Matthias Fuhrland, Christopher Praas, Jürgen Anke (HTW Dresden),
André Röder (KAPRION Technologies GmbH), 2023

Trustnet

Das Prinzip der selbstsouveränen Identitäten (SSI)

Selbstsouveräne oder selbstbestimmte digitale Identitäten sind ein Konzept, bei dem die Verwaltung der eigenen Identitätsdaten in die Hände der Nutzer gelegt wird. Der Nutzer gewinnt damit die Hoheit über seine eigenen Daten, die nur für ihn zugreifbar in seiner digitalen Wallet gespeichert sind. Die Wallet ist eine digitale Brieftasche. Vergleichbar mit dem Portemonnaie werden darin Ausweisdokumente (eID, digitaler Führerschein, Bankkarte etc.) und Nachweisdokumente (amtl. Bescheinigungen, Registerauszüge, Berechtigungsnachweise, Urkunden u. ä.) sowie werthaltige und weitere Arten von Credentials abgelegt. Mit SSI geht der Begriff der digitalen Identität deutlich über das hinaus, was im Kontext hoheitlicher Identitätslösungen (eID) diskutiert wird. Das SSI-Prinzip ist ein Gegenentwurf zu den aktuell genutzten Konzepten, bei denen ein Nutzer verschiedene Identitäten bei verschiedenen Identitätsanbietern besitzt, die in der Regel die Kontrolle über die Daten haben. Mit SSI hat der Nutzer alleinigen Zugriff auf seine ID-Daten und kann entscheiden, welche Teile davon er wem zur Verfügung stellt. ID-Dienste liefern dafür die für den Nutzer primäre Infrastruktur, z.B. in Form von sicheren Cloudspeichern oder Wallet-Apps für Smartphones. Mit SSI lassen sich nicht nur digitale Identitäten natürlicher Personen abbilden, sondern auch digitale Identitäten von juristischen Personen, hoheitlichen Entitäten undObjekten. Es lassen sich auch Beziehungen einer natürlichen Person zu anderen natürlichen Personen, zu juristischen Personen und zu Objekten digital abbilden und gesichert nachweisen. Mit dem SSI-Prinzip lässt sich jede Art von überprüfbaren Nachweisen (**Verifiable Credentials**) digital herausgeben, vorzeigen und verifizieren. Damit wird das SSI-Prinzip zum Gamechanger im Kontext des Trustnets.

Es gibt verschiedene **Rollen der Akteure im Trustnet**. Ein Akteur kann bei unterschiedlichen Interaktionen unterschiedliche Rollen einnehmen:

Der *Herausgeber (Issuer)* ist ein Akteur, der einen digitalen Nachweis ausstellt und dem ID-Inhaber übergibt. Im Ausstellungsprozess wird durch eine digitale Signatur sichergestellt, dass der Nachweis vom Herausgeber selbst stammt und dass er auf den korrespondierenden kryptografischen Schlüssel des Holders ausgestellt ist. Gleichzeitig kümmert sich der Herausgeber darum, dass die ausgestellten Nachweise ungültig gemacht werden, falls notwendig. Im Hinblick auf die hohe Vertrauenswürdigkeit hoheitlicher Register wurde für diese der Begriff *Trusted Issuer* geprägt.

Der *Inhaber (Holder)* ist ein Akteur, welcher digitale Nachweise vom Herausgeber entgegennimmt und sie sicher in seiner Wallet speichert. Die digitalen Nachweise des Inhabers können unabhängig vom Herausgeber gegenüber anderen Parteien präsentiert werden.

Die *Akzeptanzstelle (Verifier)* ist ein Akteur, welcher den Nachweis vom Inhaber entgegennimmt und ihn auf Richtigkeit überprüft. Anhand des Ausstellungsprozesses vertraut die Akzeptanzstelle dem Herausgeber und gewährt dem ID-Inhaber nach erfolgreichem Prüfprozess die angefragten Rechte.

Der *Modifizierer (Modifier)* ist ein Akteur, der in enger Beziehung zum Herausgeber steht und die Möglichkeit hat, den Nachweisstatus zu ändern. Oft ist der Herausgeber gleichzeitig auch der Modifizierer, jedoch gibt es einige Fälle, bei denen der Modifizierer eine separate Partei ist, z.B. die Polizei, die den digitalen Führerschein nach einem Verkehrsdelikt entzieht.

Die für diese Interaktionen erforderliche Wallet-App auf dem digitalen Endgerät des Inhabers besteht aus der Wallet, in der die Nachweise gespeichert werden, und einem digitalen Agent. Der Agent übernimmt dabei die digitale Kommunikation inkl. der Herausgabe und Prüfung von Nachweisen.

r

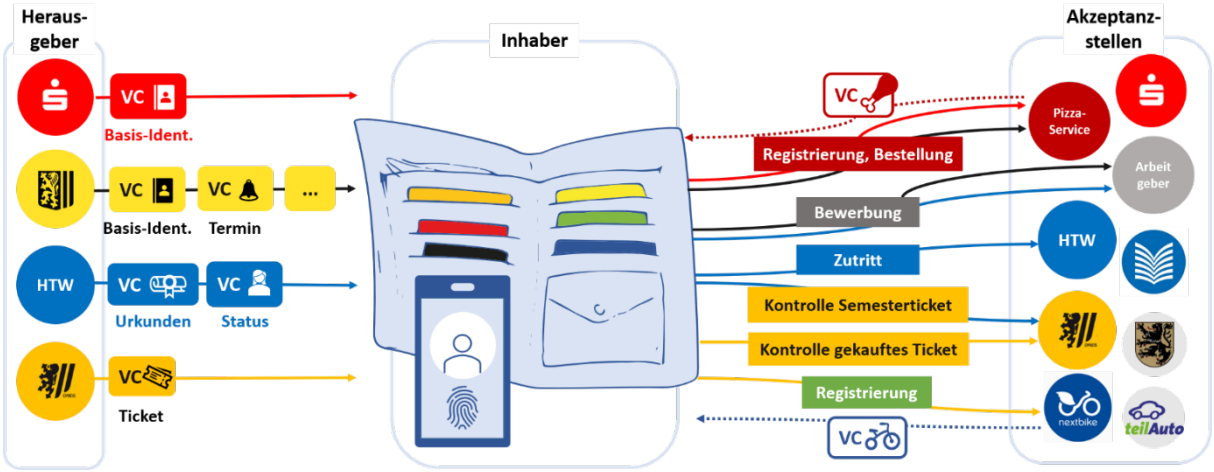

Abb. 1: einfache Rollenverteilung im SSI-Kontext

Bei Erklärungen zum SSI-Prinzip wird die Rollenverteilung üblicherweise als einfache Dreiecksbeziehung zwischen Herausgeber, ID-Inhaber und Akzeptanzstelle dargestellt (siehe Abb. 1). Die Dreiecksbeziehung entsteht, indem die Akzeptanzstelle die Herausgeberschaft eines vom Inhaber präsentierten Nachweises prüft. Betrachtet man allerdings den gesamten Prozess einer Anwendung, wird schnell klar, dass diese Rollenverteilung sich nur auf eine einzelne Interaktion bezieht. Selbst innerhalb eines einfach erscheinenden Prozesses, wie dem Kauf eines ÖPNV-Tickets, nehmen Käufer und Verkäufer nacheinander unterschiedliche Rollen ein. Das in Abb. 2 dargestellte Prozessbeispiel des Online-Kaufs einer ermäßigten ÖPNV-Monatskarte zeigt, dass innerhalb des rein digitalen Geschäftsprozesses sowohl Käufer als auch Verkäufer jeweils drei verschiedene Rollen einnehmen und dabei auch verschiedene Nachweise austauschen müssen. Entsprechend muss für diese Variabilität auf beiden Seiten die dafür erforderliche Funktionalität und Interoperabilität bei Wallet und Agent gegeben sein.

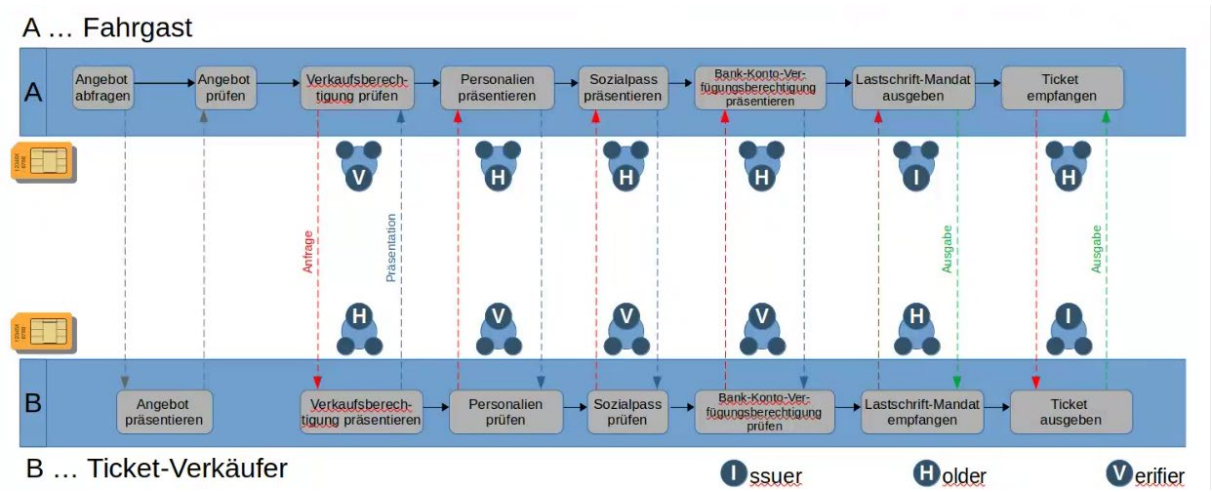

Abb. 2: Wechselnde Rollen in einem digitalen Geschäftsprozess