

Blockchain Autumn School 2020

Self-Sovereign Identity in der praktischen Nutzung

Dr. André Kudra



Vorstellung esatus AG



✓ Identity & Access



✓ Governance, Risk & Compliance



✓ IT Security



✓ Development Operations

Aktive Mitarbeit in relevanten Verbänden und Organisationen

SecurITy
Trust Seal
www.teletrust.de/taarnig
made
in
Germany

Allianz für
Cyber-Sicherheit
Partner



ISO
International
Organization for
Standardization



TeleTrust
Pioneers in IT security.



sovrin



DIN



**AG Blockchain
Leitung**

MyData



**BLOCKCHAIN
BUNDESVERBAND**

SSI für Deutschland /
IDUnion



COVID CREDENTIALS INITIATIVE



**TRUST
Over IP
FOUNDATION**

SSI für Deutschland

Konsortialpartner



BOSCH

Assoziierte Partner



Ministerium für Wirtschaft, Innovation,
Digitalisierung und Energie
des Landes Nordrhein-Westfalen



DEUTSCHE BÖRSE
GROUP

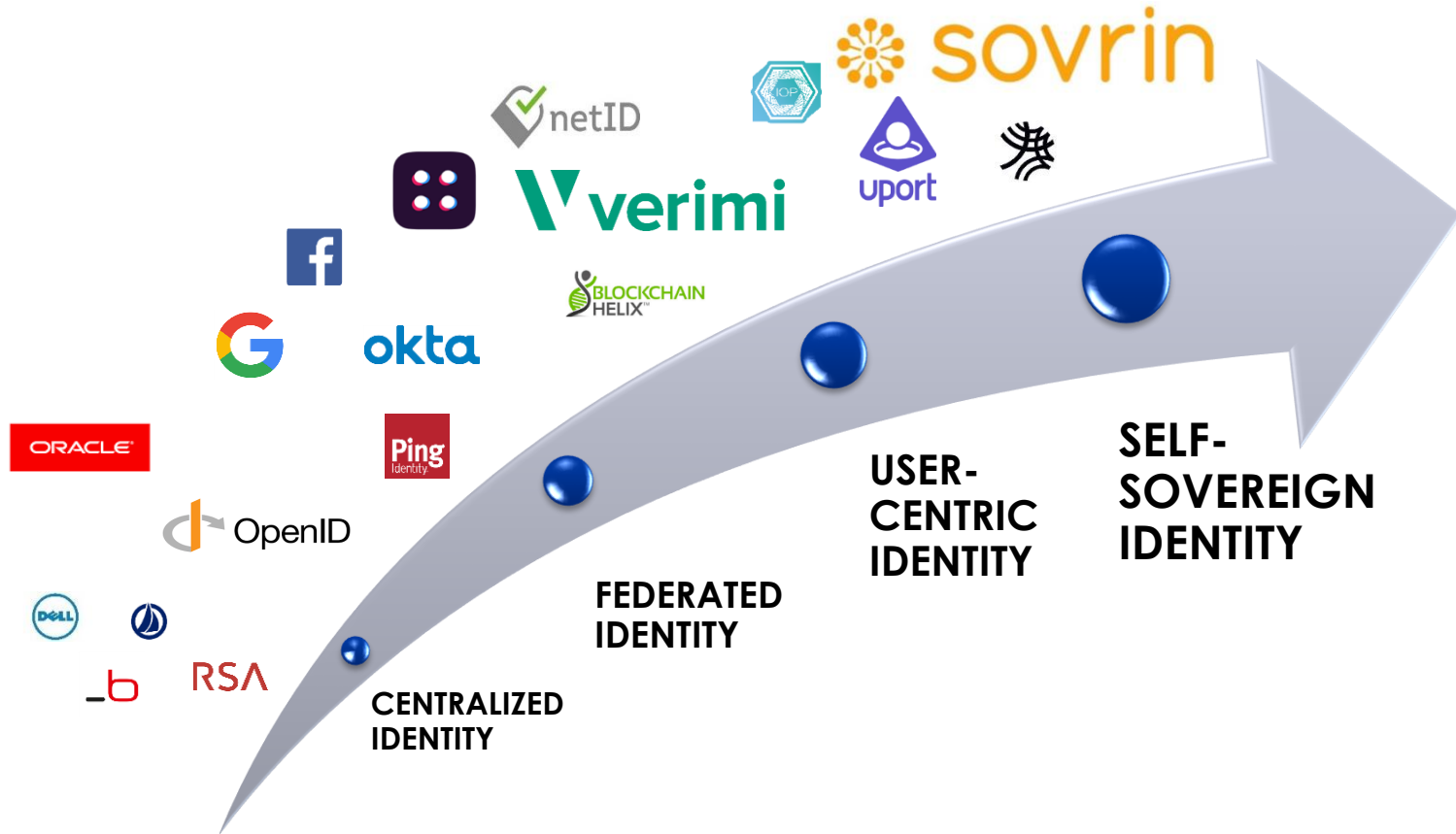


Gefördert durch:

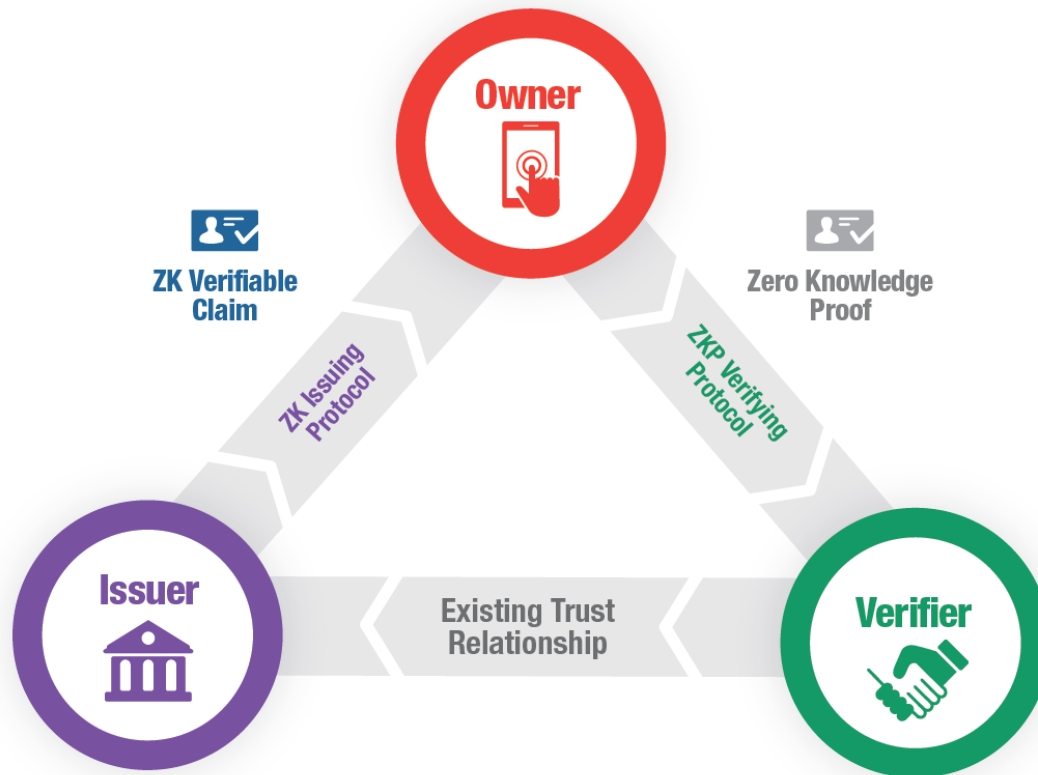


Einführung SSI

Die Entwicklung der digitalen Identität



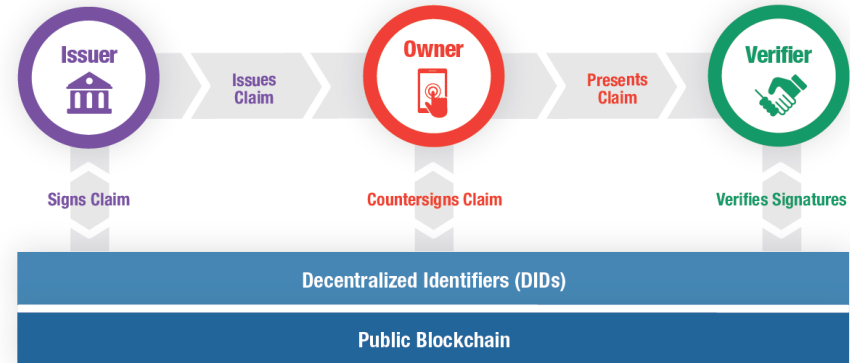
Vertrauensdreieck und Verifiable Credentials



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

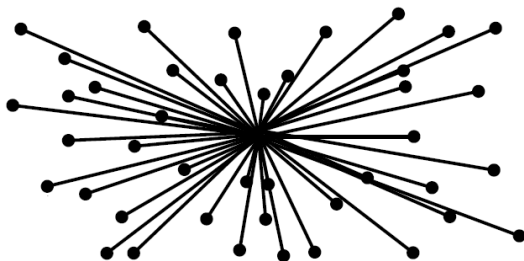
Self-Sovereign Identity, kurz SSI: Schon weit mehr als nur eine Idee

- 🔒 **Konzept** einer echten selbstverwalteten und -kontrollierten digitalen Identität
- 🔒 **Vertrauensnetzwerk**, das der vernetzten Welt noch immer fehlt
- 🔒 **Recht auf digitale Identität** als öffentliches Gut für JEDEN
- 🔒 **Technologie**, die den Nutzer in den Mittelpunkt stellt
- 🔒 **Standards**, die alle relevanten Player schon jetzt verwenden
„DIDs“ und „Verifiable Claims & Credentials“



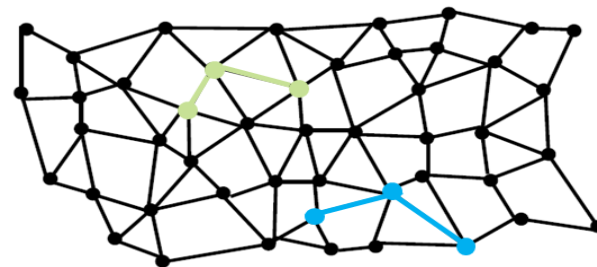
SSI löst mit Dynamik und Flexibilität zentralistische Single Points of Failure ab

Zentralistische Strukturen und technische Lösungen – wie bspw. Public Key Infrastrukturen (PKI) – lösen mit digitalen Zertifikaten spezifische funktionale Herausforderungen, insbesondere Verschlüsselung, Authentifizierung und elektronische Signatur. Dabei sind sie in der inhaltlichen Zertifikatsausgestaltung limitiert und stellen gleichzeitig einen Single Point of Failure dar. Mit der Self-Sovereign Identity tritt an deren Stelle ein flexibles und dynamisches Ökosystem, das verschiedenste Anwendungsgebiete abdeckt.



Zentralistische PKI

- Standardisiertes Verfahren, globale produktive Anwendung
- Certificate Authorities (CAs) als Vertrauensdienstleister
- Regulatorische Rahmenbedingungen definiert
- Zertifikate inhaltlich fix definiert (X.509)
- Zentrale Stelle als Single Point of Failure

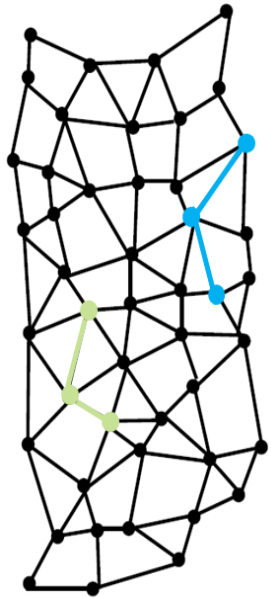


Dezentrales flexibles SSI-Netzwerk

- Jeder Teilnehmer kann Zertifikatsschemata definieren
- „Verifiable Credentials“ flexibel definier- und ausgestaltbar
- Jeder (!) kann Aussteller und Verifizierer sein
- CAs und Industrieplayer bereits engagiert in SSI
- „DIDs“ als World Wide Web Consortium (W3C) Standard

SSI bietet unmittelbare Anknüpfungspunkte für aktuelle IDPs und hebt Integrationspotenziale

Der mit Self-Sovereign Identity proklamierte und praktisch realisierte Ansatz eines „Web-of-Trust“ verschafft für jeden Teilnehmer im Netzwerk unmittelbare Anknüpfungspunkte, auch und insbesondere für klassische, zentralistische Instanzen wie Certificate Authorities oder Identity Provider. Ein SSI-Ökosystem trägt dazu bei, alle Integrationspotenziale effizient und effektiv zu heben.



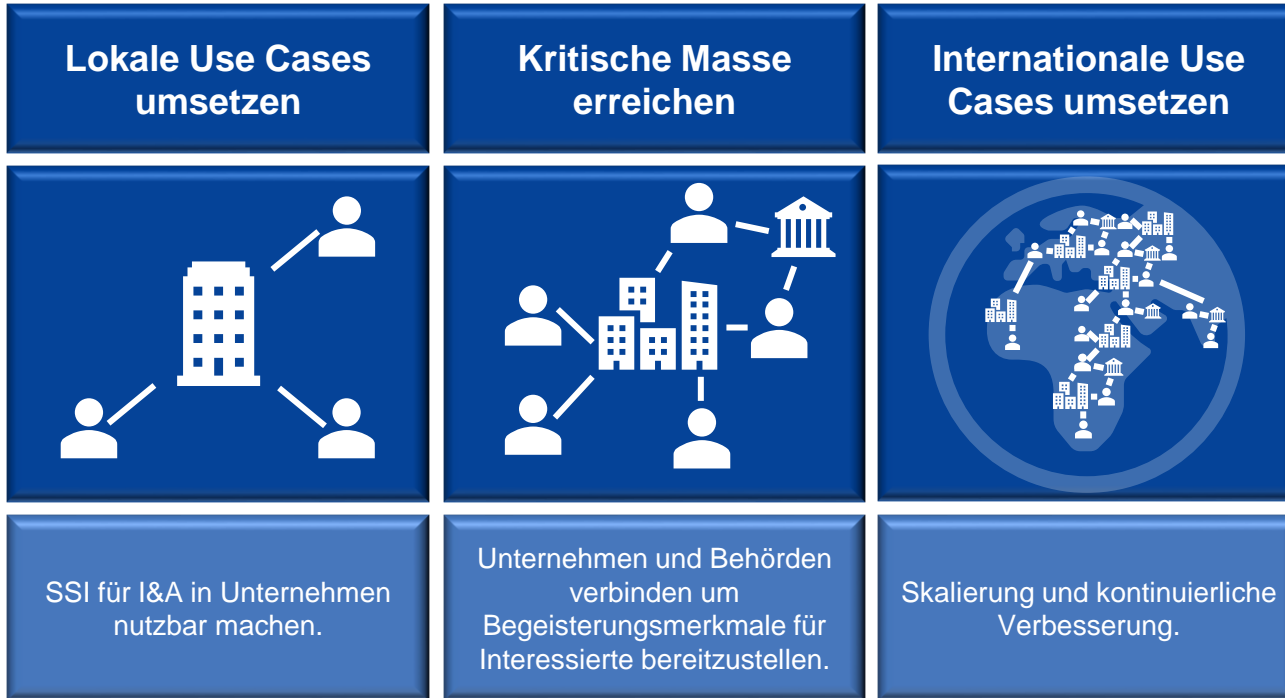
Self-Sovereign Identity

- ... ist das ideale Ökosystem zur Integration jeglicher Teilnehmer.
- ... integriert unkompliziert auch Teilnehmer, die bisher keine Interaktion hatten.
- ... liefert ein Integrationsgewebe, mit dem reale Vertrauensnetzwerke elektronisch abbildbar sind.
- ... transportiert Vertrauen und reicht es digital weiter.
- ... bietet Vertrauensdienstleistern eine Plattform für globale Diensteverbreitung (bspw. Verimi).
- ... passt sich domänenspezifischen Anforderungen flexibel an (bspw. „Know your customer“/KYC).
- ... nutzt bestehende Standards und stellt sie auf eine dezentralisierte Basis (bspw. PKI wird zur DPKI) .
- ... lässt sich leicht in gewachsene Strukturen integrieren (bspw. LDAP Berechtigungsmanagement).

SSI kompensiert die Nachteile zentralistischer Identity Provider und stärkt die Nutzerposition

	Internationale IDPs (Google, Facebook, Amazon, ...)	Lokale IDPs mit DE-Basis (Verimi, netID, id4me, ...)	Self-Sovereign Identity (Sovrin, uPort, Blockstack, ...)
Komfort	↑ Fast jeder Anwender nutzt Dienste bereits	↓ Anwender muss erst aufspringen	↓ Anwender muss erst aufspringen
Nutzungsraum	↑ Global	↓ Lokal (DE/EU)	↑ Global
Empowerment	↓ Anwender hat kaum Einfluss	↓ Anwender hat nur mittelbar Kontrolle	↑ Anwender hat vollständige Kontrolle
Datenablage	↓ Zentral bei IDP	↓ Zentral bei IDP (innerhalb EU)	↑ Ausschließlich beim Anwender
Skalierbarkeit	↑ Enorme Kapazitäten verfügbar	↑ Gegeben	↑ Designt für globale Nutzung
Sicherheit	↓ Erfolgreicher Angriff kompromittiert alles	↓ Erfolgreicher Angriff kompromittiert alles	↑ Dezentralität erschwert Angriffe massiv
Datenschutz	↓ DSGVO wird ausgehebelt	↑ DSGVO glaubwürdig eingehalten	↑ Designt für DSGVO-Konformität
Standards	↑ Standards verfügbar, produktiv genutzt	↑ Standards verfügbar, produktiv genutzt	↑ Standards verfügbar, prototypisch genutzt
Vertrauen	↓ Anwender ist „ausgeliefert“	↑ Informierte Anwender vertrauen bedingt	↑ Informierte Anwender vertrauen maximal

Die Self-Sovereign Identity Mission & Vision



Status Quo Self-Sovereign Identity (SSI) – Beispiele internationaler Vorhaben und Projekte



- BMW Förderaufruf Sichere Digitale IDs
- govdigital (Zusammenschluss öffentlicher IT-Dienstleister)
- SSI für Deutschland

- EMIL
- Digitales Corona Gesundheitszertifikat
- 5 Sovrin Stewards



- 5 Sovrin Stewards



- myIDsafe (SSI)
- 2 Sovrin Stewards



- uPort / Ethereum Foundation Zug
- 5 Sovrin Stewards



- SSI-Projekt mit Banken via Dutch Blockchain Coalition
- 5 Sovrin Stewards



- Sovrin-Credentials für Unternehmen, öffentliches Unternehmensregister
- Beantragung und Verwaltung von Zulassungen und Lizenzen
- 2 Sovrin Stewards



- EBSI eSSIF
- INATBA
- ID2020
- 25 Sovrin Stewards

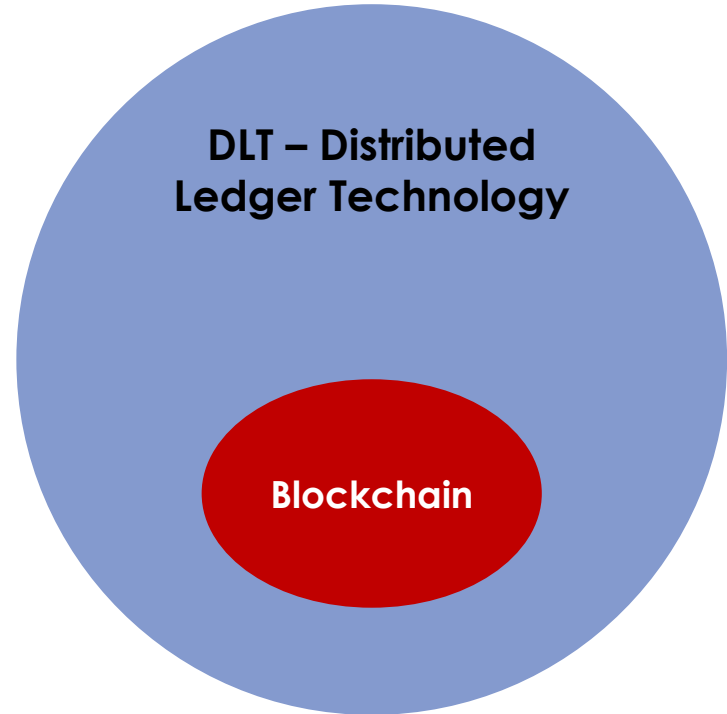


- Sovrin Network
- Trust over IP Foundation
- Covid Credentials Initiative (CCI)
- GLEIF Pilotprojekt (Organization Wallets)
- ~80 Sovrin Stewards

Blockchain Technologie

Nutzung der Distributed Ledger Technology für digitale Identitäten

- Dezentralisiertes Ledger
- Transaktionen bestätigt durch Konsens-Algorithmus
- Teilnehmer sind Nodes / Nutzer / Miner
- Alle Informationen befinden sich auf allen Nodes
- Integrität wird durch Verkettung sichergestellt
- Authentizität durch asymmetrische Verschlüsselung
- Technische Durchsetzung der CIA-Triade:
Confidentiality | Integrity | Availability
Vertraulichkeit | Integrität | Verfügbarkeit
- Geeignet für Kryptowährungen, Supply Chains, Nachverfolgungen und **digitale Identitäten!**



Blockchains sind nicht immer gleich: Öffentliches vs. Privates Blockchain-Netzwerk

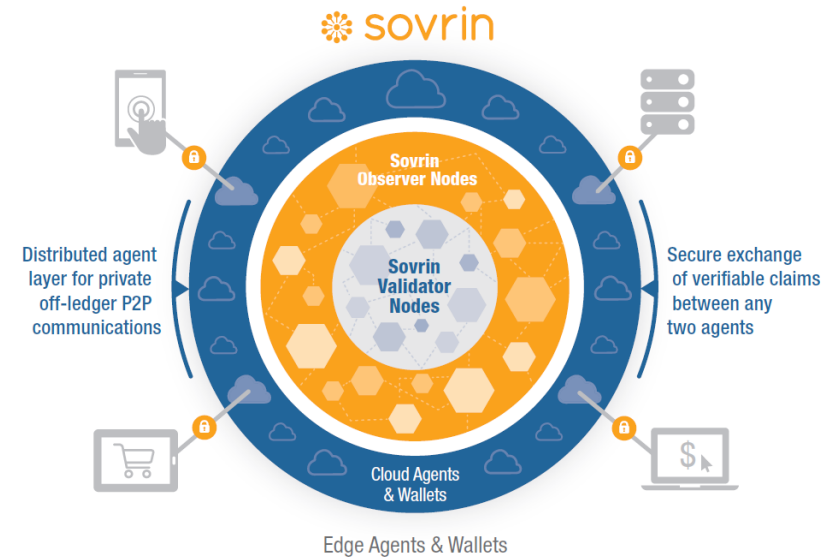
- ✓ Robustheit
 - ✓ Teure Angriffe
 - ✓ Transparenz
 - ✗ Träge Änderungen
 - ✗ Langsamer Konsens
-
- ✗ Kein sinnvolles Anwendungsszenario

		Wer kann validieren?	
		Permissionless	Permissioned
Wer hat Zugriff?	Public	<p>„Jeder darf lesen und validieren“</p>  <p>bitcoin <small>https://bitcoin.org</small></p>	<p>„Jeder darf lesen, nur Berechtigte validieren“</p>  <p>sovrin <small>https://sovrin.org</small></p>
	Private	<p>„Nur Berechtigte dürfen lesen, jeder darf validieren“</p>	<p>„Nur Berechtigte dürfen lesen und validieren“</p>  <p>c.rda <small>https://www.corda.net</small></p>

- ✓ Robustheit
 - ✓ Berechtigungen
 - ✓ Transparenz
 - ✓ Schneller Konsens
 - ✓ Rollback möglich
 - ✗ Missbrauch möglich
-
- ✓ Berechtigungen
 - ✓ Schneller Konsens
 - ✓ Rollback möglich
 - ✗ Missbrauch möglich
 - ✗ Erprobtere Datenbanken

Beispiel Sovrin: Modell für Self-Sovereign Identity & dezentralisiertes Vertrauen

- Globales DLT-basiertes Identitätsnetzwerk
- Nutzt dezentralisierte Identifikatoren (DIDs)
- Schneller und energiesparender Konsens (RBFT: Redundant Byzantine Fault Tolerance)
- Verwaltet durch Non-Profit-Organisation
- Diverse „Stewards“ verpflichten sich zu einem Trust Framework und betreiben die Nodes
- Cross-funktional mit anderen Identity Chains
- Open Source Softwarebasis
- Teil von Hyperledger Indy



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

Methoden der Konsensfindung: PoX etc.

Proof-of-Work (PoW)

Kryptographisches Rätsel – Wettlauf um einen Hashwert mit automatischer Anpassung des Schwierigkeitsgrades



Proof-of-Stake (PoS)

Verwandt mit PoW, gewichtete Zufallsauswahl des Validierers, ausschlaggebend ist der „Stake“ eines Nutzers, also der Anteil an der gesamten Menge an Token, die er besitzt



Redundant BFT / Plenum

Byzantine Fault Tolerance
(BFT) Familie

Redundantes Protokoll für Maschinenreplikation mit eingebauter Toleranz für willkürlich auftretende Fehler – DLT, nicht Blockchain



Proof-of-Authority (PoA)

Alternative zu Proof-of-Stake, die Vertrauenswürdigkeit einer Person/Organisation statt Teilnehmer mit hohem Vermögen als Validierer für die Blockchain ist ausschlaggebend



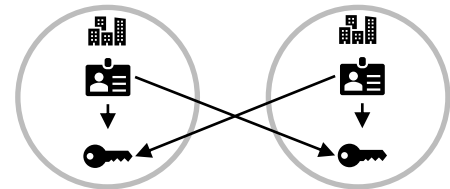
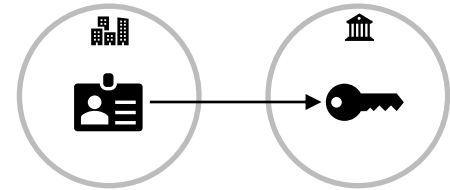
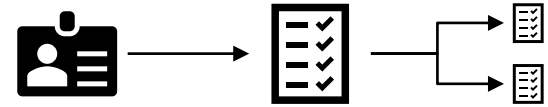
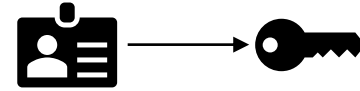
Vorstellung SeLF / Demo

SeLF Demo



Anwendungsbeispiele


- 🔒 Credentials führen zu Berechtigungen (auch physical access)
- 🔒 Credentials als Primary Source für Fakten
- 🔒 Credentials extern nutzen:
 - 🔒 Mitarbeiterangebote
 - 🔒 Nachweis des Anstellungsverhältnisses
- 🔒 Cross-Organisation Onboarding und Berechtigungsvergabe




Anbindung an Legacy und SSI-native Zielsysteme



Kompatibilitätsmatrix

 SELF SSI enablement matrix	Authentication				Authorization					
	OpenID Connect		SAML		OpenID Connect		Active Directory		Azure AD	
	SAML	OAuth 2	OpenID Connect	SSI-native	SAML	OAuth 2	OpenID Connect	LDAP	Active Directory	Azure AD
✓ supported* ✗ not supported* \$ supported (plugin required)*										
Adobe Creative Cloud	✓	✓	✗	✗	✓	✓	✗	✓	✓	✗
Adobe ID Management	✓	✓	✗	✗	✓	✓	✗	✓	✓	✗
Alibaba Cloud Service	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗
AssetSonar	✓	✗	✗	✗	✓	✗	✗	✓	✓	✗
Atlassian Confluence	\$	✓	\$	✗	\$	✓	\$	✓	✓	✗
Atlassian Jira	\$	✓	\$	✗	\$	✓	\$	✓	✓	✗
AuditBoard	✓	✗	✗	✗	✓	✗	✗	✓	✓	✗
AWS Console	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗
Azure Cloud	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗
Bloomberg Anywhere	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗
Cisco Cloud	✓	✗	✗	✗	✓	✗	✗	✓	✓	✗
DB2	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗
Dropbox Business	✓	✓	✗	✗	✗	✓	✗	✓	✓	✗
esatus SELF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Evernote	✓	✓	✗	✗	✓	✓	✗	✓	✓	✗
GitHub	✓	✓	✗	✗	✓	✗	✗	✓	✓	✗
Google Cloud	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗
Google ID Platform	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗
HP Service Manager	✓	✗	✗	✗	✓	✗	✗	✓	✓	✗

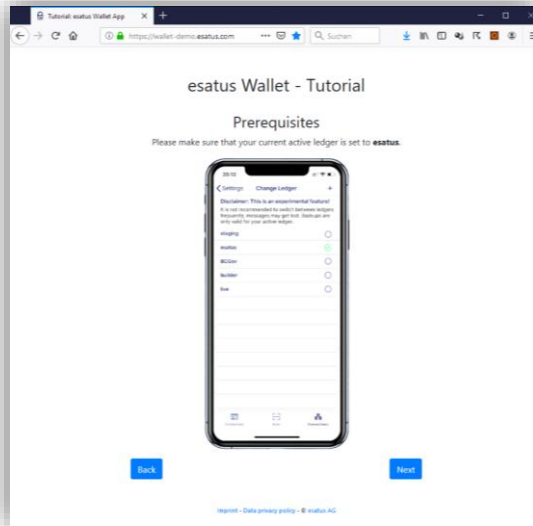
* All information is supplied without guarantee and is based on own research. ⚠

 SELF SSI enablement matrix	Authentication				Authorization					
	OpenID Connect		SAML		OpenID Connect		Active Directory		Azure AD	
	SAML	OAuth 2	OpenID Connect	SSI-native	SAML	OAuth 2	OpenID Connect	LDAP	Active Directory	Azure AD
✓ supported* ✗ not supported* \$ supported (plugin required)*										
Microfocus ALM	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗
Microsoft SQL Server	✓	✗	✗	✗	✓	✗	✗	✓	✓	✗
MySQL	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗
Nextcloud	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗
Oracle Database	✗	✓	✗	✗	✓	✗	✓	✓	✓	✗
Rocket Chat	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗
RSA Identity G&L	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗
Salesforce	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗
SAP (various apps)	✓	✓	✗	✗	✓	✗	✓	✓	✓	✗
SAP Cloud ID Platform	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗
ServiceNow	✓	✓	✗	✗	✓	✗	✓	✗	✓	✗
SharePoint (local)	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗
Slack	✓	✗	✗	✗	✗	✓	✗	✗	✓	✗
Sybase	\$	✓	✗	✗	\$	✓	✗	✓	✓	✗
Trello	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗
Workday	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗
Zendesk	✓	✓	✗	✗	✗	✓	✗	✓	✓	✗

* All information is supplied without guarantee and is based on own research. ⚠

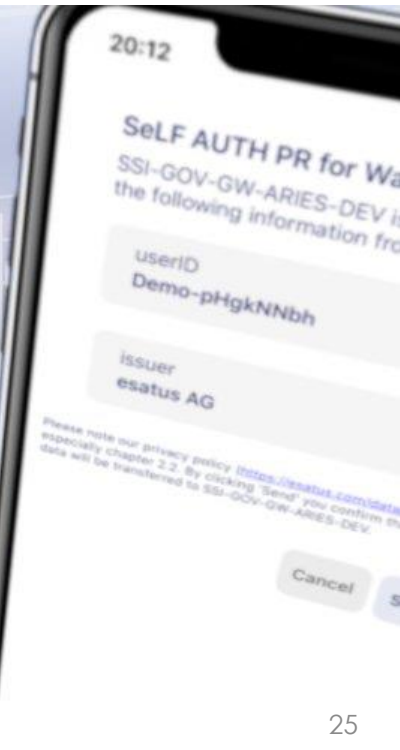
Selbst ausprobieren?

<https://wallet-demo.esatus.com>



Tutorial esatus Wallet App

esatus AG
Enforcing Information Security



esatus SeLF Rollout



https://esatus.com/files/whitepapers/esatus_SSI_Roll-out.pdf

<https://www.youtube.com/watch?v=WBilpRK6PRU>



self-ssi.com



@esatus_SeLF



@esatusself





CIO esatus AG

Dr. André Kudra

Tel.: +49 6103 90295-0

a.kudra@esatus.com

esatus AG | www.esatus.com

Copyright © 2020 esatus AG. Alle Rechte vorbehalten

Alle Inhalte, Fotos und Grafiken sind urheberrechtlich geschützt. Sämtliche Teile dieses Dokuments dürfen nicht ohne vorherige schriftliche Genehmigung durch die esatus AG weder ganz noch auszugsweise kopiert, vervielfältigt, verändert oder übertragen werden.

Herausgeber: esatus AG

Copyright Fotos: Tomasz Zajda/Fotolia; bismillah_bd/Fotolia;
tostphoto/Fotolia; envfx/Fotolia