Souveräne Digitale Identität

https://danubetech.com/

Markus Sabadello
Danube Tech GmbH
Sovrin Foundation
Wien, 14. März 2018

Markus Sabadello

- Studium Informatik und Peace&Conflict Studies
- >10 Jahre Entwicklung und Beratung zu “User-centric Identity”
- Ko-Vorsitz bei OASIS XDI Technical Committee
- Vorstandsmitglied bei XDI.org Non-Profit
- **Mitglied des Technical Governance Board bei Sovrin Foundation**
- Mitglied des Advisory Board bei Evernym, Inc.
- Mitarbeit bei Hyperledger Indy
- Mitarbeit bei W3C Verifiable Claims WG, Credentials CG, Social Web CG, u.a.
- Mitglied bei Digital Enlightenment Forum
- Consultant bei World Economic Forum “Rethinking Personal Data”
- Consultant bei Harvard Berkman Center for Internet&Society
- Consultant bei MIT Media Lab Human Dynamics Group
- **Gründer, Geschäftsführer von Danube Tech GmbH**

sovrin

DANUBE TECH GMBH

"On the Internet, nobody knows you're a dog."

sovrin

identity for all


Me
You
Amazon


Friends
Gov't
Family
Amazon
Doctor's Office
You
Google
Credit Union
Face-book
Apple
Ebay

Sovrin

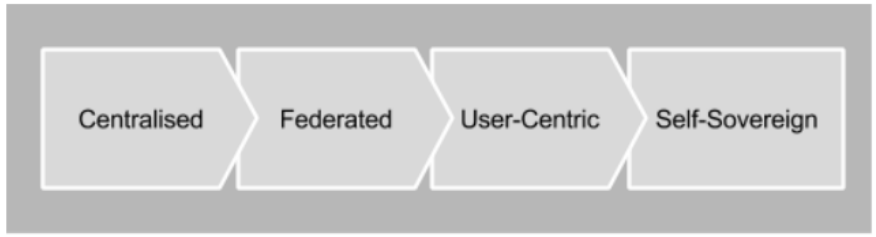


Fig 1. The evolution of online identity

- Souveräne digitale Identität (“self-sovereign identity”).
- Keine Kryptowährung, keine Smart Contracts.
- Blockchain / DLT als unabhängige Registrierungsstelle.
- Speziell für digitale Identität entwickelt.
- Öffentlich verwendbare, weltweit verfügbare Infrastruktur.
- Digitale Identität für Individuen, Organisationen, und Dinge, die von sonst niemandem modifiziert oder vernichtet werden kann.

Sovrin Technologie

Decentralized Identifiers (DIDs)

- Dezentrale Kennzahlen (Netzwerkadressen), werden bei W3C standardisiert.
- Persistent, auflösbar, kryptografisch verifizierbar: **did:sov:3k9dg356wdcj5gf2k9bw8kfg7a**
- Funktioniert mit verschiedenen Blockchains: **did:sov, did:btcr, did:v1, did:uport, …**
- Auflösung: DID → DID Document
  - Kryptografische Schlüssel.
  - Netzwerkadressen für Protokolle.

Method	DID Prefix
Sovrin	did:sov:
Bitcoin	did:btcr:
uPort	did:uport:
VeresOne	did:v1:
IPFS	did:ipid:
IPDB	did:ipdb:
Blockstack	did:stack

Decentralized Identifiers (DIDs)

```
{
    "@context": "https://w3id.org/did/v1",
    "id": "did:sov:WRfXPg8dantKVubE3HX8pw",
    "publicKey": [
        {
            "id": "did:sov:WRfXPg8dantKVubE3HX8pw#key-1",
            "type": "Ed25519VerificationKey",
            "publicKeyBase58": "lji9qTtkCydxtez_bt1zdLxVMMbz4SzWvlqgOBmURoM"
        }
    ],
    "services": [
        {
            "id": "#srv1",
            "type": "agent",
            "serviceEndpoint": "https://agent.example.com/did:sov:WRfXPg8dantKVubE3HX8pw/"
        },
        {
            "id": "#srv2",
            "type": "xdi",
            "serviceEndpoint":
                "https://xdi.example.com/did:sov:WRfXPg8dantKVubE3HX8pw/",
        }
    ]
}
```

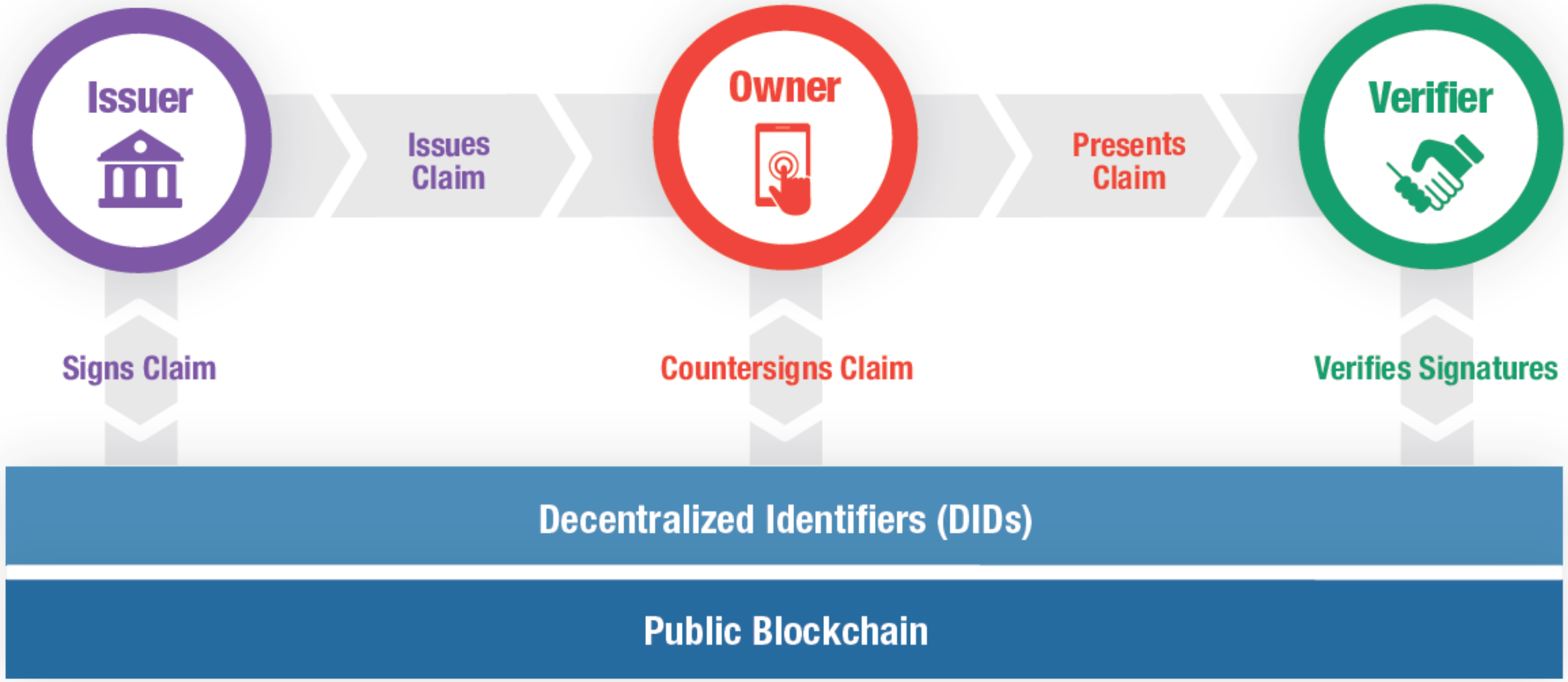
Verifiable Claims

- Identitätsdaten, die “attestiert” anstatt “selbst-behauptet” sein können.
- Kryptografisch nachweisbare Aussagen
  eines “Issuer” über ein “Subjekt”:
  - Post sagt: “Frau Müller hat eine Adresse in 1010 Wien.”
  - Universität sagt: “Herr Sabadello hat Informatik studiert.”
- Basiert auf RDF und JSON-LD Standards.

Verifiable Claims

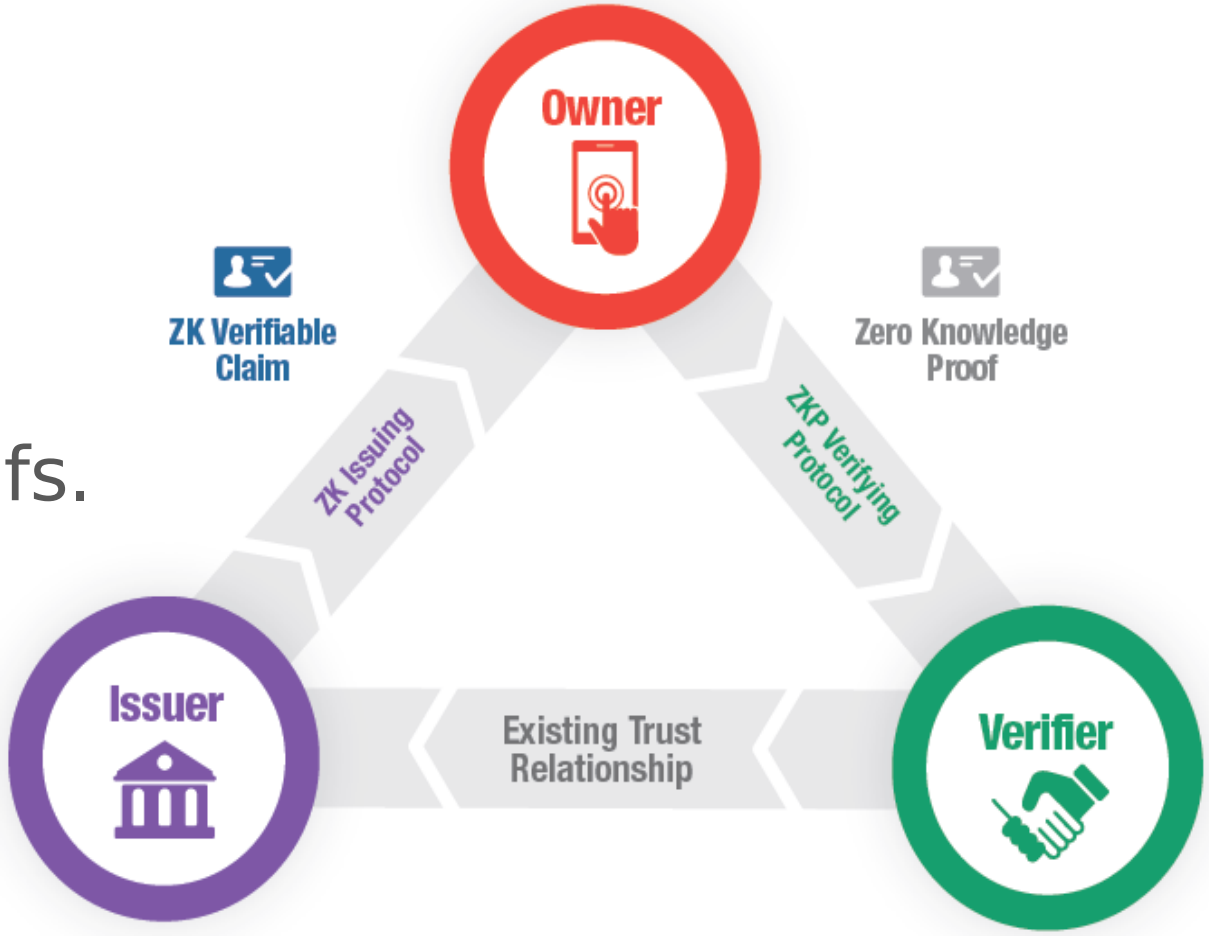

```
{
  "@context": "https://w3id.org/security/v1",
  "type": ["Credential", "AddressCredential"],
  "issuer": "did:sov:WRfXPg8dantKVubE3HX8pw",
  "issued": "2017-01-01",
  "claim": {
    "id": "did:sov:Bda9VcXbnUGFaDZSHdbEhn",
    "street": "Wallnerstraße 8",
    "postalCode": "1010",
    "city": "Vienna",
    "country": "Austria"
  },
  "signature": {
    "type": "LinkedDataSignature2017",
    "nonce": "598c63d6",
    "signatureValue": "BavEll0/I1zpYw8XNi1bgVg/sCneO4..."
  }
}
```

Verifiable Claims



Verifiable Claims

- Paarweise-pseudonyme Identifikatoren.
- Selektiver Datentransfer durch Zero-Knowledge Proofs.



SSI und eID

"Wir wollen den Bürgerinnen und Bürgern ihre Datenhoheit zurückgeben, indem sie selber und datensparsam über die Verwendung ihrer Daten entscheiden.[...] der Trafikant sieht nur das, was er wissen muss, und zwar, dass der Kunde und die Kundin das gesetzlich vorgesehen Alter erreicht haben."
- 26 Sep. 2017, Wolfgang Sobotka, Innenminister

sovrin

SSI und eID

EGIZ

Whitepaper

Self-Sovereign Identity

Whitepaper about the Concept of Self-Sovereign Identity including its Potential

Version 1.0, 13.10.2017

Andreas Abraham (andreas.abraham@egiz.gv.at)

Abstract: This document provides three main contributions. First, it details the Self-Sovereign Identity concept including its underlying blockchain technology. Second, related technologies are identified; evaluation criteria are defined and used to evaluate these technologies. Finally, the SSI potential is identified and described.

“Another big possibility is offered by the SSI system when it comes to identity derivation. With extending the SSI system, it should be possible to derive identity data from existing eID infrastructure such as eIDAS network. This is realized by transforming the identity assertion into the SSI format.”

Identity For All

Identity For All

- Geschätzte 1,1 (or 1,5) Mrd. Menschen weltweit – hauptsächlich im Globalen Süden – die keine nachweisbare institutionelle Identität haben.

iRespond

- (Digitale) Identität für Flüchtlinge an der Grenze zwischen Thailand und Myanmar

iRespond

- Int. Org. for Migration (IOM)
- Int. Rescue Committee (IRC)
- Royal Thai Government
- iRespond:
  - 80.000 registriert
  - 200.000 bis Ende März
  - 2.000.000 bis Jahresende

sovrin

12
11
0
KLMNOPQRSTUVWXYZ

Freedom Out of the Box

FreedomBox

- Persönlicher Server
- Debian Linux
- Kalender, Wiki, Blog, Messaging, Self-Hosting, Dezentralisierung, Privatsphäre

FreedomBox Dashboard | Router | Privacy | Sharing | Apps | Services | System | Documentation | Not logged in. Log in.

MENU

- Where to Get Help
- Developer's Manual
- FAQ
- FreedomBox Wiki
- About

About the FreedomBox

We live in a world where our use of the network is mediated by those who often do not have our best interests at heart. By building software that does not rely on a central service, we can regain control and privacy. By keeping our data in our homes, we gain useful legal protections over it. By giving back power to the users over their networks and machines, we are returning the Internet to its intended peer-to-peer architecture.

FreedomBox

In order to bring about the new network order, it is paramount that it is easy to convert to it. The hardware it runs on must be cheap. The software it runs on must be easy to install and administrate by anybody. It must be easy to transition from existing services.

Learn more »

Our Goal

There are a number of projects working to realize a future of distributed services; we aim to bring them all together in a convenient package.

For more information about the FreedomBox project, see the Debian Wiki.

Vielen Dank

Vielen Dank

- Markus Sabadello
- Sovrin Foundation – https://sovrin.org/
  Technical Governance Board
- Danube Tech GmbH – https://danubetech.com/
  Geschäftsführer
- markus@danubetech.com

Architektur