Self Sovereign Identity Use Cases – von der Vision in die Praxis

www.bitkom.org

bitkom

Herausgeber

Bitkom e. V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner

Patrick Hansen | Bereichsleiter Blockchain
T 030 27576-410 | p.hansen@bitkom.org

Co-Autoren

Adrian Doerk | Main Incubator
Patrick Hansen | Bitkom
Georg Jürgens | Spherity
Moritz Kaminski | Robert Bosch
Dr. Michael Kubach | Fraunhofer IAO
Oliver Terbu | ConsenSys

Satz & Layout

Katrin Krause | Bitkom

Titelbild

© Irina Vodneva – istockphoto.com

Inhaltsverzeichnis

1 Einleitung 4

2 Funktionsweise und Vision von SSI 5

3 SSI Anwendungsfall 1 – Dezentrale Dokumentation für das Lieferanten-Risikomanagement globaler Pharmakonzerne 7
3.1 Welches Problem löst dieser Anwendungsfall? 7
3.2 Wie sieht die Lösung aus? Was ist der Vorteil? 8
3.3 Wie ist die Idee zur Verwendung dezentraler Identitäten im Lieferanten-Risikomanagement entstanden? 8
3.4 Was sind regulatorische und wirtschaftliche Hürden? 9

4 SSI Anwendungsfall 2 – Zugangsverwaltung für Gebäude 10
4.1 Welches Problem löst dieser Anwendungsfall? 10
4.2 Wie sieht die Lösung aus? Was ist der Vorteil? 11
4.3 Warum ist die Verwendung von selbstbestimmten Identitäten für die Gebäudeverwaltungen relevant? 11
4.4 Was sind regulatorische und wirtschaftliche Hürden? 12

5 SSI Anwendungsfall 3 – Bildungszertifikate 13
5.1 Welches Problem löst dieser Anwendungsfall? 13
5.2 Wie sieht die Lösung aus? Was ist der Vorteil? 13
5.3 Wie entstand die Idee? 14
5.4 Was sind regulatorische und wirtschaftliche Hürden? 14

6 SSI Anwendungsfall 4 – Stammdaten- und Zertifikatsmanagement 15
6.1 Welches Problem löst dieser Anwendungsfall? 15
6.2 Wie sieht die Lösung aus? Was ist der Vorteil? 15
6.3 Wie entstand die Idee? 16
6.4 Was sind regulatorische und wirtschaftliche Hürden? 17

7 Fazit 18

1 Einleitung

In der analogen Welt stehen uns unterschiedliche Mittel zum Nachweis unserer Identität zur Verfügung. Ein besonders hohes Vertrauen besitzt hierzu der Personalausweis, da er vom Staat herausgegeben wird. Außerdem können wir ihn zum Identitätsnachweis einfach vorzeigen, müssen ihn dazu jedoch nicht aus der Hand geben und der Staat bekommt auch nicht mit, wann und wem ich meinen Ausweis zeige. In der digitalen Welt ist das etwas schwieriger: Über verschiedene Verfahren wie z.B. Post-Ident, Video-Ident, Accounts bei Sozialen Netzwerken oder die Rückantwort auf eine E-Mail weisen wir unsere Identität für verschiedene Webseiten neu aus. In der Regel stützen wir uns dabei auf dritte Identitätsdienstleister, die unsere Identität bestätigen, bei sich hinterlegen und verwalten. Dies ist zwar komfortabel, aber aus Datenschutzgründen suboptimal. Denn wir zeigen unsere Identität nicht nur wie in der analogen Welt vor. Es ist vielmehr in etwa so, also würde ein von uns beauftragtes Privatunternehmen für jede Anmeldung Kopien unseres Ausweises an die von uns genutzten Webservices versenden. Das Privatunternehmen erfährt dabei, wo und wann wir uns überall anmelden. Für einen selbst ist gar nicht immer klar, welche meiner Daten überhaupt weitergegeben werden.

Self-Sovereign Identities (SSI), welche auch als dezentrale Identitäten auf Blockchain-Basis bezeichnet werden, versprechen eine Alternative, die eine größere Kontrolle der Nutzer über ihre Daten und eine größere Datensparsamkeit im digitalen Zeitalter mit sich bringt. Im Deutschen wird der Begriff meist mit »selbstbestimmten Identitäten« übersetzt. Zwar gibt es noch Diskussionen zur genauen Terminologie der Technologie, jedoch arbeiten schon zahlreiche Unternehmen und Initiativen an dem Konzept. Auch die Bundesregierung fördert einzelne Pilotprojekte mit Millionensummen im Rahmen des **↗Förderprojektes »Schaufenster Digitale Identitäten«**, eine von vielen Maßnahmen der Blockchain Strategie der Bundesregierung.

Mittlerweile gibt es also umfangreiche Literatur, Experten, und Pilotprojekte zu Self-Sovereign Identities. Doch in der Diskussion um technische und regulatorische Hürden, internationale Standards und SSI-Fachbegriffe wie Decentralized Identifiers (DIDs) & Verifiable Credentials geht häufig unter, dass auch heute schon einiges möglich ist. In diesem Papier möchten wir deshalb einige reale Anwendungsfälle von SSI vorstellen, die in ihrer Umsetzung schon weit fortgeschritten sind. Bereits die hier aufgeführten Beispiele in speziellen Anwendungsbereichen für SSI zeigen, dass es sich hierbei nicht um ein abstraktes, futuristisches Thema handelt, sondern um Projekte mit konkreten messbaren wirtschaftlichen und gesellschaftlichen Vorteilen. Der Darstellung der Use Cases geht eine bewusst knapp gehaltene Einführung in die Funktionsweise und Vision von SSI voraus, da diese bereits vielfach an anderer Stelle erfolgt ist, wie z.B. in einer **↗Publikation** des EU Blockchain Observatory and Forum.

2 Funktionsweise und Vision von SSI

SSI bedeutet vereinfacht gesagt, dass der Nutzer seine digitale Identität selbst verwaltet, ohne von einem zentralen Identitätsdienstleister abhängig zu sein. Ein Wallet auf einem digitalen Endgerät dient der zentralen Verwaltung für den Nutzer. Dieser entscheidet selber, ob die Daten nur lokal auf seinem Endgerät oder auch verschlüsselt auf einer Cloud-Lösung gespeichert werden sollten. Die Kommunikation von Identitätsdaten erfolgt über eine peer-to-peer Verbindung. Diese wird durch DIDs ermöglicht, welche nicht nur einzigartig sind, sondern zufallsbasiert auf Nutzerseite erstellt werden. Der Staat oder andere vertrauenswürdige Stellen können nach einem Verbindungsaufbau durch den Nutzer bestimmte persönliche Identitätsmerkmale einer Person (z.B. Adresse, Alter, Ausweisnummer etc.) bestätigen. Diese werden über kryptografische Verfahren und Signaturen eindeutig der Person (bzw. dem jeweiligen Decentralized Identifier) zugewiesen. Einmal ausgestellt kann eine Person diese Bescheinigungen (Verified Credentials) ohne weitere Zustimmung des Ausstellers zur Identifizierung und Authentisierung nutzen. Durch die Verwendung der DIDs wird eine Korrelation von Nutzerdaten erschwert. Die Technologie kann von natürlichen und juristischen Personen, sowie Maschinen verwendet werden.

Die Blockchain dient hauptsächlich als Anker, um die Legitimität der ausgestellten Verified Credentials zu überprüfen, indem diese die öffentlichen Schlüssel (DIDs) der Aussteller der Verified Credentials beinhaltet. Des Weiteren ermöglicht diese (direkt oder indirekt) den Widerruf von Verified Credentials und kann auch allgemeine Daten wie z. B. Vorlagen für Verified Credentials beinhalten. Sie ist zwar ein wichtiger Baustein, aber nur einer von vielen der DPKI (decentralized public key infrastructure) Gesamtlösung.

Die Vision von SSI ist es, dem Nutzer die komplette Kontrolle über seine digitale Identität zurückzugeben. Sei es bei der Authentifizierung für bestimmte Dienstleistungen, bei der Zustimmung zur Nutzung der Daten, bei der Monetarisierung, beim Widerrufen, oder dem Nachverfolgen der Daten.

Diese Vision hat sich unter anderem die EU mit ihrem »European self-sovereign identity framework« (ESSIF) als Teil der »European blockchain service infrastructure« (EBSI) zu eigen gemacht. EBSI ist eine Blockchain-Infrastruktur-Initiative von der EU und ihren Mitgliedstaaten, die eine öffentliche Blockchain-Infrastruktur für staatliche (EU-weite) Dienstleistungen bereitstellen möchte. ESSIF wiederum baut auf dieser Infrastruktur auf, um SSI-Lösungen aufzubauen und voranzutreiben. Ziel ist es, 2022 eine blockchain-basierte Identität für Bürger bereitstellen zu können, die ähnlich wie eine analoge Brieftasche den Personalausweis, den Führerschein, eine Gesundheitskarte, den Studierendenausweis usw. in einer digitalen Brieftasche bzw. einer Wallet versammelt, über die nur der Bürger selbst die volle Kontrolle hält. In gewisser Weise sollen also Identitäten ins digitale Zeitalter mit allen seinen Vorteilen überführt werden, ohne dabei an Privatsphäre, Datenschutz, oder Datensouveränität einzubüßen. Von den bereits untersuchten und experimentierten EU-Anwendungsfällen wird wahrscheinlich das Projekt für interoperable Bildungsunterlagen, das auf der Arbeit im EuroPass-System aufbaut, am schnellsten in Produktion gehen.

Dass auf dem Weg von der Vision in die Praxis noch einige technische, regulatorische, und wirtschaftliche Hürden genommen werden müssen, ist hinlänglich bekannt und dokumentiert.

Dabei wird jedoch teilweise verkannt, dass auch heute schon SSI-Projekte mit konkreten Mehrwerten umgesetzt werden und werden können. Um das abstrakte Thema SSI zu veranschaulichen und damit zu einer breiten gesellschaftlichen und politischen Diskussion darüber beizutragen, möchten wir im Folgenden einige dieser Projekte kurz vorstellen. Unsere Hoffnung ist, dadurch das Thema noch stärker in den Vordergrund zu rücken und den Weg von der Vision in die Praxis zu beschleunigen.

3 SSI Anwendungsfall 1 – Dezentrale Dokumentation für das Lieferanten-Risikomanagement globaler Pharmakonzerne

Zur Wiederverwendung von Compliance-Dokumentationen müssen Daten vor allem manipulationssicher und hoch portabel sein

3.1 Welches Problem löst dieser Anwendungsfall?

In regulierten Industrien wie der Pharmabranche gewinnt vor dem Hintergrund von wachsenden Compliance Anforderungen das Risikomanagement von Lieferanten immer weiter an Bedeutung. Um entsprechende Risikoanalysen durchführen zu können, müssen alle Lieferanten großer Pharmaunternehmen in regelmäßigen Abständen entsprechende umfangreiche Fragenkataloge beantworten. Alternativ werden hier auch entsprechende externe Lieferantenaudits durchgeführt. Lieferanten müssen internationale Standards zu sozialen, gesundheitlichen, sicherheitstechnischen und ökologischen Bedingungen einhalten. Über Audits, Zertifikate und Selbstauskünfte wird die entsprechende Einhaltung solcher Standards gewährleistet. Die Verwaltung dieser Compliance Daten ist hierbei für alle Beteiligten komplex, kostspielig und zeitaufwändig.

Zur Erfassung entsprechender Compliance Daten nutzten Pharmaunternehmen Lieferantenmanagement-Systeme, in denen von bestehenden und potenziell neuen Lieferanten entsprechende Compliance Daten erfasst und dokumentiert werden. Trotz dieser digitalen Unterstützung, dauert eine Neuaufnahme von Lieferanten in der Branche durchschnittlich 25 bis 30 Tage. Das liegt insbesondere daran, dass geforderte Compliance Daten beim Lieferanten erst einmal zusammengetragen und dann für den Kunden ins gewünschte Format übertragen werden müssen.

Für Lieferanten der Pharmabranche heißt das, dass diese entsprechende Compliance Daten gleich mehrfach für verschiedenen Kunden in entsprechenden Systemen hinterlegen müssen, was einen entsprechend hohen administrativen Aufwand erzeugt. Um diesen Aufwand zu reduzieren wird unter Federführung der Pharma Supply Chain Initiative (PSCI) an der Standardisierung entsprechender Fragebögen gearbeitet. Dies ist ein erster Schritt zum Abbau der administrativen Aufwände. Der Aufwand zur Eingabe der Daten in den verschiedenen Systemen der Pharmaunternehmen (Lieferanten-Portale, Excel-Listen, Sharepoint Lösungen etc.) bleibt allerdings bestehen und wird in einem Verified-Credential-basierten Risikomanagement-System adressiert.

3.2 Wie sieht die Lösung aus? Was ist der Vorteil?

Pharmaunternehmen, Zulieferer und Audit-Unternehmen verfügen über eine eindeutige auf der Blockchain verankerte Identität, mit der ihre Compliance Daten kryptografisch signiert und über sichere Kommunikationskanäle ausgetauscht werden können.

Das vom Konsortium genutzte Sovrin-Netzwerk wird genutzt, um zum einen Identitäten der beteiligten Pharmaunternehmen und Lieferanten sowie standardisierte Schemata von Fragebögen zu verankern. Neben einer Blockchain ist ein weiterer Baustein dieser Technologie die Identity-Wallet, die z.B. von dem Technologie-Unternehmen Spherity angeboten wird. Mit Hilfe dieser Identity Wallets können digitale Identitäten erzeugt und verwaltet werden sowie beliebige Daten und Dateien kryptographisch gesichert ausgetauscht werden.

Erfolgt nun ein digitaler Austausch von Daten, z. B. einem beantworteten Compliance Fragenkatalog, wird dieser entsprechend von der versendenden Partei mit Hilfe der Identity-Wallet signiert. Die empfangende Partei kann im Gegenzug die Gültigkeit dieser Signatur überprüfen, um sicherzustellen, dass entsprechende Daten authentisch und auch wirklich von der richtigen Partei zugestellt wurden. Da diese Off-Chain-Dokumente mit Identitäten signiert sind, die zuvor in einer Blockchain registriert wurden, können ihre Herkunft und Zeitstempel zu Prüfungszwecken ohne großes Datenschutzrisiko bestätigt werden.

Allen Interessenvertretern des Projektes war es wichtig, eine zukunftssichere Lösung zu finden sowie nicht in die Abhängigkeit einer proprietären Technologie zu geraten, die eine ganze Branche an ein einzelnes Produkt oder Netzwerk binden würde. Einer weitere Anforderung ist die Vermeidung des sogenannten »Vendor Lock-ins« – hier konnten Spherity und SwissCom Blockchain in Kooperation die Interoperability ihrer Wallet Technologien in einem gemeinsamen Projekt erfolgreich beweisen.

3.3 Wie ist die Idee zur Verwendung dezentraler Identitäten im Lieferanten-Risikomanagement entstanden?

Die Pharma- und Gesundheitsindustrie hat diese Problematik des ineffizienten Onboardings von Lieferanten vor einigen Jahren erkannt und sich intensiv an der Optimierung beschäftigt. Die Mitglieder der Pharmaceutical Supply Chain Initiative (PSCI), einem Industriekonsortium von ca. 40 großen Pharmaunternehmen, haben sich auf eine Synchronisierung und Standardisierung vom Risikomanagement von Lieferanten geeinigt. So soll die gemeinsame Nutzung und Wiederverwendung von verifizierten Onboarding-Daten gewährleistet werden.

Ziel ist es in der Zusammenarbeit zwischen Pharmaunternehmen und Lieferanten die Zeiten für das Onboarding signifikant zu senken und für Lieferanten die Wiederverwendung einmal ausgefüllter Fragenkataloge für verschiedene Pharmaunternehmen zu ermöglichen. Auf Basis der Arbeit der PSCI hat ein führendes Schweizer Pharmaunternehmen ein Konsortium aus Pharma-

und Technologieunternehmen zusammengestellt, um einen überprüfbaren und selbstbestimmten Datenaustausch zwischen den Akteuren der Lieferkette zu ermöglichen.

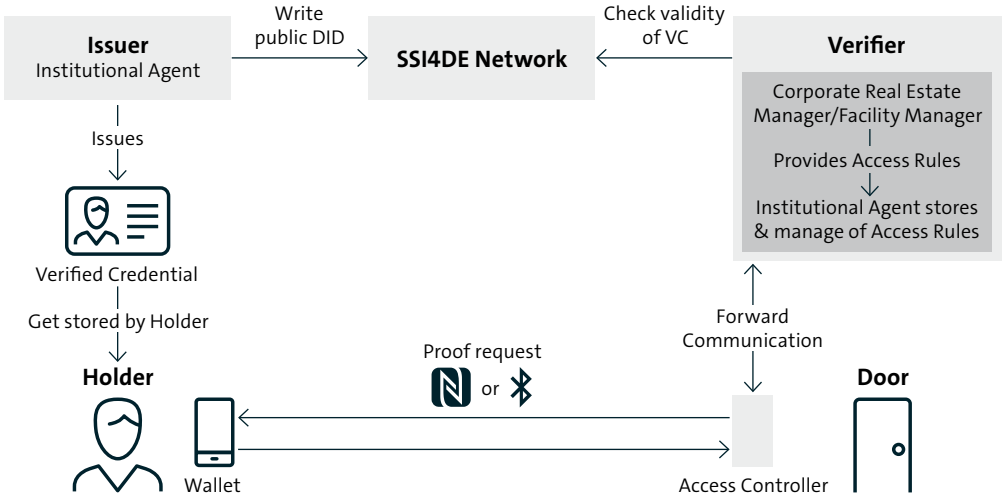
3.4 Was sind regulatorische und wirtschaftliche Hürden?

Es gibt nur wenige direkte Hürden für die weitere Einführung dieser Lösung. Die regulatorischen Hürden im Lieferanten-Risikomanagement werden von der PSCI und den Vorgaben der Compliance-Richtlinien von Pharmaunternehmen umgesetzt. Wirtschaftliche Aufwände bestehen bei der Integration von Identity Wallets in aktuell bestehende Systeme und Prozesse. Allerdings können auch Akteure ohne Risikomanagementsysteme teilnehmen, da sich aus unterschiedlichen Dateiformaten Credentials erzeugen lassen. Damit wäre die Lösung auch mit einem webbasierten Cloud Identity Wallet »barrierefrei« nutzbar für kleinere Lieferanten. Aktuell befindet sich eine entsprechende Referenzimplementierung mit anderen Pharmaunternehmen und Lieferanten in der Erprobung und soll Ende 2020 produktiv gesetzt werden.

Es gibt viele benachbarte und verwandte Anwendungsfälle in der Pharmaindustrie, die von einer größeren Klarheit über die Anforderungen an elektronische Signaturen und Siegel profitieren würden, wenn Europa vom bestehenden eIDAS-System zu mehr »Offenheit gegenüber dezentralen Systemen« überginge, die sich mit dieser Art kryptografischer Sicherheit stark mit Mechanismen für die wichtigsten Unterlagen der Industrie kombinieren lassen.

4 SSI Anwendungsfall 2 – Zugangsverwaltung für Gebäude

Der Zugang zu wirtschaftlich genutzten Objekten mittels der selbstbestimmten Identitätsverwaltung.



4.1 Welches Problem löst dieser Anwendungsfall?

Das Zugangs-Management für gewerblich genutzte Gebäude ist eine wichtige Aufgabe. Die Verwaltung von Gebäudezugängen muss sicher, nachvollziehbar, aber auch ausreichend flexibel sein. Die Anzahl der verschiedenen Personenkreise, welche Zutritt zu einem Gebäude bzw. verschiedenen Räumen benötigen, stellt für diese Branche eine große Aufgabe dar. Aktuell werden für den Zugang zu Räumlichkeiten vor allem physische Schlüssel, PIN-Nummern wie auch Near Field Communication (NFC)-Karten verwendet. Häufig werden diese auch in Kombination verwendet, was sowohl für Anwender als auch für Verwalter weniger flexibel und umso unpraktikabler ist.

Während sich Industrievertreter einig sind, dass digitale Lösungen Abhilfe schaffen können, ist deren genaue Umsetzung noch unklar. Zwar wird in anderen Teilen der Welt verstärkt auf die Gesichtserkennung bei Gebäudezugangen gesetzt, jedoch ist diese Art der Zugangskontrolle nicht erstrebenswert. Eine digitale Zugangslösung, welche oben genannte Anforderungen erfüllt und gleichzeitig die Privatsphäre von Individuen respektiert, wird aktuell von Commerz Real, dem main incubator und der Lissi Initiative im Rahmen des Innovationswettberwerbs »Schaufenster sichere digitale Identitäten« vom »SSI für Deutschland« in verschiedenen Piloten erprobt.

4.2 Wie sieht die Lösung aus? Was ist der Vorteil?

Eine zentrale Anwendung auf dem Mobilgerät ersetzt physische Schlüssel oder Karten. Zugangsberechtigungen können z.B. in der Lissi App aufbewahrt und für den Zugang zu Gebäuden oder Räumlichkeiten genutzt werden. Das Mobilgerät kommuniziert mittels NFC oder Bluetooth mit dem Zugangscontroller und übermittelt die entsprechenden Nachweise. Die zentrale Speicherung von Zugangsberechtigungen lokal auf dem Endgerät des Anwenders ist für diesen übersichtlicher und leichter zu organisieren. Für Nutzer, Unternehmen und Institutionen ergibt sich der Vorteil, dass sich eine einheitliche Gesamtlösung ergibt, welche Bescheinigungen und Zugangsverwaltung auf einer Plattform zusammenführt. Somit ist für den Anwender nur noch ein Gerät bzw. eine Anwendung für die Authentisierung für Dienstleistungen wie auch den Zutritt zu Gebäuden notwendig. Ein Smartphone wird in den meisten Fällen bereits mitgeführt. Falls der Nutzer kein mobiles Endgerät zur Verfügung hat, kann diese Technologie auch mit existierenden NFC-Karten verwendet werden.

Die Zugangsberechtigungen werden von der entsprechenden Gebäudeverwaltung vergeben. Hierfür stellt die verwaltende Autorität eine verschlüsselte Verbindung mit dem Endanwender her. Über diese peer-to-peer Verbindung können dann je nach Bedarf Zugangsberechtigungen ausgestellt und auch widerrufen werden. Die Voraussetzungen für den Zugang können individuell angepasst werden und ermöglichen eine rollenbasierte Zugangsverwaltung. So kann z.B. ein Arbeitgeber jeder Person Zutritt zu einer Räumlichkeit gestattet, solange diese nachweisen kann, ein Mitarbeiter zu sein. Auch Zugänge für betriebsfremde Mitarbeiter, beispielsweise von Reinigungsunternehmen lassen sich damit vergeben. Gleiches gilt für zeitlich begrenzte Zugangsberechtigungen, die an Wartungsfirmen oder zur Durchführung von Reparaturarbeiten vergeben werden können. Dies schafft ein hohes Maß an Flexibilität, da neue Zugangsvoraussetzungen wie auch Berechtigungen ohne größeren Aufwand oder Kosten angepasst werden können.

4.3 Warum ist die Verwendung von selbstbestimmten Identitäten für die Gebäudeverwaltungen relevant?

Der Zugang zu Gebäuden ist direkt mit der Identität einer Person verbunden. Aufgrund dessen ist eine nutzerzentrierte Perspektive notwendig, um für Individuen eine leichte Handhabung zu gewährleisten. Da die App zur Speicherung der Schlüssel auch sonstige Identitätsinformationen beinhaltet, ist es nicht notwendig für den speziellen Anwendungsfall eine neue App herunterzuladen. Die Identitätswallet dient damit nicht nur zur Speicherung von Identitätsinformationen wie dem Personalausweis, sondern könnte langfristig auch die Funktion des Schlüsselbundes übernehmen.

Sicherheitsvoraussetzungen können auch individuell angepasst werden. So ist es z.B. möglich für sehr sicherheitsrelevante Anwendungsfälle eine personenbezogene Identifizierung mit der Notwendigkeit eines Identitätsnachweises des Vertrauensniveaus signifikant gemäß der eIDAS-

Regulierung zu verlangen. Auch die Nachvollziehbarkeit kann durch die Erstellung eines Zugangsprotokolls verbessert werden. Diese Kriterien können nach Bedarf lockerer oder strikter gehandhabt werden.

Da eine personenbezogene Identifizierung häufig aufgrund von Zugangsvoraussetzungen, wie bspw. der Zuordnung zu bestimmten Personenkreisen, nicht notwendig ist, trägt diese Lösung zur Instandhaltung der Privatsphäre bei. Des Weiteren können kenntnissefreie Beweise (auch zero-knowledge-proofs genannt) genutzt werden, um das Maß an Privatsphäre weiter zu erhöhen.

4.4 Was sind regulatorische und wirtschaftliche Hürden?

Im Allgemeinen sehen wir für die Lösung keine regulatorischen Hürden. Spezifische regulatorische Hürden ergeben sich aus dem jeweiligen Einsatzbereich der Nutzergruppen und müssen individuell geprüft werden.

Um den Zugang individuellen Bedürfnissen anpassen zu können, benötigt die jeweilige Verwaltungsautorität die Möglichkeit, diese mittels einer einfachen Benutzeroberfläche anpassen zu können. Bezüglich der Hardware ist die Kompatibilität und der Zugriff auf die NFC-Schnittstellen ein wichtige Aufgabe. Diese Schließsysteme sollten z. B. das DIDComm Protokoll verstehen, um Verbindungen aufzubauen und verifizierte Bescheinigungen auszutauschen. Die Integration der Technologie in bestehende Systeme stellt die Branche jedoch noch vor eine große Aufgabe, welche nur mit gemeinsamen Bemühungen bewältigt werden kann. Die Implementierung stellt die Kommunikation aktuell via Bluetooth her.

5 SSI Anwendungsfall 3 – Bildungszertifikate

Bildungszertifikate fälschungssicher ausstellen und dezentral widerrufen

5.1 Welches Problem löst dieser Anwendungsfall?

Denken wir an Identität, so verbinden wir oftmals nur Dinge wie Name, Nationalität oder Alter. Unsere Identität besteht jedoch aus einer Vielzahl anderer Attribute und nicht nur aus jenen, die uns seit der Geburt begleiten. Darunter fallen vor allem jene, die wir uns im Laufe unseres Bildungs- und Berufsleben aneignen. Viele davon erfordern viel Einsatz und Zeit sowie hohe Kosten wie beispielsweise Abschlüsse, Diplome und Ausbildungsbescheinigungen, aber auch Empfehlungsschreiben des Arbeitgebers. Diese Informationen haben einen erheblichen Einfluss auf die Karriere, soziale Aktivitäten und die generelle Wahrnehmung einer Person.

Besonders in Zeiten der voranschreitenden Digitalisierung und Globalisierung, in der Mitarbeiter und Bewerber immer internationaler werden, wird es für den Arbeitgeber schwieriger den Bildungsweg und beruflichen Werdegang zu überprüfen. Es liegt daher Nahe, dass das Fälschen dieser Informationen ein sehr interessantes und lukratives Geschäft für Betrüger darstellt.

5.2 Wie sieht die Lösung aus? Was ist der Vorteil?

Ethense ist eine von ConsenSys Academy gemeinsam mit uPort (ConsenSys Identity) entwickelte Software, die es Universitäten, Schulen, Online-Lernplattformen und jeglicher Bildungseinrichtung ermöglicht, auf Verifiable Credentials-basierende Zertifikate an ihre Teilnehmer auszustellen. Nachdem die Teilnehmer ein Zertifikat erhalten haben, können sie diese auf ihrem Smartphone in der passenden SSI Wallet zur Wiederverwendung aufbewahren.

Eine Einrichtung verwendet dabei eine Zertifikatvorlage und entscheidet, welche Informationen das Zertifikat enthalten soll wie beispielsweise Namen des Teilnehmers, den Kurs und das Datum des Abschlusses. Danach erhalten die Teilnehmer von der Einrichtung eine E-Mail mit einem eindeutigen QR-Code. Anschließend scannt der Teilnehmer den QR-Code mittels Smartphone und wird damit zum Eigentümer des Zertifikates. Abschließend erhält die Einrichtung eine Benachrichtigung über die Entgegennahme des Zertifikats.

Das Zertifikat selbst ist zweifach kryptographisch geschützt und enthält dabei zum einen die elektronische Signatur der Einrichtung, sowie eine Kennung über die mittels Blockchain der öffentliche Schlüssel der Einrichtung zur Verifizierung abgerufen werden kann. Zum anderen enthält das Zertifikat auch die Kennung des Teilnehmers und wird bei der Weitergabe mit dem entsprechendem Schlüssel des Teilnehmers signiert, sodass sichergestellt werden kann, dass der Teilnehmer selbst, die Weitergabe veranlasst hatte. Der öffentliche Schlüssel des Teilnehmers kann wiederum mittels Blockchain abgerufen werden.

Verglichen mit bisherigen Lösungen wie beispielsweise PDF-Signaturen obliegt die Weitergabe des Zertifikates alleine dem Teilnehmer und der Empfänger kann prüfen, ob der Teilnehmer wirklich der legitime Besitzer des erhaltenen Zertifikates ist. Des Weiteren bestehen keine weiteren Abhängigkeiten zu der Infrastruktur der jeweiligen Einrichtung. Auch Einrichtungen profitieren von der erhöhten Sicherheit, da so eventuelle Marken- und Rufschäden umgangen werden können. Außerdem können diese Zertifizierungen widerrufen werden, ohne Zugriff auf das Smartphone des Teilnehmers zu haben, um im Falle des Verlustes oder Diebstahls des Smartphones Betrug entgegenzuwirken.

5.3 Wie entstand die Idee?

ConsenSys Academy ist eine auf Blockchain-spezialisierte online Lernplattform. Diese vergibt Zertifikate an Entwickler nach erfolgreicher Bewältigung eines Kurses. Bestehende Lösungen waren nicht universell genug, d.h. basierten nicht auf Standards, oder hatten sicherheitskritische Bedenken. Weitere Bildungseinrichtungen hatten zudem auch Interesse an dieser Lösung, woraus die Idee geboren wurde, eine wiederverwendbare Anwendung basierend auf Verifiable Credentials zu entwickeln.

Die Frankfurt School of Finance & Management war die erste Hochschule in Deutschland, die Zeugnisse für Studenten, die den Kurs »Certified Blockchain Expert« absolviert haben, auf Basis von Verifiable Credentials erstellt und verteilt hatte. Die Teilnehmer lernten dadurch die neue Technologie, ihre Möglichkeiten und Anwendungen in verschiedenen Branchen kennen und konnten gleichzeitig einige ihrer Vorteile persönlich erleben, indem sie den vollen Besitz des Zertifikats erhielten.

5.4 Was sind regulatorische und wirtschaftliche Hürden?

Neben der DSGVO (Datenschutzgrundverordnung) gab es keine besonderen regulatorischen Hürden. Es werden keine personenbezogenen Daten auf der Blockchain selbst gespeichert, womit diese Lösung wie jede andere Applikation, die Personendaten verarbeitet, mit dieser Verordnung in Einklang gebracht werden kann.

Grundsätzlich gibt es für Universitätszertifikate bereits großes Interesse von Seiten der Europäischen Kommission. Um hier jedoch eine universelle Nutzung zu ermöglichen, ist es notwendig sich auf ein gemeinsames Datenschema der ausgestellten Zertifikate bzw. Verifiable Credentials zwischen Bildungseinrichtungen zu einigen. Dazu wurde bereits ein entsprechendes Projekt im Rahmen von ESSIF (European Self-Sovereign Identity Framework) ins Leben gerufen.

Zudem sind Verifiable Credentials seit November 2019 offiziell ein globaler Standard der W3C, das Gremium, welches das World Wide Web (WWW) standardisiert. Dadurch sollte sich auch die Akzeptanz drastisch erhöhen.

6 SSI Anwendungsfall 4 – Stammdaten- und Zertifikatsmanagement

Stammdaten und Lieferantenzertifikate zwischen Unternehmen automatisch austauschen, validieren und aktualisieren.

6.1 Welches Problem löst dieser Anwendungsfall?

Heutzutage werden Lieferanten-, Material- oder Produktionsdaten von den Unternehmen mehrfach in verschiedenen IT-Systemen gepflegt. Für jedes Unternehmen ist es aufwändig und kostenintensiv, eine hohe Datenqualität zu erreichen. Studien ergeben Kosten aufgrund mangelnder Datenqualität von 8-12% des Unternehmensumsatzes.[1] Ein derartiges Kostenproblem hat somit eine volkswirtschaftliche Bedeutung. Eine unzureichende Datenqualität (z.B. Fehler oder Dubletten) führt nicht nur zu (Personal-)Kosten, sondern auch zu Problemen bei Liefer- und Bezahlprozessen und einem in der Folge nicht realisierten Umsatz.

Hinzu kommt der Aufwand für die Verwaltung von Zertifikaten. Eigene Zertifizierungen müssen regelmäßig an Kunden übermittelt werden. Kunden haben dabei unterschiedlichste Anforderungen an den Inhalt der Dokumente und die Art des Transfers. Mitarbeiter müssen sich immer wieder neu mit den individuellen Anforderungen der Kunden vertraut machen. Das hat unterstrukturierte Prozesse und Fehler zur Folge, wie beispielsweise fehlende oder abgelaufene Zertifikate. Andererseits prüfen Kunden die Zertifikate ihrer Lieferanten weiterhin manuell auf ihre Authentizität und Gültigkeit.

Intermediäre Plattformen zum Stammdatenmanagement können das Problem mindern, aber nicht beheben. Alle Beteiligten müssten einer einzigen Plattform vertrauen und diese nutzen, um den Datenaustausch möglichst effizient zu gestalten. Eine mögliche Monopolisierung und die damit verbundene Abhängigkeit wollen viele Firmen vermeiden.

6.2 Wie sieht die Lösung aus? Was ist der Vorteil?

Anstatt eines manuellen Datenaustausches per Email zwischen Unternehmen, ist die Herkunft von Adressdaten, Bankdaten und Lieferantenzertifikaten erstmals kryptografisch verifizierbar und der unternehmensübergreifende Austausch umfänglich automatisierbar. Eine solche branchenübergreifende Lösung wird Bosch im Kontext seines strategischen Vorausentwicklungsprojekts »Economy of Things« zusammen mit Siemens, SupplyOn und weiteren Firmen in der Automobilindustrie erproben und bereitstellen.

1 Haug, A. (2013). Master data quality barriers: An empirical investigation. Industrial Management & Data Systems 113(2):243-249

Die Daten werden beim Eigentümer selbst gespeichert, sodass die Datenhoheit des Berechtigten sichergestellt bleibt. Mittels der zur Verfügung gestellten Unternehmenssoftware können Geschäftspartner Unternehmensdaten als »Verifiable Credentials« verteilen, empfangen und automatisiert auf ihre Authentizität prüfen. Interne Datenbanksysteme werden über Konnektoren angebunden und können so weiter genutzt werden. Ändert sich beispielsweise der Sitz eines Unternehmens, wird dies automatisch den Geschäftspartnern mitgeteilt. Aufwändige Benachrichtigungsprozesse der Änderungen entfallen und Geschäftspartner haben stets die aktuellen Daten zur Verfügung. Zusammengefasst ergeben sich folgende Vorteile für Anwender:

- **Datensouveränität**: Unternehmensdaten werden beim Kunden selbst gespeichert
- **Privatsphäre**: Unternehmen können jederzeit selbst nachvollziehen, wer Zugriff auf die aktuellen Daten hat
- **Effizienz im Datenaustausch**: Eine Vertrauensinfrastruktur mit sogenannten »Verifiable Credentials« automatisiert heutige manuelle Überprüfungsprozesse von Unternehmensdaten (z.B. Lieferantenzertifikate)
- **Offenheit**: Die Berücksichtigung von globalen Standards (z.B. W3C-Standard DID) stellt die Interoperabilität zwischen verschiedenen IT-Systemen sicher und ermöglicht jedem Akteur die Teilnahme. Unterstützt wird dies durch Open-Source-Veröffentlichungen von Standardkomponenten für das Management von Unternehmensidentitäten und Zugriffsrechten

Mittels der Agentensoftware wird so erstmals ein automatisiertes und beschleunigtes Kunden- und Lieferantenonboarding möglich.

6.3 Wie entstand die Idee?

Digitale, dezentrale Identitäten von Unternehmen (DID) sind eine Voraussetzung zur sicheren Authentifizierung und Autorisierung eines unternehmensübergreifenden Zugriffs auf verschiedenste Datenelemente (Produkt, Maschine).

Die Entwicklungskooperation erfolgt im Rahmen der Arena 2036 in Stuttgart, einer Forschungsplattform für Mobilität und Industrie der Zukunft, in der zunächst der sichere Datenaustausch zwischen Maschinen fokussiert wurde. Anwendungsanalysen ergaben jedoch ein wesentlich immanenteres Problem bei heutigen Prozessen im Stammdaten- und Zertifikatsmanagement. Mittels »Verifiable Credentials« können Datenquellen automatisch verifiziert werden. Vertraut man der Quelle, werden heutige Prüfprozesse von Adressanten, Bankdaten oder Zertifikaten obsolet. Bereits heute können Unternehmen ihren Lieferanten Zertifikate ausstellen, die diese wiederrum in Onboardingprozessen bei weiteren Kunden verwenden können. Gleichzeitig profitieren Kunden von bereits ausgestellten Zertifikaten und geprüften Dokumenten, indem die eigenen Onboardingverfahren beschleunigt werden.

6.4 Was sind regulatorische und wirtschaftliche Hürden?

Es gibt keine wesentlichen regulatorischen Hürden, die gegen eine Einführung des Systems sprechen. Aus wirtschaftlicher Perspektive erleichtert eine standardisierte Datensemantik die Wiederverwendbarkeit von Unternehmensstammdaten. Entsprechende Initiativen sind vorhanden, erzielen jedoch noch keine allgemeine Marktdurchdringung. Umso mehr sind solche Initiativen mitentscheidend für eine Verbesserung bestehender Stammdaten- und Zertifikatsmanagementprozesse.

Die Herausforderung in diesem Use Case besteht darin, Interoperabilität zwischen verschiedenen Identitätsanbietern und -technologien (z.B. eIDAS) zu erreichen. Damit entsteht ein Ökosystem von Organisationen, das allen Akteuren eine Teilnahme am System ermöglicht und damit das Potenzial von »Verifiable Credentials« zur automatisierten Überprüfung von Unternehmensdaten hebt. Der Prozess kann enorm beschleunigt werden, wenn staatliche Stellen unterstützend heute bereits verfügbare Dokumente in elektronischer Form bereitstellen. Und zwar als kryptographisch überprüfbare elektronische Dokumente (Verifiable Credentials) in kompatiblen Datenformaten. Das können beispielsweise Einträge im Handelsregister sein.

Mit diesem Konzept kann die digitale Vertrauenslücke geschlossen werden, ohne Abhängigkeiten zu schaffen – eine wichtige Voraussetzung für digitale Geschäftsmodelle zwischen Unternehmen auf Augenhöhe.

7 Fazit

Self-Sovereign Identities bzw. dezentrale digitale Identitäten haben das Potenzial, unser Verständnis von – und unseren Umgang mit – Daten und Identitäten im digitalen Raum neu zu erfinden. Parallel zum stets steigenden Datenvolumen im Internet, zu den stets steigenden Datenanalysemöglichkeiten durch Künstliche Intelligenz, und der immer zentraleren Rolle von globalen Digitalkonzernen wächst auch die Bedeutung von Datensouveränität und Datensparsamkeit. Nicht zuletzt zeigt die Diskussion um die zentrale oder dezentrale Speicherung der Daten bei der von der Bundesregierung herausgegebenen Corona-Tracing-App, welche immense Bedeutung die Selbstbestimmung beim Umgang mit Daten heute hat.

Das ambitionierte Versprechen von SSI, dem Nutzer seine Kontrolle über seine digitale Identität zurückzugeben, hat sich inzwischen herumgesprochen. Die deutsche Bundesregierung, die EU Kommission, sowie etliche staatliche und private Initiativen weltweit fördern und erforschen derzeit deren Möglichkeiten. Nicht selten stehen in der Diskussion dann technische (Standards etc.) sowie regulatorische (Datenschutz, elektronische Signaturen etc.) Hürden im Vordergrund, die eine praktische Umsetzung von SSI momentan verhindern.

Vor der breiten produktiven Umsetzungsreife sind jedoch noch weitere wesentliche Herausforderungen im gesamten Ökosystem SSI zu überwinden: Wie sehen etwa die Geschäftsmodelle für die Entwicklung und den Betrieb der notwendigen Software und Services aus? Was ist der Mehrwert gegenüber klassischen Lösungen für Webshops, welche die Technologie einsetzen, um Kunden zu identifizieren? Wer bürgt in der dezentralen Architektur für das Vertrauensniveau, wie etwa der Staat für den Personalausweis und wie lassen sich ausgestellte Zertifikate zuverlässig widerrufen? Wie lässt sich die Selbstverantwortlichkeit der Nutzer bedienungsfreundlich und skalierbar umsetzen, wenn etwa, wie es ständig passiert, Zugangsdaten verloren gehen (Schlüsselmanagement)?

Zufriedenstellende Antworten auf all diese Fragen sind nicht von heute auf morgen zu erwarten. Die hier dargestellten Anwendungsfälle von SSI zur Dezentralen Dokumentation für das Risikomanagement in der Lieferkette von Pharmakonzernen (Kapitel 3), für die Zugangsverwaltung von Gebäuden (Kapitel 4), die Ausgabe und Verifizierung von Bildungszertifikaten (Kapitel 5), oder das Stammdaten- und Zertifikatsmanagement zeigen allerdings, dass sich SSI bereits heute in klar definierten Anwendungsfällen umsetzen lässt und Mehrwerte liefert. Damit möchten wir SSI zugänglicher und greifbarer machen und zu einer breiten gesellschaftlichen und politischen Diskussion beitragen, die das Thema zweifellos verdient. Denn nur dadurch entsteht die notwendige Dynamik um die hohen Hürden zu nehmen und den Weg von der Vision in die Praxis weiter zu ebnen.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 1.900 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org