Digitale Identitäten - Legitimationen zur Nutzung kommunaler Angebote

Dr. Michael Schmitt
regio iT Gesellschaft für Informationstechnologie mbh
kontakt_reallabor@fit.fraunhofer.de

Ausgangssituation und Problemstellung

Die Nutzung kommunaler Dienstleistungen erfordert oft analoge Ausweise und Bescheide. So gibt es beispielswiese Bibliotheksausweise, Städte-Pässe, Senioren-Pässe, Familienausweise und Ehrenamtskarten, etc., die teilweise zusammen mit einem Personalausweis vorgelegt werden müssen, um Dienste nutzen zu können. Teils werden auch Vergünstigungen bei bestimmten Voraussetzungen und der Vorlage der Bestätigung eines Amtes gewährt. So wird etwa der Eintritt in städtische Museen und Schwimmbäder rabattiert für bestimmte Benutzergruppen. Die sichere Identifikation der Benutzer ist in vielen Anwendungsfällen eine zwingende Voraussetzung. Eine Benutzung digitaler kommunaler Dienstangebote erfordert bislang in der Regel separate Registrierungen für jedes einzelne Angebot. Beispielsweise ist die Anmeldung in einem Bürgerportal unabhängig von dem Online-Zugang der Stadtbibliothek und wiederum eine andere als die Anmeldung bei den Portalen des städtischen Energieversorgungsunternehmens oder den Verkehrsbetrieben für die Verwaltung der Abonnements des städtischen ÖPNV. Üblich ist eine Anmeldung mit Benutzername und Kennwort - und dies trotz der bekannten Nachteile dieser Methodik hinsichtlich Sicherheit und Komfort, der Abhängigkeit von dem Serviceanbieter und der Gefahr einer Kompromittierung der Systeme des Anbieters und der ggfs. daraus folgenden Offenlegung persönlicher Daten.

Lösungsansatz

Zielsetzung ist es, mit Hilfe einer digitalen Identität den Zugang zu kommunalen Angeboten zu erleichtern und sicherer zu gestalten. Dazu sollen persönliche Berechtigungen als Attribute zu einer digitalen Identität zugewiesen werden. Dies können z.B. folgende sein:

- Attribut ‚Meldeadresse' für die Nutzung einer Stadtbibliothek (wenn bereits aus dem Wohnort auf das Recht der Bibliotheksbenutzung für alle Bürger der Kommune geschlossen werden kann)
- Attribut ‚Inhaber des Städte-Passes' für die Gewährung verschiedener Vergünstigungen
- Attribut ‚Schulwegticket' für die Benutzung des ÖPNV

Bedeutsam für die Akzeptanz und das Erzielen einer Erleichterung bei der Benutzung ist die Bündelung möglichst vieler Attribute von unterschiedlichen Institutionen als Herausgeber auf eine gemeinsame digitale Identität. Eine Verteilung auf jeweils spezifische Identitäten für jeden separaten Dienst würde die Akzeptanz und Gebrauchstauglichkeit reduzieren und erscheint nicht zielführend.

Eine mögliche Form der Realisierung dieses Lösungsansatzes stellt die Technologie der selbstbestimmten digitalen Identitäten (*Self-Sovereign Identity*, SSI) dar. Hierbei handelt es sich um eine universelle Methodik für Identitäten und Nachweise, bei der die Belege für Herkunft und Integrität von Attributen in einer Blockchain bzw. einem Distributed Ledger gespeichert und diese dort für überprüfende Instanzen bereitgestellt werden. Das Attribut selber wird dem Besitzer bzw. Inhaber zugewiesen, der es als Teil seiner digitalen Identität in einer mobilen App in Form eines „Identitäts-Wallets" aufbewahrt. Der Inhaber kann einzelne Attribute seiner digitalen Identität aus diesem Wallet auf Anfrage nach eigenem Ermessen verfügbar machen und behält damit die Kontrolle darüber, wer welche persönlichen Daten von ihm erhält. In der Blockchain werden keine persönlichen Daten gespeichert, sondern nur sogenannte *Decentralised Identifiers* (DID), die nach einem Standard des World

Wide Web Consortium (W3C) global eindeutige Referenzen darstellen. Die Blockchain dient als dezentraler unveränderlicher Speicher der Transaktionen von DIDs.

Die Attribute dieses Modells werden *Verifiable Credentials* (VC) bzw. überprüfbare Berechtigungsnachweise genannt und mit einem Datenmodell gemäß eines W3C Standards beschrieben. Der Ansatz ergibt insgesamt ein Benutzer-zentriertes Modell der Verwaltung von Identitäten, das im Gegensatz zu der traditionellen Verwaltung von Identitätsdaten in isolierten Datensilos der Dienstanbieter steht.

Die Methodik wurde bereits in verschiedenen *Technologie-Stacks* implementiert und ist sowohl von kommerziellen Herstellern als auch als Open Source Lösung verfügbar. Sie ist sehr universell anwendbar und es scheinen daher viele weitere Anwendungsfälle in dem Bereich der Daseinsvorsorge mit *Self-Sovereign Identity* realisierbar zu sein. Zur Veranschaulichung des Prinzips ist als Beispiel der Anwendungsfall ‚Zugang zum Online-Angebot einer Stadtbibliothek' in der nachfolgenden Abbildung dargestellt.

Neben den Implementierungen für die Ausstellung, Verwaltung und Überprüfung einzelner Attribute ist auch die Anmeldung an Webanwendungen bzw. Portalen mit dieser Methodik möglich, die den gebündelten Zugriff auf mehrere Dienstleistungen erlauben.

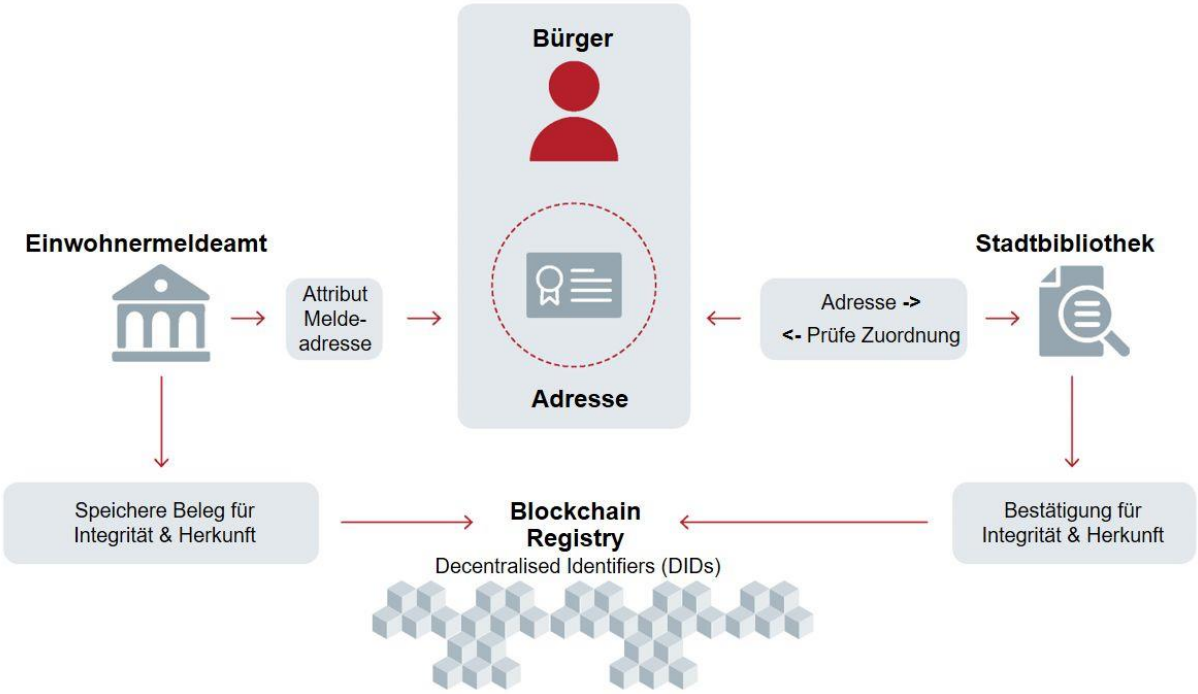

Abbildung 1: Self-Sovereign Identity mittels Blockchain / DLT.

Zu den Vorteilen digitaler Identitäten zählt insbesondere auch die Möglichkeit der sicheren digitalen Überprüfung hinsichtlich der Echtheit und Aktualität. An die Stelle von Tinte und Papier in Verbindung mit Merkmalen zur Erschwerung von Fälschungen treten mathematische Verfahren der Kryptographie.

Registerauszüge, die bislang als Nachweise für die weitere Verwendung in einer Vielzahl von Prozessen erforderlich sind und einem Inhaber in Papierform ausgehändigt wurden, können nun digital ausgestellt werden. Ein Entzug von Berechtigungen ist ebenfalls möglich und kann unmittelbar wirksam werden im Gegensatz zu den üblichen Befristungen zur Beschränkung einer Gültigkeitsdauer auf analogen Medien.

Wird das zugrundeliegende Blockchain-Netzwerk durch verschiedene Institutionen betrieben, so ist sichergestellt, dass die gespeicherten Transaktionen unveränderlich und stets verfügbar sind. Die digitalen Identitäten sind dadurch samt der Berechtigungsnachweise nicht mehr abhängig von einer zentralen Autorität. Idealerweise werden die Knoten des Netzwerks in öffentlichen Institutionen (Rechenzentren von Bund, Ländern und Kommunen) betrieben, nach Governance Grundsätzen deutscher oder europäischer Vereinbarungen

administriert und unterliegen damit der entsprechenden.

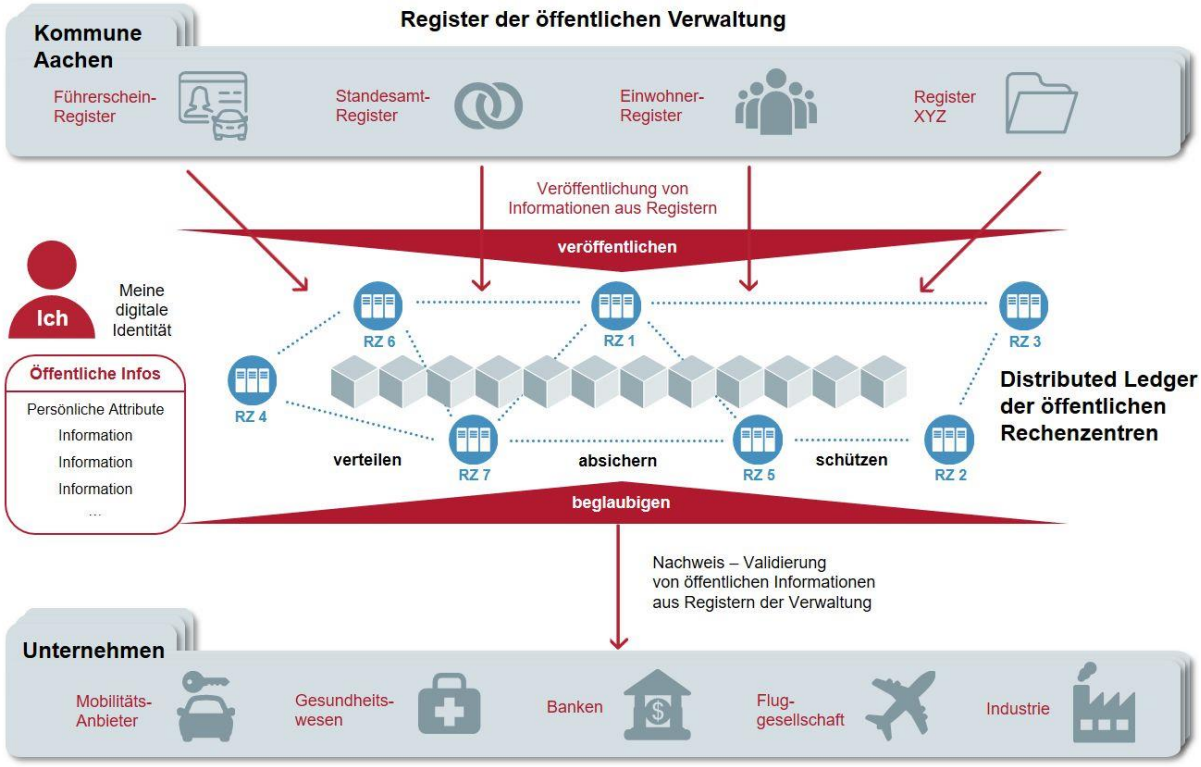

Abbildung 2: Registerauszüge als persönliche Attribute einer digitalen Identität.

Herausforderungen für die Umsetzung

Wichtig ist einfache Bedienung und der einfache Zugang aller Akteure zu der Infrastruktur für die Berechtigungsnachweise. Eine elementare Herausforderung ist die Etablierung eines Standards für die Interoperabilität zwischen verschiedenen Systemen zur Speicherung der digitalen Identitäten, so dass universell verwendbare „digital identity wallets" zum Einsatz kommen können. Auch wenn es wünschenswert wäre, dass keine zu große Diversifikation mit spezifischen Wallets je Anwendungsgebiet eintritt, kann nicht damit gerechnet werden, dass sich nur eine Lösung am Markt durchsetzt. Daher kommt der Interoperabilität eine große Bedeutung zu.

Des Weiteren muss sichergestellt werden, dass in den ausstellenden Institutionen (*Issuer* von *Verified Credentials*) beglaubigte Attribute nur durch entsprechend berechtigte Personen einem Inhaber zugewiesen werden können.

Schließlich ist es für jeden Benutzer sehr einfach, eine beliebige Anzahl an digitalen Identitäten selber zu erstellen. Diesen Identitäten können auch Berechtigungsnachweise zugeordnet werden. Ob aber eine digitale Identität tatsächlich zu einer angegebenen Person gehört, muss durch eine befugte und glaubhafte Institution einmalig bestätigt werden. Dieser Prüfprozess kann z.B. in einem Einwohnermeldeamt oder einer anderen Behörde durch den Abgleich der persönlichen Daten einer vorsprechenden Person durchgeführt werden. Alternativ wäre ein Abgleich mit den Daten des Personalausweises über die eID-Funktion vorstellbar, um die Angaben einer digitalen Identität zu verifizieren.

Das Erzielen einer kritischen Masse an ausstellenden Institutionen und Berechtigungsnachweisen ist für eine allgemeine Akzeptanz des Verfahrens wichtig. Erst dadurch kann ein europäischer Gegenpol zu den internationalen Konzernen mit ihren bereits weit verbreiteten Modellen des ‚federated identity Management' aufgebaut werden.

Stakeholder

Zu den Stakeholdern des Einsatzes von *Self-Sovereign Identity* in den Prozessen der Legitimation für die Nutzung kommunaler Dienstleistungen zählen einerseits die Herausgeber

von Attributen. Diese sind vielfach in den Ämtern der Kommunalverwaltungen zu sehen. Andererseits treten Ämter auch in der Rolle der Prüfer von Nachweisen auf, die von anderen Ämter ausgestellt wurden, und können somit von der Digitalisierung der Prozesse und Nachweiserstellung auch selber profitieren.

In den Anwendungsbereichen der Daseinsvorsorge sind insbesondere die Bürger, die eine der kommunalen Dienstleistungen nutzen möchten, ebenfalls Stakeholder. Darüber hinaus adressieren digitale Identitäten mit den Berechtigungsnachweisen auf Basis der Informationen aus amtlichen Registern viele Prozesse der Privatwirtschaft in den unterschiedlichsten Branchen.