

Self-Sovereign Identity – Ökosystem digitaler Identitäten



ONLINE KÖNNEN WIR SEIN, WER ODER WAS WIR WOLLEN. DOCH WIE STELLT MAN SICHER, DASS EINE ONLINE-IDENTITÄT DER WAHRHEIT ENTSPRICHT? DIE SELF-SOVEREIGN IDENTITY IST EINE NEUE ART, IN DER DIGITALEN WELT VERTRAUEN HERZUSTELLEN – UND GEHT WEIT ÜBER DAS DERZEITIGE VERSTÄNDNIS VON IDENTITÄT HINAUS.

FACHARTIKEL

_CATHARINA DEKKER

Consultant

Ergon Informatik AG

_MICHAEL DOUJAK

Product Manager Airlock

Ergon Informatik AG

Erschienen im SMART insights 2022 Magazin

ergon

smart
people –
smart
software®

Prinz, Model oder Milliardenerin: Online können Menschen alles sein – und es ist schwierig, Online-Identitäten offiziell zu prüfen. Das soll sich bald ändern. Was in der physischen Welt die Identitätskarte oder der Reisepass ist, soll im Digitalen die Self-Sovereign Identity (SSI) werden. Sie ermöglicht es, physische Identitätsnachweise in die digitale Welt zu übersetzen. Standardisiert und vertrauenswürdig, hochgradig fälschungssicher, verifizierbar – und nicht zuletzt datenschutzkonform.

Username und Passwort reichen nicht

Wer sich heute bei einem Webdienst identifizieren muss, braucht dafür einen Usernamen und ein Passwort. Die meisten Dienstanbieter nutzen ein lokales Identitätsmodell, um ihre User eindeutig zu identifizieren. Das hat viele Nachteile. Anbieter stehen in der Pflicht, diese Daten sicher zu verwalten – und erleiden bei einer Datenpanne finanziellen Schaden durch Folgekosten und Reputationsverlust. Nutzer:innen müssen die vielen verschiedenen Accounts und Passwörter verwalten, was mit Aufwand verbunden ist. Um dem Abhilfe zu bieten, hat sich in den letzten Jahren die föderierte Identität etabliert: Nutzer:innen können sich mit dem Login eines anderen Dienstes wie Google oder Facebook identifizieren. Dieses Single Sign-on ist vor allem für Zugänge mit geringeren Sicherheitsanforderungen sinnvoll. Für Unternehmen, die auf eine stärkere

Authentifizierung angewiesen sind, reicht das aber nicht aus. Hier ist eine dezentrale Identifikation wichtig.

Rechtliche Rahmenbedingungen schaffen

Die rechtlichen Rahmenbedingungen für international anerkannte dezentralisierte Identitäten werden gerade erarbeitet. Nachdem das Schweizer Stimmvolk die E-ID 2021 abgeschmettert hat, strebt der Schweizer Gesetzgeber eine selbstverwaltete Identität SSI an. Die Vernehmlassung zum neuen Gesetz soll Mitte 2022 eröffnet werden. Die EU hat ein Framework für eine europäische SSI erstellt, Pilotprojekte sind für die kommenden Jahre geplant. Auch Nordamerika geht diesen Weg: Die Standardisierungsorganisation W3C erarbeitet derzeit einen Standard für Self-Sovereign-Identitäten. Aus datenschutzrechtlicher Sicht ist die SSI eine gute Lösung: Sie funktioniert im Einklang mit den zurzeit verbreiteten Regelungen zur Verarbeitung von personenbezogenen Daten. Zudem erleichtert eine dezentrale Identifikation das Datenmanagement für Anbieter: Dank dem Peer-to-Peer-Charakter der SSI sind grundsätzlich weniger Dienstleister in die Datenmanagementkette involviert. Und weil sie weniger sensible Daten speichern, haben Datenpannen weniger dramatische Folgen.

Nutzer:innen haben die Daten in der Hand

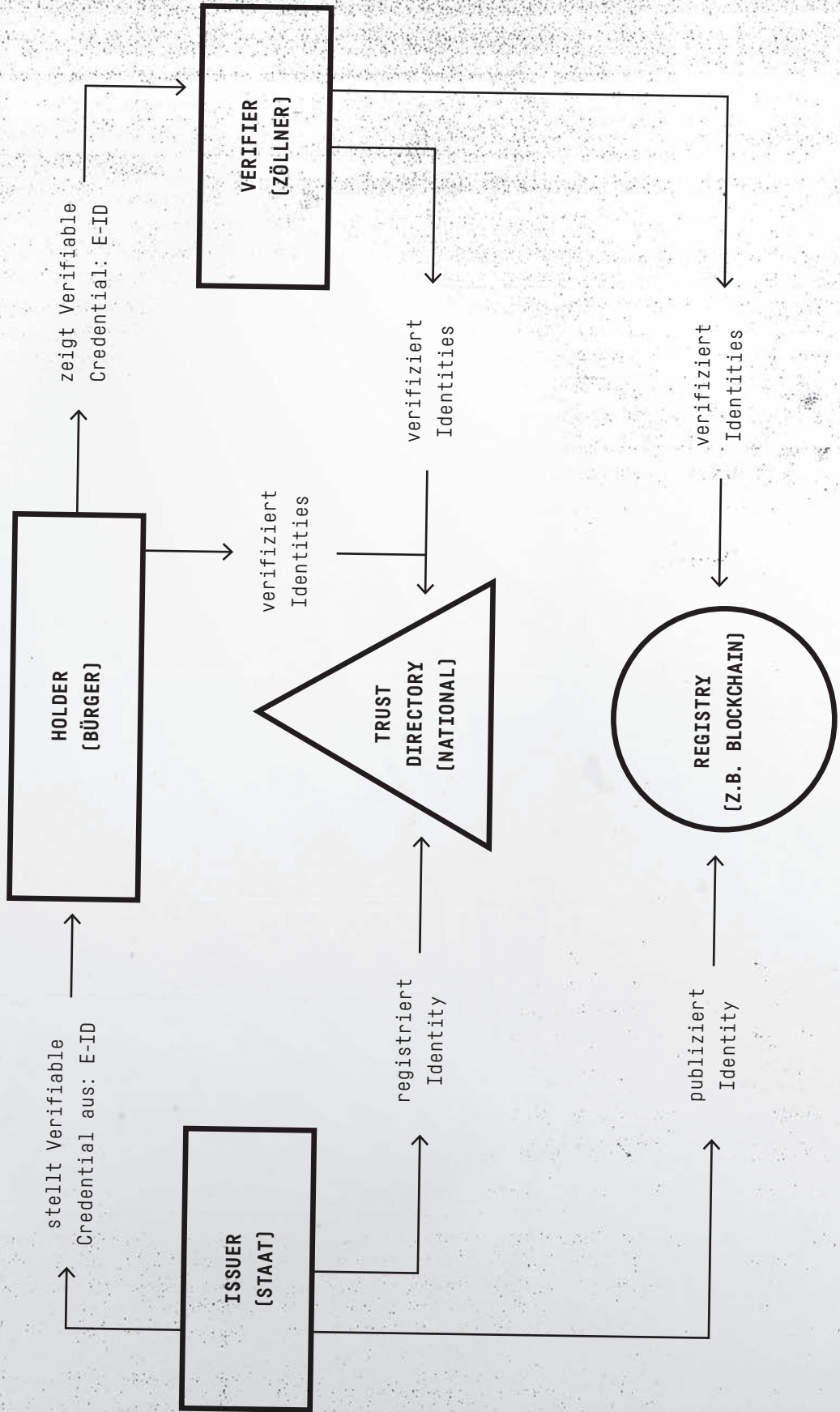
Die Dezentralisierung der SSI ist ein Paradigmenwechsel: Es sind nicht mehr die Anbieter, die Authentifizierungsdaten

verwalten, sondern die Nutzer:innen selbst. Dazu speichern sie verifizierte Identitätsdaten – sogenannte Credentials – in einer Wallet auf dem Smartphone oder einem anderen Gerät. Vom Führerschein über ein Zeugnis bis zur Social-Media-Historie sind diese Credentials weit breiter gefasst als der analoge Reisepass oder die Identitätskarte. Ein Issuer bezeugt die Richtigkeit der Credentials elektronisch – und die Anbieter, auf Neudeutsch Verifier, überprüfen sie ebenfalls auf elektronischem Weg. Welche Daten ein Verifier sieht, entscheiden die Besitzer:innen der Wallet: die Holder oder Nutzer:innen. Denn sie, und nur sie, haben die Hoheit über ihre Daten – ein Privileg, das auch mit Pflichten einhergeht. Wer beispielsweise seine Wallet verliert, muss sich um Ersatz für alle Ausweise und Dokumente kümmern. Dafür entfallen komplizierte Login-Verfahren und die damit einhergehende Passwortverwaltung.

Das kann die SSI im Alltag

Eine SSI hat viele Vorteile. Banken beispielsweise profitieren von der anerkannten digitalen E-ID: Statt in der Filiale vor Ort oder einem komplizierten Online-Identifizierungsverfahren reicht es, wenn der:die Kund:in die Wallet zückt und die erforderlichen Credentials bereithält. Die Automiete wird dank SSI ebenfalls einfacher, wenn das Kopieren von Identitätskarte und Führerausweis entfällt. Womöglich können Mieter:innen sogar direkt einsteigen und losfahren,

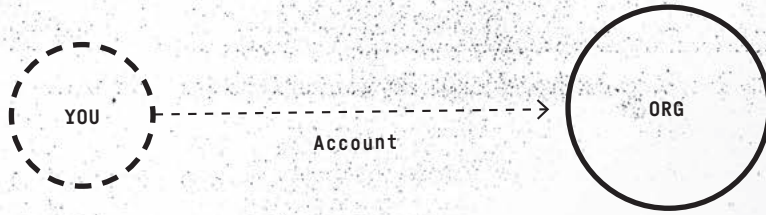
SSI-Konzept am Beispiel der E-ID



Drei Arten von Digital Identities

Beschreibung

SILO



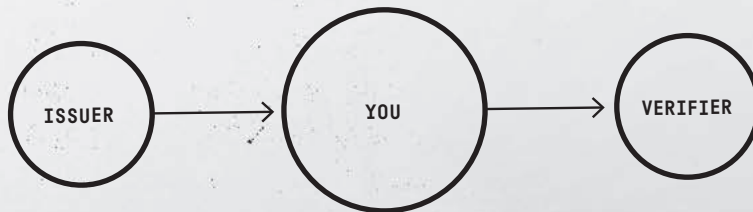
- Benutzer:innen pflegen einen eigenen User Account für jeden Anbieter
- Das älteste und am meisten verwendete Modell der digitalen Identitätsbeziehung

IDENTITY PROVIDER



- Benutzer:innen pflegen ihren User Account bei einem Identitätsanbieter
- Der Identitätsanbieter bestätigt die Identität gegenüber Dienstleistern

SSI



- Holder [Benutzer:in] hat eine eigene Wallet und speichert darin seine verifizierten, persönlichen Daten
- Issuer, denen der Holder vertraut, dürfen Daten in sein Wallet legen
- Verifier [Dienstleister] erhält nur die Daten, die Holder freigeben

Pros

- Weit etabliert
- Dienstanbieter verwaltet Compliance, Haftung und andere Risiken
- Guter Schutz der Privatsphäre, weil keine zentrale Stelle involviert ist
- Gut akzeptiert in der Bevölkerung

Contras

- Skaliert sehr schlecht für Individuen
- Wiederverwendung von Passwörtern ist ein Sicherheitsrisiko
- Personen verlieren den Überblick. Wo habe ich Profile kreiert?
- Jeder Dienstanbieter muss ein Experte für Identitätsmanagement und Sicherheit werden
- Die Authentifizierung ist einseitig und nicht gegenseitig → ermöglicht Phishing

- Benutzer:innen können die Anzahl direkt gepflegter User Accounts (und Passwörter) reduzieren
- Identitätsanbieter bieten ein SSO Erlebnis
- Für Dienstanbieter einfach und mit wenig Integrationsaufwand umzusetzen

- Ungenügender Schutz der Privatsphäre: Der Identitätsanbieter kennt alle meine Dienstanbieter
- Nur wenige Dienstanbieter akzeptieren Identitätsanbieter
- Die meisten Identitätsanbieter arbeiten auf tiefem Vertrauensniveau und sind ungeeignet für E-Banking oder Gesundheitswesen
- Der Identitätsanbieter verfügt über einen grossen Bestand an persönlichen Informationen → Sicherheitsrisiko
- Die Authentifizierung ist einseitig und nicht gegenseitig → ermöglicht Phishing
- Funktioniert nur für Personen und nicht für die Authentifizierung von Firmen oder Dingen

- Holder behalten die Kontrolle über ihre Daten
- Hoher Schutz der Privatsphäre, weil es keine zentrale Instanz gibt, die den Holder überwachen könnte
- Verifier erhalten verifizierte Daten
- Issuer können Daten für ungültig erklären (z.B. Wohnadresse)
- Daten können nach einer gewissen Zeit die Gültigkeit verlieren (z.B. Billett)
- Standardisiert und interoperabel → keine Herstellerabhängigkeit
- Beim Anbieterwechsel gehen die eigenen Zugangsdaten/Beziehungen/Historien nicht verloren

- Standards sind erst am Entstehen und können sich noch ändern
- Lösungen, wie Holder ihr Wallet gegen Defekt oder Verlust schützen, müssen noch erarbeitet werden
- Vorbehalte und Sicherheitsbedenken in der Bevölkerung, weil die Technologie komplex und noch wenig verbreitet ist

«SSI revolutioniert unsere digitalen Interaktionen.»

_Catharina Dekker, Consultant,
catharina.dekker@ergon.ch



weil das smarte Auto den Fahrzeugschlüssel als Verifiable Credential (VC) in der Wallet findet und prüft.

Auch digital zertifizierte Dokumente wie Zeugnisse oder Diplome erleichtern den digitalen Bewerbungsprozess - und potenzielle Arbeitgeber prüfen die Echtheit der Unterlagen automatisiert.

Um einen Jugend- oder Seniorenrabatt zu gewähren, muss das Alter der Person bekannt sein. Es besteht aber keine Notwendigkeit, einem Verkehrsbetrieb oder einem Museum das exakte Geburtsdatum offenzulegen. Wenn man dazu noch berücksichtigt, dass in der Schweiz 99,999% aller Personen durch den vollständigen Namen und das Geburtsdatum eindeutig identifiziert sind, dann wird klar, dass die Bearbeitung des Geburtsdatums aus Sicht des Datenschutzes besonders kritisch ist.

Im E-Commerce profitieren Händler dank SSI von einer sofortigen Bonitätsprüfung und einem schnellen Bezahlprozess. Und zwar mit einem Credential, das direkt mit der Bank der Käufer:innen verknüpft ist. Sichergehen können auch Käufer:innen, dass sie beim richtigen Online-Shop einkaufen und kein Geld verlieren - durch Überprüfung der Händler-Credentials.

Breit gefasster Identitätsbegriff

Credentials sind nicht zwingend auf Individuen begrenzt. Auch Unternehmen und Institutionen können eine SSI erhalten und diese in der Kommunikation mit Kund:innen und Lieferanten nutzen. Das kann zum Beispiel die neue Bankbeziehung für die Rechnungsstellung an Kund:innen oder der aktuelle Handelsregisterauszug für Lieferanten und Partner sein. Es wäre sogar vorstellbar, dass autonome Fahrzeuge ihre eigene Wallet bekommen, mit der sie

dann etwa gegenüber Mautstellen oder Werkstätten wirtschaftlich autark agieren könnten. Ihre «Identität» wäre in diesem Fall zum Beispiel an die Fahrzeugidentifikationsnummer gebunden.

Diese Beispiele zeigen, dass das Potenzial der SSI enorm ist. Löst der Staat das Henne-Ei-Problem der Einführung, so dürften sich immer mehr Use Cases auch wirtschaftlich rechnen. Zumal die Digitalisierung mit Riesenschritten weiter voranschreitet. Das McKinsey Global Institute hat prognostiziert, dass im Jahr 2030 die Nutzung digitaler Identitäten in Industrieländern einen wirtschaftlichen Wert von 3% des Bruttoinlandsprodukts freisetzt, in Schwellenländern sogar von 6%.

Lässt sich Vertrauen verwalten?

Bei allen Vorteilen, die eine Self-Sovereign Identity mit sich bringt, gibt es auch



«Die Frage ist nicht, ob SSI kommt. Sondern wann.»
 _Michael Doujak, Product Manager
 Airlock, michael.doujak@ergon.ch

Herausforderungen. Wie stellt man zum Beispiel sicher, dass die Issuer wirklich vertrauenswürdig sind? Eine Lösung liegt im Aufbau vertrauenswürdiger Verzeichnisse. Hier können sich Issuer - beispielsweise eine Krankenkasse - prüfen lassen und erhalten einen Eintrag, den Verifier und Holder einsehen können. Für Behörden bietet sich ein staatliches Verzeichnis an. So wird Vertrauen quasi verwaltet. Ein anderes Problem liegt im Life Cycle Management der Credentials. Wie lassen sie sich rechtssicher aktualisieren? Was geschieht, wenn jemand seine Wallet verloren hat oder ein Credential mit Ablaufdatum versehen worden ist? Auch hier gilt es, einen Weg zu finden, digitales Vertrauen zu schaffen.

Early Adopters profitieren
 Auch wenn es noch offene Fragen gibt: Self-Sovereign

Identity wird enorme wirtschaftliche Werte freisetzen. Wer schon jetzt erste Erfahrungen damit sammeln will, kann vorhandene Open-Source-Technologien nutzen. Mit einem gelungenen Proof-of-Concept erkennen Unternehmen die Möglichkeiten der neuen Technologie und können sie besser abschöpfen. Denn SSI ist viel mehr als eine digitale Identitätskarte: Sie führt den Begriff der Identität in

Dimensionen, die sich heute noch nicht erahnen lassen. Wenn wir als Nutzer:innen unsere digitale Identität voll unter Kontrolle haben, verändert das auch unseren Umgang mit Privatsphäre im digitalen Raum. Wir können zwar keine Prinzen, Models oder Milliardenerinnen sein - aber unsere digitalen Beziehungen und Interaktionen werden eine neue Gestalt annehmen. />

Lust auf mehr?

**Digitalisierungsvorhaben
 Zukunftsmacher:innen
 Tech-Trends**

Jetzt bestellen
ergon.ch/smart2022

