Self-Sovereign Identity (SSI)

→ Das souveräne europäische Ökosystem für Identitätsdaten

Prof. Dr. (TU NN)

Norbert Pohlmann

Professor** für **Informationssicherheit
Leiter** des **Instituts für Internet-Sicherheit - if(is)
Vorstandsmitglied** des **Verbands der Internetwirtschaft - eco
Vorstandsvorsitzender** des **Bundesverbands IT-Sicherheit - TeleTrusT

Self-Sovereign Identity
→ Motivation

- Derzeit **dominieren im Cyber-Raum** zentrale ID-Provider wie Google, Facebook und Apple die **Verwaltung von Identitätsdaten** bei sehr vieler IT-Dienste weltweit.

- Diese Situation schafft eine **große Abhängigkeit der Gesellschaft**, **Unternehmen** und **Nutzer** in Bezug auf den **Fortgang der Digitalisierung**.

- (Monopolistischen) ID-Provider nutzen **sensible personenbezogenen Daten** für eigene Werbezwecke oder stellen diese weiteren Unternehmen zur Verfügung, um damit **Geld zu verdienen**.

- Das **schwächt die Privatsphäre der Nutzer** und hat Folgen bezüglicher der **Akzeptanz für unsere digitale Zukunft**.

- Self-Sovereign Identity (SSI) wird helfen, **diese Probleme** zu lösen und ist **ein Digitalisierungsbeschleuniger** für unsere Gesellschaft.

Self-Sovereign Identity
→ Grundsätzliche Idee

- Self-Sovereign Identity oder abgekürzt SSI soll dazu beitragen, die **digitale Zukunft in Deutschland** und in der **EU** souverän, sicherer und vertrauenswürdiger zu gestalten.

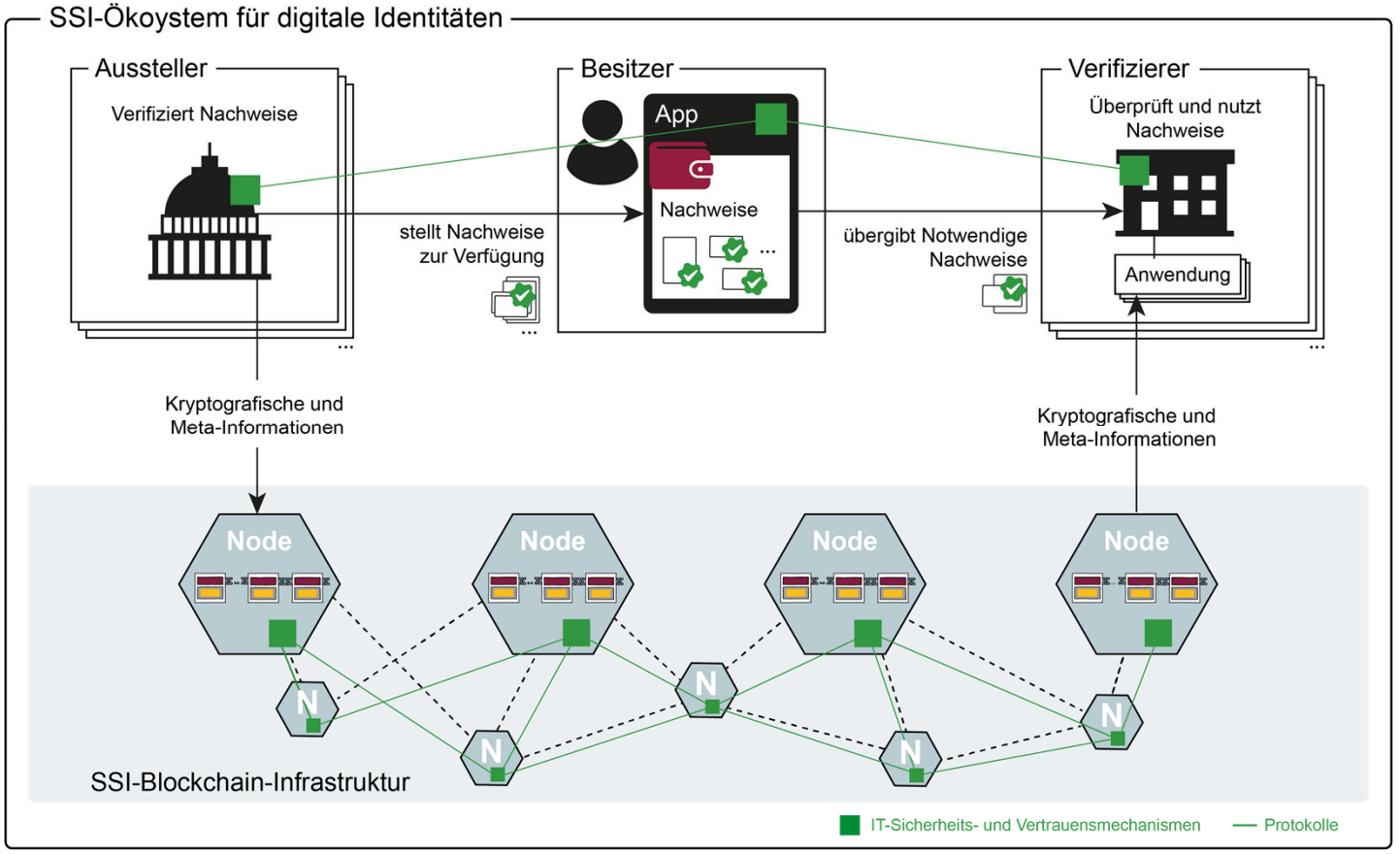
- Die Idee ist, dass **Nutzer wie Bürger oder Mitarbeiter** ihre digitalen Identitäten und weitere digitale Nachweise **selbstbestimmt verwalten** und deren **Weitergabe eigenständig kontrollieren**.

- Diese digitalen Nachweise sind durch Anwendungen, die die Informationen in den digitalen Nachweisen in ihren Prozessen benötigen, **automatisiert verifizier- und verarbeitbar**.

- Das schafft **mehr Datenschutz** und einen **höheren Grad an Digitalisierung** in vielen Prozessen.

Self-Sovereign Identity
→ Architektur

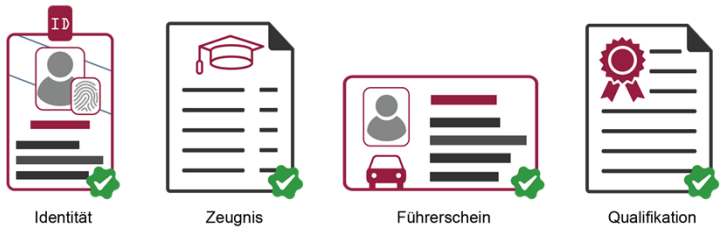
- Im SSI-Ökosystem spielen **drei Akteure eine Rolle**, die gemeinsam einen Vertrauensdienst – die SSI-Blockchain-Infrastruktur - nutzen.



Self-Sovereign Identity
→ Aussteller von digitalen Nachweisen

Aussteller stellen verifizierbare digitale Nachweise aus und sind:

- **Einwohnermeldeamt**, Straßenverkehrsamt, **Schulen- und Hochschulen**, Unternehmen, **Berufsverbände**, Behörden, **Qualifizierungsorganisationen**, TÜVs oder **weitere Unternehmen,** die hier ein Geschäftsmodell für sich sehen.



Verifizierbare digitale Nachweise sind:

- **Bescheinigungen der Identität** (wie Personalausweis, Firmen-/Dienstausweis …),
- **Führerscheine** (für Auto oder Motorrad …),
- **Zeugnisse** (wie Abitur, Bachelor, Master, Promotionsurkunden …),
- **Bestätigungen** (zum Beispiel Teilnahmebestätigung, Buchungsbestätigung, Echtheitsbestätigung, Impfbestätigung …)
- **Befugnisse** (wie Amtsbefugnis, Aufenthaltsbefugnis …),
- **Qualifikationen** (zum Beispiel Weiterbildungsnachweise, Personenzertifikate …),
- **Mitgliedsausweise** (für Fitnessstudien, Vereine, ADAC und so weiter),
- **Kundenkarten** (wie Bonuskarten, Vielfliegerprogramme …)
- und vieles mehr

Self-Sovereign Identity
→ Besitzer oder Nutzer

- Ein Besitzer oder Nutzer hat in der Regel auf seinem **mobilen Endgerät** eine entsprechende **SSI-App** mit einem **digitalen Portemonnaie**, die sogenannte **SSI-Wallet** in der die verifizierbaren digitalen Nachweise sicher gespeichert sind.

- Es ist auch möglich, als Alternative oder Ergänzung zur App einen Cloud-Agent zu nutzen.

- Die **Nutzer** können alle **verifizierbaren digitalen Nachweise** von den entsprechenden **Ausstellern anfordern**, wenn sie dazu eine Berechnung haben und in ihre **SSI-Wallet sicher ablegen**.

- Damit sind sie in der Lage, **selbstbestimmt** und **souverän** diese verifizierbaren **digitalen Nachweise** oder **bestimmte Attribute** oder **Teile daraus** den entsprechenden Anwendungen **zur Verfügung zu stellen**.

- Dies sollten die Nutzer nur dann tun, wenn die Anwendung die Inhalte der **digitalen Nachweise** wirklich **für die Umsetzung der eigentlichen Aufgabenstellung benötigen**.

Self-Sovereign Identity
→ Zero-Knowledge-Proof

- Ein weiteres wichtiges **Feature für den Schutz der Privatheit** und **Souveränität des Nutzers** wird mithilfe von sogenannten **Zero-Knowledge-Proof** umgesetzt.
- Damit ist es möglich, sicher und vertrauenswürdig nur **bestimmte Attribute anonym** oder **Teile** aus den Nachweisen **zu beweisen**.
  - Das der Nutzer über **18 Jahre alt** ist
  - Das der Nutzer **zu einem bestimmten Unternehmen gehört**
  - Das der Nutzer schon **zweimal gegen Corona geimpft** worden ist
- Diese **Attribute** oder **Teile** aus digitalen Nachweisen **können bewiesen werden**, **ohne weitere** und für die Anwendung nicht wichtigen **Informationen** zur Verfügung zu stellen.
- Der **Zero-Knowledge-Proof** hilft in vielen Fällen, **Datenschutzaspekte** einfach und wirkungsvoll umzusetzen, weil nur bestimmte Attribute überprüft werden, ohne datenschutzrelevante Informationen übertragen zu müssen.

Self-Sovereign Identity
→ Verifizierer oder Anwendungen

- Anwendungen, die die **digitalen Nachweise** für ihre spezielle Aufgabenstellung benötigen, bekommen diese oder **Teile davon** oder nur Aussagen über **bestimmte Attribute** von den Nutzern zur Verfügung gestellt.
- Diese können von der Anwendung vollkommen automatisiert, in einem digitalisierten Prozess sicher und eindeutig verifiziert und bearbeitet werden.
- Damit wird eine höhere Sicherheit bei der Nutzung von Nachweisen erzielt.
- Bei physischen Nachweisen müssen oft ungeschultes Personal die Verifikation mit allen Fehlern umsetzen.
- **Bei den Anwendungen entsteht der größte Vorteil**, weil die Prozesse mithilfe der digitalen Nachweise **automatisiert** und damit **effizient** und **kostengünstig** umgesetzt werden.

Self-Sovereign Identity
→ Blockchain-Infrastruktur

- Damit die **digitalen Nachweise verifiziert** werden können, brauchen wir einen **Vertrauensdienst**.
- Eine **moderne Blockchain-Infrastruktur** ist für die **Souveränität** und die **Skalierbarkeit** des SSI-Ökosystems besonders gut geeignet *(Konsortium)*.
- Das bedeutet, die Akteure sind auf der Basis dieses dezentralen Blockchain-Netzwerks in der Lage, die **Echtheit**, den **Ursprung** als auch die **Unversehrtheit** der digitalen Nachweise **zu überprüfen**, ohne dass die SSI-Blockchain die Nutzer oder die ausgestellten digitalen Nachweise kennt.
- Im SSI-Ökosystem können und werden **mehrere unterschiedliche SSI-Blockchain-Netzwerke** im Sinne Network-of-Networks eingebunden sein.
- Das macht das Ökosystem skalierbar und effizient bei der Umsetzung in verschiedenen Bereichen.
- Beispiele von möglichen verschiedenen SSI-Blockchain-Netzwerken sind: Government, Banken, Smart City, Industrie-Branchen, Gesundheitswesen … und das in verschiedenen Ländern wie Bundesländer, EU-Länder.
- Alle zusammen bieten **als Ganzes** einen **einheitlichen Vertrauensdienst**.

Self-Sovereign Identity
→ Beispiel: Auto-Anmietung

- Wer schon einmal ein Auto gemietet hat, kennt die folgende Situation:
- **Der Mitarbeitende des Autovermieters** braucht eine gefühlte Ewigkeit, um Ausweis, Führerschein, Kreditkarte, Reservierung und Gutscheine zu prüfen und **die Daten im PC zu erfassen**.
- Mit **Self-Sovereign Identity (SSI)** würde **dieser Vorgang** wesentlich **vereinfacht** und dadurch **erheblich verkürzt**:
  - Am Schalter angekommen, wird ein QR-Code vom Kunden gescannt.
  - Anschließend werden die digitalen Nachweise vom Kunden freigegeben und ein Vertrag digital signiert – danach erfolgt die Übergabe der Autoschlüssel.
  - Quasi **simultan** und **automatisiert** laufen die **Prozesse sicher** und **vertrauenswürdig** im Hintergrund ab.
- Ein schönes Beispiel, welchen **Effekt SSI bei der Digitalisierung** hat.
  - Der Auto-Vermieter hat ein sehr **hohes Einsparungspotenzial**, weil alles automatisiert abläuft.
  - Der Kunde bekommt sein Auto sehr viel schneller und muss **nicht lange warten**.

Self-Sovereign Identity
→ Weitere Aspekte

Gesellschaftliche Relevanz
- Digitalisierung: hoher gesellschaftlicher Relevanz *(zu viele nicht effiziente Prozesse)*.
- **Problem:** Unternehmen nutzen persönlichen Daten wirtschaftlich.
- Das **Recht auf Privatsphäre** gilt als Grundrecht und ist in allen modernen Demokratien verankert. Wird aber **im Cyber-Raum** zurzeit **nicht wirklich berücksichtigt.**
  → Das SSI-Ökosystem löst das Problem

Wirtschaftliche Relevanz
- Händisch durchgeführte Abläufe und vorhandene Medienbrüche.
- Die Umsetzung von digitalen Identitäten und Nachweisen hat einen hohen wirtschaftlichen Nutzen. Laut der MGI Studie 3 bis 4 Prozent des BIP (2030)
  → 3 % in Deutschland im Jahr 2020 wären 100 Mrd. Euro gewesen.

Technologische Souveränität
- Ist ein zunehmend wichtiger Faktor *(Wertschöpfungsanteil: IT, Internet und Daten)*
- Wie brauchen unabhängige Gestaltungsmöglichkeiten *(Schlüsselbranchen: gezielter Kompetenzaufbau und Schlüsseltechnologien entwickelten).*
- **SSI-Technologien ist ein Schlüsselbereich** *(größere Autonomie in Bezug auf die Nutzung und Verwertung von persönlichen Daten)*
  → höheren Gard an Digitalisierung

Self-Sovereign Identity
→ Zusammenfassung

- Das SSI-Ökosystem **löst Abhängigkeiten von Monopolisten** und gibt uns die **Freiheit**, die digitale **Zukunft unabhängiger** und damit erfolgreicher zu gestalten.
- **Self-Sovereign Identity (SSI)** sorgt als **Digitalisierungsbeschleuniger** für **eine schnellere, sichere und vertrauenswürdige Digitalisierung**.
- Die **Nutzer** können **selbstbestimmt** ihre Identitätsdaten und weitere digitale Nachweise an Anwendungen weitergeben.
- Das schafft einen **hohen Grad an Privatsphäre**, an **werteorientierter IT** und **-Diensten** und damit eine **hohe Akzeptanz für die digitale Zukunft**.

Self-Sovereign Identity

→ Wir brauchen eine souveränes europäische Ökosystem für Identitätsdaten

Prof. Dr. (TU NN)

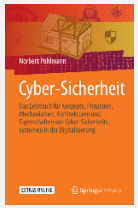
Norbert Pohlmann

Professor** für **Informationssicherheit
Leiter** des **Instituts für Internet-Sicherheit - if(is)
Vorstandsmitglied** des **Verbands der Internetwirtschaft - eco
Vorstandsvorsitzender** des **Bundesverbands IT-Sicherheit - TeleTrusT

Anhang / Credits

Wir empfehlen

- **Cyber-Sicherheit**
  Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2019
  https://norbert-pohlmann.com/cyber-sicherheit/



- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/cyberschutzraum

CYBER SCHUTZRAUM

- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/

(M) MASTER internet-sicherheit.

Besuchen und abonnieren Sie uns :-)

WWW
https://www.internet-sicherheit.de

Facebook
https://www.facebook.com/Internet.Sicherheit.ifis

Twitter
https://twitter.com/_ifis

https://twitter.com/ProfPohlmann

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Quellen Bildmaterial

Eingebettete Piktogramme:
- Institut für Internet-Sicherheit – if(is)

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
https://www.it-sicherheit.de/

Literatur

J. Hoang, N. Pohlmann: „Was Self-Sovereign Identity (SSI) unverzichtbar macht – Bausteine einer sicheren, selbstbestimmten digitalen Identität (Id)“, IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, DATAKONTEXT-Fachverlag, 4/2021
https://norbert-pohlmann.com/artikel/was-self-sovereign-identity-ssi-unverzichtbar-macht/

N. Pohlmann: „Eine vertrauenswürdige Zusammenarbeit mit Hilfe der Blockchain-Technologie“, Buch: „Cybersecurity Best Practices - Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden“, Herausgeber: M. Bartsch, S. Frey; Springer Vieweg Verlag, Wiesbaden 2018

M. Mollik, N. Pohlmann: „Trust as a Service – Vertrauen als Dienstleistung – Validierung digitaler Nachweise mit der Blockchain“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 3/2019

D. Bothe, L. Lazzati, N. Pohlmann, A.-J. Sinnaeve, K. Wittek: “An SSI Based System for Incentivized and Self-determined Customer-to-Business Data Sharing in a Local Economy Context”, IEEE E-TEMS 2020, Dortmund 2020

D. Bothe, N. Pohlmann: „Self-Sovereign Identity - Autonom und sicher in der Smart Economy“, IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, DATAKONTEXT-Fachverlag, 5/2020

N. Pohlmann: „Self-Sovereign Identity (SSI) auf Basis der Blockchain-Technologie“, Blockchain-Insider:
https://www.blockchain-insider.de/self-sovereign-identity-ssi-auf-der-basis-der-blockchain-technologie-a-1026752/

N. Pohlmann: „Self-Sovereign Identity (SSI) und seine Verwendung“, Security-Insider:
https://www.security-insider.de/self-sovereign-identity-ssi-und-seine-verwendung-a-1026740/

N. Pohlmann: „Self-Sovereign Identity (SSI)“, Glossar „Cyber-Sicherheit“
https://norbert-pohlmann.com/glossar-cyber-sicherheit/self-sovereign-identity-ssi/

N. Pohlmann: **Lehrbuch „Cyber-Sicherheit“,** Springer Vieweg Verlag, Wiesbaden 2019
ISBN 978-3-658-25397-4s

Weitere Artikel siehe: https://norbert-pohlmann.com/artikel/