Self-Sovereign Identity als Lösungsansatz

Digitale Selbst-bestimmung erreichen

Aktuell wird ein neuer Vorschlag für das E-ID-Gesetz erarbeitet. Self-Sovereign Identity ist einer der drei Ansätze für die Lösung. Es ist ein neues Paradigma für den Umgang mit digitalen Identitäten, das derzeit im Rampenlicht steht und rasch konkret Form annimmt.

→ VON HARTMUT KARL KEIL UND ROMAN ZOUN

DIE AUTOREN

Hartmut Karl Keil
ist Innovation Software Engineer bei Adnovum Incubator und SSI-Experte bei Adnovum.

Dr.-Ing. Roman Zoun
ist Innovation Architect bei Adnovum Incubator und SSI-Entwickler bei Adnovum.
→ **adnovum.ch/incubator**

Wer kennt das nicht: Sie wollen einen neuen Service nutzen, vielleicht auch nur schnell ein Paar Schuhe im Internet kaufen. Dann kommt die Aufforderung, sich zu registrieren. Weil es am schnellsten und einfachsten geht, erledigen Sie das mit einem Identity Provider wie Google, Facebook und Co. Wir alle machen das und wir alle haben mittlerweile unsere Bedenken: Denn die Identity Provider wissen nun ganz genau, wann und wie oft wir welche Services im Internet nutzen. Ähnliche Bedenken waren auch ein Grund für die Ablehnung der E-ID-Vorlage bei der Abstimmung im März 2021.

KEIN VERTRAUEN IN ZENTRALE PROVIDER

Als Benutzer stehen wir vor einem Dilemma: Einerseits wollen wir eine einheitliche Identität bei allen Services, andererseits aber keinen zentralen Identity Provider, der diese verwaltet und den Services zur Verfügung stellt. Self-Sovereign Identity (SSI) ist ein neues Konzept, das einen Ausweg aus diesem Dilemma bietet. Denn SSI erlaubt es dem Benutzer, seine Identität selbstständig zu verwalten. Den Services bietet es die Möglichkeit, diese Benutzeridentität zu verifizieren. Nicht umsonst wird SSI als mögliche Lösung der E-ID in der Schweiz und in Europa diskutiert: Es gilt als nächste Evolutionsstufe im Identity Management. Bevor Self-Sovereign Identity jedoch im vollen Umfang genutzt werden kann, muss das neue Konzept von den Akteuren akzeptiert werden.

IDENTITY MANAGEMENT MIT SSI

Im Konzept von SSI gibt es drei Rollen: den «Issuer» (Aussteller), den «Holder» (Eigentümer) und den «Verifier» (Prüfer). Die Aussteller sind vertrauenswürdige Institutionen oder Firmen, die digitale Nachweise ausstellen, zum Beispiel einen Personalausweis oder ein Diplom. Das können etwa eine Gemeindeverwaltung, eine Universität oder auch eine Bank sein. Bei Self-Sovereign Identity heissen diese digitalen Nachweise «verifiable credentials» und enthalten kryptografisch gesicherte Daten. Diese digitalen Nachweise werden vom Eigentümer in einer mobilen Wallet-Applikation auf dem Smartphone gespeichert. Bei den Prüfern handelt es sich um Services wie ein E-Shop oder eine Autovermietung, die Daten der Nutzer abfragen wollen. Dazu sendet der Service eine Anfrage an das mobile Wallet des Benutzers und dieser entscheidet dann, welche Daten er dem Service sendet. Der Service kann kryptografisch überprüfen, ob die erhaltenen Daten von einem Aussteller ausgegeben wurden, dem er vertraut.

BEWEISEN STATT OFFENBAREN

Ein wesentlicher Aspekt von Self-Sovereign Identity ist, dass mit den drei Rollen Aussteller, Eigentümer und Prüfer ein ganzes Ökosystem aufgebaut werden kann. Folgende Anwendungsfälle als Beispiel: Der Nutzer Stefan installiert eine Wallet-Applikation auf seinem Smartphone, um seine digitalen Nachweise dort zu speichern. In einem ersten Schritt benötigt er eine Basis-ID, also einen digitalen Nachweis seiner persönlichen Daten wie Name, Vorname, Geburtsdatum und Heimatort. Diese Basis-ID wird von einer staatlichen Stelle herausgegeben.

Die digitale Basis-ID kann Stefan nun nutzen, um sich bei einem Service (Prüfer), zum Beispiel einem Weinshop, anzumelden. Der Service fragt dazu nach den Attributen Name und Vorname der Basis-ID. Stefan muss anschliessend aktiv die Freigabe dieser Daten in seiner Wallet-Applikation akzeptieren. Der Service kann nun einerseits den Nutzer persönlich begrüssen und weiss andererseits, dass dieser eine gültige Basis-ID hat. Dabei müssen die Daten nicht immer offengelegt werden. Hierfür bietet Self-Sovereign Identity eine Möglichkeit an, Ja-/Nein-Fragen zu beantworten. Mit der sogenannten «Zero Knowledge Proof»-Technologie ist es beispielsweise möglich, dass Stefan dem Service beweist, dass er über 18 Jahre alt ist, ohne sein Geburtsdatum offenzulegen.

«Self-Sovereign Identity ändert grundlegend die Art und Weise, wie wir mit persönlichen Daten in der digitalen Welt umgehen»

Hartmut Karl Keil und Roman Zoun

Stefan möchte nun einen digitalen Nachweis seiner Krankenversicherung erhalten. Er registriert sich dazu auf der Website seiner Krankenversicherung, die alle Attribute seiner Basis-ID abfragt. Die Krankenversicherung kann mit diesen Daten sicherstellen, dass Stefan bei ihr versichert ist, und sendet ihm den gewünschten digitalen Krankenversicherungsnachweis. Stefan hat nun zwei digitale Nachweise in seiner Wallet-Applikation gespeichert: die Basis-ID und den Krankenversicherungsnachweis.

NEUES PARADIGMA FÜR PERSÖNLICHE DATEN

Self-Sovereign Identity bringt ein neues Paradigma mit sich, das ein Umdenken erfordert in der Art, wie wir mit persönlichen Daten umgehen und wie wir diese speichern. Der Eigentümer entscheidet aktiv, welche Daten wem offenbart werden; dabei können Daten aus verschiedenen digitalen Nachweisen kombiniert werden.

Beispiel Arztbesuch: Der Nutzer Stefan würde dem Arzt den Namen und Vornamen aus seiner Basis-ID sowie seine Versicherungsnummer aus seinem Krankenversicherungsnachweis zeigen. Dieses Kombinieren von digitalen Nachweisen erfordert wie bereits erwähnt ein Umdenken in der Datenhaltung, da jeder Aussteller nur die wirklich nötigen Daten ausgeben und verwalten muss. Dadurch wird Redundanz vermieden und eine einfachere Handhabung bei Änderungen ermöglicht, etwa des Namens, da nur die Basis-ID neu ausgestellt werden muss.

NUR EINE FRAGE DER ZEIT

Self-Sovereign Identity ist eine Technologie, die ein neuartiges, an den tatsächlichen Bedürfnissen der Nutzer orientiertes Konzept bietet und eine Vielzahl an neuen Anwendungsfällen ermöglicht. Mit dem neuen Paradigma gibt es keine zentrale Stelle, die persönliche Daten verwaltet und das Nutzerverhalten ausspähen kann. Allein der Nutzer hat seine Daten in der Hand und kontrolliert sie. Mit Zero Knowledge Proof bietet SSI zusätzlich die Möglichkeit, Ja-/Nein-Fragen zu beantworten, ohne die Daten preiszugeben. Dieses Feature führt zu mehr Sicherheit für den Nutzer und besserem Datenschutz bei den angebotenen Services. Die digitalen Services profitieren nebst dem Datenschutz, den SSI per Design anbietet, von der vereinfachten Digitalisierung firmenübergreifender Prozesse. Das Vertrauen in die Aussteller und digitalen Services kann mithilfe der Global Legal Entity Identifier Foundation (einer Art globalem Unternehmensregister) noch verstärkt werden.

Die Self-Sovereign-Identity-Technologie ist noch relativ jung, umso rasanter sind die Fortschritte in ihrer Entwicklung. Neben dem Maturitätsaspekt müssen auch die Akteure (Verwaltung, Serviceanbieter und Nutzer) das neue Paradigma annehmen. Denn es ändert grundlegend die Art und Weise, wie wir mit persönlichen Daten in der digitalen Welt umgehen. ←

Self-Sovereign Identity sieht vor, dass die digitalen Nachweise von Nutzerinnen und Nutzern in einer mobilen Wallet-App auf dem Smartphone gesichert werden

Bilder: Adnovum