Bankstil

Selbstverwaltete Digitale Identitäten für Personen und Maschinen

Aktuelle Marktentwicklung und Ausblick

Ralf Keuper

November 2019

Zusammenfassung **2**

Einführung **4**

Definition: Selbstverwaltete Digitale Identitäten **6**

Initiativen, Lösungen, Startups **7**

Idealtypischer Ablauf **10**

Selbstverwaltete Digitale Identitäten für Maschinen **12**

Agentenbasierte Identitäten als Bindeglied **14**

Blockchain nicht zwangsläufig Mittel der Wahl **16**

eIDAS und SSI **17**

Hindernisse **18**

Potenzielle Geschäfts- und Rollenmodelle **20**

Ausblick **22**

Zusammenfassung

Im Internet haben wir die für eine freiheitliche Gesellschaft paradoxe Situation, dass die Nutzer nicht autonom über die Verwendung ihrer digitalen Identitäten entscheiden können. Bislang scheint das die Mehrzahl der Nutzer nicht sonderlich zu beunruhigen. Meldungen und Berichte über Identitätsdiebstähle und Datenskandale sorgen zwar für Empörung, auf das Verhalten der Nutzer im Internet hat das indes kaum Auswirkungen.

Mit der Möglichkeit, auf sichere und komfortable Weise die eigenen digitalen Identitäten selbständig zu managen, könnte sich das ändern. Noch steckt die Entwicklung, insbesondere in Deutschland, in den Kinderschuhen. Dennoch sind in vergangenen Jahren weltweit zahlreiche Initiativen und Lösungen entstanden, die für die Verbreitung selbstverwalteter Digitaler Identitäten sorgen wollen, wie Sovrin oder der Bundesverband Blockchain (Bundesblock). Auch die Unternehmen erkennen langsam das Potenzial selbstverwalteter Digitaler Identitäten, wenn es darum geht, Betrug zu verhindern und die Kundenbindung zu stärken. Die Nutzer und Kunden hätten den Vorteil, selber über die Herausgabe und Verwendung ihrer Identitätsdaten entscheiden zu können. Nur die Daten, die für einen bestimmten Vorgang nötig sind, werden freigegeben. Weiterhin können die Nutzer sich anonym mit ihrer verifizierten Identität bewegen; sie müssen sich also nicht mehr mit ungewünschter Werbung beschäftigen. Denkbar ist, dass die Nutzer ihre Daten Dritten - gegen Entgelt oder bessere Konditionen - zur Verfügung stellen.

Identitätsdienstleister haben die Chance, sich über die Qualität der von ihnen verifizierten Identitäten/Identitätsmerkmale und durch Zusatzservices von ihren Mitbewerbern abzusetzen.

Großes, weitgehend noch ungenutztes Potenzial schlummert bei den Identitäten für Maschinen. Vorstellbar sind Technologiedatenmarktplätze, auf denen die Identitätsmerkmale (Claims) der Maschinen gehandelt werden. Die Maschinen agieren dabei weitgehend autonom. Mittel- bis langfristig könnte daraus eine neue Asset-Klasse entstehen. Der Industrie und den Anlegern würden sich dadurch ganz neue Einnahme- und Finanzierungsquellen eröffnen.

Der vorliegende Report kommt zu dem Ergebnis, dass, wenn wir in Deutschland und Europa unseren Wohlstand erhalten und an der Wahlfreiheit der Bürger als dessen Quelle festhalten wollen, kaum ein Weg an der

Einführung zumindest dezentraler, nach Möglichkeit jedoch selbstverwalteter Digitaler Identitäten vor bei führt.

Einführung

Angesichts der wachsenden Zahl von Identitätsdiebstählen und Datenskandalen fühlen sich die Nutzer im Internet zunehmend unbehaglich. Das hat bislang jedoch noch nicht zu einem veränderten Nutzerverhalten geführt. Die Abhängigkeit von den großen Plattformen und Diensten wie facebook und Google ist inzwischen so groß, dass der Versuch, sich aus dieser Umklammerung zu befreien, zwecklos erscheint. Hinzu kommt, dass sich die Nutzer an den Komfort der Services gewöhnt haben und einem Wechsel zu anderen Anbietern, so sie überhaupt vorhanden sind, nicht ernsthaft ins Auge fassen. In der Tat: Die vorhandenen Alternativen sind kaum verlockend – wer will sich auf einer Plattform bewegen, die von seinen Freunden und Bekannten nicht genutzt und von den etablierten Lösungen nicht unterstützt wird. Außerdem kann man seine Identitätsdaten nicht mitnehmen. Die volle Kontrolle über ihre Daten haben die Nutzer ohnehin nicht. Was genau mit ihren Daten geschieht, bleibt unklar.

Sicherlich hat die Datenschutzgrundverordnung zu einer Sensibilisierung bei den Unternehmen bei der Verwendung der personenbezogenen Daten der Kunden geführt. Gleichwohl bleibt es beim Kurieren an den Symptomen. Besser wäre es, die Probleme an der Quelle zu beheben, d.h. bei den digitalen Identitäten, mit denen sich die Nutzer, wie mit den Logins von facebook und Google, im Netz bewegen. Das würde bedeuten, den Nutzern die Kontrolle über ihre Digitalen Identitäten zurückzugeben. Nur sie bestimmen, wer, für welchen Zweck und für wie lange die personenbezogenen Daten einsehen kann. Hoffnung versprechen die Lösungen, die unter dem Sammelbegriff *Selbstverwaltete Digitale Identitäten* (Self Sovereign Identities) zusammengefasst werden.

Auch Maschinen sollten künftig die Möglichkeilt haben, über die Verwendung ihrer Identitätsmerkmale autonom bestimmen zu können. Daraus könnten neue Asset-Klassen und Einnahmequellen für Unternehmen und Anleger entstehen.

In den letzten zwei Jahren sind überall auf der Welt Initiativen und Lösungen entstanden, die sich dem Prinzip der Selbstverwalteten Identitäten verschrieben haben. Deutschland ist auch hier, wie auf vielen anderen Gebieten der Digitalisierung, nur schwach vertreten. Eine der wenigen Stimmen hierzulande ist der Bundesblock, der im vergangenen Jahr sein Positionspapier zu den Selbstverwalteten Digitalen Identitäten veröffentlicht

hat. Daneben sind einige Startups dabei, die Idee Wirklichkeit werden zu lassen. Dennoch: Gemessen an der wirtschaftlichen Bedeutung und dem immer noch vorhandenen technologischen und wissenschaftlichen Potenzial, ist Deutschland bei der Entwicklung und Anwendung Selbstverwalteter Digitaler Identitäten im Vergleich zu den meisten Nachbarländern, rückständig. Das steht im Kontrast zu dem föderativen, dezentralen Gliederung des Landes, die nicht immer vorteilhaft ist, hier jedoch ihre Stärken zur Geltung bringen könnte.

Inzwischen haben Politik und Wirtschaft, wie auf dem jüngsten Digitalgipfel in Dortmund, erkannt, wie wichtig die digitale Souveränität für ein Land und einen Kontinent ist. Digitale Souveränität meint Selbstbestimmung, wie sie der humanistischen Tradition Europas entspricht. Selbstbestimmung heißt nicht völlige Unabhängigkeit, sondern bedeutet die Fähigkeit, zwischen mehreren Alternativen wählen zu können. Das gilt besonders auf der Ebene der Individuen. Eine florierende Wirtschaft ist heute mehr denn je auf selbständig handelnde und denkende Individuen angewiesen, die wiederum einzigartige Unternehmen bilden, wie im Mittelstand. Das jedenfalls sollte der europäische Ansatz sein.

Die vorliegende Publikation verfolgt das Ziel, eine Übersicht über den aktuellen Markt für Selbstverwaltete Digitale Identitäten und die wichtigsten sich abzeichnenden Trends zu geben.

Definition: Selbstverwaltete Digitale Identitäten

Welche Voraussetzungen müssen digitale Identitäten erfüllen, um als selbstverwaltet zu gelten? Vor einigen Jahren hat Christopher Allen in The Path to Self-Sovereign Identity zehn Kriterien benannt, die Selbstverwaltete Digitale Identitäten abdecken müssen.

Prinzipien Selbstverwalteter Digitaler Identitäten (Christopher Allen)

Existenz *– Nutzer muss über eine unabhängige (personale) Existenz verfügen.*

Kontrolle: *Nutzer haben die volle Kontrolle über ihre Digitalen Identitäten.*

Zugang*: Nutzer müssen unbeschränkten Zugriff auf ihre Identitäten haben.*

Transparenz*: Funktionsweise der Systeme und Algorithmen muss transparent sein.*

Persistenz*: Identitäten müssen dauerhaft und kohärent sein.*

Portabilität*: Identitätsdaten müssen zwischen verschiedenen Services portabel sein.*

Interoperabilität*: Die Identitäten müssen an möglichst vielen Stellen verwendbar sein.*

Konsens: *Nutzer müssen der Verwendung ihrer Identitäten zustimmen.*

Minimalisierung: *Offenlegung nur der wirklich benötigten Identitätsmerkmale*

Schutz*: Rechte der Nutzer müssen geschützt werden.*

Die meisten Projekte und Initiativen im SSI-Umfeld berufen sich auf die von Allen formulierten Prinzipien[1].

[1] In dem Workshop Self Sovereign Identity (SSI) zählt esatus weitere Merkmale und Vorteile selbstverwalteter Identitäten auf.

Initiativen, Lösungen, Startups

Als Antwort auf die zunehmende Abhängigkeit der Nutzer von den großen Datenkonzernen und der häufig fehlenden Transparenz über die Verwendung der Daten, haben sich in den letzten Jahren zahlreiche Initiativen gebildet, die Selbstverwalteten Digitalen Identitäten zum Durchbruch verhelfen wollen. Daneben haben Startups auf der ganzen Welt entsprechende Lösungen entwickelt. Einen großen Anteil stellen Lösungen und Initiativen, bei denen Fragen der Betrugsprävention und die Kundenbindung im Vordergrund stehen. Einen weiteren Schwerpunkt bilden Lösungen, welche Digitale Identitäten und Payments kombinieren. Nur wenige Lösungen konzentrieren sich auf die Bereitstellung Selbstverwalteter Digitaler Identitäten rein aus Nutzersicht.

Im privatwirtschaftlichen Bereich sind es vor allem Banken und Telekommunikationsunternehmen, die ihren Kunden die Möglichkeit geben wollen, ihre digitalen Identitäten selbst zu verwalten, wobei die Banken wiederum als erste Anlaufstelle und Vertrauensanker fungieren. Auf der anderen Seite sind regionale Regierungen wie in Alberta (Kanada) und Katalonien bestrebt, die Bürgernähe durch die Unterstützung selbstverwalteter Digitaler Identitäten zu stärken. Es fällt auf, dass Regionen mit einem ausgeprägten Hang zur Autonomie, wie Schottland, Flamen und Katalonien, beim Thema SSI besonders engagiert sind. Auf nationalstaatlicher oder gar EU-Ebene gehen die Bestrebungen derzeit nicht über Fördermaßnahmen und die Veröffentlichung von Positionspapieren hinaus. Neben Banken und Telekommunikationsunternehmen bieten auch einige IT-Unternehmen eigene Lösungen an. Die bevorzugte Technologie der meisten Initiativen und Applikationen/Wallets ist die Blockchain. Was die geografische Verteilung betrifft, ist Europa gut vertreten. Die USA sind im Vergleich dazu eher unterrepräsentiert. Zwar stammen viele Initiativen wie Sovrin aus den USA, im Land selber jedoch ist die Resonanz in Wirtschaft und Gesellschaft sowie bei staatlichen Stellen eher verhalten, was sicherlich auch damit zusammenhängt, dass Google, facebook, Apple und Amazon hier besonders präsent sind. Zu den wenigen Ausnahmen zählt der US-Bundesstaat Illinois.

In der nachfolgenden Tabelle sind die im Rahmen dieser Studie recherchierten Lösungen, Initiativen und Startups aus aller Welt aufgeführt.

Name	Träger / Initiator / Hersteller
Selfkey	Stiftung
myIDsafe	Konsortium (Österreichische Staatsdruckerei, Banken, Medien- und Technologieunternehmen)
Cordentity	Mit Corda verbundene Systemintegratoren, Beratungsfirmen und Softwarehäuser
Opera	Opera
Seraph ID	Swisscom Blockchain
IdentiCAT	Staat Katalonien
Findy	Findy Konsortium
Jolocom	Jolocom
streetcredid	Streetcred
Blockchain Helix	Helix AG
uPort	ConsenSys
Civic	Civic
Tykn	Tykn B.V.
EverID	Everest.org
Shocard	ShoCard
Soramitsu	Soramitsu
Peer Mountain	PeerMountain
Evernym	Evernym
Workday	Workday
Metadium	Metadium Technology
Spaceman ID	Spaceman ID
Xertify	Xertify
Lissi	main incubator, Konsortium
Digital Scotland	DigitalScot.net, Digital Identity Scotland, Schottische Regierung
Flemish ID	Flämische Regierung, Stadt Antwerpen, Digipolis und Informatie Vlaandern, Jolocom
Illinois	The Illinois Blockchain Initiative
XRide	Pilotprojekt (T-Labs, IBM, Riddle&Code, Deutsche Bahn, Jolocom, ComforCharge, Ubirch, G+D, Simple Mobility) Elektroscooter
openPDS	MIT
IRMA	The Privacy by Design Foundation

Re:claimID	Fraunhofer AISEC
SITA	SITA
Iconloop	Korea Technology Finance Corporation
Alberta Credential Ecosystem	Konsortium (Banken, Telkos Unternehmen, öffentliche Institutionen)
Korea Financial Telecommunication and Clearing Institute	Konsortium (Banken, Telkos Unternehmen, öffentliche Institutionen)
MyCUID	US-amerikanische Genossenschaftsbanken
Stadt Zug (Schweiz)	Stadt Zug, Consensys, uPort, ti&m
Schweizerische Bundesbahnen	SBB, Linum Labs
Uniris	Privat (Gründer)
ISAEN	ISÆN (Individual perSonal data Auditable addrEss)
Hardware Car Wallet	Daimler, Riddle & Code, evan network, Blockchain Helix
weeve	Next Big Thing AG
Spherity	Gründer und High Tech Gründerfonds
orbiterchain	Orbiter.de GmbH

Idealtypischer Ablauf

In dem Beitrag Chancen der Self-Sovereign Identities (SSI) aus Sicht von Unternehmen für das Identity & Access Management (IAM) stellt Dr. André Kudra am Anwendungsfall „Neue Mitarbeiterin benötigt Zugriff“ einen typischen Ablauf bei der Verwendung selbstverwalteter digitaler Identitäten vor. In vereinfachter Form lässt sich der Prozess am Beispiel der ChainID, des Prototyps des main incubators, beschreiben[2]:

- Der Kunde lädt eine App (Identity Wallet) auf sein Mobiltelefon.
- Eine Bank oder eine andere Institution bestätigt verschiedene Identitätsinformationen (sogenannte Claims) über den Kunden (dies können beispielsweise KYC-Daten aber auch Kreditkarteninformationen sein)
- Die Identitätsinformationen werden auf dem Identitätswallet des Kunden abgespeichert.
- Der Nutzer kann die Identitätsinformationen dazu verwenden, sich bei Dritten z.B. Mobilitätsunternehmen oder Onlineshops zur Registrierung und Identifizierung anzumelden und dabei gleichzeitig nachweisen, wer die Information bestätigt hat.
- Die Bestätigung funktioniert über eine Public-Key-Infrastruktur.
- Anstelle einer Certificate Authority wird die Blockchain, in diesem Fall das Hyperledger Indy Framework genutzt. Unternehmen und Institutionen agieren dort als sogenannte Vertrauensanker.

Das Identitätswallet ist dabei in der Lage, Identitätsinformationen von verschiedenen Unternehmen und Institutionen zu speichern. Das Besondere dabei ist, dass jede Verbindung zwischen Nutzer und Unternehmen mit einem separaten DID (Decentralized Identifier) versehen wird, d.h. jeder Nutzer kommuniziert fortan mit jedem Unternehmen über einen eigenen DID (pairwise pseudonymous DIDs)[3]. über die Sovrin Blockchain. In der Blockchain selber sind keine personenbezogenen bzw. Identitätsdaten gespeichert.

Der Nutzer kann über eine Eingabemaske im Wallet, die über verschiedene Eingabefelder und Felddefinitionen verfügt, zusätzlich unverifizierte Claims

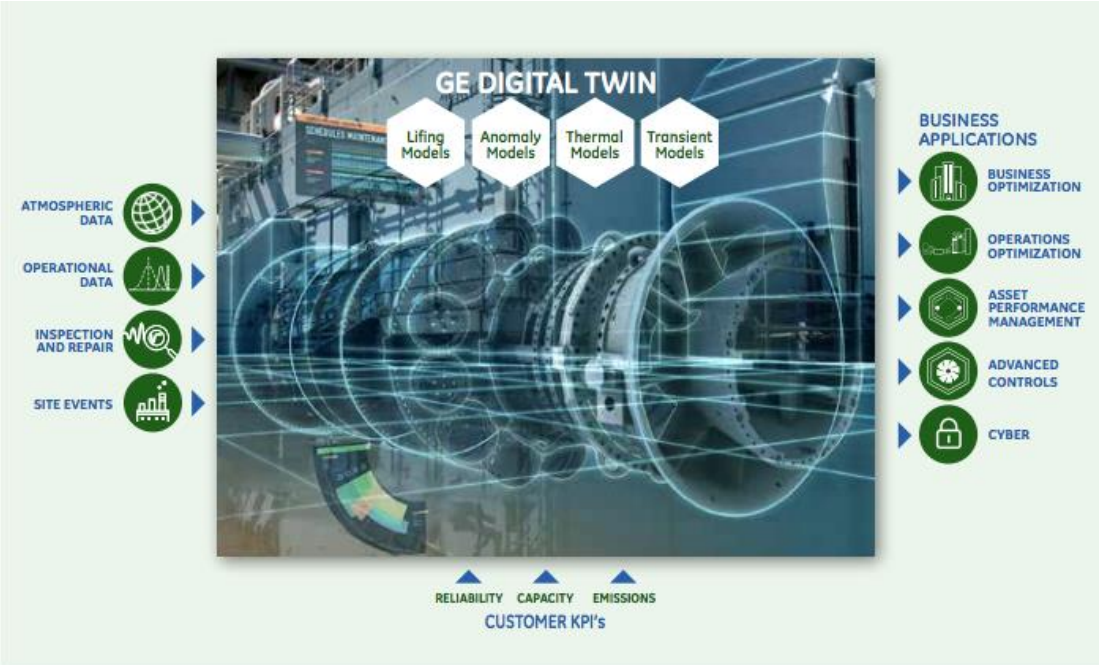
[2] Chain ID – der SSI-Prototyp des main incubators
[3] Blockchain trifft Digital Identity

(Merkmale) über sich selbst erstellen, dies kann z.B. die Risikoneigung oder Anzahl der Familienmitglieder sein. Die Verifizierung der Identitätsdaten erfolgt über die Sovrin Blockchain. In der Blockchain selber sind keine personenbezogenen bzw. Identitätsdaten gespeichert.

Selbstverwaltete Digitale Identitäten für Maschinen

Nicht nur Menschen werden künftig ihre digitalen Identitäten eigenverantwortlich managen oder diese Aufgabe an andere Institutionen/Akteure delegieren, auch Maschinen müssen die Kontrolle über die Herausgabe bestimmter sie betreffender Informationen haben. Wenn Maschinen demnächst über Unternehmens- und Ländergrenzen hinweg autonom mit Maschinen verhandeln und miteinander Transaktionen durchführen, dann ist es wichtig, dass nur die für den Vorgang nötigen Informationen offengelegt werden.

Die Maschine bekommt einen Digitalen Zwilling[4] zur Seite gestellt, der Auskunft über die wesentlichen Eigenschaften der Maschine gibt und sie Dritten gegenüber repräsentiert, wie z.B. bei Flugzeugturbinen (siehe Schaubild)[5]. Der Digitale Zwilling der Turbine liefert über Sensoren z.B. Zustandsdaten (Temperatur), die für die Wartung genutzt werden können. Deutet sich der Verschleiß eines Bauteils an, kann dieses Teil einige Zeit vor einem möglichen Ausfall ausgewechselt werden. Weiterhin kann am Digitalen Zwilling die Hinzufügung weiterer oder die Entfernung bestehender Komponenten simuliert werden[6].

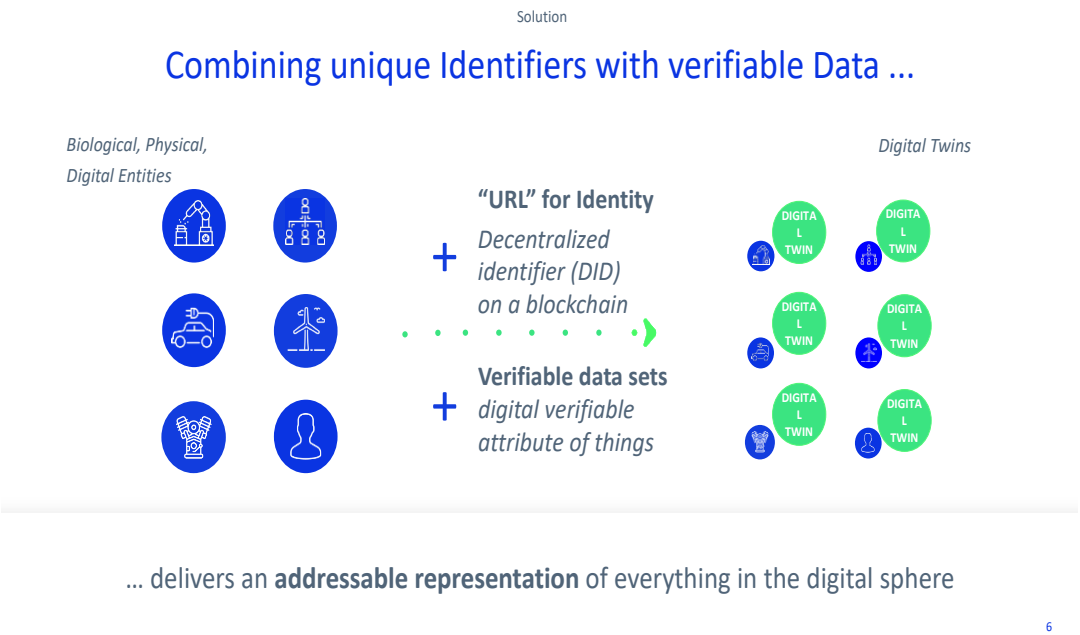


[4] Was ist ein Digitaler Zwilling?
[5] GE Digital Twin. Analytic Engine for the Digital Power Plant
[6] Informativ in dem Zusammenhang ist Digital Twins in Logistics von DHL Trend Research

Ein digitaler Zwilling kann aus weiteren bestehen. So können ganze Fertigungsstraßen einer Smart Factory oder Schaltschränke als Digitale Zwillinge abgebildet werden.

Der digitale Zwilling bekommt für seine eindeutige Identifizierung eine eigene Identität.

Wie wäre es, wenn eine Maschine bzw. ihr digitaler Zwilling, wie bei den Selbstverwalteten Identitäten für Personen, in Eigenregie nur bestimmte Informationen über sein Verhalten und Zustand mitteilt? An der Umsetzung dieser Vision arbeitet das Startup Spherity durch eine Kombination von Digitalen Zwillingen, Agententechnologien und eindeutigen, sicheren Identitäten. Dabei werden die Identitäten mit den verifizierten Daten der Maschine verbunden.



Quelle: Spherity

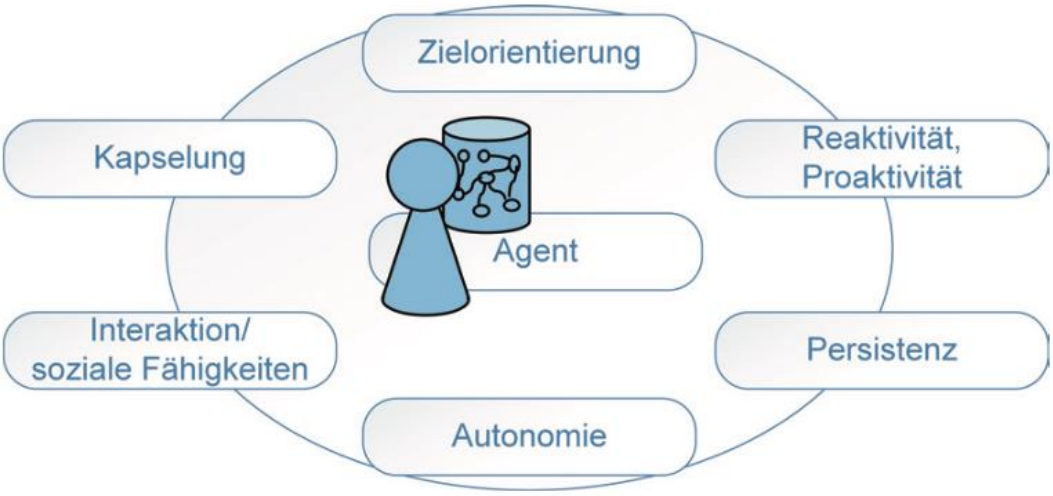
Agentenbasierte Identitäten als Bindeglied

Die Agententechnologie bietet sich dazu an, die Kommunikation und Koordination der verschiedenen Akteure (Personen, Maschinen, Geräte) zu gewährleisten. In dem Positionspapier Agenten zur Realisierung von Industrie 4.0 des VDI wird aufgezeigt, wie sich Agententechnologie und Industrie 4.0 verbinden lassen.

Zunächst zu der Frage, was unter einem Softwareagenten zu verstehen ist. Jacques Ferber gibt folgende Definition eines Softwareagenten:

> *Agenten sind in der Lage, zu agieren und nicht nur logisch zu schließen, wie in der klassischen Künstlichen Intelligenz. .. Agenten führen Aktionen aus, die ihre Umwelt verändern und damit selbst die Voraussetzungen für ihre zukünftigen Entscheidungen beeinflussen. Sie können auch untereinander Mitteilungen austauschen (kommunizieren); das ist eine der wesentlichen Formen der Interaktion zwischen Agenten. Sie agieren innerhalb einer Umwelt, außer, .., bei reinen Kommunikationsagenten, bei denen alle Aktionen auf Kommunikation reduziert werden können (in: Multiagentensysteme. Eine Einführung in die Verteilte Künstliche Intelligenz)*

Die wesentlichen Eigenschaften von Softwareagenten in grafischer Darstellung.



Salazar, L. A. C.; Mayer, F.; Schütz, D.; Vogel-Heuser, B.: Platform Independent Multi-Agent System for Robust Networks of Production Systems. In: IFAC-Paper- sOnLine (2018) 51, pp. 1261–1268

Der VDI unterscheidet zwischen Kommunikations-, Kunden-, Anlagen-, Management- und Koordinationsagenten.
In der Industrie 4.0 fällt den Koordinationsagenten die Aufgabe zu, die Assets (Anlagen, Maschinen, Komponenten) zu repräsentieren und ihrem Auftrag zu agieren. Zusammen bilden Kommunikation- und Koordinationsagenten ein Multiagentensystem.

Agenten, die als Verwaltungsschale von Assets fungieren, müssen nicht nur die Eigenschaften des von ihnen vertretenen Assets vollumfänglich abbilden, sondern auch deren Fähigkeiten. Die Agenten haben als Verwaltungsschale die Aufgabe, diese Fähigkeiten zu publizieren und anderen Agenten verfügbar zu machen.

Jeder Agent erhält ID, in der seine Adresse und seine Eigenschaften hinterlegt sind.

Die ID ermöglicht eine eindeutige Identifizierung und wird in der Regel nach ISO 29002-5 (z. B. bei ecl@ss) oder durch eine URI/URL (z. B. zur Verfügung gestellt durch die NAMUR) definiert. Die Attribute selbst werden in der IEC 61360 definiert. Einschlägige Normen dieser Reihe (z. B. IEC 61360-4 bzw. IEC-CDD) helfen bei der Identifikation der relevanten, im Idealfall standardisierten, Merkmale bzw. Attribute.

Hier besteht die Möglichkeit, die Attribute des Agenten über seine ID zu verwalten. Der Agent könnte also seine Attribute selbst verwalten. Ein Agent kann sowohl eine Person wie auch eine Maschine vertreten. Weiterhin können sie mehr oder weniger anonym agieren, d.h. nicht in jedem Fall muss der Agent seine Identität offenlegen, sofern eine Instanz im Hintergrund für die Richtigkeit der Identitäten garantiert – wie es im Konzept der Selbstverwalteten Identitäten vorgesehen ist[7].

Insofern handelt es sich hierbei in Konzept bei dem, auf einer abstrakten Ebene betrachtet, es relativ unerheblich ist, ob der Agent eine natürliche Person oder eine Maschine vertritt. Zu klären ist die Frage, inwieweit einem Agenten rechtsverbindliches Handeln zugeschrieben werden kann[8].

[7] Agentenzentrierte Identitäten für Industrie 4.0
[8] Softwareagenten als Rechtssubjekte

Blockchain nicht zwangsläufig Mittel der Wahl

Es hat häufig den Anschein, als wäre die Blockchain die einzige Technologie, die den Anforderungen selbstverwalteter Digitaler Identitäten entspricht. Tatsächlich ist es so, dass die meisten Projekte und Lösungen die Blockchain-Technologie verwenden, wobei Hyperledger Indy die bevorzugte Plattform ist. Dennoch ist es durchaus möglich, selbstverwaltete Digitale Identitäten auch ohne Blockchain zu realisieren. In dem Paper Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology kamen die Autoren zu dem Ergebnis, dass zwar viele Punkte für die Blockchain sprechen; von einer generellen Überlegenheit der Blockchain-Technologie im Bereich SSI könnte jedoch nicht die Rede sein[9].

> *Both blockchain-based and other Self-Sovereign Identity solutions show to fulfill most of the evaluation criteria. The importance lies in the differences between solutions in both variants. Blockchain-based solutions definitely meet more properties on average than the others. IRMA shows that it is possible to create an SSI solution without blockchain-technology. We conclude that blockchain-technology is a good foundation to build a Self Sovereign Identity solution, but it is not a necessity.*

[9] Sind selbstverwaltete Digitale Identitäten nur mit der Blockchain realisierbar?

eIDAS und SSI

Mit der eIDAS-Verordnung wurde ein Rechtsrahmen verabschiedet, der die grenzüberschreitende elektronische Identifizierung und Abwicklung elektronischer Transaktionen im EU-Binnenmarkt regelt. Damit soll die digitale Wirtschaft in der EU gestärkt werden. Hauptmerkmal ist die eIDAS-konforme Fernsignatur mittels der eID[10].

Wie passen nun eIDAS und Selbstverwaltete Digitale Identitäten zusammen?

Dieser Frage widmet sich der Beitrag eIDAS-supported Self-Sovereign Identity. eIDAS selber liefert das Rahmenwerk; die eigentliche Identifizierung bzw. die Bereitstellung verifizierter Merkmale erfolgt außerhalb:

> *However, it must be noted that, from the point of view of those third parties, these identification data would be self- asserted, as they cannot rely on the eIDAS node to verify them. This is because eIDAS eID is meant to be used for authenticating when accessing to services, but not for providing claims about identity that can be verified by others different from those who are requesting the authentication.*

Weiterhin:

> *Here is precisely where the trust framework created by the eIDAS Regulation can play a key role, since it does not require a previous relationship between the parties for verifying their identities in the digital world; they can rely on the verification done by the entities entitled for that: trust service providers and identity providers of the electronic identification schemes.*

eIDAS und SSI widersprechen sich nicht. Mittels Decentralized Identifiers kann beispielsweise die Identität der Person von einem Händler auch unter eIDAS verifiziert werden.

> *… they can verify the true identity (in the sense that it is legally enforceable under eIDAS) of the DID owner by validating the qualified electronic certificate associated to that DID.*

[10] Selbstverwaltete Digitale Identitäten und eIDAS – wie passt das zusammen?

Hindernisse

Damit selbstverwaltete Digitaler Identitäten massentauglich werden, müssen noch einige Hindernisse überwunden werden. Das betrifft zum einen mehr technische Fragen, wie die Nutzererfahrung und die Wiederherstellung des Private Key im Verlustfall, zum anderen Fragen der Skalierung, d.h. wie können Selbstverwaltete Digitale Identitäten die kritische Masse erreichen. Die Diskussion wird überwiegend auf einer technologischen Ebene geführt. Das Konzept der Blockchain, Schlagworte wie Kryptografie und Public Key-Infrastructure überfordern die meisten Menschen, bzw. die Bereitschaft ist gering, sich mit den Tiefen der Technik zu beschäftigen. In dem Positionspapier Self-sovereign Identity A position paper on blockchain enabled identity and the road ahead, herausgegeben vom Blockchain Bundesverband, verweisen die Autoren auf die verschiedenen Herausforderungen.

> *It also means that we cannot rely on technology alone but that there must also be non- technical measures in place, including laws, regulations, and "off-chain" governance mechanisms, as well as the application of existing legal constructs like guardianship, delegated access, and powers of attorney and other proxy contracts. SSI is not self- sovereign unless it is truly identity for all.*

Größte Hindernisse, das räumen die Autoren ein, sind die Skalierung bzw. Akzeptanz bei den Nutzern und rechtliche Fragen. Außerdem müssten viele Anbieter, bis hin zu ganzen Branchen, ihr Geschäftsmodell ändern. Unser derzeitiges (europäisches) Rechtssystem ist mit den Anforderungen selbstverwalteter souveräner ID's nur bedingt kompatibel. Eine offene Frage ist die Wiederherstellung des Private Keys im Verlustfall[11].

Die Komplexität der Lösungen müsste deutlich abnehmen, um den normalen Nutzer nicht zu überfordern und abzuschrecken:

> *… we have to break the status quo of centrally-managed, digital identity where each interaction is routed through a third party. This habit will be very hard to break and requires SSI solutions to be tenfold better as compared to the convenience of centralized identity solutions, while being enriched with the unique capabilities of a universal identity layer.*

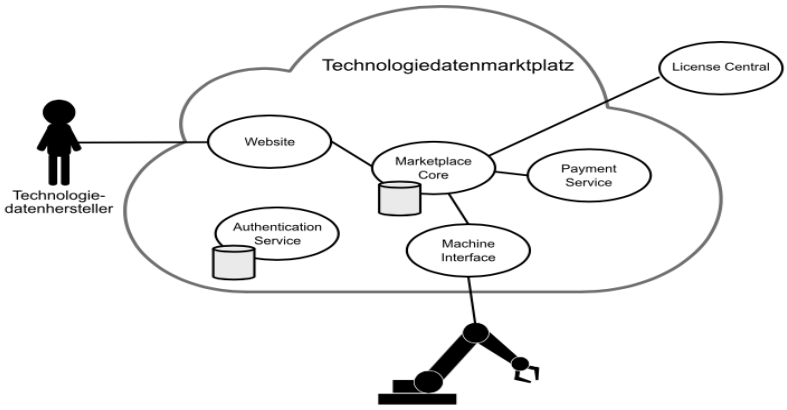
[11] Self-sovereign Identity: A position paper on blockchain enabled identity and the road ahead

Darüber hinaus stellt sich die Frage, ob die Nutzer tatsächlich ihre Identitäten selbst verwalten wollen oder ob es dazu entsprechender Institutionen, wie Identity Banks, bedarf. Der Nutzer würde die Aufgabe zur Verwaltung seiner digitalen Identität(en) an eine bankähnliche Institution delegieren, die mit vertrauenswürdigen Softwareagenten („Custodians“) arbeitet.

Potenzielle Geschäfts- und Rollenmodelle

Die Mehrzahl der derzeitigen Anwendungsfälle stammt aus dem IAM-Umfeld, d.h. das sichere und rechtskonforme Onboarding der Kunden und der Mitarbeiter steht im Vordergrund. Die Verbesserung der Kundenbindung durch den Einsatz selbstverwalteter Digitaler Identitäten ist ein weiterer Punkt. Bei der Gelegenheit kann sich das Unternehmen, die Bank oder die staatliche Institution als technologisch fortschrittlich und als Vertreter einer Position präsentieren, die großen Wert auf das Recht für Selbstbestimmung legt.

Selbstverwaltete Digitale Identitäten, bzw. deren verifizierte Merkmale (Claims), lassen sich verwerten. So ist vorstellbar, dass Nutzer bestimmte Merkmale, wie z.B. über ihr Kaufverhalten oder ihre Vorlieben für bestimmte kulinarische Genüsse, ihr Fahrverhalten oder ihr Sportpensum, Dritten wie Datenmarktplätzen, Unternehmen oder Forschungsinstituten zur Verfügung stellen. Unternehmen können Maschinendaten ebenfalls Datenmarktplätzen anbieten, um Erfahrungen mit anderen Unternehmen zu teilen und auf diese Weise Verbesserungspotenzial, wie in der Produktionssteuerung, im Service, beim Material oder in Wartung, identifizieren zu können[12].



Architektur des Technologiedaten-Marktplatzes. Quelle: Forschung für mehr IT-Sicherheit in Industrie 4.0

Über den Marktplatz soll ein Maschinenbetreiber benötigte Technologiedaten, die für die Fertigung mit einer Werkzeugmaschine notwendig sind, künftig kostengünstig und mit einer bedarfsgerechten Lizenz für seine Maschine erwerben können. Die Idee orientiert sich im Wesentlichen an bereits existierenden Marktplätzen, wie beispielsweise einem E-Book-Store. Ziel ist es, die Arbeit der Unternehmen effizienter und flexibler zu gestalten (Quelle: Der Technologiedatenmarktplatz - Die Idee).

[12] Marktplätze für Technologiedaten

Das IoT-Startup weeve bietet Unternehmen auf Basis der Blockchain Technologie eine Infrastruktur an, mit der es möglich ist, Datenmarktplätze aufzubauen. Neben Technologiedaten-Marktplätzen könnten Technologiedatenfonds als langfristige Anlagemöglichkeit fungieren[13]. Die Datendividende richtet sich danach, wie werthaltig die Daten sind. Eine weitere Möglichkeit besteht für Maschinenbetreiber darin, die Maschine mit den daraus erzeugten Daten zu bezahlen. Ein große Bedeutung könnte sog. Custodian Wallets zukommen, welche das Management der Identitäten und Daten für die Nutzer und Maschinen übernehmen[14].

Der Bundesverband Blockchain sieht weiteres Potenzial für Identity Service Provider, die sich auf bestimmte, qualitativ hochwertige Merkmale von Personen spezialisieren.

Reusable and portable Verifiable Credentials could motivate a race-to-the-top for the best or highest quality Issuers for a particular use case. Issuers of Credentials, such as verification services, trust services providers, and other entities that provide Verifiable Credentials can directly compete with each other in offering their services in the market. This effectively creates a B2C market for trusted identity data and attestations in contrast to the status quo of services are bound to B2B interactions and associated with high barriers of entry to the market (Quelle: Self-sovereign Identity - A position paper on blockchain enabled identity and the road ahead)

Die Nutzer ziehen daraus im Idealfall den Vorteil, auf Basis ihrer Daten/Merkmale die für sie am besten geeigneten Produkte oder Services zu bekommen. Nervige Werbung gehört damit der Vergangenheit an. Je besser die Daten sind, um so günstiger die Angebote auf Unternehmensseite, da die Unternehmen nicht mehr die Existenz des Kunden und die Bonität zuvor prüfen müssen.

[13] Digitale Finanzierungsmodelle für die Industrie 4.0
[14] What is a custodian wallet?

Ausblick

Noch ist nicht abzusehen, inwieweit sich Selbstverwaltete Digitale Identitäten durchsetzen werden. Die öffentliche Diskussion, nicht nur in Europa, sondern vor allem auch in den USA, deutet darauf, dass das Klima für Google und facebook, wie überhaupt für die Technologiekonzerrne, rauer wird. Mit Libra und Calibra präsentiert sich facebook als Anwalt der Nutzer in Sachen Datenschutz und Identifizierung. Apple grenzt sich bewusst von Google und facebook ab, indem das Unternehmen dem Datenschutz und der Privatsphäre große Bedeutung einräumt. Ähnlich verhält es sich mit Microsoft, das sich als Verfechter dezentraler Digitaler Identitäten präsentiert. Das könnte der Verbreitung selbstverwalteter Digitaler Identitäten im Sinne von Christopher Allen den Wind aus den Segeln nehmen. Die Nutzer könnten es vorziehen, in ihrer gewohnten digitalen Umgebung zu bleiben und sich mit „Self Sovereign Identities Light“ zufrieden geben. Abzuwarten bleibt, ob es in naher Zukunft, wie vom Bankenverband jüngst gefordert[15], einen digitalen Euro, der an digitale Identitäten für Personen und Maschinen gekoppelt ist, geben wird. Sofern der Eindruck nicht täuscht, vollzieht sich momentan in den westlichen Ländern ein Wertewandel, der sich an dezentralen Organisationsformen und humanistischen Prinzipien (Selbstverantwortung, Technik als Mittel und nicht Zweck) orientiert, um damit der Machtkonzentration, wie sie in der aktuellen Plattformökonomie Realität ist, entgegen zu wirken. Die verschiedenen Login-Allianzen werden, so die Überzeugung der vorliegenden Studie, nur ein Durchgangsstadium, eine Brückentechnologie auf dem Weg zu selbstverwalteten Digitalen Identitäten sein. Die bis dato doch sehr überschaubare Akzeptanz der SSO-Lösungen spricht für diese Annahme.

Wie in anderen Technologiefeldern auch, wird die Verbreitung selbstverwalteter Identitäten nur dann gelingen, wenn sie von entsprechenden Standards unterstütz wird, wie mit DID und Verifiable Claims & Credentials (W3C). Ob mit der Zunahme dezentraler Organisationsformen auch die Individualität der Menschen gefördert wird, ist nicht sicher – es besteht hier kein Automatismus. Das Beispiel China, wo die Regierung sich verstärkt mit der Blockchain-Technologie auseinandersetzt, zeigt, dass eine ihrem Wesen nach dezentrale Technologien auch in Gesellschaften, die sich am Kollektiv orientieren, eingesetzt werden könnte. Wenn es stimmt, dass sich der

[15] Digitaler Euro in Kombination mit digitalen Identitäten für Personen und Maschinen

Wohlstand der westlichen Länder, wie es u.a. John Stuart Mill beschrieben hat[16], in einem hohem Maß der Förderung der Individualität der Bürger verdankt, dann sind Selbstverwaltete Digitale Identitäten für Personen und Maschinen künftig wichtige Treiber für den Wohlstand. Die Wahlfreiheit und weitgehende Autonomie der Nutzer und Maschinen (!) sind demnach die logische Fortführung unseres Wirtschaftsmodells unseres Wirtschaftsstils.

[16] Über die Freiheit

Impressum

Kontakt

Ralf Keuper

Kolpingstr. 3

33428 Harsewinkel

E-Mail: ralf.keuper@bankstil.de

Autor: Ralf Keuper

V.i.S.d.P.: Ralf Keuper

November 2019