A LIGHTWEIGHT TRUST MANAGEMENT INFRASTRUCTURE FOR SELF-SOVEREIGN IDENTITY

Michael Kubach and Heiko Roßnagel

Fraunhofer IAO

?

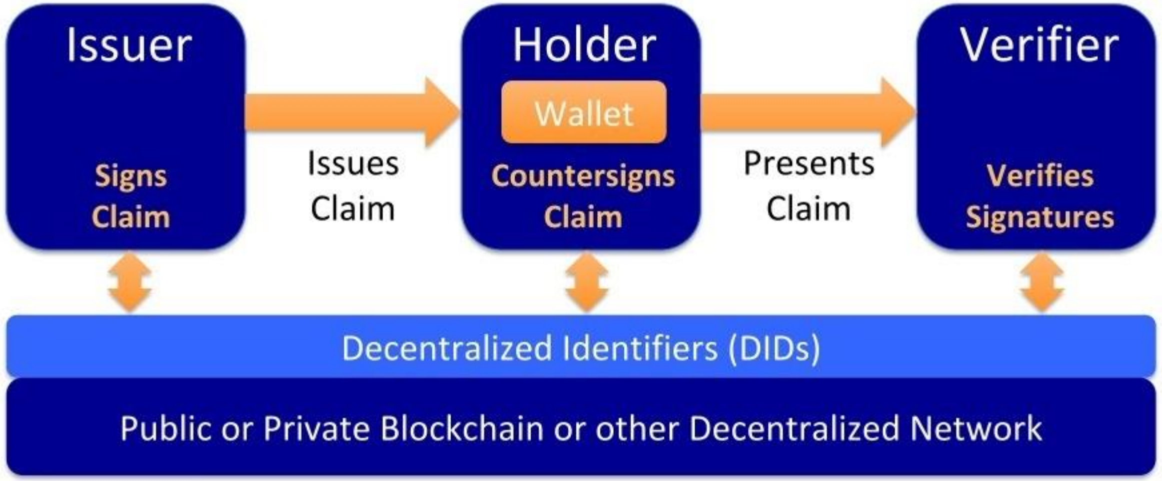
Agenda

- Introduction
- Trust-related challenges in Self-sovereign identity approaches
- Previous and related work
- TRAIN as a lightweight trust management infrastructure for SSI

Introduction

SSI – Self-Sovereign Identity

- Term goes back to the *Ten Principles of Self-sovereign Identity* postulated by [Al16]
- Aims to allow users to fully own and manage their digital identity without having to rely on a third party
- Usually, a DLT is used to build a decentralized Public Key Infrastructure. End users usually manage keys and credentials in smartphone application "wallets"



Drummond Reed - https://www.slideshare.net/SSIMeetup/decentralized-identifiers-dids-the-fundamental-building-block-of-selfsovereign-identity-ssi CC BY-SA 4.0

- Verifiable Credentials, Zero Knowledge Proofs, Selective Disclosure
- *"the next evolutionary step in the development of digital identities"* [DE20], the "*future of digital identity"* [Si18]

Challenge of the Root of Trust in Digital Transactions

For doing business, to provide services etc. we increasingly rely on digital transactions between:

Natural

Persons

Organizations

Legal Persons

Devices

Things

But how can we know whether a remote someone/something is trustworthy?

One approach

Trust Infrastructures based on State-run Regulatory Processes (e.g. eIDAS)

Limited to certain trust domains, not very flexible, centralized and only partially compatible with the SSI vision.

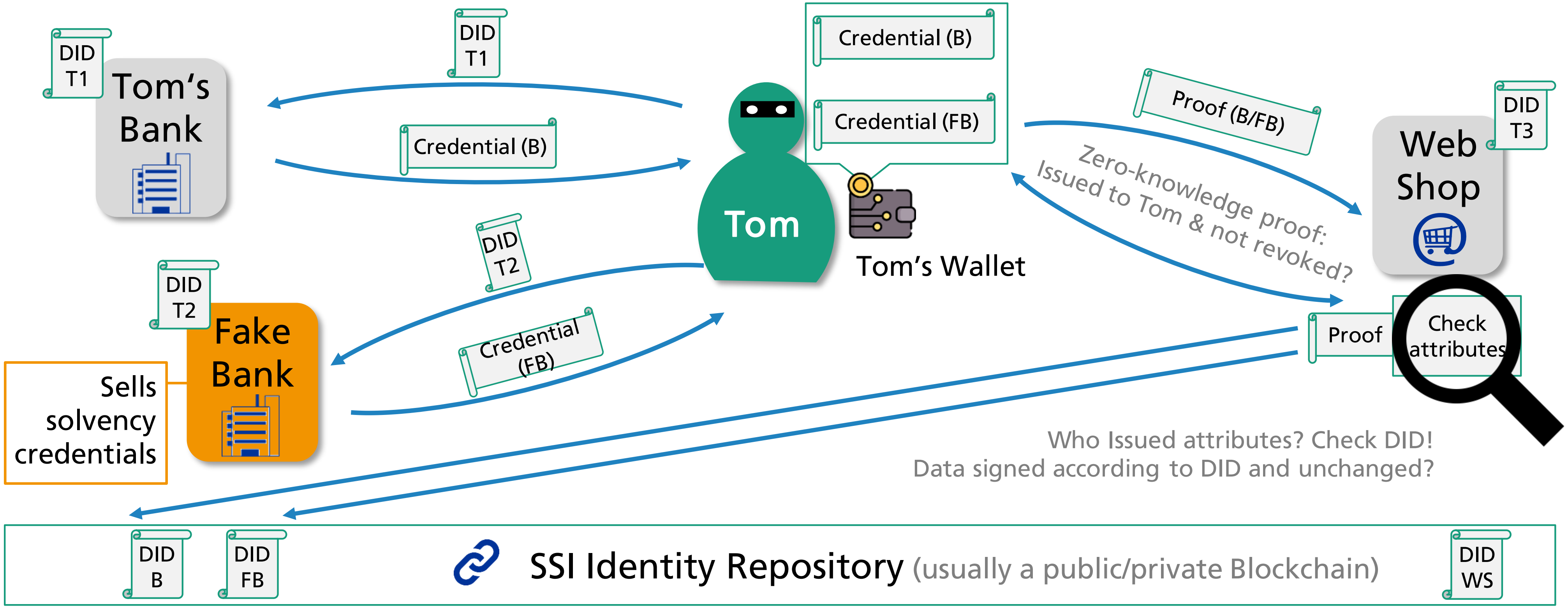
Trust-related challenges in Self-sovereign identity approaches

- SSI approaches put a high emphasis on the user’s control over their data.
- E.g. in the Principles of Self-sovereign identity [Al16], the interests of other stakeholders of the identity ecosystem are not considered.
- Trust requirements of the other relevant stakeholders in the identity ecosystem are also essential for the adoption of an identity technology [ZR12]
- **Relying parties (RP)/service providers (SP) are of particular importance**: they offer services that end users want to use with their digital identity / credentials

➡ **Focus on two particular Aspects: Trust Anchor and Automation**

Absence of a natural trust anchor

What if evil Tom wants to order something he cannot afford? (simplified)



Automated trust management

Identity and trust management is getting more complex

- Amount of identity information is steadily increasing, e.g. through IoT
- Use cases getting more complex (new work, complex value networks…)
- Breaking up of identity data silos as a major goal of SSI
- Effort for manual management of trust raises fast across many trust domains, organizations, devices etc.

Automation of trust management is necessary to achieve scalable solutions

- Trust policies required that can be expressed in a formalized way
- Automated verification of transactions against trust policies

Previous and related work

Challenge recognized by important players such as Trust over IP Foundation and EBSI ESSIF

Proposed solutions:

- Centralized governance layers and trust frameworks with trust anchors and/or trust intermediaries
  - ➔ Contradicts open and decentral SSI-Approach
- Reliance on the market to decide about the trustworthiness of actors
  - ➔ Re-occurring problem with fraud (Fake Banks etc.), automation hardly possible, oligopoly
- Traditional hierarchical solutions for trust management such as hierarchical PKIs
  - ➔ Scalability and flexibility for large number of entities? Acceptance of common trust root?
- Incorporation of existing Trust Schemes, e.g., through SSI eIDAS Bridge
  - ➔ Focused on a single trust domain

TRAIN as a lightweight trust management infrastructure for SSI

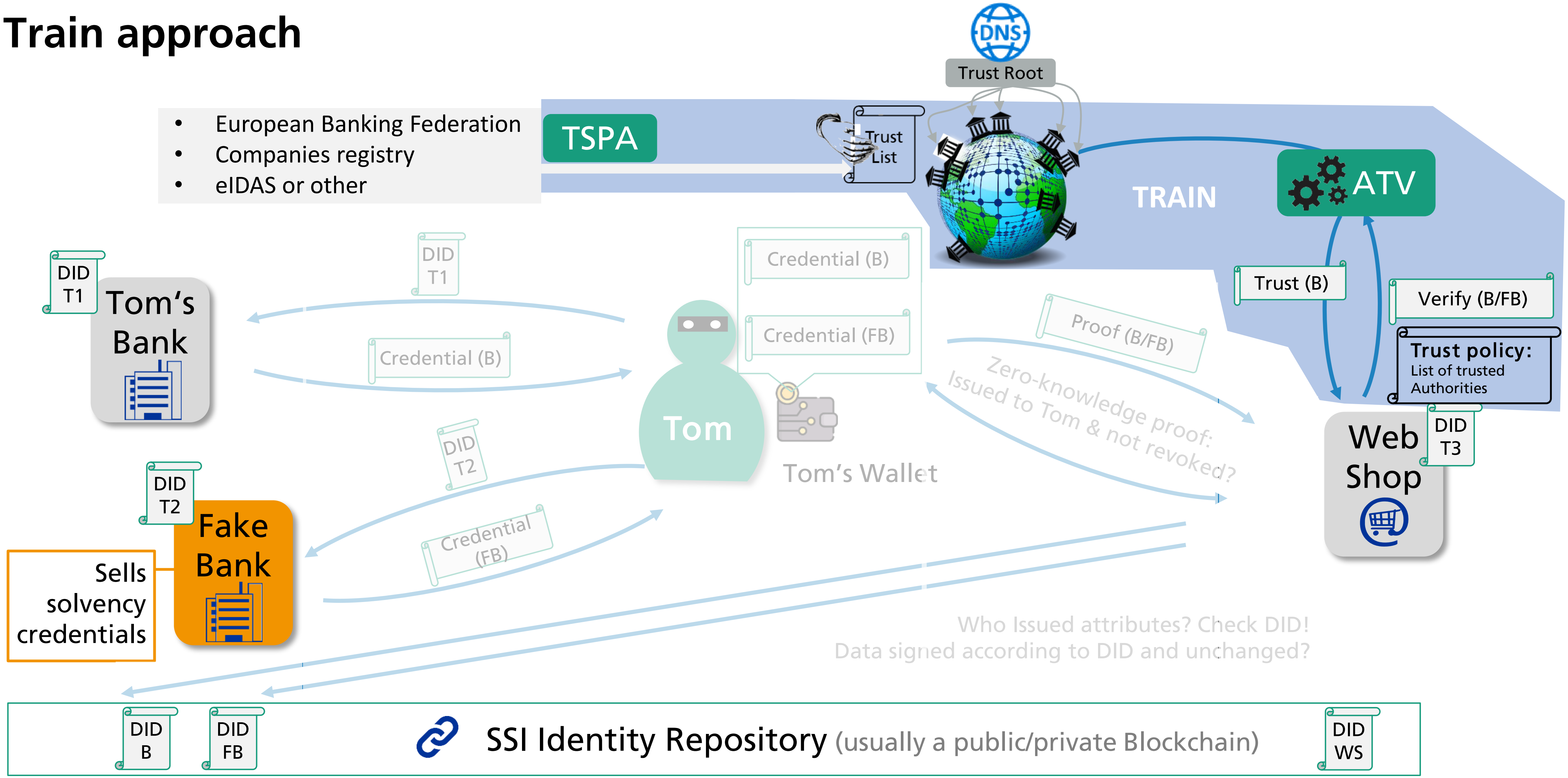
Aim of the Solution

1. Everyone can issue credentials, trust decision remains with the verifier
2. If needed, verifiers can decide to consider supporting institutions for trust decisions
3. Allow for automation through policies, trust schemes, LoAs etc.

TRAIN approach

- Automatic Trust Verifier (**ATV**) component facilitates verifier's trust decision based on policies
- Trust Scheme Publication Authorities (**TSPAs**) publishes trust schemes and trust lists (ETSI TS 119 612) of trusted authorities
- **DNS** (DNSSEC) as root of trust across domains

Train approach



- European Banking Federation
- Companies registry
- eIDAS or other

TSPA

Trust Root

Trust List

TRAIN

ATV

Trust (B)

Verify (B/FB)

Trust policy:
List of trusted Authorities

DID T1

Tom's Bank

DID T1

Credential (B)

Credential (B)

Credential (FB)

Tom

Tom's Wallet

DID T2

Fake Bank

Sells solvency credentials

DID T2

Credential (FB)

Proof (B/FB)

Zero-knowledge proof:
Issued to Tom & not revoked?

Web Shop

DID T3

Who Issued attributes? Check DID!
Data signed according to DID and unchanged?

DID B

DID FB

SSI Identity Repository (usually a public/private Blockchain)

DID WS

What TRAIN is – and is not:

TRAIN **does not** restrict anyone from issuing credentials

TRAIN **does not** impose or outsource trust decisions

TRAIN **does** enable **participating actors** to use a global, known and trusted infrastructure to:

- Publish and Retrieve trust relevant information e.g., on issuers of credentials
- Verify trust relevant information according to self-defined policies
- Determine trust assurance levels
- Make **autonomous** decisions

TRAIN **leverages** the existing global Domain Name System (DNS) and is based on the work of the H2020 project LIGHT^{est} (G.A. No. 700321).

Conclusion

- Trust requirements of verifiers not to be disregarded – as pivotal for adoption as end users’
- Trust verification goes beyond cryptography and needs to be scalable
- Hierarchical and “anarchic” approaches to trust management not convincing

TRAIN:

- Leverages an existing trust anchor (DNS)
- Enables creation, publication and discovery of trust schemes in multiple trust domains
- Decision remains with the verifier that is supported in his decision making

Challenges and next steps:

- Adoption of TRAIN by the SSI ecosystem that is developing fast
- Support verifiers formulating policies and enrolment of issuers

More info

ESSIF-TRAIN

https://gitlab.grnet.gr/essif-lab/infrastructure/fraunhofer/

NGI ESSIF-LAB

https://essif-lab.eu/essif-train-by-fraunhofer-gesellschaft/

<First name last name [et. al.]>(ed.): < book title>,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn <year> 1

Applying assurance levels when issuing and verifying credentials using Trust Frameworks

Victor Martinez Jurado[1], Xavier Vila[2], Michael Kubach[3], Isaac Henderson Johnson Jeyakumar[3], Albert Solana[2], Matteo Marangoni[1]

Abstract: Technical interoperability of the issuance, presentation, and verification of verifiable credentials (VC) across domains of trust is a current challenge for self-sovereign identity. We present an approach incorporating different levels of assurance and trust domains in an eIDAS compliant way. This is illustrated through a use case with real-world relevance: the issuance and cross-border usage of the European Health Insurance Card.

Keywords: eIDAS, self-sovereign identity, SSI, trust, trust frameworks, verifiable credentials

1 Introduction

When providing electronic services in a cross-border context, providers should have in place practices, policies, and other controls to provide assurance and evidence to the governor bodies of different trust schemes that effective practices are in place. The whole ecosystem benefits from this practice since consumers (holders, verifiers) can rely on the authorities and on the applied trust schemes to provide the needed assurance on the services consumed. The eIDAS regulation [Eu14] provides a such framework for determining the assurance levels of electronic identification schemes. However, eIDAS is focused on the EU, while many other domains of trust exist and even more could be defined. Hence, it would be advantageous if individuals or groups (industry organizations, NGOs, etc.) of verifiers could define for themselves their required trust standards and refer to self-defined trust schemes or schemes defined by other trustable entities besides the EU.

This paper describes the concept jointly developed by SICPA, Validated ID, and Fraunhofer in the EU NGI ESSIF Lab [ES21], demonstrating the issuance, presentation, and verification of verifiable credentials (VC), incorporating different domains of trust. Firstly, we demonstrate how we can leverage the SSI-eIDAS Bridge to provide legal confirmation of the identity of the issuer (using a Qualified Electronic Certificate) and a legal basis for attributing a VC to an issuer (by using electronic seals); and secondly, we propose the TRAIN approach as means to verify that an issuer was authoritative to issue a VC (by integration in a trust scheme infrastructure) so it can be trusted by the verifier. The use case chosen to illustrate this concept is the European Health Insurance Card.

[1] SICPA SA, Av. de Florissant 41, 1008 Prilly, Switzerland, firstname.lastname@sicpa.com
[2] Validated ID, C/ Aragó 179, 08011 Barcelona, Spain, firstname.lastname@validated.id
[3] Fraunhofer IAO, Nobelstr. 12, 70569 Stuttgart, Germany, firstname.lastname@iao.fraunhofer.de

Martinez Jurado et al. Applying assurance levels when issuing and verifying credentials using Trust Frameworks

➔ Illustrative use case and interop demo

Thanks for your attention!

Questions? Remarks? Get into contact!

Fraunhofer Institute for Industrial Engineering IAO

Team Identity Management

www.hci.iao.fraunhofer.de

Nobelstraße 12 | 70569 Stuttgart
Hardenbergstraße 20 | 10623 Berlin

Dr. Michael Kubach

+49 711 970-2428
michael.kubach@iao.fraunhofer.de

Dr. Heiko Roßnagel

+49 711 970-2145
heiko.rossnagel@iao.fraunhofer.de