esatus® AG
Enforcing Information Security

Identity & Access Management (IAM) for Applications with Self-Sovereign Identity (SSI)

Disrupt Meetup Digital Identity
Achieving Digital Self Sovereignty Through Blockchain
Frankfurt am Main, 26 February 2019

Featured content | Session goals

esatus AG
Enforcing Information Security

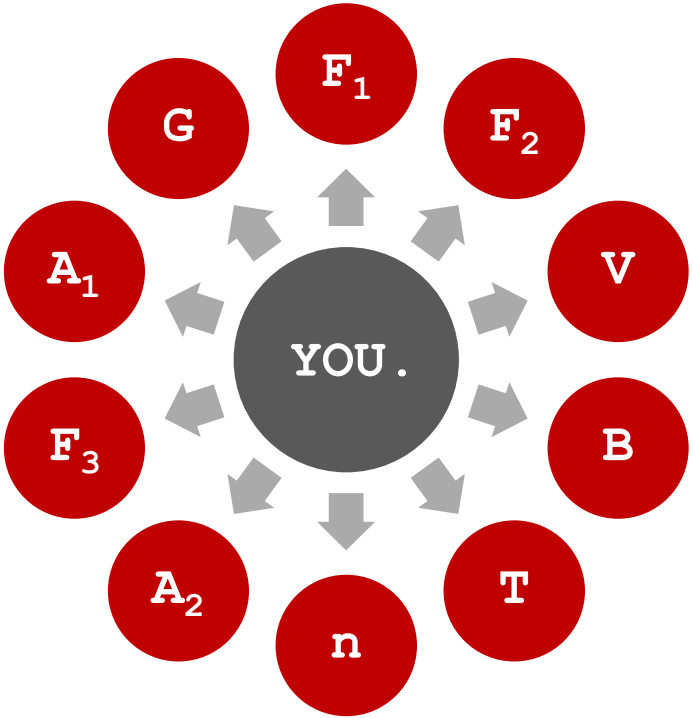
- Addressing identity issues with Self-Sovereign Identity (SSI)
- Insight into international standardization initiatives
- Introducing relevant terminology
- Reviewing status quo of technological frameworks
- Presenting the Identity & Access use case

- Introduce SSI to an IT-related community
- Obtain valuable perspectives for shaping solutions

Digital identity is one of the hardest problems in our networked world

esatus® AG
Enforcing Information Security

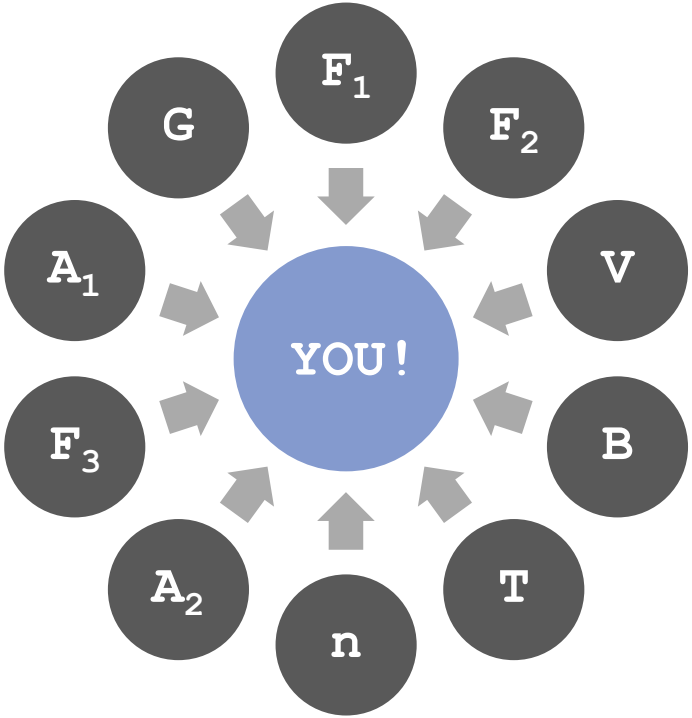
- In a networked world, machines have identities, people don't
- Every online service we use lures as into creating a new digital identity
- Handling accounts and password is a constant struggle – a hard to win battle
- Services collect data about us – to their own benefit & undisclosed purposes
- A digital identity of this kind can be revoked or its rules can be changed
- YOU ARE NOT IN CONTROL!
  YOU SHOULD BE!!!



With Self-Sovereign Identity a user regains full control over his data

esatus® AG
Enforcing Information Security

- A Self-Sovereign Identity is 100% owned and controlled by an individual
- No one else can read it, use it, turn it off, take it away without its owner's consent
- An SSI is private, highly secure, and moves around with you
- Everything is centered around the user – exactly how it should be
- **BRING YOUR OWN IDENTITY** ultimately becomes possible



International Blockchain Standardization via International Organization for Standardization (ISO)

esatus® AG
Enforcing Information Security

- **ISO/TC 307 Blockchain and distributed ledger technologies**
- Scope: Standardisation of blockchain technologies and distributed ledger technologies.
- Started in 2016
- Secretariat Standards Australia
- Two annual onsite meetings
- 41 Participating Members, 11 Observing Members
- Diverse liaisons outside of ISO

EC - European Commission, EEA Inc. - Enterprise Ethereum Alliance Inc., FIG - International Federation of Surveyors, IEEE - Institute of Electrical and Electronics Engineers, OECD - Organisation for Economic Co-operation and Development, ITU - International Telecommunication Union, SWIFT – Society for Worldwide Interbank Financial Telecommunication, UNECE - United Nations Economic Commission for Europe

Group	Content
ISO/TC 307/AG 1	SBP Review Advisory Group
ISO/TC 307/AHG 1	Liaison Review Ad Hoc Group
ISO/TC 307/CAG 1	Convenors coordination group
ISO/TC 307/JWG 4	Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Blockchain and distributed ledger technologies and IT Security techniques
ISO/TC 307/SG 2	Use cases
ISO/TC 307/SG 7	Interoperability of blockchain and distributed ledger technology systems
ISO/TC 307/WG 1	Foundations
ISO/TC 307/WG 2	Security, privacy and identity
ISO/TC 307/WG 3	Smart contracts and their applications
ISO/TC 307/WG 5	Governance

https://www.iso.org/committee/6266604.html

Standard and/or project under the direct responsibility of ISO/TC 307 Secretariat

esatus® AG
Enforcing Information Security

ISO/CD 22739	Terminology
ISO/NP TR 23244	Overview of privacy and personally identifiable information (PII) protection
ISO/DTR 23245	Security risks, threats and vulnerabilities
ISO/NP TR 23246	Overview of identity management using blockchain and distributed ledger technologies
ISO/CD 23257	Reference architecture
ISO/AWI TS 23258	Taxonomy and Ontology
ISO/AWI TS 23259	Legally binding smart contracts
ISO/DTR 23455	Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems
ISO/NP TR 23576	Security management of digital asset custodians
ISO/NP TR 23578	Discovery issues related to interoperability
ISO/NP TS 23635	Guidelines for governance

https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0

Decentralized Identity Foundation (DIF)

https://identity.foundation/images/logo-white-small.png

esatus AG
Enforcing Information Security

- **DIF Mission** — Developing the foundational components of an open, standards-based, decentralized identity ecosystem for people, organizations, apps, and devices.

- **DIF Focus** — DIF is an engineering-driven organization focused on developing the foundational elements necessary to establish an open ecosystem for decentralized identity and ensure interop between all participants.

  Technical Specifications. Groups in DIF develop specifications and emerging standards for protocols, components, and data formats that implementers can execute against.

  Reference Implementations. Beyond specifications, DIF members develop open source reference implementations of the technical components and protocols they create.

  Industry Coordination. As the leading industry organization in the Decentralized Identity space, DIF seeks to align industry participants to advance their common interests.

- **DIF Groups** — **Identifiers, Names, and Discovery.** Identify and locate people, organizations, and devices without centralized systems of identifiers.

  Storage and Compute. Secure, encrypted, privacy-preserving storage and computation of data.

  Claims and Credentials. Ability to verify the claims and assertions of identities is key in establishing trust among entities on a decentralized system that lacks a centralized hierarchy.

https://identity.foundation

DIF Members

https://identity.foundation

Coordinated Identity Workshops

esatus® AG
Enforcing Information Security

https://www.weboftrust.info/images/wot-logo.png

Rebooting Web-of-Trust (RWOT) – hosted by Christopher Allen

This facilitated design workshop is focused on the creation of the next generation of decentralized web-of-trust based identity systems. Objectives are:

- Build the next generation of Web-Of-Trust based identity systems.
- Showcase the scope of potential applications for decentralized trust models.
- Bring together the top contributors in web of trust and similar applications.
- Explore developing tools that might be useful to funders and researchers.
- Discuss and suggest requirements to drive adoption in the Web-of-Trust model.

https://www.weboftrust.info

https://internetidentityworkshop.com/wp-content/uploads/2018/10/iiw-dog-logo.png

Internet Identity Workshop (IIW) – organized by Phil Windley

The Internet Identity Workshop has been finding, probing and solving identity issues twice every year since 2005. We meet in the Computer History Museum in Mountain View, CA. Every IIW moves topics, code and projects downfield. Name an identity topic and it's likely that more substantial discussion and work has been done at IIW than any other conference. IIW is at its heart a participatory conference, it is an Open Space unConference. It has no keynotes or panels, so it's about getting stuff done. IIW brings together the largest concentration on the planet of talent dedicated to designing and building identity systems that empower individuals.

https://internetidentityworkshop.com

World Wide Web Consortium (W3C)

https://www.w3.org/Icons/w3c_home

- **About W3C** — The World Wide Web Consortium (W3C) is an international community where Member organizations, a full-time staff, and the public work together to develop Web standards. Led by Web inventor and Director Tim Berners-Lee and CEO Jeffrey Jaffe, W3C's mission is to lead the Web to its full potential.
- **W3C Mission** — The W3C mission is to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web. W3C's standards define key parts of what makes the World Wide Web work.
- **W3C Groups** — A variety of W3C groups enable W3C to pursue its mission through the creation of Web standards, guidelines, and supporting materials. Community and Business Groups offer more ways for innovators to bring work to W3C.
- **Credentials Community Group** — The mission of the W3C Credentials Community Group is to explore the creation, storage, presentation, verification, and user control of credentials. We focus on a verifiable credential (a set of claims) created by an issuer about a subject — a person, group, or thing — and seek solutions inclusive of approaches such as: self-sovereign identity; presentation of proofs by the bearer; data minimization; and centralized, federated, and decentralized registry and identity systems. Our tasks include drafting and incubating Internet specifications for further standardization and prototyping and testing reference implementations.

https://open-stand.org/wp-content/uploads/2014/08/blog-080214-new-header.png

https://www.w3.org/Consortium | https://www.w3.org/community/credentials

W3C Credentials Community Group – Identity-relevant Standardization Contributions

esatus AG
Enforcing Information Security

- **Decentralized Identifiers (DIDs) v0.11**

  Draft Community Group Report, 23 August 2018

  Decentralized Identifiers (DIDs) are a new type of identifier for verifiable, "self-sovereign" digital identity. DIDs are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority. DIDs are URLs that relate a DID subject to means for trustable interactions with that subject. DIDs resolve to DID Documents — simple documents that describe how to use that specific DID. Each DID Document contains at least three things: cryptographic material, authentication suites, and service endpoints. Cryptographic material combined with authentication suites provide a set of mechanisms to authenticate as the DID subject (e.g. public keys, pseudonymous biometric protocols, etc.). Service endpoints enable trusted interactions with the DID subject.

- **Verifiable Claims Use Cases 1.0**

  Final Community Group Report, 01 May 2017

  A verifiable claim is a qualification, achievement, quality, or piece of information about an entity's background such as a name, government ID, payment provider, home address, or university degree. Such a claim describes a quality or qualities, property or properties of an entity which establish its existence and uniqueness. The use cases outlined here are provided in order to make progress toward possible future standardization and interoperability of both low and high-stakes claims with the goals of storing, transmitting, and receiving digitally verifiable proof of attributes such as qualifications and achievements. The use cases in this document focus on concrete scenarios that the technology defined by the group should address.

- **Verifiable Claims Data Model and Representations 1.0**

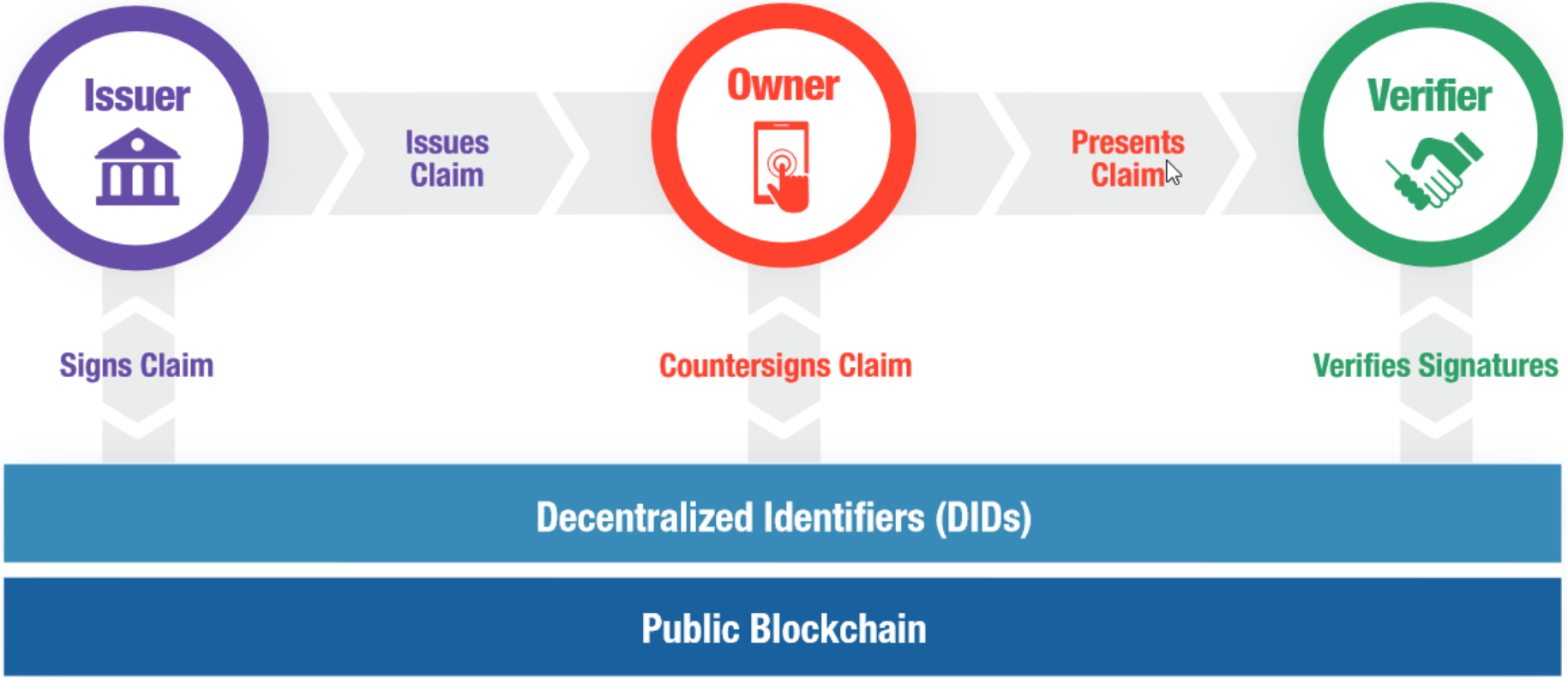
  Final Community Group Report, 01 May 2017

  A self-sovereign architecture for verifiable claims is one where the holder of a verifiable claim is in complete control of their identifier, where their verifiable claims are stored, and how they are used. There is currently no widely used self-sovereign, privacy-enhancing standard for expressing and transacting verifiable claims (aka: credentials, attestations) via the Web. This specification describes a data model for a digital identity profile and a collection of digital entity credentials that assert verifiable claims about that identity profile. It also describes how to express that data model in JSON, JSON-LD, and WebIDL.

https://w3c-ccg.github.io/did-spec | https://www.w3.org/2017/05/vc-use-cases/CGFR/2017-05-01 | https://www.w3.org/2017/05/vc-data-model/CGFR/2017-05-01

Blockchain, DIDs und Claim Signing

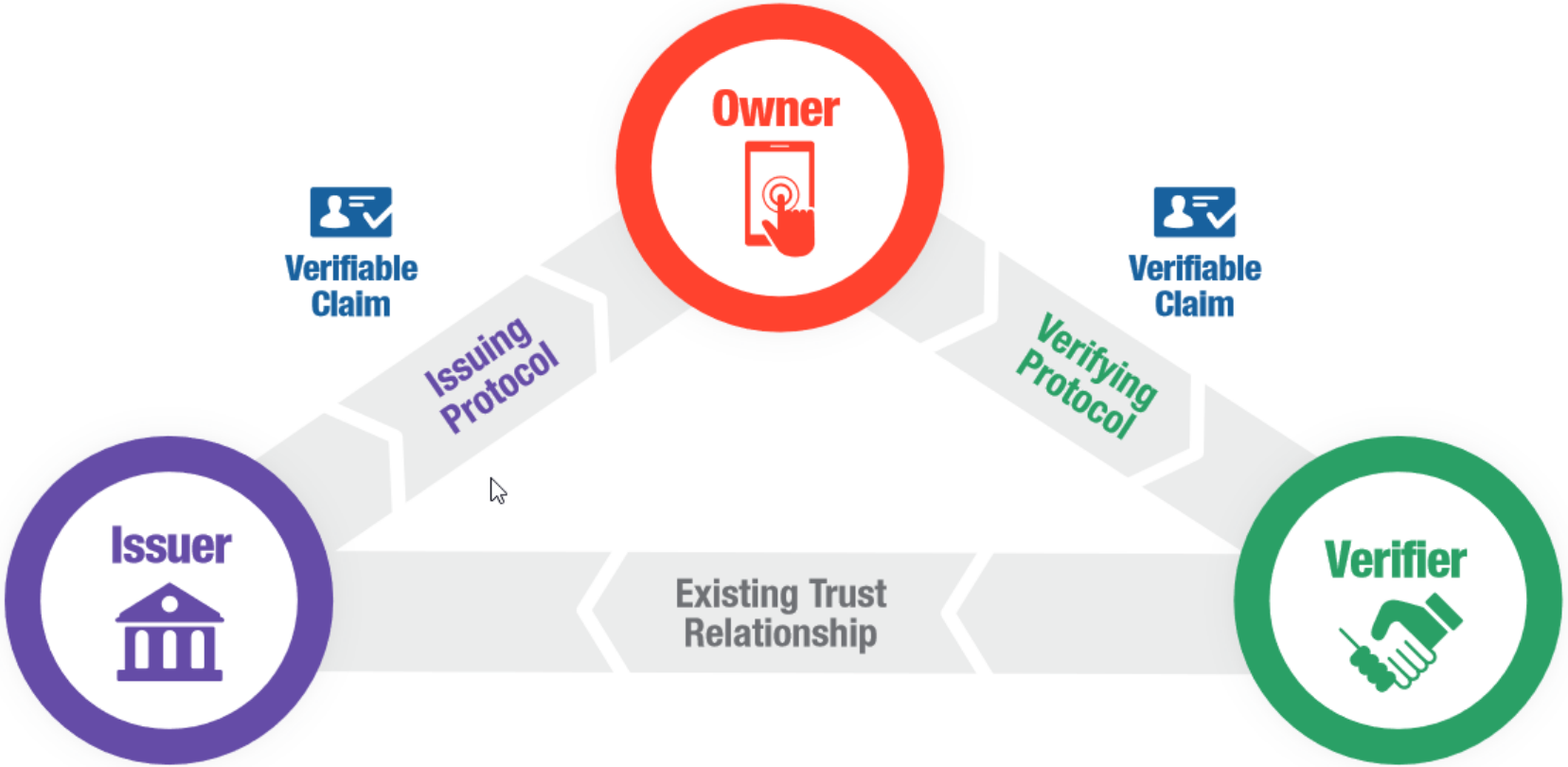
esatus AG
Enforcing Information Security



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

Verifiable Claims

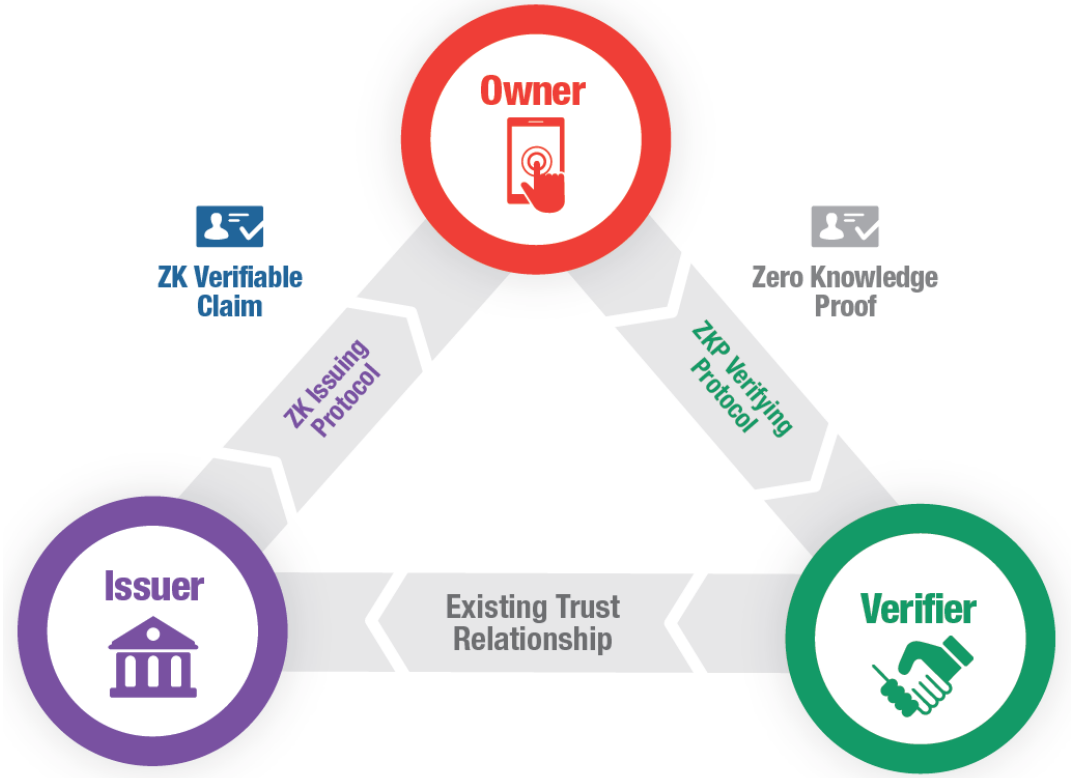
esatus AG
Enforcing Information Security



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

Zero Knowledge Proof

esatus® AG
Enforcing Information Security

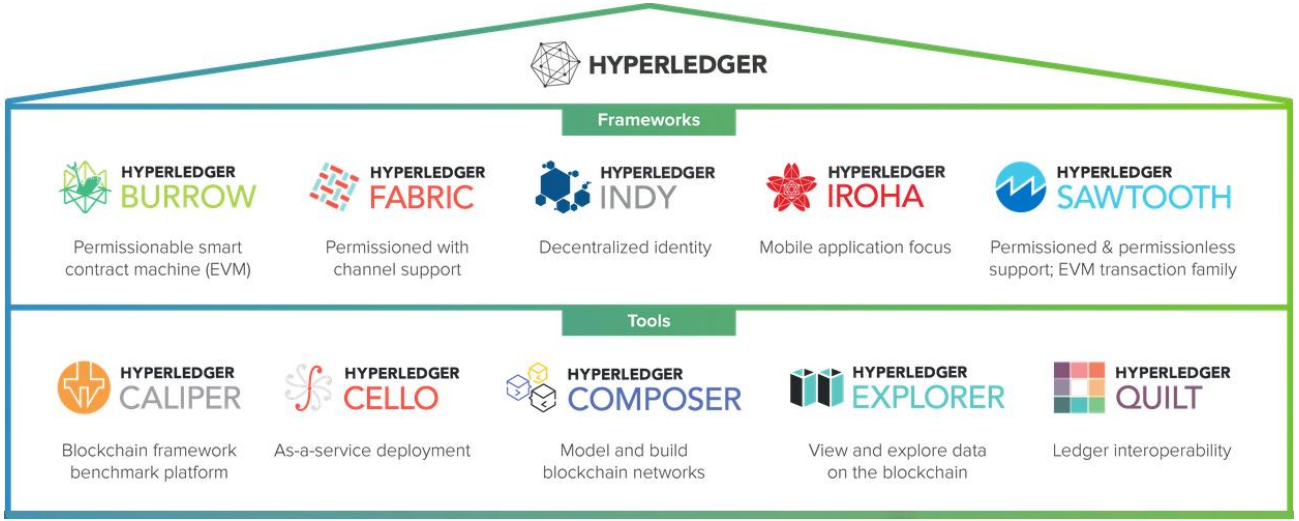


Source: Sovrin™: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust - A White Paper from the Sovrin Foundation - Version 1.0 - January 2018

Hyperledger

https://www.hyperledger.org/wp-content/uploads/2016/09/logo_hl_new.png

- **Hyperledger Mission** — Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, Internet of Things, supply chains, manufacturing and Technology.
- **Indy** — Hyperledger Indy is a distributed ledger, purpose-built for decentralized identity. It provides tools, libraries, and reusable components for creating and using independent digital identities rooted on blockchains or other distributed ledgers for interoperability.
- **Frameworks & Tools – „Greenhouse“**



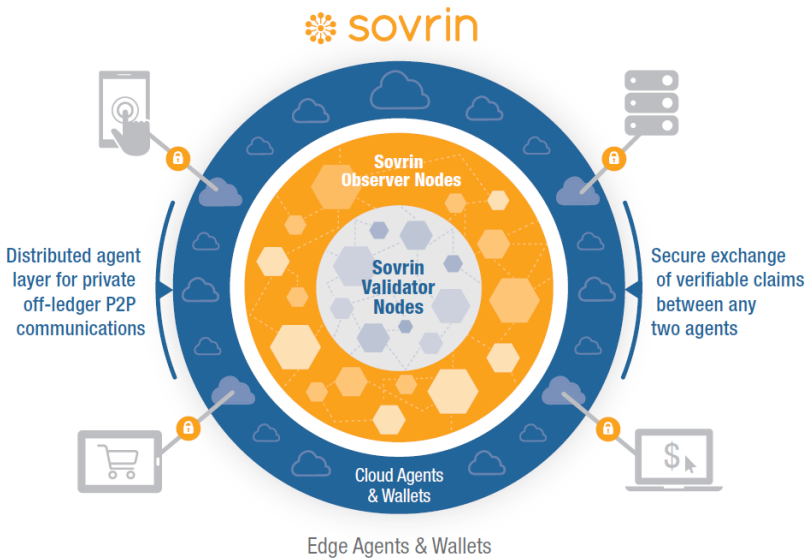
https://www.hyperledger.org

https://www.linuxfoundation.org/wp-content/uploads/2017/06/LF_logo_NEW_H_W.png

Example: A model for Self-Sovereign Identity & decentralized trust

esatus AG
Enforcing Information Security

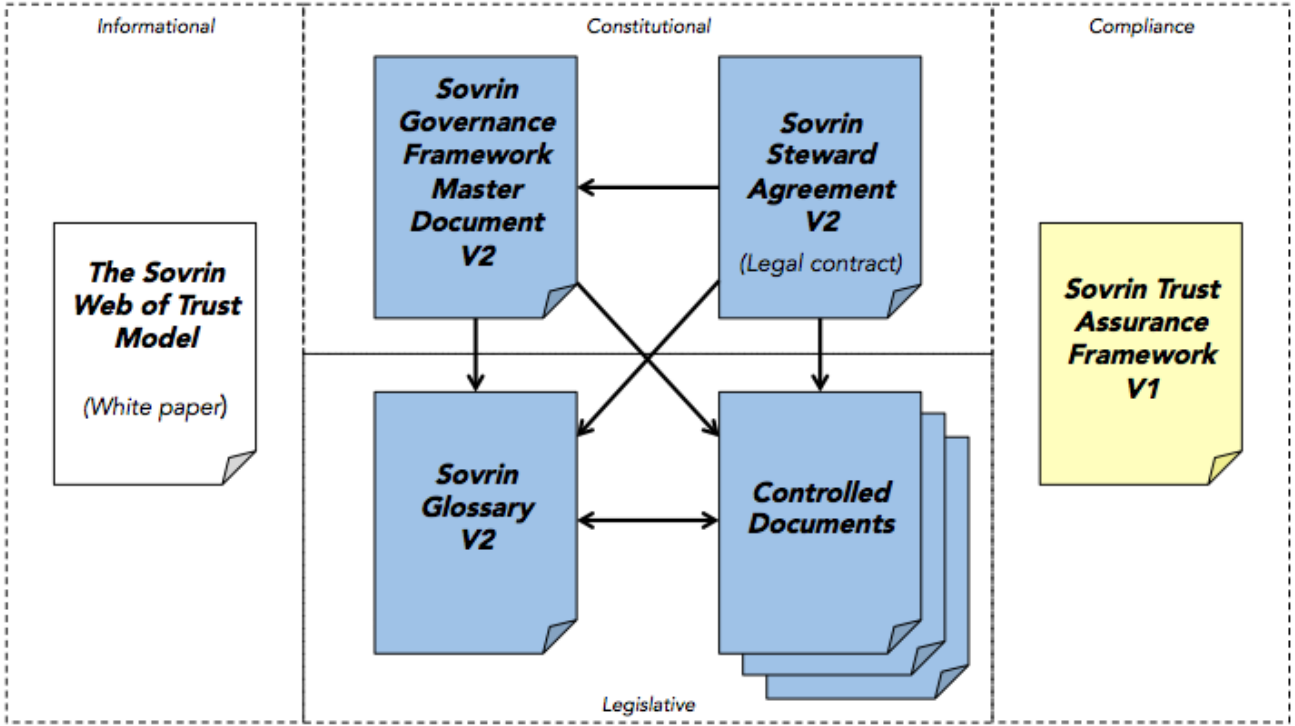
- Global DLT-based identity network
- Uses Decentralized Identifiers (DIDs)
- Fast and low-energy consensus (RBFT: Redundant Byzantine Fault Tolerance)
- Governed by not-for-profit foundation
- Diverse "stewards" commit to trust framework & operate validator nodes
- Cross-operational with others
- Open-source software basis
- Part of Hyperledger Indy



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

Overview Sovrin Governance Frameworks V2

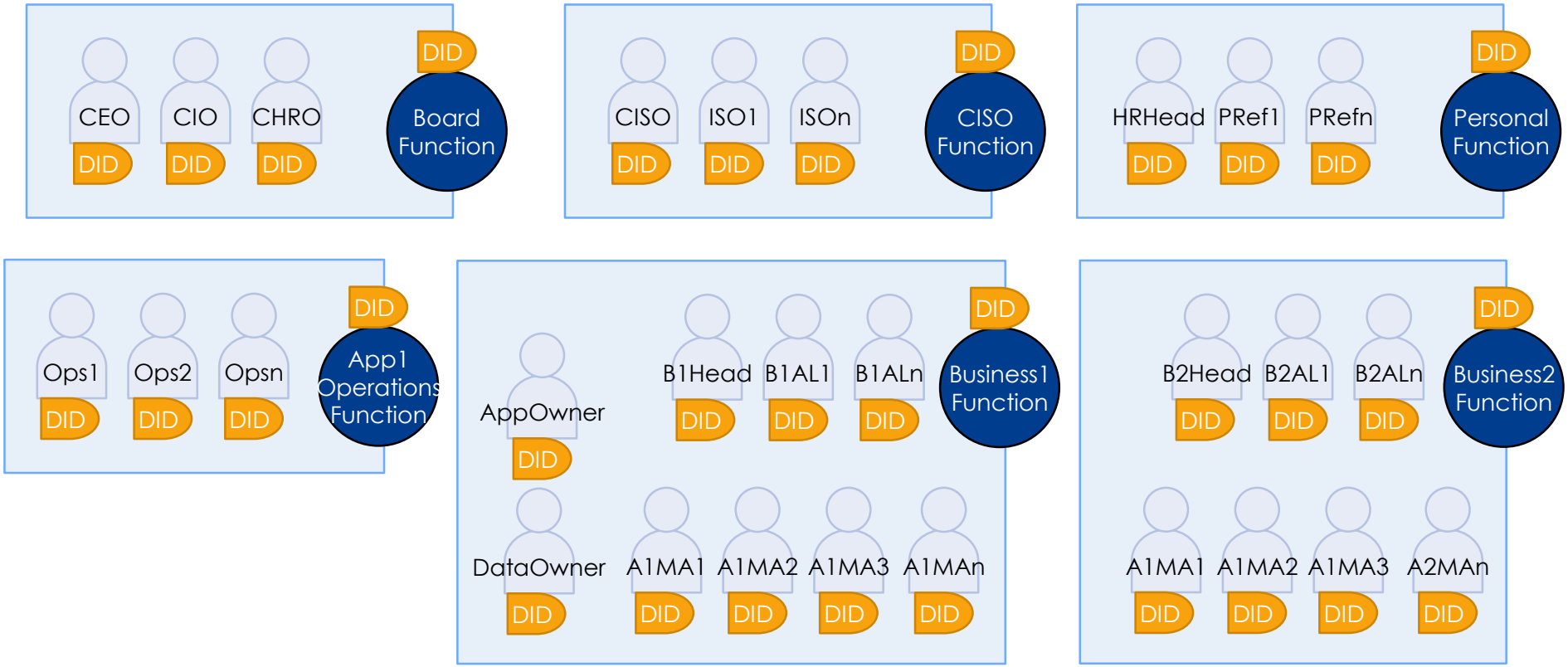
esatus AG
Enforcing Information Security



https://sovrin.org/wp-content/uploads/2018/11/sovrin-governance-framework-diagram-v2.png

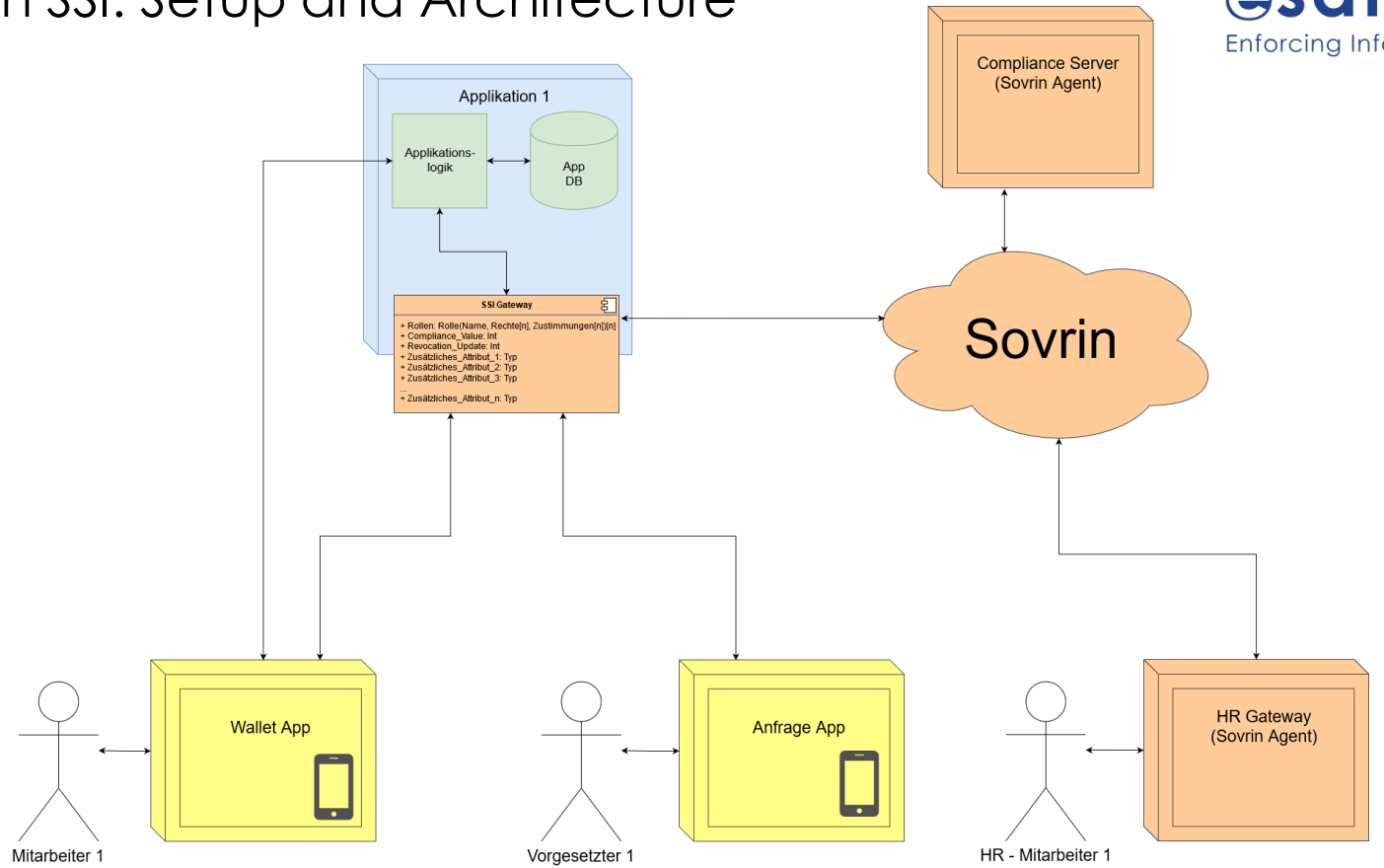
IAM Players in a SSI Ecosystem

esatus AG
Enforcing Information Security



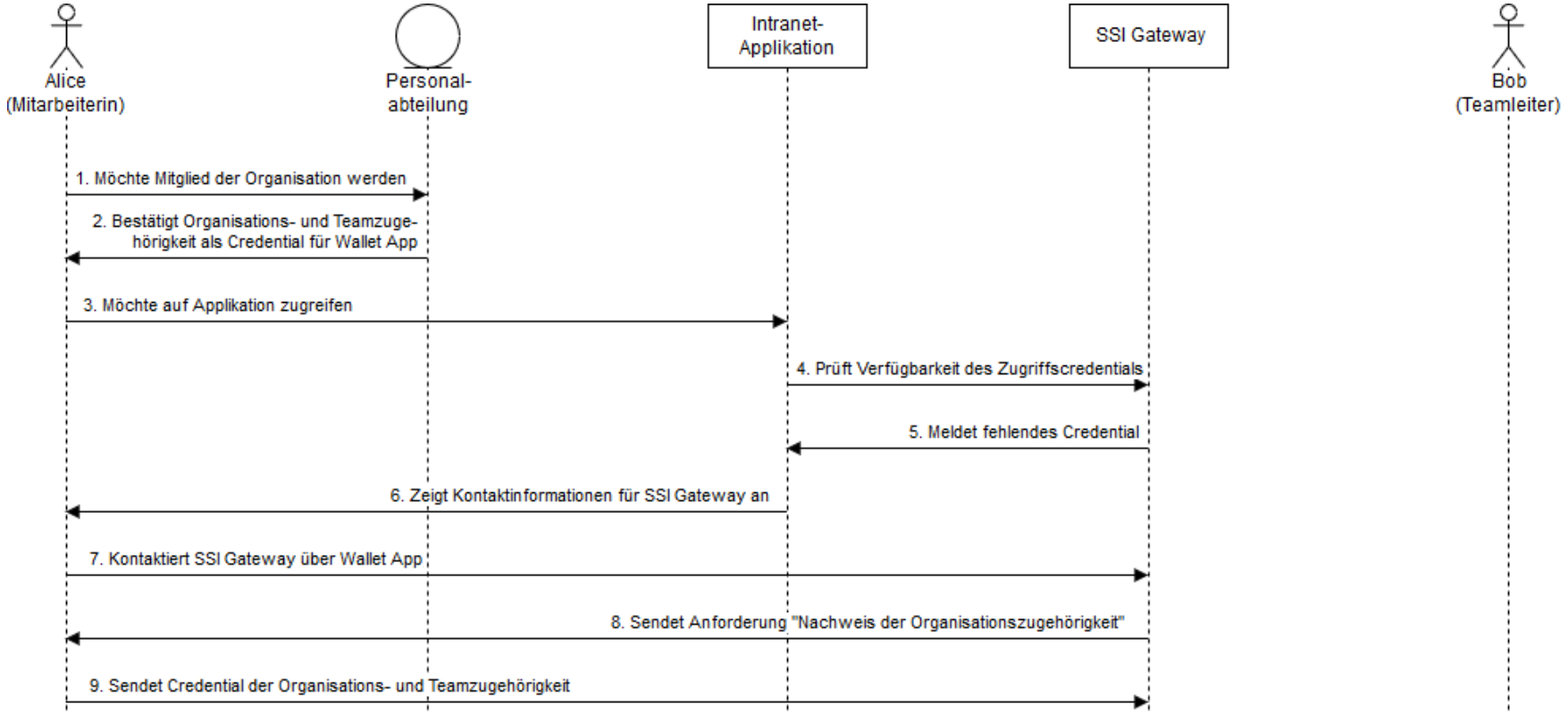
IAM with SSI: Setup and Architecture

esatus AG
Enforcing Information Security



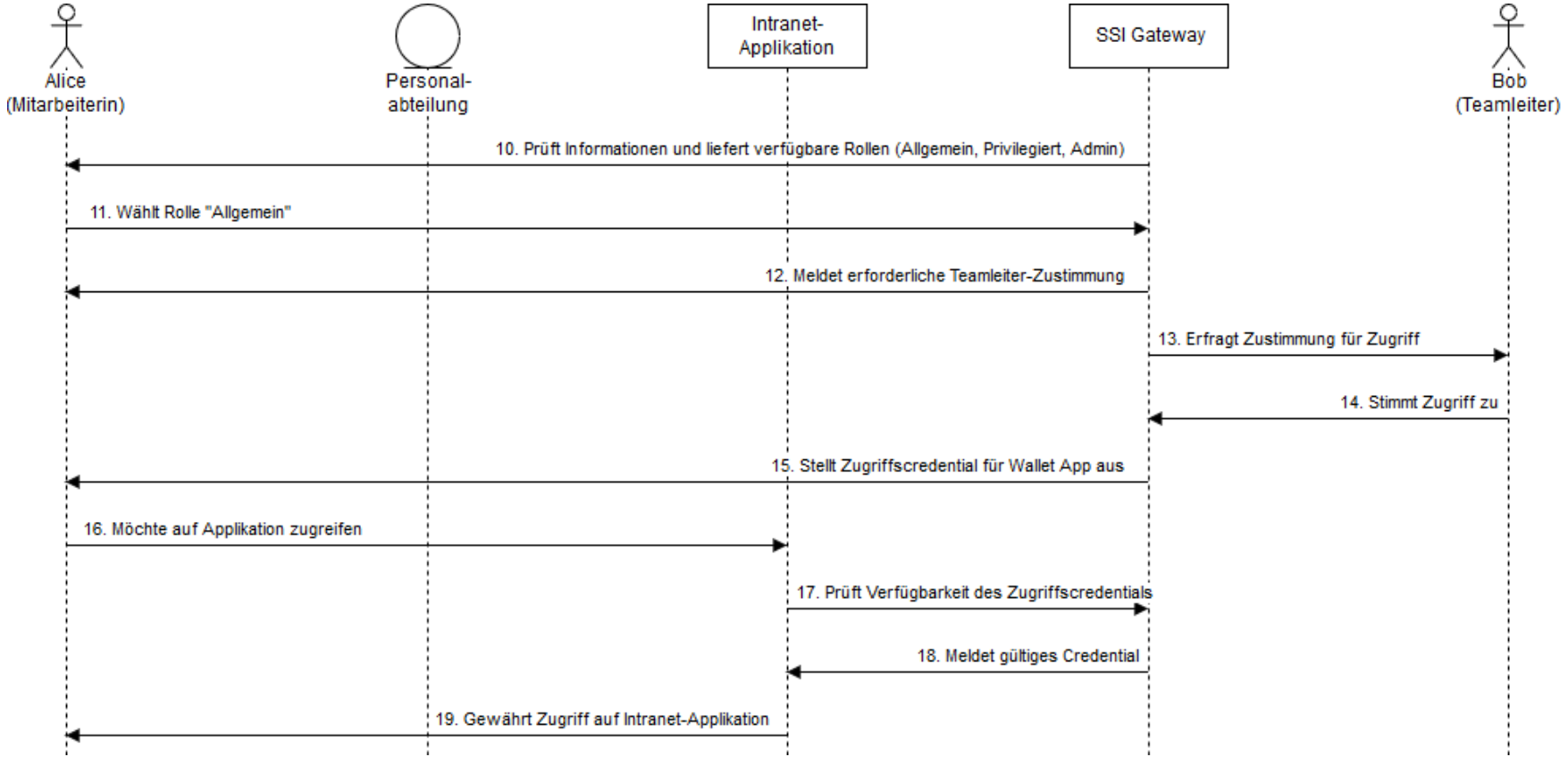
IAM meets Self-Sovereign Identity

esatus AG
Enforcing Information Security



IAM meets Self-Sovereign Identity cont‘d

esatus AG
Enforcing Information Security



Questions and Discussion

esatus® AG
Enforcing Information Security

esatus® AG
Enforcing Information Security

Thank you for your Contribution!

Your esatus Blockchain Contact

esatus AG
Enforcing Information Security

CIO esatus AG und Leiter Blockchain AG TeleTrusT

Dr. André Kudra

Telefon: +49 6103 90295-0

Mail: a.kudra@esatus.com

Copyright

esatus AG
Enforcing Information Security

Herausgeber: esatus AG

Copyright Fotos: Tomasz Zajda/Fotolia; bismillah_bd/Fotolia; tostphoto/Fotolia; envfx/Fotolia; Gunnar Asmy/Adobe Stock; Alexander Limbach/Adobe Stock; SG-design/Adobe Stock; Perfect Vectors/Adobe Stock; Vikivector/Adobe Stock; raven/Adobe Stock; Graphic in Motion/Adobe Stock; vectorfusionart/Adobe Stock; Елизавета Акимова/Adobe Stock; Tierney/Adobe Stock; DaiPhoto/Adobe Stock; Feng Yu/Adobe Stock; HQUALITY/Adobe Stock; jonnysek/Adobe Stock; metamorworks/Adobe Stock; area51uk/Adobe Stock