TeleTrusT @ it-sa 365

Digitale Plattform it-sa 365, 16.03.2022

Self-Sovereign Identity (SSI) in Deutschland – Projekte mit Strahlkraft für die globale Community

Dr. André Kudra

TeleTrusT-Vorstandsmitglied, CIO esatus AG

Agenda

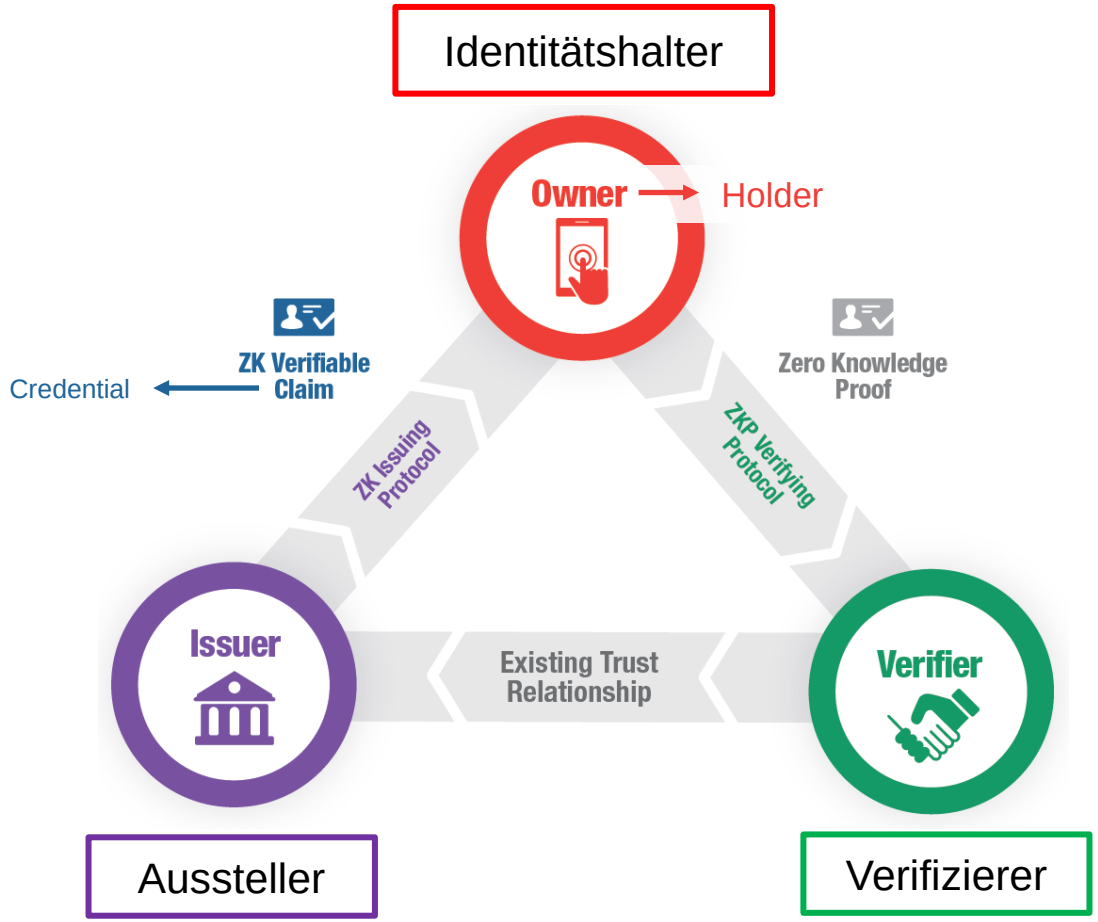
- **SSI in aller Kürze**
- **Projekte mit Strahlkraft**
- **Erfolgsfaktoren**
- **TeleTrusT IT-Sicherheitsagenda 2029**

SSI als Grundlage eines europäischen Ökosystems

SSI ist eine Technologie, die den Nutzer in den Mittelpunkt stellt. Sie ermöglicht eine selbstbestimmte, selbst verwaltete digitale Identität für Alle.

Der Nutzer (Identitätshalter) hat die Kontrolle über seine persönlichen Daten und entscheidet, wem und zu welchen Zwecken er seine Identitätsdaten mittels digitaler Credentials zur Verfügung stellen möchte.

Grundlage dafür ist das Vertrauens-netzwerk.



Original Source: Sovrin™: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust – A White Paper from the Sovrin Foundation - Version 1.0 - January 2018

SSI-Entwicklungen auf europäischer Ebene: TeleTrusT-Kommentierung zur eIDAS Neufassung

- TeleTrusT begrüßt den Vorschlag der Europäischen Kommission, durch eine novellierte eIDAS-Fassung vertrauenswürdige und sichere Digitale Identitäten für alle Europäer zu etablieren.
- Arbeitsgruppe "Blockchain" und Arbeitskreis "Forum elektronische Vertrauensdienste" haben die am 3. Juni 2021 publizierten Entwürfe analysiert und kommentiert:
  - **Self-Sovereign Identity (SSI) wird berücksichtigt und ermöglicht - ein Vertrauensmodell für SSI wird geschaffen**
  - Implementing Acts sind zu harmonisieren und möglichst viele sind zu implementieren, um ein "Level Playing Field" zu erreichen
  - Eine Umsetzungsförderung - auch der Kommunen - für Implementierung und Kommunikation sollte erfolgen
  - EU Trusted List ist der Vertrauensanker für die Datenautobahn - sie ist eine Stärke der eIDAS und sollte der zentrale Vertrauensanker bleiben
  - Die Verpflichtung, in Browsern Qualified Website Authentication Certificates (QWACs) anzuzeigen, wird unterstützt

Quelle: https://www.teletrust.de/publikationen/stellungnahmen

Schaufensterprojekte des Bundesministerium für Wirtschaft und Klimaschutz (BMWK)

- Der **Innovationswettbewerb "Schaufenster Sichere Digitale Identitäten"** fördert herausragende Ansätze für neue ID-Ökosysteme, in denen sich Anwender und Anwenderinnen im Alltag mit ihrem Smartphone gegenüber Dienstleistern oder Behörden digital ausweisen können.
- Vier Schaufensterprojekte wurden vom BMWK ausgewählt:
  - ID-Ideal
  - SDIKA
  - ONCE
  - IDunion ← Fokus auf Self-Sovereign Identity

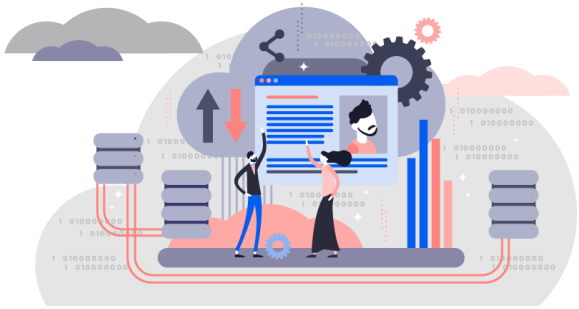
Quelle: https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Projekte_Umsetzungsphase/projekte_umsetzungsphase.html

IDunion: Ein offenes Ökosystem für vertrauensvolle Identitäten

➔ Aufbau eines offenen Ökosystems für die dezentrale Identitätsverwaltung, welches weltweit nutzbar ist und sich an europäischen Werten und Regularien orientiert.

Im Zentrum der Lösung für selbstbestimmte Identitäten – sog. Self-Sovereign Identities (SSI) – steht per Definition immer der Nutzer.

Über 45 Projektpartner sind beteiligt, 15 werden für die Umsetzung von 35+ Anwendungsfällen über drei Jahre Projektlaufzeit vom BMWi gefördert.



Zentrale Aspekte des Netzwerkbetriebs sind Sicherheit, Wirtschaftlichkeit, Nutzerfreundlichkeit und Datenschutzkonformität.

Quelle: https://idunion.org

SSI-Pilotprojekte des Bundeskanzleramtes

Alle relevanten verifizierbaren und personalisierten Nachweise sollten dem Nutzer digital zur Verfügung stehen, z.B. in einer Wallet

Die Bundesregierung

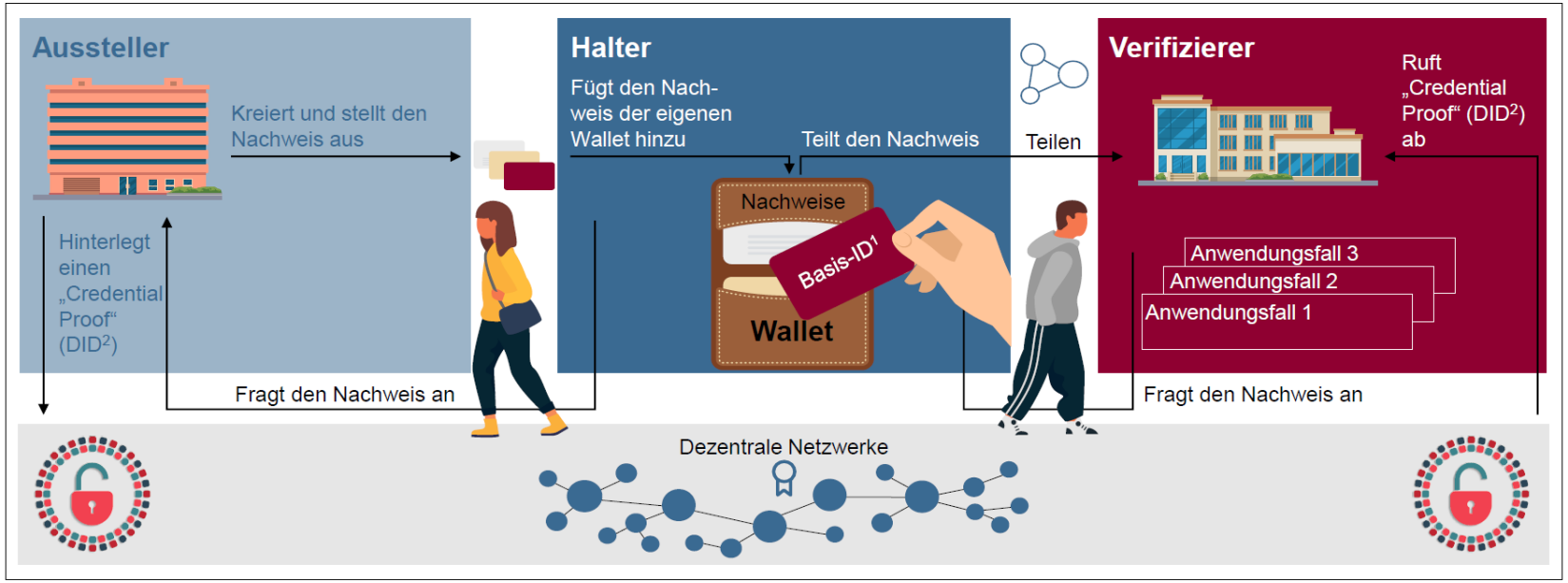
7

Quelle: https://www.bundesregierung.de/breg-de/suche/oekosystem-digitale-identitaet-1960124

SSI-Pilotprojekte des Bundeskanzleramtes

Grundlage für das Ökosystem ist der SSI-Ansatz – Nutzer im Zentrum mit voller Hoheit über seine eigenen Daten

Die Bundesregierung



Konkret bedeutet dies für die Anwendungsfälle, die im Rahmen des Projektes ausgewählt werden:

- Nachweise werden nach SSI-Standards ausgestellt
- Verifikation der Nachweise sollte für die Dauer des Projektes über das seitens des Projektes bereitgestellte SSI-basierte Netzwerk erfolgen ("blinde Verifizierung")
- Der Halter verfügt durch die Nutzung einer SSI-basierten Wallet über alle Nachweise

10

1. Entspricht dem Umfang des Personalausweises
2. Decentralized Identifier

Quelle: https://www.bundesregierung.de/breg-de/suche/oekosystem-digitale-identitaet-1960124

➔ Akzeptanz der Technik

- Auch von kritischen Stakeholdern
- Erfüllung höchster Sicherheitsanforderungen ist zu belegen

➔ Regulatorische Konformität

- Governance des Ökosystems ist unerlässlich für Integration in relevante Jurisdiktionen
- Unterschiedliche Vertrauensniveaus sind zu unterstützen

➔ Relevanz

- Ökosystem muss nützlich sein für viele Anwendungsfälle, idealerweise über Organisations- und Ländergrenzen hinweg
- Niedrige Einstiegshürden für alle Stakeholder

➔ Nutzer:innenfreundlichkeit

- Einfache Handhabung und gefällig in der Anmutung – optimale "UX"
- Offen und zugänglich für alle

➔ Datensparsamkeit und Privatsphäre

- Nicht überall ist eine Personenidentifikation erforderlich und es werden ggf. nur wenige Daten benötigt
- Anonyme Verwendung von Nachweisen und selektive Offenlegung von Attributen müssen möglich sein

Ausführlicher zum Nachlesen in der DuD

➔ Aktuelle Veröffentlichung im Springer Journal "Datenschutz und Datensicherheit" (DuD):

Self-Sovereign Identity (SSI) in Deutschland: Projekte mit Strahlkraft für die globale Community

- Details zur Publikation: https://link.springer.com/article/10.1007/s11623-022-1555-1
- Von Springer zur Verfügung gestellter Online-Leselink: https://rdcu.be/cEp9D

TeleTrusT IT-Sicherheitsagenda 2029 – IT-Sicherheit in der Digitalisierung

TeleTrusT-Forderungen

1. Klares Bekenntnis zu unbeschränkter IT-Sicherheit
2. Technologische Souveränität im Bereich IT-Sicherheit schaffen - für eine werteorientierte, sichere und vertrauenswürdige digitale Zukunft
3. **Auf- und Ausbau von IT-Sicherheitsinfrastrukturen für Bürger, Unternehmen und Verwaltung fordern und fördern**
4. Mehr IT-Sicherheitstechnologie "Made in Germany" in der Praxis
5. Verbot der Kompromittierung von IT-Sicherheit, keine Backdoors, Staatstrojaner oder geschwächte Verschlüsselung
6. Europäische IT-Sicherheitsgesetze für eine erhöhte Rechts- und Investitionssicherheit - klar, konsolidiert und agil

Quelle: https://www.teletrust.de/teletrust-it-sicherheitsagenda

Kontakt

- TeleTrusT-Vorstandsmitglied
- CIO der esatus AG
- Leiter der Arbeitsgruppe "Blockchain" und des Arbeitskreises "Secure Platform" bei TeleTrusT
- Trust over IP (ToIP) Steering und Executive Committee Member
- Trustee der Sovrin Foundation

- Dr. André Kudra
- Tel.: +49 6103 9029-0
- a.kudra@esatus.com

- esatus AG | www.esatus.com