

Innovative VERWALTUNG

Praxis

Wie selbstverwaltete Identitäten mit Self Sovereign Identity die Verwaltung verändern können.



Bescheinigungen mittels Blockchain neu gedacht

Ob Unternehmen oder Bürgerinnen und Bürger: Alle benötigen immer wieder Bescheinigungen von Behörden zur Vorlage bei Dritten. Übliche Papierbescheinigungen ziehen aber aufwendige Prozesse und Medienbrüche nach sich. Selbstverwaltete Identitäten mit Self Sovereign Identity könnten die Verwaltung grundlegend verändern.

Autor

Ansgar Knipschild

verantwortet den Blockchain-Bereich bei mgm technology partners. ansgar.knipschild@mgm-tp.com

Dr. Daniela Kühne

ist Referentin in der Sondereinheit Zentrale Steueraufsicht beim Bayerischen Landesamt für Steuern. daniela.kuehne@lfst.bayern.de

Prof. Dr. Nils Urbach

ist Professor für Wirtschaftsinformatik, insbesondere Digital Business und Mobilität an der Frankfurt University of Applied Sciences sowie Mitgründer und Leiter des Fraunhofer Blockchain-Labors. nils.urbach@fim-rc.de

ie Herausforderungen der Verwaltung im Umgang mit Bescheinigungen auf Papier sind allgegenwärtig und die Nachteile offensichtlich. Neben Medienbrüchen sind manuelle Bearbeitungen fehleranfällig und verlangsamen die Prozesse für alle Beteiligten. Außerdem besteht für Papierbescheinigungen ein erhöhtes Fälschungsrisiko. Zudem können sie nur schwer widerrufen werden. Nachweise mit einem definierten Gültigkeitsende erforden wiederum regelmäßige Aktualisierungen durch Antrag oder Anfrage, Bearbeitung, Ausstellung und Versand und damit wiederkehrende Ressourcenbelastung auf Antrags- und Behördenseite. Vor diesem Hintergrund wurden oftmals von einzelnen Behörden individuell vorangetrieben - Systeme wie beispielsweise das elektronische Grundbuch zur Verwaltung von Personen- und Unternehmenseigenschaften geschaffen. Gegenüber papierbasierten Prozessen ist das zunächst ein Fortschritt. Doch spezifischen Systemen mangelt es meist an Interoperabilität, was zu Komplexitäten bei den beteiligten Parteien führt. Dies bedeutet, dass Bürgerinnen und Bürger sowie Unternehmen für jede Interaktion mit unterschiedlichen Behörden eine eigene Anwendung nutzen müssen. Zudem müssen Authentisierungs- und Authentifizierungsprozesse für die Nutzung von IT-Systemen und für die Erbringung von Nachweisen mehrmals redundant durchgeführt werden. Somit können digitale Nachweise über Personen- oder Unter-

Kompakt

- SSI eignet sich vor allem für domänenübergreifende Nachweise, bei denen Ausstellung und Überprüfung separat geschehen, etwa die Kombination von Identitätsnachweis und einer spezifischen Bescheinigung.
- Um das Potenzial von SSI maximal auszuschöpfen, sollten sich viele unterschiedliche Akteurinnen und Akteure als Issuer und Verifiers beteiligen.
- SSI steht für ein nutzerfreundliches Identitätsmanagementsystem, das alle Identitätsmerkmale und -bescheinigungen in einer Anwendung komfortabel zur Verfügung stellt.
- Alternative Lösungsansätze sollten evaluiert werden, um einen Ansatz zu identifizieren, der am besten geeignet ist.

nehmenseigenschaften, wie beispielsweise über steuerliche Identifikationsmerkmale, aufgrund mangelnder Interoperabilität nur selten behörden- oder institutionenübergreifend genutzt werden. Diese geringe Nutzerfreundlichkeit führt oftmals zu einer niedrigen Akzeptanz solcher Systeme seitens der Unternehmen sowie der Bürgerinnen und Bürger.

Digitale Nachweissysteme noch in den Kinderschuhen

Die Gründe für das Fehlen eines behördenübergreifenden Ökosystems für digitale Nachweise sind vielfältig. Um die Autonomie und Dezentralität von Behörden zu wahren, könnten die bereits existierenden, dezentral betriebenen IT-Systeme miteinander verknüpft werden. Dies wäre jedoch eine enorme Herausforderung im Hinblick auf Komplexität und Kosten, weil mit jedem weiteren System eine exponentielle Anzahl an Schnittstellen zu unterschiedlichen Bestandssystemen geschaffen und gepflegt werden müsste. Dabei ist zu erwarten, dass die Anzahl der potenziell zu verbindenden Insellösungen weiter ansteigt: Die Digitalisierung von Nachweisprozessen steht noch am Anfang.

Eine alternative Lösung ist ein neues, gemeinsam betriebenes System. Um dies zu realisieren, müssten sich Behörden und Verwaltungsorgane auf den Ebenen Bund, Länder und Kommunen auf ein System einigen. Das ist insbesondere vor dem Hintergrund der in Deutschland stark ausgeprägten föderalen Strukturen allerdings nicht zu erwarten. Zudem erschweren sowohl einschlägige Datenschutzregularien als auch das Verfassungsrecht die zusätzliche Zusammenführung von Bürgerdaten an einer zentralen Stelle. Das Bundesmeldegesetz regelt beispielsweise die Verantwortlichkeiten für die Erfassung und Speicherung von Meldedaten. Die zentrale Datenverarbeitung ohne Einbezug der betroffenen Bürgerinnen und Bürger ist so nur unter bestimmten Voraussetzungen und in spezifischen Anwendungsfällen möglich.

Vor dem Hintergrund der Probleme der bisherigen Prozesse zum Nachweis von Personen- oder Unternehmenseigenschaften wird ein einheitliches Identitätsmanagement notwendig. Viele Identitätsmanagementsysteme beruhen aktuell jedoch auf zentralen und hierarchischen Strukturen wie beispielsweise dem x.509-Standard. Diese werden den Anforderungen eines föderalistischen Systems nicht gerecht. Demgegenüber stehen dezentrale, föderalistische Systemlandschaften, die sehr hohe Infrastrukturaufwendungen verursachen. Dazu zählt beispielsweise auch die europaweite eIDAS-Infrastruktur. Diese skalieren schlecht und sind entsprechend meist nur für begrenzte Anwendungsfälle geeignet.

Blockchain-Ansatz als Teil der Lösung

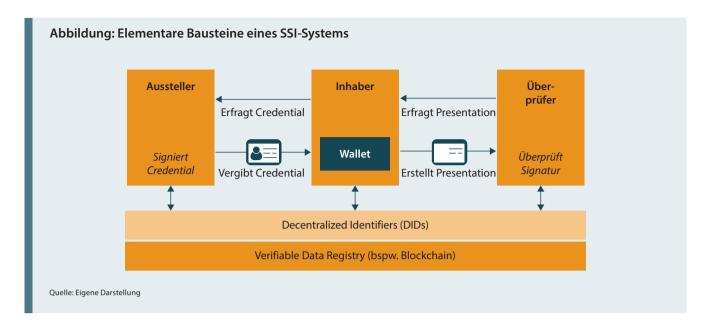
Um diese Probleme zu bewältigen, kann das neu gedachte Identitätsmanagementkonzept "Self-Sovereign Identity" (kurz: SSI) eingesetzt werden. SSI bildet ein dezentrales Identitätsmanagement ab, das einen ausgeprägten Fokus auf die Datenhoheit der Nutzerinnen und Nutzer legt. Alle digitalen Daten, die die Identität einer Person betreffen, werden durch diese gehalten, verwaltet und freigegeben. Die darstellbaren Informationen sind dabei nicht auf reine Stammdaten beschränkt. Auch Nachweise und Bescheinigungen können als Personen- oder Unternehmenseigenschaften mittels SSI abgebildet werden, beispielsweise auch Steuerdaten. Hierzu zählen steuerliche Identifikationsmerkmale oder Einkommensgrößen, die von der Finanzbehörde ausgestellt oder durch den Steuerbescheid festgesetzt werden. Ähnlich zu Prozessen aus der analogen Welt erhalten Unternehmen sowie Bürgerinnen und Bürger einen Nachweis mittels eines digitalen Zertifikats und können dieses bei Bedarf anderen Stellen vorzeigen. Das Gegenüber kann die Validität des Zertifikats in Echtzeit überprüfen, ohne den Aussteller kontaktieren zu müssen. Eine solche SSI-Lösung lässt sich in fünf Softwarebestandteile unterteilen (siehe Abbildung):

- Verifiable Credentials sind die zentralen Artefakte zum Austausch und Nachweis von Identitätsattributen zwischen den zentralen Rollen einer SSI-Lösung.
- Die Rollen wiederum bilden im Rahmen der Issuer-Holder-Verifier-Beziehung das Grundgerüst aller Interaktionen. Jedes Verifiable Credential wird von einem Issuer erstellt, von einem Holder aufbewahrt und darin enthaltene Informationen dem Verifier in Form einer Verifiable Presentation vorgezeigt. Das ist ein Abbild des Verifiable Credentials und kann nur bestimmte Attribute oder sogenannte Range-Proofs enthalten. Damit lässt sich beispielsweise beweisen, dass eine Person älter als 18 Jahre alt ist, ohne jedoch die anderen Attribute wie Name und Adresse vorzuzeigen.
- Schließlich erlaubt ein Verifiable Data Registry, zumeist in Form einer Blockchain, den beteiligten Parteien, die Authentizität und Gültigkeit eines Verifiable Credentials zu überprüfen.
- Um möglichst die Privatsphäre der Nutzerinnen und Nutzer zu schützen, können diese bei Bedarf unter wechselnden **Identifiern** auftreten. Dafür sorgt der DID-Standard ("Decentralized Identifiers") für eine Ende-zu-Ende-verschlüsselte, bilaterale Kommunikation.
- Die einzelnen Verifiable Credentials sowie kryptografische Schlüssel werden dabei in **Digital Wallets** aufbewahrt – zum Beispiel in Form einer Handy-App.

SSI-Einsatz für die steuerliche Erfassung

Da sich mithilfe des SSI-Konzepts auch sehr spezifische Nachweise abbilden lassen, haben das Bayerische Staatsministerium für Digitales und das Bayerische Landesamt für Steuern gemeinsam mit ausgewählten Partnern eine Machbarkeitsstudie durchgeführt. Das Ziel: die Erprobung von SSI für den Nachweis über die steuerliche Erfassung von Händlern im E-Commerce.

Im Fokus stand die Digitalisierung eines bestehenden papierbasierten Pro-



zesses. Hintergrund war das seit dem 1. Januar 2019 geltende Gesetz über die sogenannte Marktplatzhaftung. Es verpflichtet Marktplätze dazu, Informationen über die auf ihren Plattformen agierenden Anbieter aufzuzeichnen. Die Aufzeichnungspflichten über deren Identität und steuerliche Erfassung konnten dabei zunächst über die Einholung einer "Bescheinigung über die Erfassung als Steuerpflichtiger (Unternehmer)" erfüllt werden.

Kommt der Marktplatz der Verpflichtung zur Einholung der Bescheinigung nicht nach, so haftet dieser für die nicht entrichtete Steuer aus Lieferungen, die auf dem Marktplatz begründet worden sind. Im Inland steuerpflichtige Händlerinnen und Händler beantragen die Bescheinigung aktuell als Papierdokument. Es bescheinigt ihnen, steuerlich erfasst zu sein. Die ausgestellte Papierbescheinigung wird von den Steuerpflichtigen an den Marktplatz übermittelt und von diesem aufbewahrt.

Dieser Prozess führt gerade bei den Marktplätzen zu hohen Aufwendungen, da die jeweiligen Papierbescheinigungen händisch geprüft werden müssen. Zudem ist die Authentizität des Dokuments schwer nachprüfbar: Neben einem Dienststempel und der Unterschrift des Ausstellenden gibt es keine weiteren Schutzmaßnahmen für das Dokument. Das gilt auch für den Gültigkeitsstatus einer Papierbescheinigung, der sich nicht aktualisieren lässt. Sobald sich beispielsweise eine Onlinehändlerin oder -händler beim zuständigen Finanzamt abmeldet, erlischt die steuerliche Erfassung. Das müsste Auswirkungen auf den Nachweis haben, etwa durch Einzug der ausgegebenen Papierbescheinigung. Dies ist jedoch nicht praktikabel, da die Händlerin beziehungsweise der Händler das Dokument mit vergleichsweise wenig Aufwand vervielfältigen kann. Auch eine Mitteilung an die Marktplätze ist ausgeschlossen, schließlich ist der Finanzbehörde nicht zwingend bekannt, auf welchen Marktplätzen eine Händlerin/ein Händler Umsätze generiert.

Fälschungssicherheit und Gültigkeitsregister

Die oben genannten Punkte lassen großes Potenzial durch eine Digitalisierung der Prozesse erkennen. Vor allem könnte SSI durch inhärente Eigenschaften wie Fälschungssicherheit und ein hohes Maß an Datenschutz eine wichtige Infrastruktur für den Nachweis steuerlicher Informationen bieten. Das Bayerische Landesamt für Steuern hat in der Machbarkeitsstudie entsprechend den bisher papierbasierten Prozess als Grundlage ge-

nutzt, um diesen prototypisch mit SSI zu digitalisieren.

Statt eines Papierdokumentes werden in einem SSI-System Verifiable Credentials ausgegeben und anstelle einer Brieftasche oder Dokumentenmappe wird eine digitale Wallet zur Aufbewahrung der Nachweise genutzt. Auf Antrag einer Händlerin/eines Händlers stellt die zuständige Finanzbehörde nach positiver Prüfung der erforderlichen steuerlichen Erfassung durch Abgleich mit den gespeicherten Stammdaten ein Verifiable Credential aus. Hierbei ist nun auch die Deaktivierung eines Verifiable Credentials möglich, beispielsweise wenn sich eine Händlerin/ein Händler beim zuständigen Finanzamt abmeldet: Auf der Blockchain wird dazu parallel ein Gültigkeitsstatus registriert. Mit Erhalt ihres/seines Verifiable Credentials kann die Händlerin/der Händler anschließend ähnlich zum aktuellen Papierdokument seine steuerliche Erfassung nachweisen. Durch Einsatz der Blockchain kann zudem gegenüber dem Marktplatz nachvollziehbar bewiesen werden, dass das Verifiable Credential nicht widerrufen wurde, die Händlerin/der Händler also noch steuerlich erfasst ist.

Im Gegensatz zu zentralistischen digitalen Identitätssystemen erfolgt die Informationsweitergabe beim SSI-Konzept

stets bilateral und nur unter Aktivwerden der Identitätsinhaberin beziehungsweise des -inhabers, in diesem Fall die Onlinehändlerin/der Onlinehändler. Zur Verifizierung der Gültigkeit muss der Aussteller durch den Verifier nicht kontaktiert werden. Entsprechend besitzt die Identitätsinhaberin/der Identitätsinhaber die volle Hoheit über ihre/seine Daten und kann selbst entscheiden, wer Einsicht auf welche Attribute bekommt. Weiterhin baut das SSI-System auf einer Reihe von offenen Standards auf, denen jede Organisation ebenfalls folgen und so Gebrauch von den ausgestellten Verifiable Credentials machen kann.

Dieser Ansatz lässt sich auf zahlreiche weitere Verfahren übertragen, in denen Nachweise von einer Organisation ausgestellt werden, eine weitere Person oder Organisation als Dateninhaberin beziehungsweise -inhaberin auftritt und im Nachweis enthaltene Eigenschaften einer interessierten Drittpartei bewiesen werden müssen. So wäre es in Zukunft beispielsweise möglich, bei der Beantragung eines Kredits den Namen und Wohnort mit einem Personalausweis-Verifiable-Credential und die Höhe des Einkommens mit einem Steuerbescheid-Verifiable-Credential sicher und einfach nachzuweisen. Durch ihre Arbeit konnten die beteiligten Projektpartner zeigen, dass sich SSI gut dazu eignet, Unternehmen sowie Bürgerinnen und Bürgern einen einfachen und selbstbestimmten Datenaustausch mit unterschiedlichen Behörden und Unternehmen zu ermöglichen. Credentials können von einer Partei an Unternehmen sowie Bürgerinnen und Bürger ausgestellt werden und diese können die darin hinterlegten Informationen fälschungssicher einer weiteren Partei vorzeigen. Es hat sich gezeigt, dass sich SSI insbesondere für solche Nachweise eignet, die domänenübergreifend genutzt werden: in allen Fällen, in denen die Datenausstellung und -überprüfung unabhängig voneinander durch verschiedene Parteien erfolgen können sollte.

Entstehung eines Ökosystems

Durch den dezentralen Charakter von SSI und den Einsatz von Blockchain können die verschiedensten Parteien von solch einem System profitieren. Denkbar sind also organisations- und sogar staatenübergreifende Nachweisprozesse. Ein übergreifendes Ökosystem vereinfacht zudem die Umsetzung solcher Systeme erheblich. Es muss zur Nachweisprüfung also nicht zunächst das verantwortliche System gesucht und angefragt werden, sondern es kann eine gemeinsame, dezentrale Infrastruktur genutzt werden. So werden hohe Integrationsaufwendungen fast vollständig vermieden und treten nur ein einziges Mal durch die Anbindung an die Blockchain auf.

Unternehmen sowie Bürgerinnen und Bürger profitieren gleichermaßen von SSI. Durch die Einbindung verschiedener Parteien in einem offenen und dezentralen Ökosystem können Unternehmen sowie Bürgerinnen und Bürger in Zukunft mit nur einer einzigen App Nachweise von verschiedenen Organisationen sammeln und diese unabhängig an unterschiedlichen Stellen vorzeigen. Abschließend wurde in dem Projekt auch eingängig die Datenschutzkonformität des Systems analysiert. Nach erster Evaluation können die strengen DSGVO-Vorgaben eingehalten werden, da auf der Blockchain keine personenbezogenen Daten gespeichert werden.

Neben dem Bayerischen Staatsministerium für Digitales fördert auch der Bund forschende SSI-Initiativen. Das BMWi unterstützt beispielsweise im Innovationswettbewerb "Schaufenster sichere di-

gitale Identitäten" bis zu vier große Schaufensterprojekte mit mehr als 50 Millionen Euro. Das große Interesse beruht insbesondere darauf, dass Bescheinigungen und Nachweise im Alltag fast überall anzutreffen sind. Entsprechend existieren in jedem Unternehmen und in jeder öffentlichen Institution eine Vielzahl unterschiedlicher Prozesse, die vom Einsatz von SSI profitieren könnten.

Fazit: Durch sichere und interoperable Identitäten könnten papierbasierte Bescheinigungen oder die Notwendigkeit von redundanten Anmeldungen und Nachweisen der Vergangenheit angehören. Somit lässt sich festhalten, dass ein entsprechendes SSI-Ökosystem sowohl für Bürgerinnen und Bürger, Unternehmen als auch für Behörden große Vorteile bietet. Es lohnt sich also, sich frühzeitig mit dem Konzept SSI auseinanderzusetzen und auch in den ersten Schritten, beispielsweise im Rahmen eines Prototyps, bereits im Sinne eines größeren übergreifenden Ökosystems zu denken.

Weiterführende Informationen finden Sie im Whitepaper "Einsatz der Blockchain-Technologie in der Steuerverwaltung" vom Bayerischen Landesamt für Steuern: https://insights.mgm-tp.com/SSI-LfSt



Blockchain



Rehfeld, D. (2021): Mit Blockchain zur digitalen Verwaltung, in: innovative Verwaltung, 3, S. 24-25, https://go.sn.pub/yczCjx

Meinel, C., Gayvoronskaya, T. (2020): Das sollten Sie wissen, um die Blockchain-Technologie zu verstehen, in: Blockchain, Berlin, Heidelberg, S.17-38, https://go.sn.pub/ThoHCu

IMPRESSUM:

Sonderausgabe 2021 in Kooperation mit mgm technology partners GmbH, Taunusstr. 23, 80807 München, www.mgm-tp.com; Springer Fachmedien Wiesbaden GmbH, Postfach 1546, 65173 Wiesbaden, Amtsgericht Wiesbaden, HRB 9754, USt-IdNr. DE311484199

GESCHÄFTSFÜHRER:

Stefanie Burgmaier I Andreas Funk I Joachim Krieger

PROJEKTMANAGEMENT: Anja Trabusch

TITELBILD: © iStockphoto



mgm | public sector

Digitale Transformation. Digitale Souveränität.









