

Die Arbeitskreise »Blockchain« und »Digitale Identitäten« des Bitkom stellen die zentralen Thesen und Inhalte ihrer Mitgliedertreffen hier in kompakter Form vor.

# Effiziente Identitätsverwaltung: Einblicke in SSI, DLT und KYC-Prozesse

## Einführung

Die Blockchain-Technologie kann eine wichtige Rolle bei der Verwaltung digitaler Identitäten spielen. Sie bietet eine dezentrale, sichere und transparente Methode, um Identitätsdaten zu speichern und zu verifizieren. Durch die Verwendung von kryptografischen Signaturen können Nutzerinnen und Nutzer die Kontrolle über ihre eigenen digitalen Identitäten behalten und diese sicher mit verschiedenen Diensten teilen, ohne ihre sensiblen Informationen preiszugeben. Anknüpfend an den ↗ Bitkom-Leitfaden »Vertrauen stärken: Praktischer Leitfaden zu digitalen Identitäten, SSI & DLT« haben die Bitkom-Arbeitskreise Blockchain und Digitale Identitäten bei einer gemeinsamen Sitzung darüber gesprochen, wie Blockchain-Technologie zu sicheren und effizienten Digitalen Identitäten beitragen kann. Die zentralen Thesen der Sitzung werden hier kurz zusammengefasst.

## Die zentralen Thesen

- **Bestehende Lösungen für sichere dezentrale digitale Identitäten müssen integriert werden.**

Auf europäischer Ebene gibt es eine Reihe von Standards, Frameworks und Regulierungen, die einen Rahmen für sichere, dezentrale digitale Identitäten schaffen. Auch für DLT als Infrastruktur für digitale Identitäten existiert die European Blockchain Services Infrastructure (EBSI). Diese Infrastruktur sollte auch auf deutscher Ebene in Betracht gezogen werden, wenn es um interoperable und erprobte Standards zu dezentralen Identitäten geht. Für Deutschland geht es hierbei um den Blick über den Tellerrand, da es in anderen europäischen Ländern bereits funktionale Anwendungsfälle mit hoher Usability gibt.

## DLT-Technologie kann auch behördenintern zu massiven Effizienzsteigerungen führen.

Trotz einer allgemein zu beobachtenden Vernachlässigung von Blockchain im Kontext der öffentlichen Verwaltung, offenbaren einzelne Anwendungsfälle die Vorteile der Technologie im Zusammenhang mit Digitalen Identitäten. Sowohl die Identifizierung von Personen, die mit einer Behörde kommunizieren, Leistungen erbringen, etc. als auch die interne Kommunikation und Weitergabe von Informationen können so effizienter gestaltet werden. Insbesondere länderübergreifend agierende Behörden können hiervon profitieren.

## Qualifizierte Siegel können als eIDAS-Tool schon heute zur Ausstellung von Credentials genutzt werden.

Während ganz Europa auf die eIDAS 2.0-Verordnung wartet, gibt die eIDAS-Verordnung von 2014 schon heute die Möglichkeit, mit ihren Mitteln qualifizierte Zertifikate auszustellen. Das bekannte SSI-Dreieck könnte mit eIDAS-Mitteln dadurch ergänzt werden, dass der Issuer eines Verifiable Credentials per Fernsiegeldienst dieses selbst siegelt. Somit könnten bereits heute qualifiziert gesiegelte Verifiable Credentials flächendeckend ausgerollt und durch QEAs in einem zweiten Schritt mit Inkrafttreten der eIDAS 2.0 Verordnung ersetzt werden. Es gilt, sich die eIDAS-Tools zunutze zu machen und so, v. a. im B2B-Bereich, die Digitalisierung zu beschleunigen.

## Insbesondere im B2B-Bereich muss über eIDAS 2.0 hinaus eine internationale Perspektive in die Governance von SSI einbezogen werden.

SSI bietet interessante Möglichkeiten, Sicherheitsmerkmale auf neue Art und Weise zu denken, bringt jedoch auch Herausforderungen mit sich, wie z. B. das Teilen und Zeichnens von Credentials im Familienumfeld für minderjährige Familienmitglieder. Außerdem stellt sich die Frage nach international interoperablen Systemen, über eIDAS hinaus. Multinationale Unternehmen bewegen sich in mehreren Rechtsräumen und müssen deswegen eine Reihe unterschiedlicher Regularien beachten. Hoheitliche, SSI-basierte Dokumente haben andere Sicherheitskriterien als lokal einsetzbare Nachweise und brauchen daher eine neue Art von Governance.

Eine detaillierte Dokumentation des virtuellen Arbeitskreistreffens Blockchain vom 23.09.2023 befindet sich im [Bitkom Mitgliederportal](#), u. a. mit den Impulsvorträgen:

- Sichere dezentrale digitale Identitäten zwischen EBSI, eIDAS 2.0 und ARF–Projekte und Anwendungsfälle in Europa (Steffen Schwalm, msg)
- Self-Sovereign und Digital Identity im BAMF (Tobias Konsek, BAMF)
- Qualifizierte Siegel für Credentials im EUDI-Wallet Ökosystem (Christian Seegebarth, D-Trust)
- Vertrauenswürdige Identitätsansätze mit SSI durch Trust Modeling (Dr. Marc Henniges, d-fine & Robert Heinze, G+D)



**Benedikt Faupel**  
Bereichsleiter Blockchain  
T 030 27576-410  
[b.faupel@bitkom.org](mailto:b.faupel@bitkom.org)



**Clemens Schlepner**  
Referent Vertrauensdienste &  
Digitale Identitäten  
T 030 27576-424  
[c.schlepner@bitkom.org](mailto:c.schlepner@bitkom.org)