

# BBS Basics

Joel Robles & Miguel Schweizer

19.10.2023

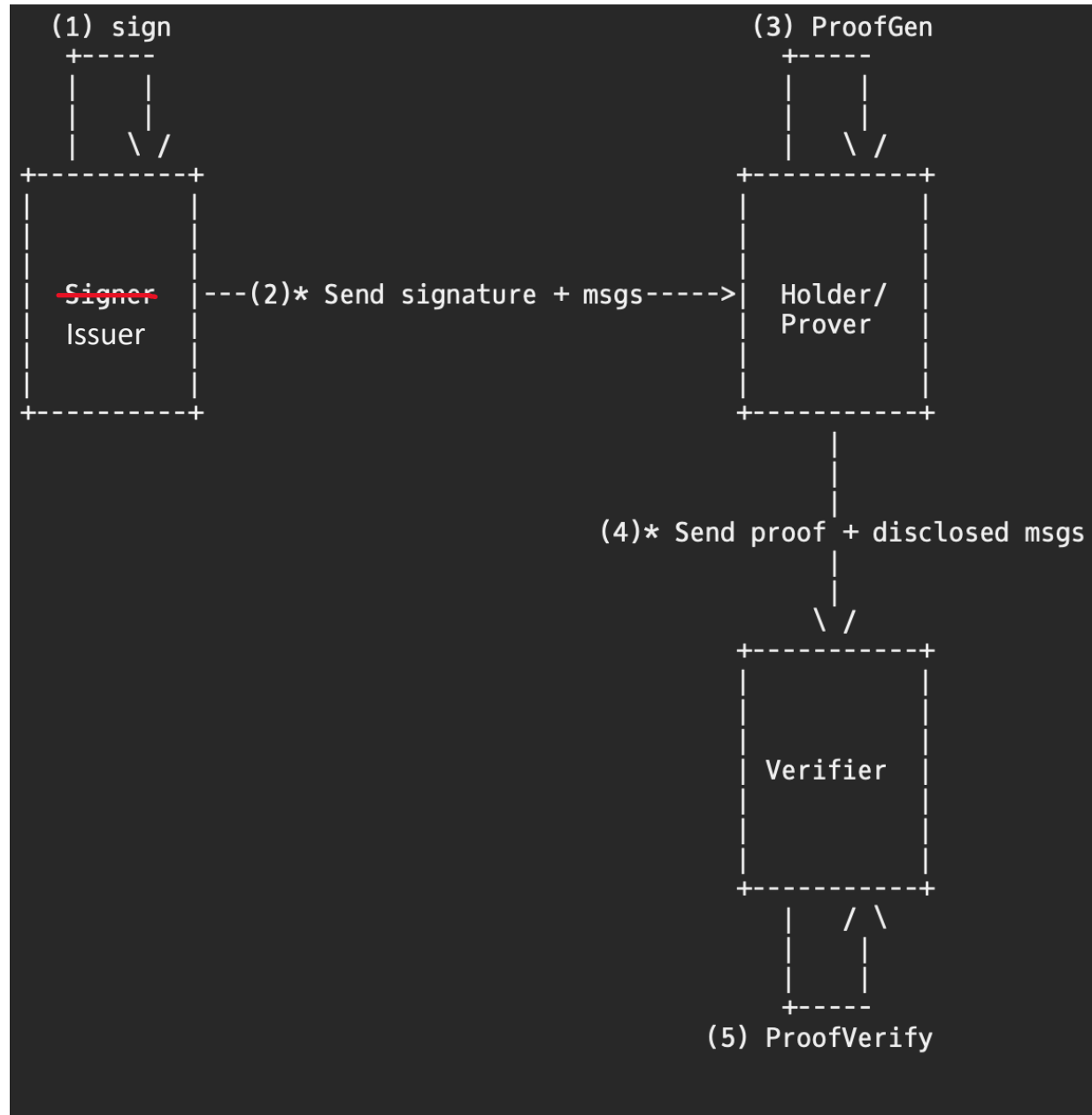
Project 2

BFH TI



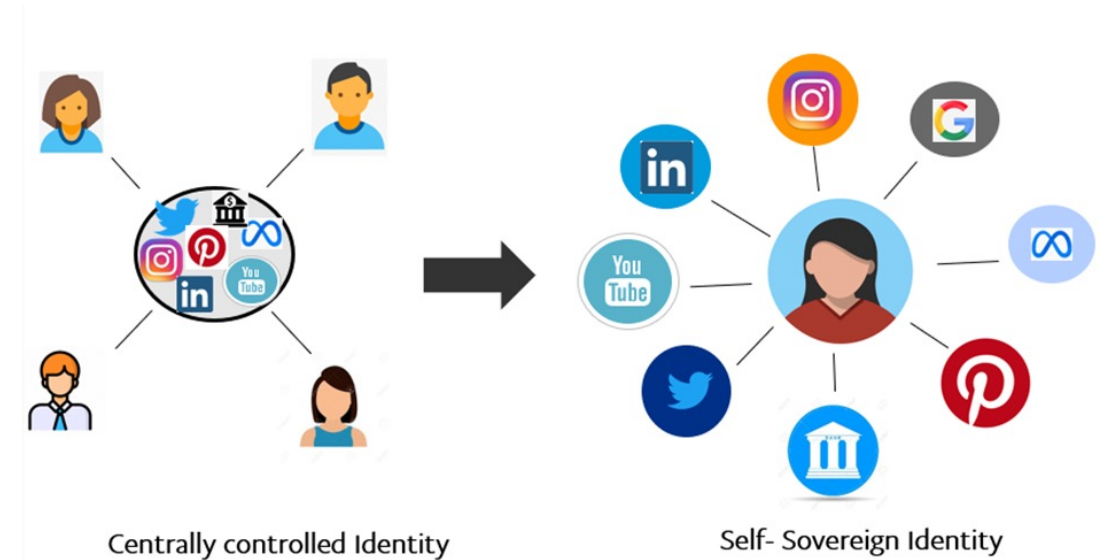
# BBS or BBS+?


- BBS was first introduced in 2004 by Boneh, Boyen, and Shacham
- Cast as standalone in 2004 by Camenisch and Lysyanskaya
- In 2006 BBS+ was introduced, which was provably secure  
Is in the process of standardization
- In 2023 Tessaro and Zhu showed that BBS is secure, BBS+ is 💀



# Self-Sovereign Identity (SSI)

- SSI is a model
- Manages digital Identities
- Individuals or cooperations have complete ownership

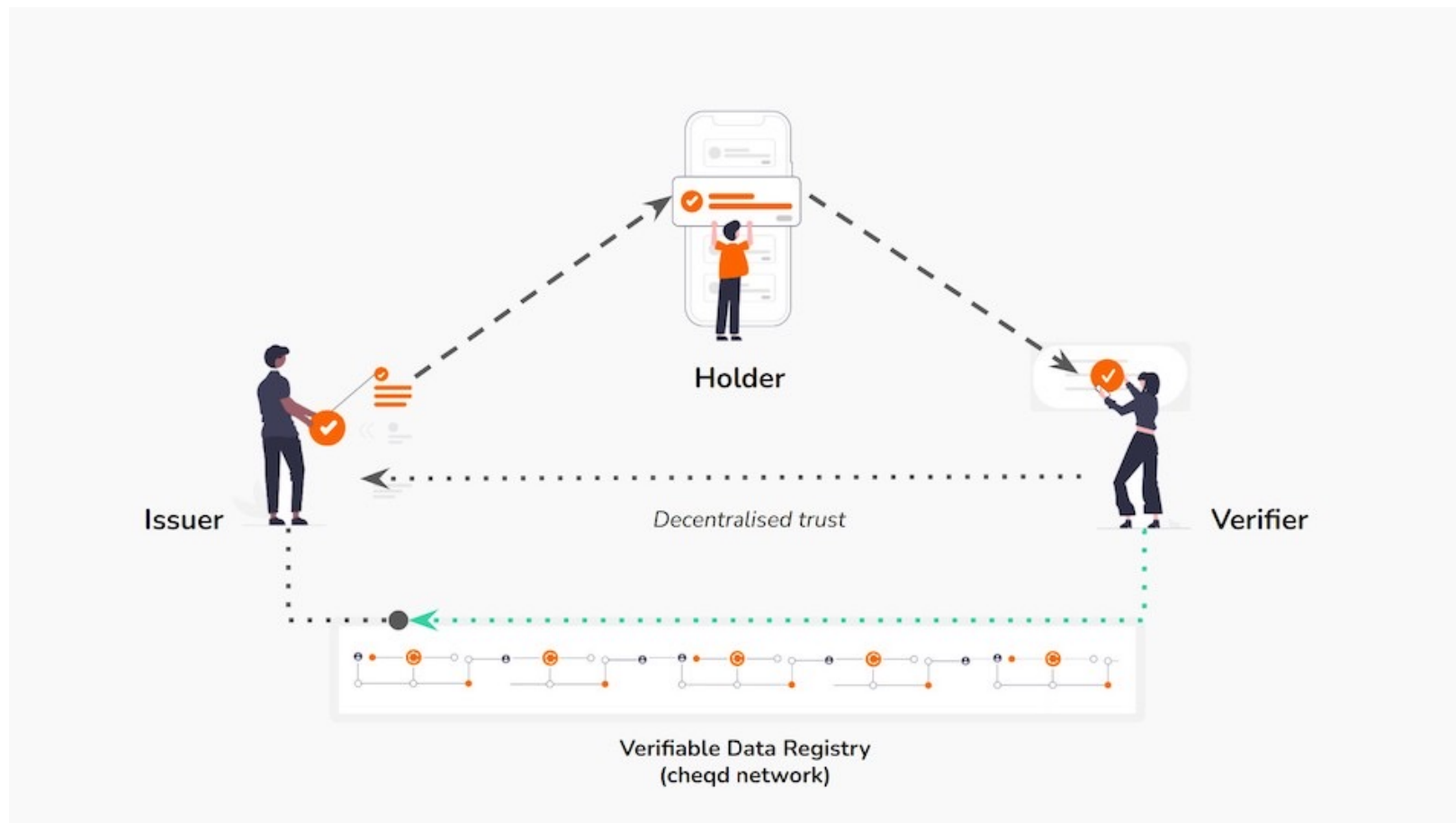




# Verifiable Credentials (VCs)

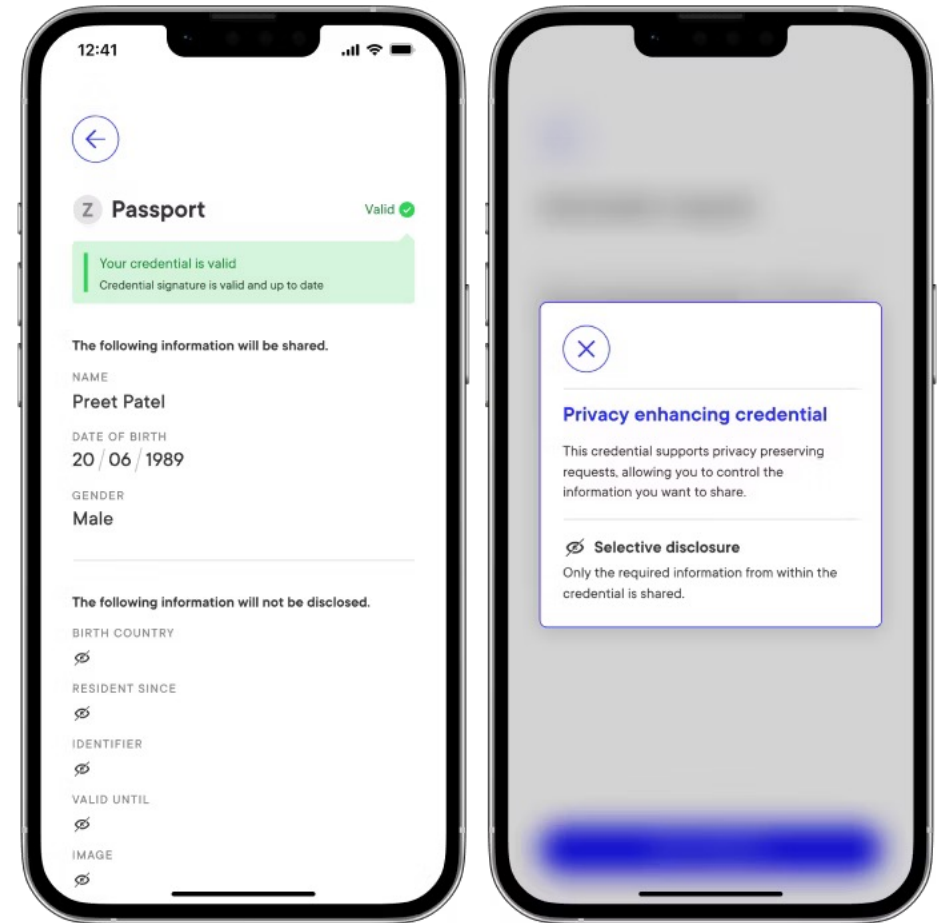
- W3C standard
- Digital cryptographically verifiable credentials
- Stored on digital devices

# Trust Triangle



# Selective Disclosure

- Holder chooses what to disclose
- Disclosing messages reveals no information about undisclosed messages



# Unlikable proofs

- Generated proofs cannot be linked
- Verifier cannot determine signature
- Proofs guarantee the integrity and authenticity





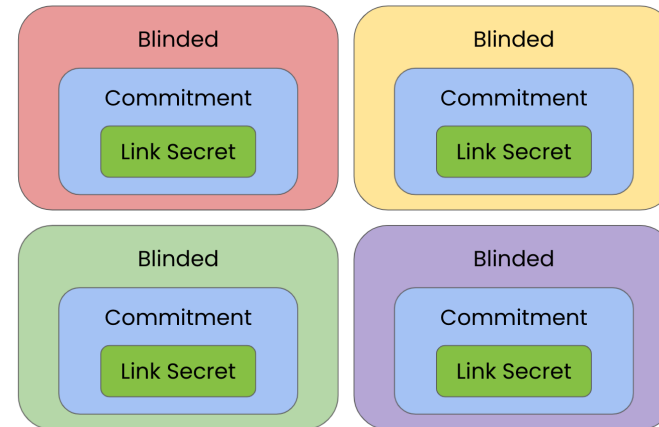
# Zero-knowledge Proof (ZKP)

- Lower version of proof-of-knowledge
- Attributes:
  - completeness
  - soundness
  - zero-knowledge



# Link Secrets

- Is a random number
- Wrapped with a commitment
- Can be blinded



# Link Secrets in BBS

- Proofs possession
- Can be used to link VCs

