Bosch Research

Economy of Things – Contributions to the Community

Self-Sovereign Identities (SSI): nutzerzentriertes Konzept für ein datensparsames Identitätsmanagement

Renningen, 18. November 2021 – Damit Privatpersonen, Unternehmen und Dinge digital sicher interagieren, Geschäfte machen und sich vernetzen können, ist ein vertrauenswürdiges und verlässliches Identitätssystem nötig. Wenn die Authentifizierung von Mensch, Organisation und Maschine zudem sehr nutzerzentriert sein soll, ist ein Ansatz gefragt, der Datensparsamkeit und -souveränität in den Mittelpunkt stellt. „Weil die Kontrolle und Selbstbestimmtheit über die eigenen Daten ein höchst erstrebenswertes Ziel ist, bauen wir gemeinsam mit Innovationspartnern ein Identitätssystem auf, das ohne zentralisierte Datensammler auskommt und von vielen Teilnehmern gleichermaßen betrieben wird“, so Dr. Nik Scharmann, Projektdirektor des strategischen Vorausentwicklungsprojekts „Economy of Things“ (EoT) bei Bosch Research. Der Ansatz der Wahl lautet Self-Sovereign Identities, kurz SSI.

SSI-Technologie: dezentral und domänenübergreifend

Prägende Merkmale einer solchen Identitätsdaten-Infrastruktur sind ihr dezentraler Aufbau, Datensparsamkeit und ihre domänenübergreifende Funktionsweise. Wenn digitale Identitäten dezentral verwaltet werden, sind diese folglich unabhängig von einer Zwischeninstanz, die die Daten speichert und zentral verwaltet. Denn sobald Dritte als zentrales Scharnier im Spiel sind, verlieren Anwendende meist die Kontrolle darüber, was mit den Daten geschieht und wer sie einsehen kann. Ganz anders bei SSI, hier werden die Identitätsattribute wie eine Maschinen-ID, persönliche Geburtsdaten oder Firmenstammdaten direkt beim Eigentümer der Identität verwaltet, die Identität selbst dezentral: Den einen zentralen Dienst, der wie bei Logins oder Passnachweisen mittels Video-Ident von einem Dritten kontrolliert wird, gibt es bei der SSI-Technologie nicht. Mit SSI werden nur die öffentlichen Schlüssel, die zur Verifikation von Identitätsmerkmalen notwendig sind, dezentral gespeichert – zum Beispiel auf einer Blockchain. Diese Blockchain wird dezentral von vielen unabhängigen Servern betrieben und schützt damit deutlich besser gegen den Einfluss und vor Manipulation einzelner Akteure. Experten sprechen in diesem Zusammenhang von Distributed Ledger Technologies (DLT). Dabei handelt es sich im Identitätskontext technisch betrachtet um eine dezentrale Synchronisationsschicht für kryptographisches Material, das zur Verifikation von Attributen notwendig ist – eine sogenannte „decentralized Public Key Infrastructure (dPKI)“. Globale Standards, die im World Wide Web Consortium und in der Decentralized Identity Foundation vorangetrieben werden, sowie Open-Source-Veröffentlichungen von Standardkomponenten, sollen die Interaktion verschiedener IT-Systeme sowie die Teilnahme jedes Akteurs unabhängig von Dritten ermöglichen.

Die Identitäten können dabei von jedem Akteur selbst erzeugt und verwaltet werden – ohne Klartextdaten an einen externen Dienst abgeben zu müssen beispielsweise. „Die SSI-Technologie vernetzt Menschen, Unternehmen und Maschinen durch eine einheitliche Basis und baut damit Hürden in der digitalen Interaktion ab“, ist Stephan Hoeh, Head of Product Area User Management bei Bosch.IO, überzeugt. Er ist bei der Bosch-Tochter dafür zuständig, dass der SSI-Ansatz zu Produktentwicklungen führt. Das kann nutzerseitig in folgenden Anwendungen münden: Anstatt bei jeder Aktion wieder neu Daten pauschal preisgeben zu müssen – beim Kauf eines Bahntickets, bei der Fahrt mit dem Mietwagen, beim Einchecken ins Hotel – zücken User

Contact: Nik Scharmann, Project Director “Economy of Things”, Nik.Scharmann.ext@de.bosch.com
Christian Heise, Deputy Project Director “Economy of Things”, Christian.Heise.ext@de.bosch.com

eine Art digitales Portemonnaie (Wallet) und erlauben den Zugriff, ohne unnötig Daten aus der Hand zu geben. Denn mit SSI können Identitätsdaten selektiv preisgegeben werden, d.h. Eigentümer und Eigentümerinnen der Daten können wählen, welche Daten oder auch nur Auszüge von Dokumenten unter welchen Umständen geteilt werden sollen. Nur der Nachname beispielsweise. Durch die Nutzung von kryptographischen Verfahren kann bewiesen werden, dass diese Auswahl von Daten wahrhaftig auf die korrekten Identitätsdaten verweist. Die Herausgabe von Informationen reduziert sich durch die SSI-Technologie auf ein notwendiges Minimum – und das über alle Branchen und Sektoren hinweg: „Das SSI-System ist in der Lage, sehr viele Domänengrenzen zu überwinden ohne die Kontrolle über Daten abgeben zu müssen. Das können die gängigen Lösungen am Markt nicht so einfach abbilden“, sagt Nik Scharmann.

Die Herausgabe von Identitätsdaten reduziert sich durch die SSI-Technologie auf ein notwendiges Minimum – und das über alle Branchen und Sektoren hinweg.

Einsatz in kollaborativen Datenraumprojekten

SSI nimmt in Deutschland und auch Europa gerade Fahrt auf, angetrieben durch das Entstehen kollaborativer Datenraumprojekte. Neben Fragen rund um SSI besteht die große Herausforderung darin, alle Akteure so zu steuern, dass der Nutzen des Ökosystems für alle im Vordergrund des Handels steht. Damit eine Ökonomie der Dinge offen, neutral und nachhaltig betrieben werden kann und ohne monopolähnliche Plattformbetreiber auskommt, braucht es ein Regelwerk (Good Governance), in dem die notwendige Struktur und der Prozess der Zusammenarbeit transparent dargelegt sind. Die Regeln der Governance werden durch Verträge festgeschrieben und sichern der Kooperation so Rechtssicherheit und Stabilität. Die Kunst ist, die richtige Balance zu finden zwischen Veränderung und Festlegung des Regelwerks. Große Kooperationsprojekte rund um Datenplattformen haben in der Vergangenheit gezeigt, dass klassische Organisationsstrukturen nicht hilfreich sind, um langfristig wirtschaftlich effizient zu arbeiten. Gleichzeitig können vollständig dezentralisierte digitale Plattform keine Organisation ersetzen! Deshalb ist es das Forschungsziel des EoT-Teams, technische Dezentralisierung und zentrale Steuerungsorgane im Sinne eines optimalen ökonomischen Systems zu kombinieren. Nik Scharmanns Fazit: „Wir sind entschlossen, die vielschichtigen Herausforderungen der Kryptologie, Ökonomie, Rechtswissenschaften und Softwareentwicklung zu meistern, um eine resiliente Business-Grundlage für erfolgreiche kooperative Datenräume zu schaffen.“