SSI Lecture Series

Dr. Ivan Gudymenko
ivan.gudymenko@t-systems.com

Danil Tolonbekov
danil.tolonbekov@t-systems.com

See also our video interviews on YouTube
Digital business: for 27 years

Employees: around 2,100 (digital) experts, project enthusiasts, consultants, students, developers, nerds, salespeople, managers, Telekom fans, innovators, service professionals & testers

Revenue in 2021: 200 m. €

Average age: 37

Share of women: 33%

Customer projects and services in 2021: 2,992

Hours worked on customer projects and services 2021: 1,642,422

Working style: agile, flexible, professional, reliable, digital
How we are different

Technology-independent advice, strong partners

We use and understand what we sell.

Everything from a single source: from backend to frontend

Highly-secure networks and data centers belonging to Deutsche Telekom AG

Zero Distance in nine cities

Berlin
Bonn
Dresden
Hamburg
Jena
Leipzig
Munich
Rostock
Stuttgart

Certified processes and accredited test center

24/7 service with a named point of contact

We love complex projects
Self-Sovereign Identity
Our SSI Team

Self-Sovereign Identity

T·Systems
Let's power higher performance

SSI Lecture Series 18.11.2022
Ecosystem of Self Sovereign Identity: CATA Awards
Problem Statement: ID Information Verification

- Have you ever had to show your ID to someone to obtain a service or simply to be let in?

- Have you ever had privacy concerns?

Problem Statement: All or Nothing Paradigm
Problem Statement: All or Nothing Paradigm

Not all ID attributes are required to obtain a service!
Solution to the all-or-nothing Problem: Selective Disclosure

All or Nothing

VS.

Selective disclosure

• Proving only the required attributes
• Statements about the attributes are also supported
  • e.g. “over 18”, etc.

Self-sovereign Identity Paradigm enables Selective Disclosure!
Example: Privacy-Preserving Age Verification

Yes, see statement: > 18

Are you older than 18?

- No unnecessary details about the person are revealed (only “>18”)
- The validity of the statement can be verified (>18 is valid)
- A significant privacy gain (no further personally identifiable information must be revealed)
Seven Laws of Identity

Kim Cameron’s Laws of Identity

1. User Control and Consent
   Technical identity systems must only reveal information identifying a user with the user’s consent.

2. Minimal Disclosure for a Constrained Use
   The solution which discloses the least amount of identifying information and best limits its use is the most stable long-term solution.

3. Justifiable Parties
   Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

4. Directed Identity
   A universal identity system must support both “omni-directional” identifiers for use by public entities and “unidirectional” identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

5. Pluralism of Operators and Technologies
   A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

6. Human Integration
   The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

7. Consistent Experience Across Contexts
   The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

Kim Cameron
former Chief Architect of Identity at Microsoft

Taken from https://www.identityblog.com/?p=1065
Conventional Centralized Identity Management

- Centralized ID Management
- The organization is responsible for maintaining the compliance (sec, privacy, ...)
- Susceptible to targeted attacks
Notable Attacks in the past

Facebook Cambridge Analytica
User's data acquired and used for political purposes
87 million affected

Equifax
Sensitive data including credit card numbers compromised
148 million affected

Equifax to Pay $575 Million

Yahoo
Hackers stole personal data of users
500 million affected
**Identity vs. Identifier**

- Organizations maintain **IDENTIFIERS** for their customers. It is **THEIR** identifier.
- Organizations **LEND** credentials to humans. Humans are **PRESENTED** by a lended credentials.
- Humans have no control over the data maintained by organizations.
- Portability of data and vendor lock-in are challenges.

versus

- Persons/human beings have **IDENTITY** and retain control over it (and its properties).
- Not account-based.
- Shift in control over the properties and attributes of an identity.
„Privacy of an entity is the result of negotiating and enforcing when, how, to what extent, and in which context which data of this entity is disclosed to whom.“ [1]

Self Sovereign Identity: paradigm shift

- User has personal data under control
- The users can selectively disclose attributes
Anonymous Credentials by design are correlation resistant

- User has personal data under control
- The users can selectively disclose attributes

No correlation is possible
Selective Disclosure
SSI Components – Roles

Issuer
(issues credentials)

Holder
(holds credentials)

Verifier
(verify credentials)

Digital Wallet/
Agent

Ledger

Employee ID

ISSI Lecture Series
18.11.2022
SSI Agents and Wallets Interaction

Taken from Sovrin Glossary V3
Verifiable Credentials

Issuer
Issues VCs

Holder
Acquires, stores, presents VCs

Verifier
Verifies VCs

Verifiable Data Registry
Maintains identifiers and schemas

Issue Credentials
Send Presentation

Verify Identifiers and use Schemas
Register Identifiers and use Schemas

Taken from https://www.w3.org/TR/vc-data-model/
Decentralized ID: a New „IPs“ of SSI Networks

**EXAMPLE 1:** A simple DID document

```
{
    "@context": [
        "https://w3id.org/security/suites/ed25519-2020/v1",
        "https://w3.org/ns/did/v1"
    ],
    "id": "did:example:123456789abcdefgхи",
    "authentication": [{
        // used to authenticate as did:... paid
        "id": "did:example:123456789abcdefgхи#keys-1",
        "type": "Ed25519VerificationKey2020",
        "controller": "did:example:123456789abcdefgхи",
        "publicKeyMultibase": "zh3C2AVvLMv6gmMNam3uVAg2PfkcGCwDwnZn6z3wXmqPV"
    }]
}
```

Taken from https://www.w3.org/TR/did-core/
State of the art in SSI
Hyperledger Aries Design

The Internet

Other Agents

Distributed Ledger

Aries Cloud Agent – Python

Core Capabilities

Aries Protocols

REST API

Controller

Events

Requests

Application Business Logic
Aries Agent
Wallet DB
Tails Server
Issuer API
Controller
Cloud Holder API
Verifier API
SSI Service Layer
BKAMT Cloud Layer
Mediator
Indy Ledger
End User Layer
ID Wallet
Third party backend
API
Backend
SSI Connector Layer – Color Scheme
- Shows the opensource components
- Shows the components that will be developed
SSI Lecture Series 18.11.2022
Use Case: Online Elections

Self-Sovereign Identity and Confidential Computing

https://youtu.be/TC5VKjBhPPQ?t=659
The Big „T“ is an active player

Lissi Wallet  ID Wallet by Govt  Esatus Wallet
Thank you for your attention! Questions?