des Nachweises ziehen. Neben der Echtheit muss auch die Gültigkeit des Verifiable Credentials sichergestellt werden. Dies wird mittels eines sog. Akkumulators, welcher oftmals auf einem dezentralen Register durch den Aussteller hinterlegt ist, nachvollzogen werden.

Abbildung zwei illustriert ein Anwendungsbeispiel, wie Self-Sovereign Identity im Behördenwesen funktionieren kann. Bei der betrachteten Ausgangssituation möchte ein Bürger seinen Wohnsitz anmelden. Dazu benötigt er gegenüber dem Einwohnermeldeamt einen Nachweis darüber, dass er tatsächlich bereits den Einzug in die Wohnung vorgenommen hat. Er ist im Besitz eines Wallets auf Self-Sovereign-Identity-Basis und fragt daher seine Vermieterin, ihm ein digitales Zertifikat in Form eines Verifiable Credentials auszustellen, welches seine Anschrift bescheinigt. Dieses Zertifikat entspricht der analogen Wohnungsgeberbestätigung und kann von ihm in seiner Wallet gespeichert werden. Nach Aufforderung durch das Einwohnermeldeamt, einen Nachweis für den Einzug zu erbringen, erzeugt der Bürger eine Verifiable Presentation.

Diese Ableitung aus dem digitalen Nachweis steht kryptografisch in direkter Verbindung zu dem von der Vermieterin ausgestellten Bestätigung, minimiert den Inhalt der Daten jedoch auf das für den Prozess Wesentliche: Die Authentizität und Validität der Wohnungsgeberbestätigung sowie die notwendigen Daten wie die Adresse. Nun ist der Bürger im nächsten Schritt in der Lage, diese Informationen mit der Behörde zu teilen. Das Einwohnermeldeamt kann sich durch kryptografische Verfahren demnach darauf verlassen, dass der Nachweis, den der Bürger erzeugt hat, echt und gültig ist.

Diese verwendeten Mechanismen bedeuten, dass, ähnlich zur analogen Welt, der Verifier den Issuer nicht kontaktieren muss, um Echtheit und Gültigkeit sicherzustellen. Die vier Elemente Verifiable Credentials, Decentralized Identifiers, Wallets und Register bilden die Grundpfeiler für vertrauensvolle digitale Interaktionen, indem sie das fälschungssichere und gleichzeitig datenschutzkonforme Nachweisen von Attributen ermöglichen.

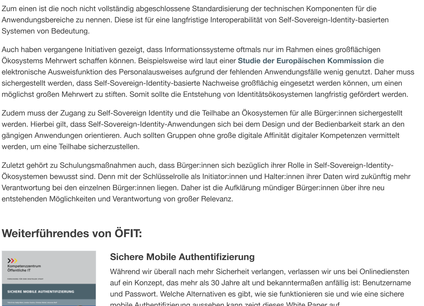

Abbildung 2: Die elementaren Bausteine eines Self-Sovereign-Identity-Systems (Fraunhofer FIT)

Im Gegensatz zu den bisher beleuchteten Identitätsmanagementsystemen liegen alle spezifischen Identitätsmarkmale und -nachweise jeweils in den Wallets der Nutzer:innen. Mit diesem dezentralen Ansatz verfügen die Nutzer:innen permanent über die Kontrolle ihrer Daten und können sie bei Bedarf freigeben. Zudem haben die Nutzer:innen die Möglichkeit, durch kryptografische Methoden ihre Daten selektiv preiszugeben. Dies bedeutet, dass beispielsweise die Einhaltung eines Mindestalters mithilfe von Personalausweisdaten bewiesen werden kann, ohne das genaue Geburtsdatum preiszugeben.

Somit verspricht Self-Sovereign Identity eine hohe Kontrolle über das Teilen von Daten, Privatsphäre durch kryptografische Methoden und eine gesteigerte Nutzerfreundlichkeit, da Self-Sovereign Identity im Vergleich zu bisherigen Identitätsmanagement-Lösungen für universelle Nachweise genutzt werden kann.

Mehrwerte von Self-Sovereign Identity für die öffentlichen Dienste

Die jüngsten Gesetzesinitiativen auf nationaler wie europäischer Ebene demonstrieren, dass die Digitalisierung der Verwaltung ein zentrales Bestreben der Politik ist. Dies zeigt beispielsweise das Registermodernisierungsgesetz oder das Onlinezugangsgesetz. Letzteres verpflichtet Bund und Länder dazu, bis spätestens Ende 2022 ihre Verwaltungsleistungen über Portale anzubieten. Für die Umsetzung dieses Vorhabens werden Mechanismen sowohl zur Anforderung als auch Bereitstellung von Nachweisen von großer Relevanz.

Ähnlich sollen auf europäischer Ebene Verwaltungsservices mithilfe des Single Digital Gateways grenzübergreifend verfügbar gemacht werden. Dabei gewinnt auch Self-Sovereign Identity auf europäischer Ebene an Bedeutung. So benennt der kürzlich veröffentlichte Entwurf der zweiten europäischen Verordnung über die elektronische Identifizierung und Vertrauensdienste (eIDAS 2.0), Self-Sovereign Identity als eine Möglichkeit, eine Umgebung umzusetzen, welche hohe Nutzerkontrolle, Sicherheit und Flexibilität verspricht.

Die Anwendung von Self-Sovereign Identity in der öffentlichen Verwaltung bietet sowohl für die Bürger:innen als auch für die beteiligten Organisationen Vorteile. Viele aktuell noch papierbasierte Nachweisprozesse erfordern ein manuelles Übertragen von Daten. Dies führt zu Medienbrüchen und einer verringerten Datenqualität. Durch das Vorzeigen von Nachweisen in Form von Verifiable Credentials können diese Nachweisprozesse automatisiert und die Datenqualität gesteigert werden. Zudem sind papierbasierte Dokumente oftmals nicht fälschungssicher, wohingegen Verifiable Credentials einen hohen Schutz gegen Datenfälschung bieten.

Die Gesetzesinitiativen demonstrieren das Bestreben, die öffentliche Verwaltung den digitalen Entwicklungen anzupassen. Dabei deckt sich das Self-Sovereign Identity Paradigma mit den hierfür erforderlichen Anforderungen und kann daher die öffentlichen Organe bei der Umsetzung und Einhaltung des neuen rechtlichen Rahmens unterstützen.

Fazit und Ausblick

Self-Sovereign Identity ist ein vielversprechendes und vielfältiges Konzept für digitales Identitätsmanagement. Von der Kombination aus Datenschutzsicherheit und hohen Potenzialen in der automatischen Datenverarbeitung könnten neben der Privatwirtschaft auch die öffentlichen Dienste profitieren. Trotzdem sind noch einige Herausforderungen vor dem produktiven Einsatz von Self-Sovereign Identity zu bewältigen, die unter anderem durch die Neuheit des Konzepts bedingt werden.

Zum einen ist die noch nicht vollständig abgeschlossene Standardisierung der technischen Komponenten für die Anwendungsbereiche zu nennen. Diese ist für eine langfristige Interoperabilität von Self-Sovereign-Identity-basierten Systemen von Bedeutung.

Auch haben vergangene Initiativen gezeigt, dass Informationssysteme oftmals nur im Rahmen eines großflächigen Ökosystems Mehrwert schaffen können. Beispielsweise wird laut einer **Studie der Europäischen Kommission** die elektronische Ausweisfunktion des Personalausweises aufgrund der fehlenden Anwendungsfälle wenig genutzt. Daher muss sichergestellt werden, dass Self-Sovereign-Identity-basierte Nachweise großflächig eingesetzt werden können, um einen möglichst großen Mehrwert zu stiften. Somit sollte die Entstehung von Identitätsökosystemen langfristig gefördert werden.

Zudem muss der Zugang zu Self-Sovereign Identity und die Teilhabe an Ökosystemen für alle Bürger:innen sichergestellt werden. Hierbei gilt, dass Self-Sovereign-Identity-Anwendungen sich bei dem Design und der Bedienbarkeit stark an den gängigen Anwendungen orientieren. Auch sollten Gruppen ohne große digitale Affinität digitaler Kompetenzen vermittelt werden, um eine Teilhabe sicherzustellen.

Zuletzt gehört zu Schulungsmaßnahmen auch, dass Bürger:innen sich bezüglich ihrer Rolle in Self-Sovereign-Identity-Ökosystemen bewusst sind. Denn mit der Schlüsselrolle als Initiator:innen und Halter:innen ihrer Daten wird zukünftig mehr Verantwortung bei den einzelnen Bürger:innen liegen. Daher ist die Aufklärung mündiger Bürger:innen über ihre neu entstehenden Möglichkeiten und Verantwortung von großer Relevanz.

Weiterführendes von ÖFIT:

Sichere Mobile Authentifizierung

Während wir überall nach mehr Sicherheit verlangen, verlassen wir uns bei Onlinediensten auf ein Konzept, das mehr als 30 Jahre alt und bekanntermaßen anfällig ist: Benutzername und Passwort. Welche Alternativen es gibt, wie sie funktionieren sie und wie eine sichere mobile Authentifizierung aussehen kann zeigt dieses White Paper auf.

Thilo Ernst, Nadja Menz, Jaroslav Svacina, Christian Welzel, Johannes Wolf (2019)

Berlin: Fraunhofer FOKUS: Kompetenzzentrum Öffentliche IT

Zur Publikation

Safety und Security aus dem Blickwinkel der Öffentlichen IT

Durch die anhaltende Durchdringung unserer Gesellschaft mit Informationstechnologie verschwimmt die Grenze zwischen Safety und Security zusehends. Das Whitepaper widmet sich der Vielschichtigkeit des Themas Sicherheit und zeigt die dazugehörigen Handlungsfelder und Forschungsfragen auf.

Nadja Menz, Petra Hoepner, Jens Tiemann, Frank Koußen (2015)

Berlin: Fraunhofer FOKUS: Kompetenzzentrum Öffentliche IT

Zur Publikation