Der Arbeitskreis Digitale Identitäten stellt die zentralen Thesen und Fragen seines Mitgliedertreffen hier in kompakter Form vor.

Mehrwerte dezentraler Wallet-Technologie bei isolierten und föderierten Identitäten – ein Blick über eIDAS 2.0 hinaus

Einführung

Die Herausforderungen bei der Bereitstellung digitaler Identitäten drehen sich vor allem um Fragen wie die Organisation des Vertrauens, Interoperabilität, die Ausgestaltung von Usability und Nutzerkomfort sowie im Sicherheitsbereich die Vermeidung von Über-Identifizierung durch bedarfsgerechte Prozesse, das Speichern von Nutzerdaten sowie das Verhindern einer Profilbildung. Der AK Digitale Identitäten beschäftigt sich in seinen Sitzungen mit diesen Anforderungen und stellt dazu eine Reihe von Fragen und Thesen auf.

Die zentralen Thesen und Fragen

Brauchen wir eine klare Unterscheidung für die Verwendung des Begriffs „Wallet“? (Cloud-basiert / dezentral mobil)

Aus technischer Sicht ist es wichtig, zwischen Cloud- und Edge-Wallets zu unterscheiden. Andererseits stellt sich mehr die Frage, wie viel Macht die Anbieter haben? Können sie auf die Daten zugreifen und diese gegebenenfalls ändern oder nicht? Cloud-Anbieter können besser auf die Daten zugreifen als dezentrale Anbieter. Nach eIDAS soll jedoch jeder Nutzer die Kontrolle über seine Daten haben. Hier wird es interessant sein zu sehen, was nach eIDAS bei Cloud-basierten Wallets passiert. Es gibt also nicht nur die Unterscheidung zwischen Cloud und dezentral mobil, sondern auch die Frage, was mit den Daten geschieht. Dazu gehört nicht nur die Speicherung, sondern auch die Organisation von Zugriffen und das Consent-Management.

These 1: Dezentrale Wallet-Technologie beinhaltet verschiedene Nutzenversprechen.

Auch im Rahmen des Bitkom werden diese Versprechen immer wieder diskutiert. Zentrale Nutzen sind insbesondere folgende:

- **Kostenreduktion** durch die Organisation von IT-Sicherheit ohne Datenhaltung und -management in zentralen Rechenzentren.
- **Verbesserte Usability** über das Mobilgerät durch Offline Use.
- **Flexibles Datenmanagement** durch Normalisierung von Daten zur Vereinfachung der Interoperabilität.
- **Datensparsamkeit** durch Weitergabe von einzelnen Attributen.
- **Datenschutz** durch Verhinderung von Profilbildung.
- **Selbstbestimmung** inkl. Integration des Nutzers in die Geschäftsmodelle bei der Nutzung persönlicher Daten.

In dieser Diskussion kommt jedoch eine wichtige Frage oft zu kurz: wie kann ein Problem in der realen Welt gelöst werden? Welche Probleme gibt es, welche Technologien haben wir zur Hand, wie können wir das gestellte Problem damit lösen? In der Diskussion um Nutzungsversprechen neuer Technologien müssen also die tatsächlichen Endverbraucher bewusst ins Zentrum der Debatte gestellt werden.

These 2: Die Welt „Isolierte, Föderierte und Dezentrale Identitäten“ wird es auch in 10 Jahren noch geben.

Isolierte und föderierte Identitäten sind heute in einer Reihe von Use Cases bereits etabliert und werden, wenn das Anwendungsvolumen betrachtet wird, häufiger genutzt als die neu aufkommenden dezentralen Identitäten. Es gibt also an sich keinen Anlass, dieses System zu verändern. Sollte das Szenario eintreten, dass dezentrale Identitäten eines Tages die Systeme dominieren sollten, muss dennoch in einer Übergangsphase ein Ökosystem geschaffen werden, die alle drei Systeme miteinander interoperabel verbindet. Hierzu kann die Wallettechnologie beitragen, indem bestimme Aspekte der Technologie in den etablierten Systemen angewendet werden. Die Interoperabilität der drei Systeme ist umso wichtiger, als dass es in Zukunft eine Vielzahl an Wallets geben wird, die von im In- und Ausland von staatlichen und privaten Issuern angeboten werden. Wie viele Wallets Nutzende zukünftig haben werden, ist die interessantere Frage, da davon auszugehen ist, dass es sowohl „Single-Wallet“ als auch „Multiple-Wallet“ User geben wird. Die Anzahl der Wallets auf den Endgeräten der Nutzenden wird sich auch entscheidend danach richten, in welchen Bereichen die Use Cases für Wallets liegen werden und vor allem, ob diese Wallets eine gemeinsame Infrastruktur oder für unterschiedliche Use Cases unterschiedliche Infrastrukturen gebraucht werden. Die Nutzung von Wallets ist kein Selbstzweck, sondern ein Werkzeug um auf Services zugreifen zu können. Die Vereinbarkeit isolierter, föderierter und dezentraler Identitäten wird in der Entwicklung digitaler

Identitäten, auch im Rahmen der Schaufensterprojekte, noch zu wenig mitgedacht, ist aber zentral für die Entwicklung eines echten, interoperablen Ökosystems.

Frage 2: Braucht es für die Nutzung mobiler Wallet-basierter Ansätze unbedingt das Vorhandensein eines dezentralen Ökosystems?

Eine Umkehrung der Frage wäre die Frage danach, ob es Use Cases gibt, in denen mit nicht-dezentralen Ökosystemen gearbeitet werden kann.

Die Antwort hängt stark davon ab, wie das Ökosystem auszusehen hat, um die Probleme der Nutzenden zu lösen. In der Ausgestaltung von Wallets und den ihnen zugrunde liegenden Systemen geht es darum zu überlegen, welche Aufgaben es in der realen Welt gibt, die mit einer Wallet zu erledigen sind. Davon abhängig sollte z.B. das jeweilige Sicherheitsniveau der Wallet festgelegt werden. Die Mehrheit der Use Cases benötigen kein hohes Sicherheitsniveau und spielen sich überwiegend im self-declared Bereich ab. Die Ausgestaltung des Ökosystems sollte sich also an den Nutzenden orientieren.

Die Ausgestaltung von Wallets und eines Ökosystems muss sich an den Bedarfen der Nutzenden und an den zu lösenden Problemen orientieren.

Frage 3: Wie organisieren wir den Übergang zu dezentralen Identitäten und erschaffen ein gemeinsames Ökosystem?

Wenn davon ausgegangen wird, dass dezentrale Lösungen föderierte und isolierte Systeme nicht ersetzen, sondern ergänzen werden, muss die Rolle von Wallets zur Vereinheitlichung der beiden bestehenden Systeme diskutiert werden.

Systeme können über Standards zusammengeführt werden, indem durch neue Standards von dezentralen auf isolierte Systeme zugegriffen werden kann. Außerdem können dezentrale Systeme (Wallets) in existierende Systeme eingebaut werden, sodass in Zukunft bei Identifizierungsprozessen für isolierte oder föderierte Systeme auch eine Wallet genutzt werden kann. Interfaces müssen also vereinheitlicht und anschließend Wallets in die existierenden Systeme eingebunden. In diesem Kontext darf wieder der Bedarf der Nutzenden nicht vergessen werden und Sicherheitsniveaus bedarfsorientiert festgelegt werden.

Wie organisieren wir den Übergang zu dezentralen Identitäten und erschaffen ein gemeinsames Ökosystem?

Die zur Sitzung des AK Digitale Identitäten vom 13.09.2023 zugehörenden Unterlagen finden Sie im Bitkom Mitgliederportal. Dort finden Sie die Impulsvorträge von

- Dr. Dominik Deimel, comuny GmbH zu den *Mehrwerten dezentraler Wallet-Technologien bei föderierten und isolierten Identitäten*
- Jens Viere, Bayrisches Staatsministerium für Digitales zum *bundesweit einheitlichen Unternehmenskonto*
- Lars Hupel, G+D zu *Privatsphäre und Anonymität im Digitalen Euro*
- Dr. Marlen Jurisch & Dr. Ostertag zum *München Portal der Zukunft*

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Clemens Schleupner | Referent Vertrauensdienste & Digitale Identitäten
T 030 27576-424 | c.schleupner@bitkom.org

Verantwortliches Bitkom-Gremium
AK Digitale Identitäten