

A glowing orange 'U' key is shown in a close-up, slightly angled view. The key is illuminated from within, creating a bright orange glow. It is set against a dark, blurred background of a computer keyboard.

The role of domain name systems in the context of self-sovereign identities

ID:SMART workshop 2024


Who we are

SSE - Secure Systems Engineering GmbH

SSE is a boutique consultancy for enterprise IT security. As passionate experts in research, engineering, defensive and offensive security, we provide comprehensive support for organizations and projects at any stage. Our specialized teams are dedicated to deliver actual benefit from acting as a fullscale security team closely integrated with development to testing businesses with the mindset of an attacker.


culture

 Clear statements

 Actionable results

 Tailored experience

people

 Handpicked experts

 Intrinsic development

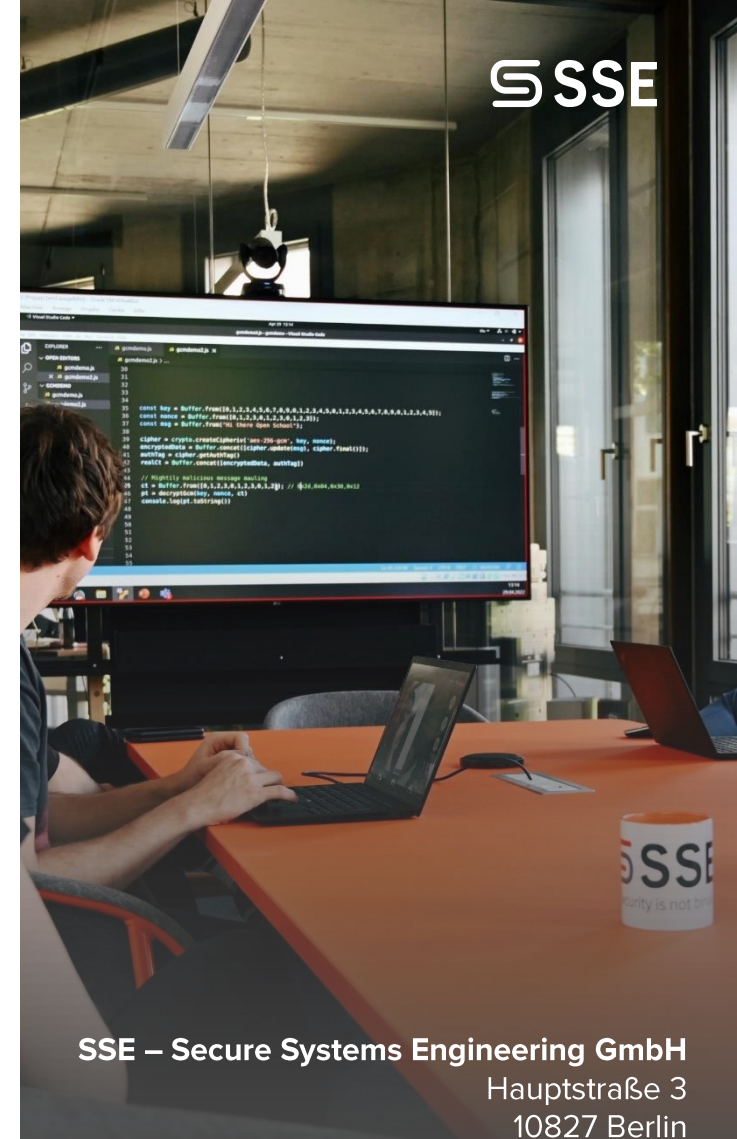
 Dedicated mindset



Build Resilience
Defensive Security

Challenge Resilience
Offensive Security

Train Resilience
Training & Awareness



SSE – Secure Systems Engineering GmbH
Hauptstraße 3
10827 Berlin

+49 30 2000 7892
office@securesystems.de

www.securesystems.de

To protect identities effectively, you need to differentiate

The path through the identity topic is not straightforward, but has junctions

Mapping the different aspects of an identity



Different views on the concept of identity

Psychological

The way in which **people perceive and understand themselves** because of their biographical development in constant interaction with their social environment

Philosophical

The sum of the characteristics acquired during life that form the **personality and character** of a person and make her or him unique within society.

Formal (e.g. governmental)

The sum of attributes that **uniquely identify** an entity (e.g. a person) **in a register** of entities. Mostly those attributes are supplemented by additional attributes assigned to this entity.



Security objectives related to identities

Example of new technologies (such as AI):

A person must not be discriminated against based on a self-perception or position in society that deviates from the social or mathematical norm.

Example of data protection: The characteristics of a person that define them and form their personality may not be unlawfully obtained, misused or published without authorization.

Example authentication: Entities may not illegally obtain the attributes of another entity in a register - in other words, they are not allowed to not impersonate someone else.



This is not a formally scientific and complete illustration and mapping. Rather, it is **intended to highlight the different aspects and challenges of the topic of identity.**



In this talk, we follow the path of identity in the sense of **identification, authentication and authorization**. In terms of security objectives, we are talking about the **protection of credentials**.

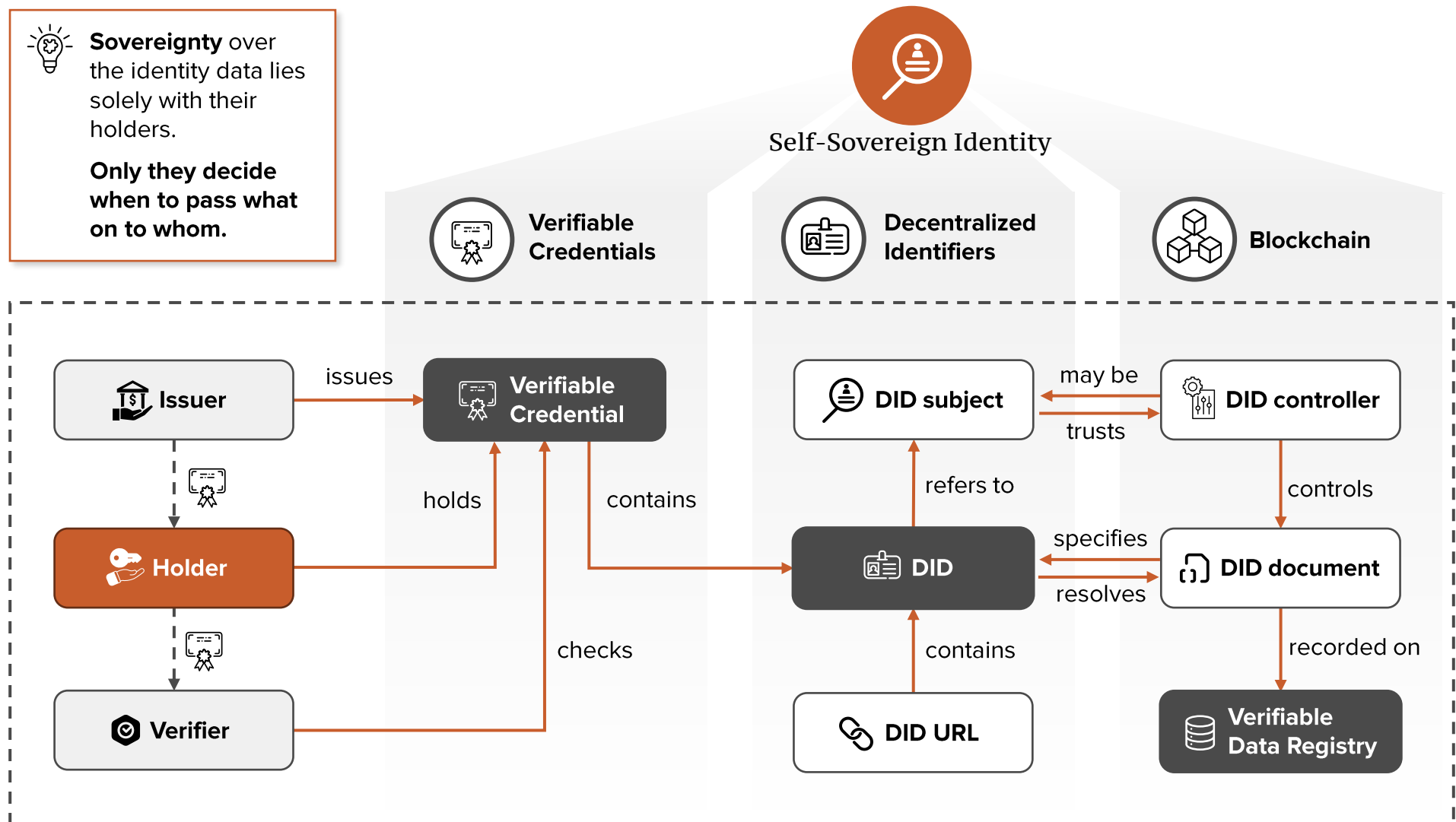
How to prove an identity claim in a self-sovereign manner

Overview of the ecosystem of sovereign identities



Sovereignty over the identity data lies solely with their holders.

Only they decide when to pass what on to whom.





See <https://www.dock.io/post/decentralized-identifiers>; w3.org/TR/did-core

The Trust Over IP foundation

The hourglass model of Trust over IP foundation is based on the layer model of the Internet

Summary of the Trust Over IP layer model

| |  Technology Stack | Governance Stack  |
|--|---|---|
| Layer 4 Definition of standards for Applications involved in a specific ecosystem | Application Ecosystems | Ecosystem Governance Frameworks |
| Layer 3 Definition of standards for elementary sovereign identification processes | Trust Task Protocols | Trust Task Governance Frameworks |
| Layer 2 Definition of security standards for wallets and the exchange of data between them | Peer-to-Peer Communication | Agent/Wallet Governance Frameworks |
| Layer 1 Definition of standards for decentralized identifiers (DID) in the ecosystem | Public Utilities | Utility Governance Frameworks |

See trustoverip.org/toip-model/

Trust Over IP (ToIP) foundation



Founded in 2020 by the Linux Foundation with the aim of creating a **standard for a decentralized digital trust infrastructure** on the Internet

- The core objective: Creation of a **decentralized** architecture for **self-sovereign** identities
- The ID ecosystem is organized in a **layered model** based on the Internet architecture
- Both **technical** and **governance** aspects are considered



The current version does not reveal strategies for cross-border use cases involving large numbers of issuers of different nationalities.

How Domain Name Systems (DNS) come into play

The community is working on solutions to address current gaps in the ToIP concept

❗ Issue 1

As a purely technical standard, the human factor is sometimes missing out. The identifiers used are difficult for people to evaluate and memorize.

👤 Example

Try to **memorize** or **evaluate** the following identity:

```
did:ethr:0x5:0xf9940e77102df898
561e44ff7b0d31538e7f96027f36b1a
7b2f051cddf322aec7f03e594adaaaf
565bbfd88344be6c6aec71831787e16
cc7f19815b7145b0c37b6b5ea4e9de4
afccb0fd738420e6a1cc
```

⚙️ Idea (Network Working Group et al)

Establishment of a translation mechanism from easy-to-remember but unique identifiers to technically readable decentralized identifiers (DID).

❗ Issue 2

The standard does currently not address sufficient use cases in which issuers and verifiers work together internationally.

👤 Examples

#1: The employer in Singapore wants to make sure that the digitally created **certificates** of the German applicant qualify her to be accepted for the job. There is **no database of issuers** of the respective certificates.

#2: Proof of age is required to attend a concert of an international star. Digital national ID cards, driving licenses, student or school ID cards can be used for this purpose. There is **no global archive of authorized issuers** in this set of possibilities that can be used here.

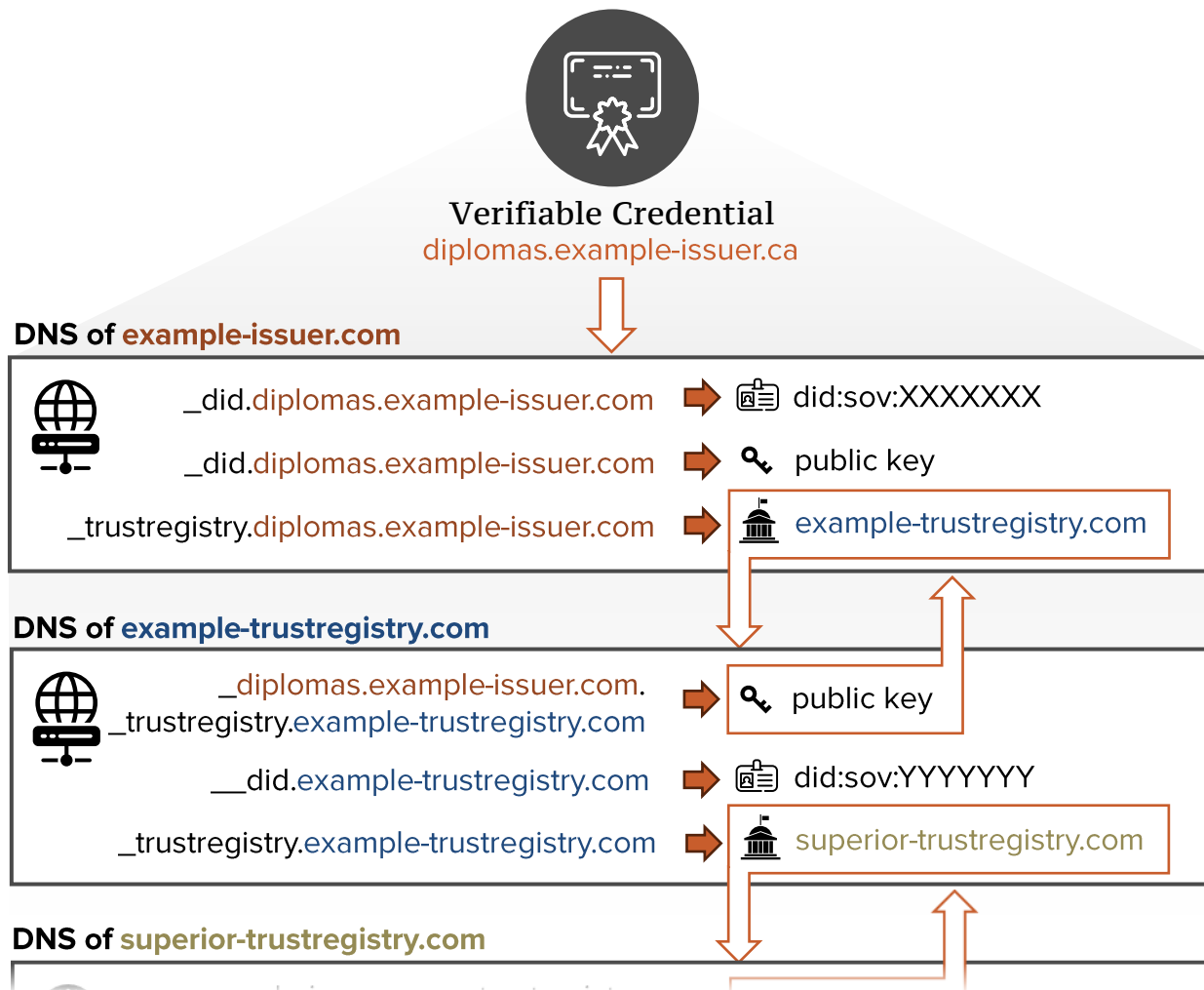
⚙️ Idea (Canadian Internet Registration Authority et al)

Provision of a trust registry to determine the authorization of individual issuers and to establish a global chain of trust.

How Domain Name Systems (DNS) come into play

Suggestions from the community to enhance identification processes by using DNS

DNS to DID and trust chain through Trust Registries



Domain Name System



Developed in 1980s for name resolution on the internet.
Today, thanks to DNSSEC, a **distributed key value store** with data integrity protection.

- Proposals for the use of DNS in the context of the ToIP initiative come from the **Network Working Group** and the **Canadian Internet Registration Authority (CIRA)**
- Translation** of technical and difficult-to-memorize DIDs into an understandable form (Domain or E-Mail)
- Provision of the public **key material** of DIDs
- Establishment of a **trust store** for the **authorization of issuers** and the creation of **chains of trust**

Conclusion

The subject of secure identification across borders is complex and has kept the community, companies and researchers busy for years

- There is no uniform understanding of what an identity is, which makes it difficult to protect it. It makes sense to focus on the protection of data and credentials in order to concretize the challenge.
- The Internet is probably the most complex global construct created by humans. It makes sense for the ToIP Foundation to use the structures created here to establish an architecture for cross-border identification
- With over 3 billion requests per day in the Cloudflare ecosystem alone, DNS is one of the most successful decentralized key-value stores, supported by nearly every device on the Internet down to IoT devices. The introduction of DNSSEC has added an important security feature to it. It therefore makes sense to discuss its potential role in the global identification challenge.

SSE – Secure Systems Engineering GmbH

Let's get in touch



Contact me

Daniel Augustin

Managing Director

daniel.augustin@securesystems.de

Hauptstraße 3
10827 Berlin

+49 (0)30 2000 7892
office@securesystems.de