# Who is to be identified?

## The importance of flexible identifiers in identity ecosystems.


Ben Biedermann

February 2023

# Contents

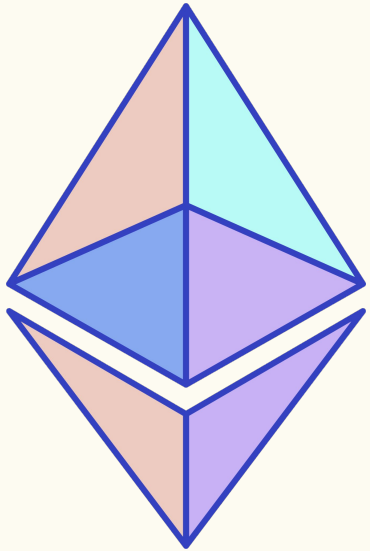
# Introduction

# Security and Sovereignty

- The use of sovereignty and security as characteristics of technical systems in the field of information and communication technology (ICT) is not self-explanatory. These terms are value-laden and deeply rooted in political theory. The reasons for thinking them together for ICT, thus, should be well defined and explained.

- Moreover, self-sovereign identity (SSI) claims to to provide individuals with secure and sovereign identities by using cryptographic algorithms and decentralised infrastructure (Preuschkat, A.; Reed, D., 2021).

# The driving forces behind SSI adoption



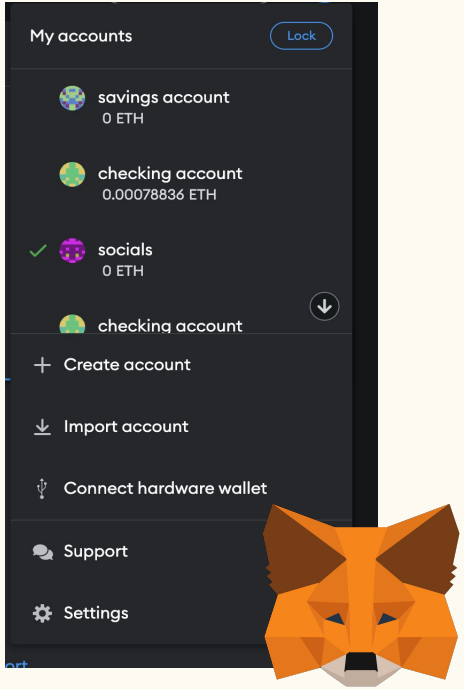
Web3

and

the state

# Origin Stories

# Web3 and where we came from



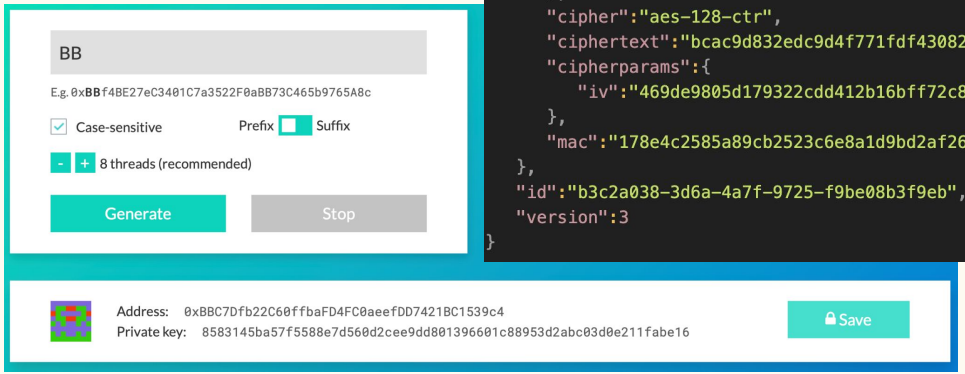

Metamask wallet application

- as Web3 or crypto wallet, Metamask is a predecessor of many SSI wallets
- EIP 4361: “Sign-In with Ethereum” introduces characteristics of identity wallets (Chang, 2021)
- modular key storage for many identifiers
- multiple accessible keys enable key rotation
- key deprecation is explicitly encouraged

# Persistent and transparent, but *modular* keys

*"A private key is made up of 64 hex characters and can be encrypted with a password. [...] The public key is generated from the private key using the Elliptic Curve Digital Signature Algorithm [1]. You get a public address for your account by taking the last 20 bytes of the Keccak-256 hash of the public key and adding 0x to the beginning". (Smith et al., 2023)*


```
{
  "address":"0xbbc7dfb22c60ffbafd4fc0aeefdd7421bc1539c4",
  "crypto":{
    "kdf":"pbkdf2",
    "kdfparams":{
      "c":262144,
      "dklen":32,
      "prf":"hmac-sha256",
      "salt":"ca3f1d3c3b2fc76dcf2f3c0c5007f570d3ba3ea34ad8778caa02600250cfeb22"
    },
    "cipher":"aes-128-ctr",
    "ciphertext":"bcac9d832edc9d4f771fdf430823b3cf3dc31b2bba1d38583a3c88014a21d64d",
    "cipherparams":{
      "iv":"469de9805d179322cdd412b16bff72c8"
    },
    "mac":"178e4c2585a89cb2523c6e8a1d9bd2af266693dfc3b1d1467bf203d2e7a50775"
  },
  "id":"b3c2a038-3d6a-4a7f-9725-f9be08b3f9eb",
  "version":3
}
```

# Wallets: a low-level means for device binding?

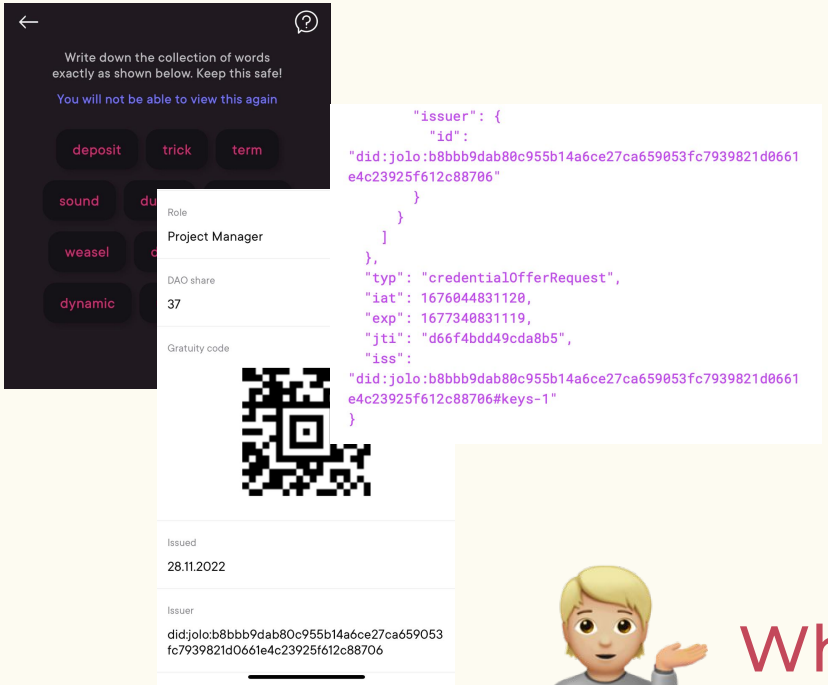
*"He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection"* (Foucault, 1995, pp.202).

## A NOTE ON WALLETS

An account is not a wallet. An account is the keypair for a user-owned Ethereum account. A wallet is an interface or application that lets you interact with your Ethereum account.

# Shaping Adoption

# Citizen wallets and where we are headed




- SSI wallets do not allow active and modular key management
- private or public keys are hidden
- Mnemonic backup is the closest one gets to see the key material
- public keys, or decentralised identifiers (DIDs) of issuers are still visible

## What about the user?

# Social technologies and governance

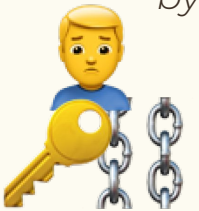
*Social technology transforms social expertise for a purpose, develops ideas for the solutions for social problems. Thus, it also establishes itself as a part of modern government[.]*

*[T]he switch to contemporary social technology [, however,] takes a step towards [...] the market [to] allow governing via networks and also for self-determination of the individual, who has to act as an active responsible citizen.* (Leibetseder, 2011 , pp. 14)

# DIDs, modularity and persistent identifiers

*"Our solution models subjects of identities as "Holders" in possession of trustable, claim-based digital identities. Holders are provided persistent virtual ownership over the "root" of their identity in the form of local private key generation and storage. Jolocom users maintain exclusive control of their private keys by default."* (Jolocom, 2019, p. 11)

*"The Jolocom framework [...] stores DIDs on the public permissionless Ethereum blockchain. DID documents (DDO) describe how to use a specifc [sic!] DID and may contain additional attributes. By default, DDOs are stored on the IPFS. Credentials are under the entire control of the user. Jolocom allows for the generation of child DIDs that can hide that credentials concern the same person."* (Kondova, 2020, p. 343)



Claims by the industry versus research findings

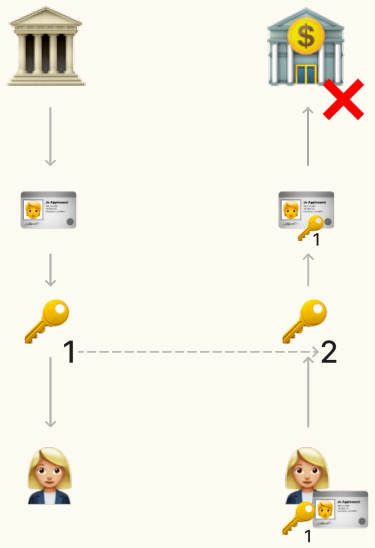
# Keeping Promises

# Privacy, anonymity, and the right to be forgotten

*"By privacy,* I understand the condition in which other people are deprived of access to either some information about you or some experience of you.

For the sake of economy, I will shorten this and say that *privacy is the condition in which others are deprived of access to you."* (Reiman, 1995, p.30)

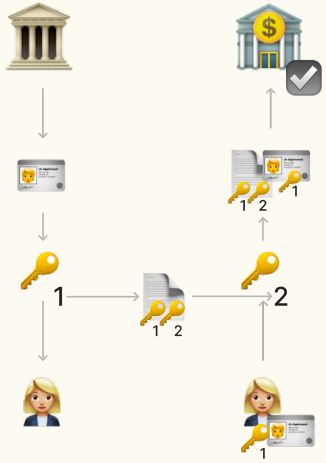
# Minimally modular did:key implementations




local only and pairwise identifiers

- This implementation has similarities to the wallet architecture of Metamask.
- It allows users to manage multiple identifiers.
- Identities for one identifier cannot be migrated to another key.
- Users have a high risk of being correlated by issuers and verifiers.

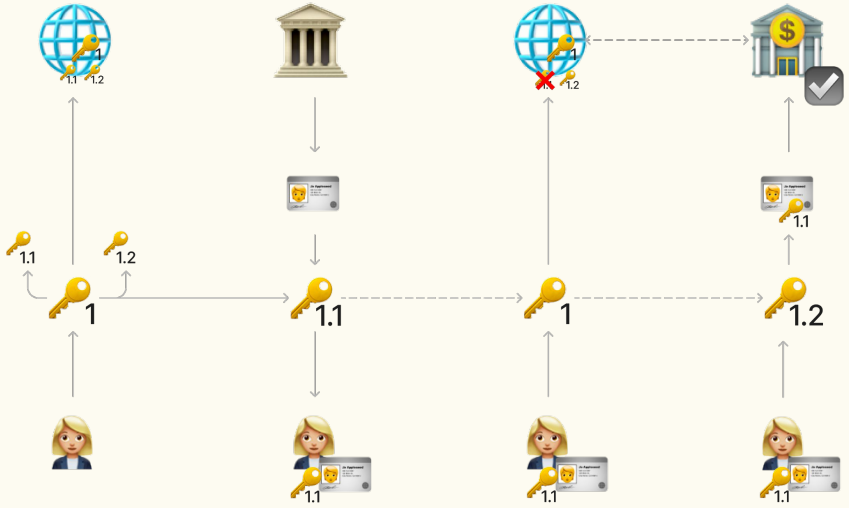
# KERI flavoured key rotation with did:key




local only and pairwise identifiers with key event log

- Loosely adheres to the principles of did:keri, and features a key event log (KEL) (Smith, 2019).
- The KELs comply out of the box with the verifiable credential data model v.1 (W3C, 2022)
- a lightweight implementation for key rotation
- correlation risks remain unaddressed
- allow salted hash claim-blinding

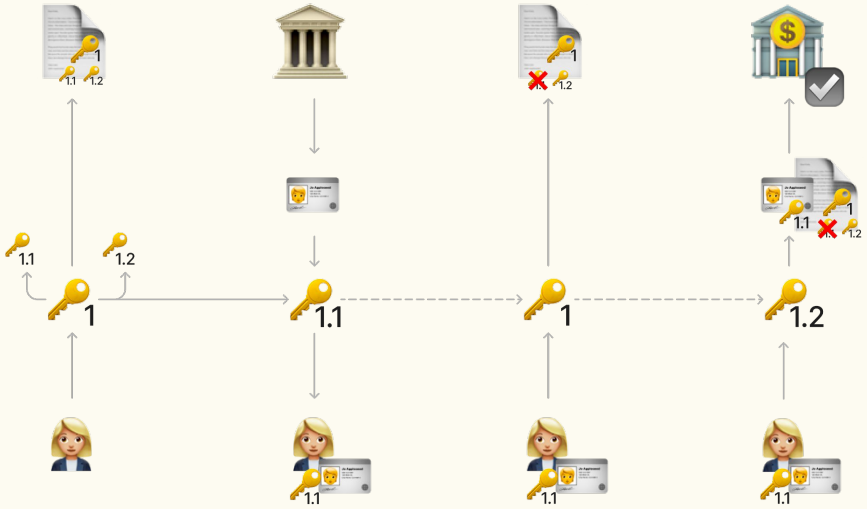
# DID:KERI with witnesses




globally resolvable and anywise identifiers with key event log

- did:keri uses witnesses as substitutes for known distributed ledgers
- Introduced by Smith (2019), KELs enable key rotation and function as self-addressing identifiers.
- This example uses a hash of the KEL as identifier (read DID) and requires a DDO.
- Derived keys can reduce the frequency of rotating keys.

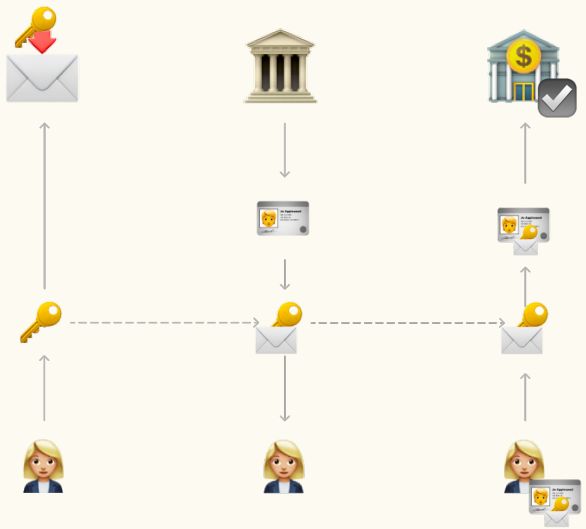
# DID:KERI without witnesses or VDRs for




locally resolvable and anywise identifiers with key event log

- KELs can be self-addressing DIDs without the need for DDOs.
- The infrastructure can neglect verifiable data registries (VDRs).
- Identifiers are any-wise and correlation risks remain.
- Derived keys can reduce the frequency of rotating keys.

# Anonymous Credentials (AnonCreds)



local only and pairwise identifiers with blinded key commitments

- AnonCreds use non-interactive zero-knowledge proofs (ZKPs)
- blinded Pedersen key commitments make identities non-correlatable (Zundel, 2021)
- BLS 12-318 curves could upgrade did:methods to compete (Looker et al., 2023)
- AnonCreds are not a did:method, but allow the DID to be a single use identifier
- Modular wallets with persistent identifiers then only appeal to non-human holders

# Conclusions

# General requirements for DID:Methods

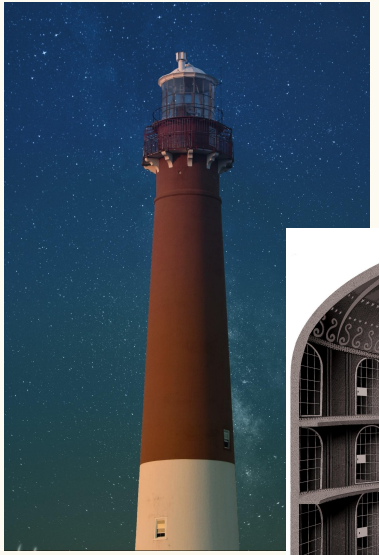
- We expect issuers and verifiers to require did:methods to be
  - globally resolvable,
  - are comprised of long-lived identifiers, which are,
  - updateable, with the possibility for key rotation, which are,
  - potentially anchored on use case-specific VDRs, e.g. distributed databases.

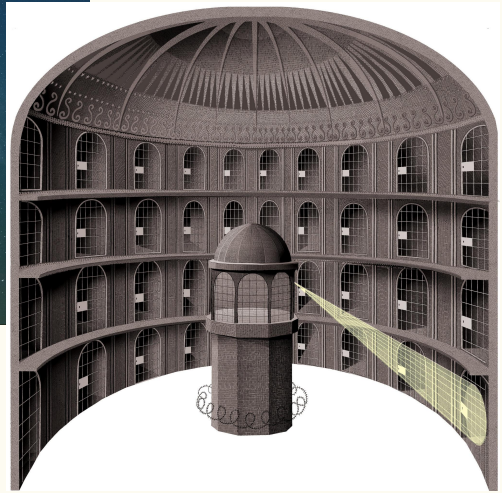
- We anticipate holders to require privacy preserving and pair-wise identifiers.
  - Such identifiers should be short-lived, as well as,
  - quick and cheap to create.

- Yet, requirements by credential-holding legal entities will differ from those by holders, who are natural persons.

- All did:methods used within the EU/ EEA must comply with GDPR.

# The contextuality of technology





The ethically acceptable use of technology is contextual of its societal framework. No did:method or credential standard is *a priori* harmful.

Yet, the direction of SSI risks subjecting individuals under insurmountable responsibility guised by sovereignty and security.

Projects like SDIKA then must built Lighthouses instead of Panoptica.

# References


- Chang, Wayne et al. (2021). ERC-4361: Sign-In with Ethereum. Off-chain authentication for Ethereum accounts to establish sessions. Last accessed: 2023-02-10.
- Chelsea College of Arts. (2015). The Bricklayer and the Artist. Panopticon. https://www.pangaeasculptorscentre.com/wordpress2016/wp-content/uploads/2015/06/01-The-Bricklayer-and-the-Artist-panopticon2-1024x1013.jpg. Last accessed: 2023-02-10.
- Foucault, Michel. (1977). Überwachen und Strafen. Die Geburt des Gefängnisses. Übersetzt von Walter Seitter. Frankfurt: Suhrkamp.
- Jolocom. (2019). A Decentralized, Open Source Solution for Digital Identity and Access Management. Whitepaper. Version 2.1. https://jolocom.io/wp-content/uploads/2019/12/Jolocom-Whitepaper-v2.1-A-Decentralized-Open-Source-Solution-for-Digital-Identity-and-Access-Management.pdf. Last accessed: 2023-02-10.
- Kondova, Galia; Erbgut, Jörn. (2020). Self-Sovereign Identity on Public Blockchains and the GDPR. SAC '20: Proceedings of the 35th Annual ACM Symposium on Applied Computing. March 2020. Pages 342–345. https://doi.org/10.1145/3341105.3374066.
- Leibetseder, Bettina. (2011). A critical review on the concept of sociotechnology. Socialines Technologijos. Vol. 1, Iss. 1. Vilnius.
- Kubiak, Boris. (2023). Vanity-Eth. ETH vanity address generator.https://vanity-eth.tk/. Last accessed: 2023-02-10.
- Longley, Dave et al. (2022). The did:key Method v0.7. Draft. A DID Method for Static Cryptographic Keys. Decentralised Identity Foundation (DIF).https://w3c-ccg.github.io/did-method-key/. Last accessed: 2023-02-10.
- Looker, T. et al. (2023). The BBS Signature Scheme. Decentralized Identity Foundation (DIF). CFRG Working Group. https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html#name-terminology. Last accessed: 2023-02-10.
- MetaMask. (2018). Brand Resources. https://github.com/MetaMask/brand-resources. Last accessed: 2023-02-10.
- MetaMask. (2023). A ConsenSys Formation. URL: https://metamask.io/about/. Last accessed: 2023-02-10.
- Preuschkat, A.; Reed, D. (2021). Self-Sovereign Identity. Decentralized Digital Identity and Verifiable Credentials. A. Preuschkat & D. Reed (eds.) Ed. 1. p.. 3–20. Manning.
- Pedersen, Torben Pryds. (1998). Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. Springer.
- Ethereum Foundation. (2023). Brand Assets. https://ethereum.org/en/assets/#brand.
- Reiman, Jeffrey H. (1995). Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future. Santa Clara High Technology Law Journal. Volume 11. Issue 1. http://digitalcommons.law.scu.edu/chtlj/vol11/iss1/5.
- Smith, Corwin et al. (2023): Ethereum accounts. Ethereum Foundation. https://ethereum.org/en/developers/docs/accounts/#account-creation. Last accessed: 2023-02-10.
- Smith, S. M. (2019). Key Event Receipt Infrastructure (KERI). arXiv. https://doi.org/10.48550/ARXIV.1907.02143
- Tailor, Troy. (2017). Brown and white lighthouse. https://unsplash.com/photos/P2LXO25eUsk. Last accessed: 2023-02-10.
- World Wide Web Consortium (W3C). (2022). Verifiable Credentials Data Model v1.1. https://www.w3.org/TR/vc-data-model/
- Zundel, Brent. (2021). How Does a Verifier Know the Credential is Yours?. Evernym. https://www.evernym.com/blog/how-does-a-verifier-know-the-credential-is-yours/. Last accessed: 2023-02-10.

JOLOCOM

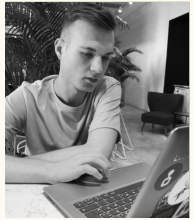
sdika
Schaufenster Sichere Digitale Identitäten Karlsruhe

Supported by:

Federal Ministry
for Economic Affairs
and Climate Action

on the basis of a decision
by the German Bundestag

BEN BIEDERMANN



Project Manager

ben@jolocom.com

t.me/benedictiner