Web 3.0

The trusted web

What we'll discuss

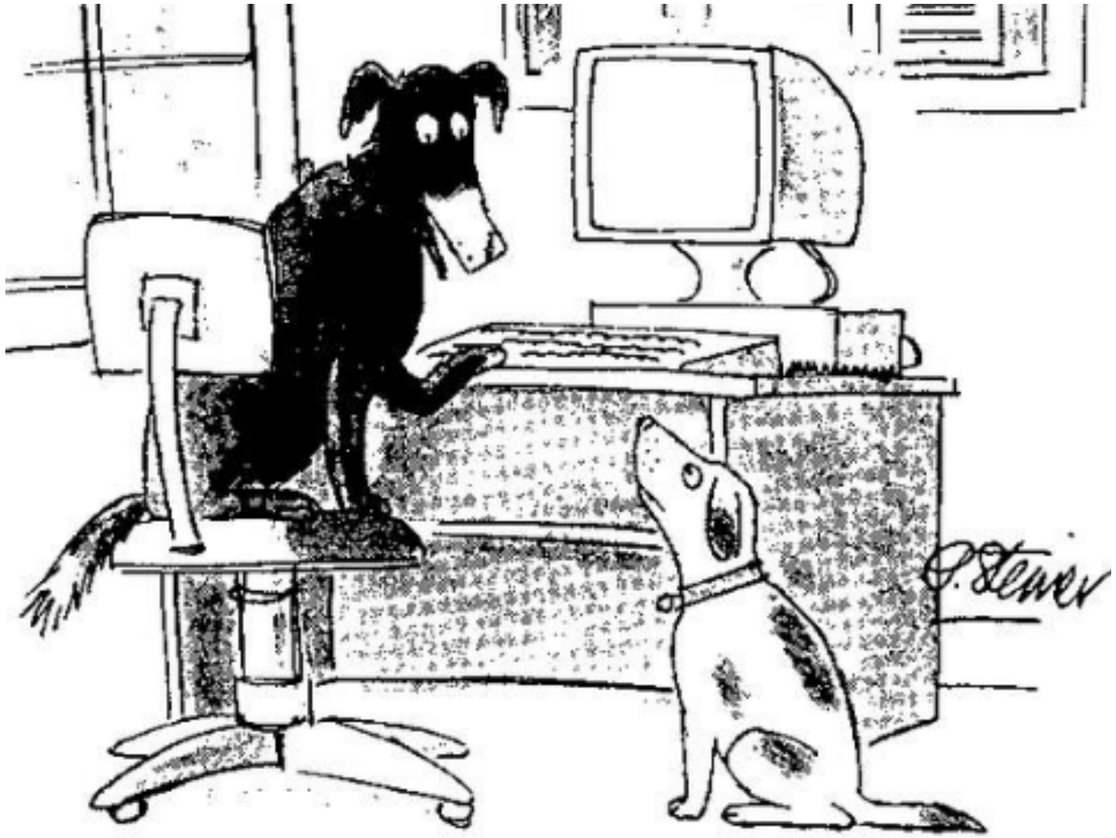
Index

- What is trust?
- A brief history of digital identity
- The problems with centralized digital identity management models
- Self-sovereign identity
  - Principles
  - Decentralized identifiers (DIDs)
  - Verifiable credentials (VCs)
  - Selective disclosure
  - Zero-knowledge proofs
- Relevant questions for the final presentation

What is trust?

On the internet

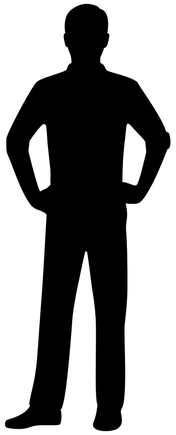
You don’t know who you’re dealing with



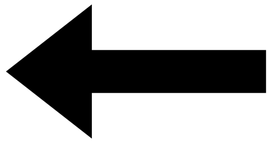
"On the Internet, nobody knows you're a dog."

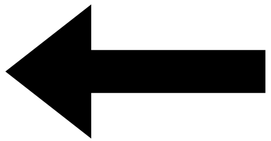
How do we know someone is who they say they are?

Trust in the physical world

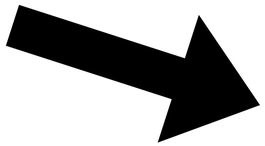


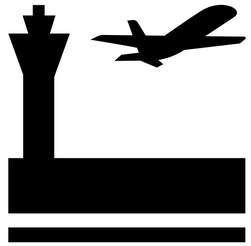
You





Government

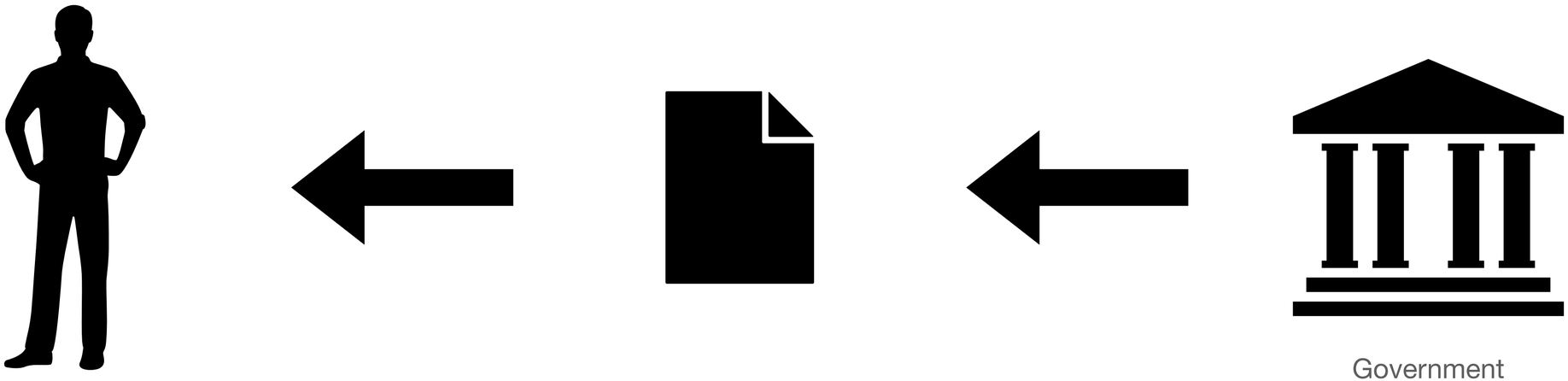




Customs

Security features

Trust in the digital world



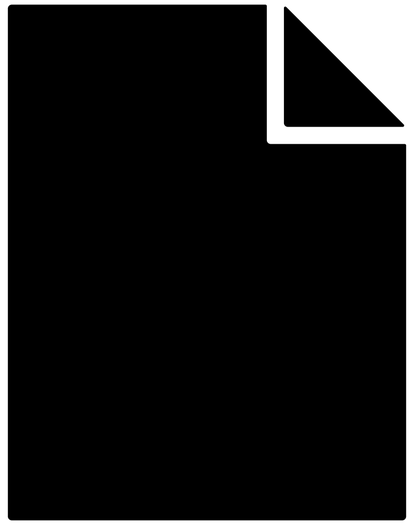
You

Government

Customs

Security features

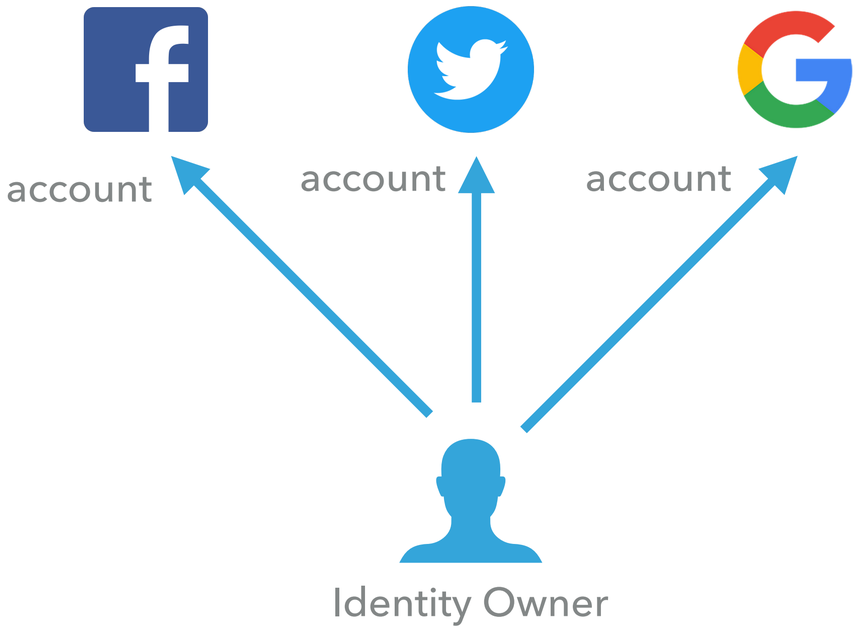
Well… No



A brief history of digital identity

The siloed model

- An organization issues to you (or allows you to create) a digital identity that you can use to access its services.
- Trust between you and the organization is typically created through the use of ‘shared secrets’ (passwords, pins, biometrics).
- The organization stores at least some of your personal data in its data ‘silo’.
- Credentials are created and managed separately for every relationship you have.



The siloed model - pros and cons

PROS

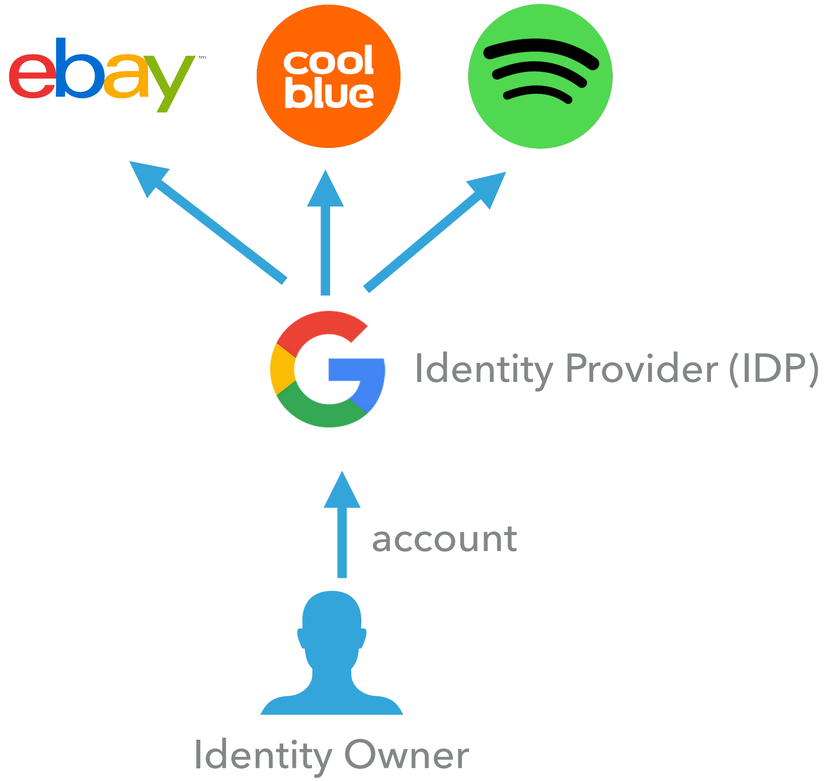
- Widely established
- Well known
- Straightforward to use
- Established a pairwise unique credential for each relationship

CONS

- It forces users to manage and maintain dozens or even hundreds of credentials, one for each app, service or relationship.
- Authentication is:
  - One-way (open to phishing) rather than mutual
  - Session-based rather than persistent
  - It requires organizations to store personal information about its users, thus requiring them to become somewhat of an identity and security expert.

The federated model

- A third-party organization acts as an Identity Provider (IDP) between you and the organization or service you are trying to access, providing a **single sign-on** experience.
- Trust between you and the IDP is maintained through shared secrets (same as the siloed model).
- Federates the login through protocols such as OAuth, SAML and OpenID Connect.



The federated model - pros and cons

PROS

- Enables users to access many applications and services using a single credential.
- Simplifies authentication
- Reduces usernames and passwords

CONS

- A third party is now in the middle of every interaction, saying “Trust me”.
- The value of the shared secrets has increased, since it is now used for many applications and services (making it more interesting to hackers).
- The IDP becomes a large trove of personal information (again, making it more interesting to hackers).
- As with the siloed model, authentication is:
  - One-way (open to phishing) rather than mutual
  - Session-based rather than persistent

Other problems with centralized identity

An introduction to self-sovereign identity

Self-sovereign identity

“Self-sovereign identity (SSI) is a term used to describe the digital movement that recognises an individual should own and control their identity without the intervening administrative authorities.”

Sovrin Foundation

The 10 guiding principles by Christopher allen

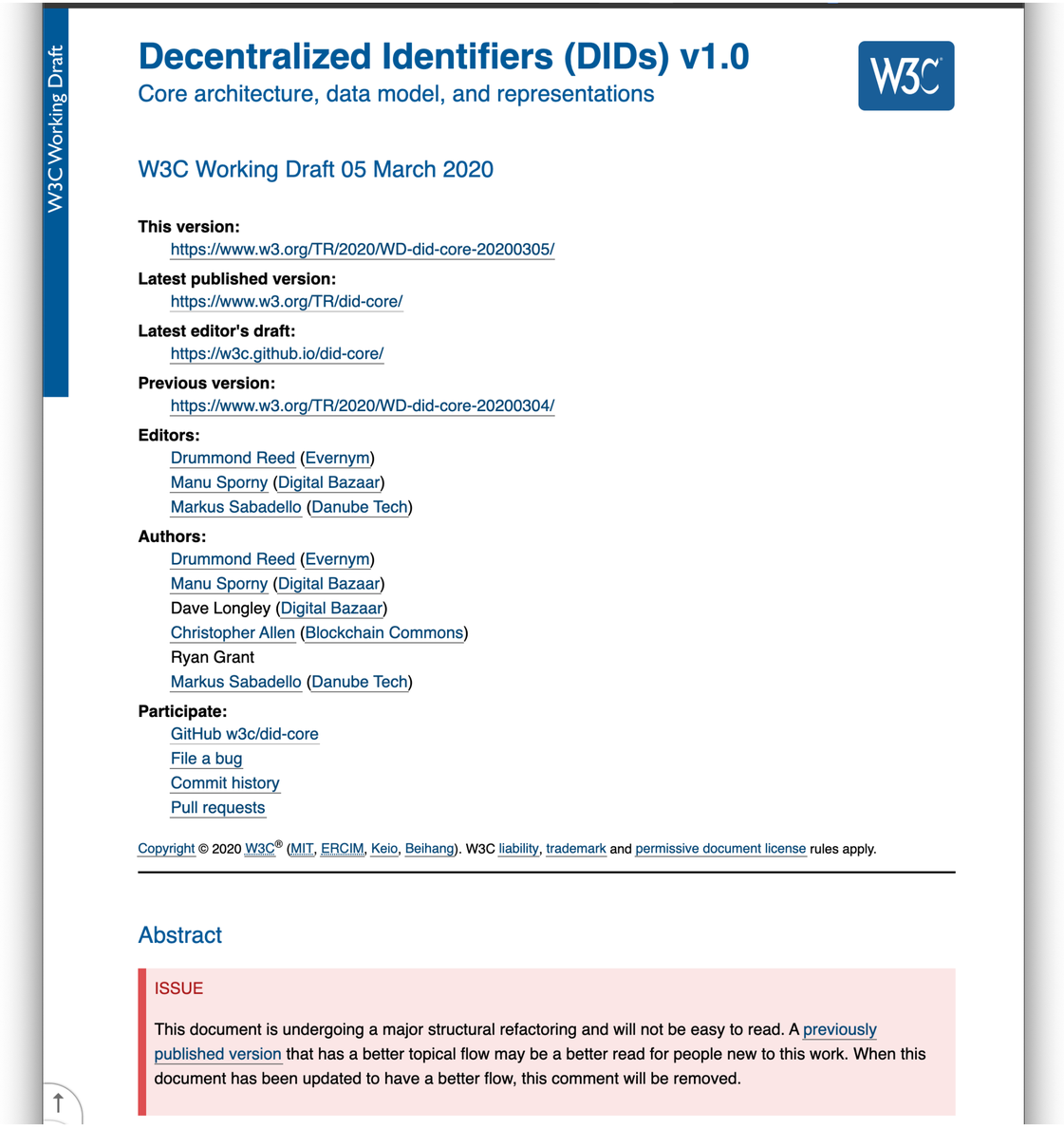
- **Existence** — *Users must have an independent existence.*
- **Control** — *Users must control their identities.*
- **Access** — *Users must have access to their own data.*
- **Transparency** — *Systems and algorithms must be transparent.*
- **Persistence** — *Identities must be long-lived.*
- **Portability** — *Information and services about identity must be transportable.*
- **Interoperability** — *Identities should be as widely usable as possible.*
- **Consent** — *Users must agree to the use of their identity.*
- **Minimisation** — *Disclosure of claims must be minimised.*
- **Protection** — *The rights of users must be protected.*

Self-sovereign identity…

- Is a philosophy rather than a technology.
- Lets the individual control their identity.
- Cuts out the middle man (the identity provider or IDP)

W3C standards - decentralized identifiers

“A globally unique identifier that does not require a centralized registration authority because it is registered with distributed ledger technology or other form of decentralized network.”



W3C Working Draft

Decentralized Identifiers (DIDs) v1.0

Core architecture, data model, and representations

W3C Working Draft 05 March 2020

This version:
https://www.w3.org/TR/2020/WD-did-core-20200305/

Latest published version:
https://www.w3.org/TR/did-core/

Latest editor's draft:
https://w3c.github.io/did-core/

Previous version:
https://www.w3.org/TR/2020/WD-did-core-20200304/

Editors:
Drummond Reed (Evernym)
Manu Sporny (Digital Bazaar)
Markus Sabadello (Danube Tech)

Authors:
Drummond Reed (Evernym)
Manu Sporny (Digital Bazaar)
Dave Longley (Digital Bazaar)
Christopher Allen (Blockchain Commons)
Ryan Grant
Markus Sabadello (Danube Tech)

Participate:
GitHub w3c/did-core
File a bug
Commit history
Pull requests

Abstract

ISSUE

This document is undergoing a major structural refactoring and will not be easy to read. A previously published version that has a better topical flow may be a better read for people new to this work. When this document has been updated to have a better flow, this comment will be removed.

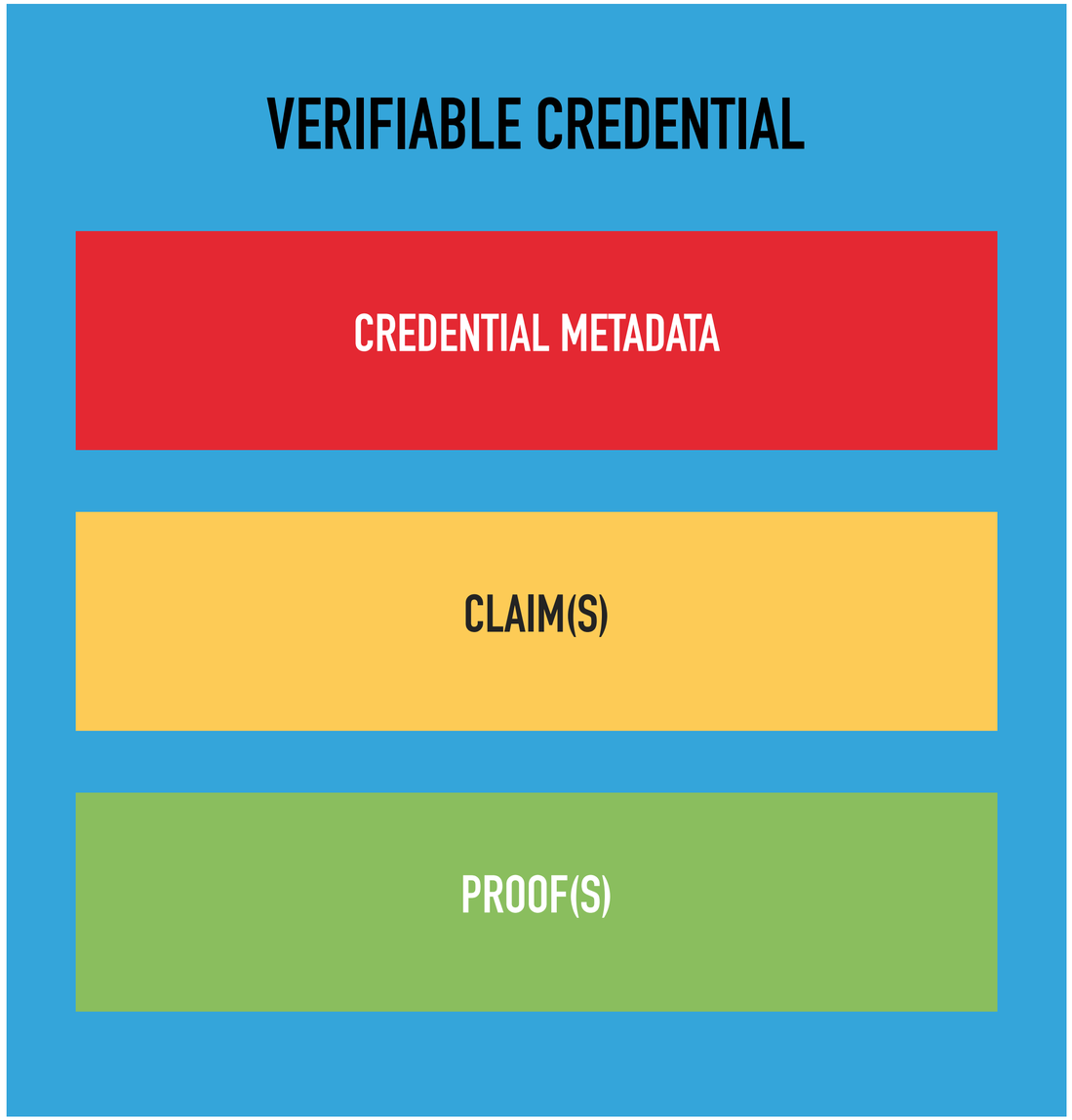
Decentralized Identifiers

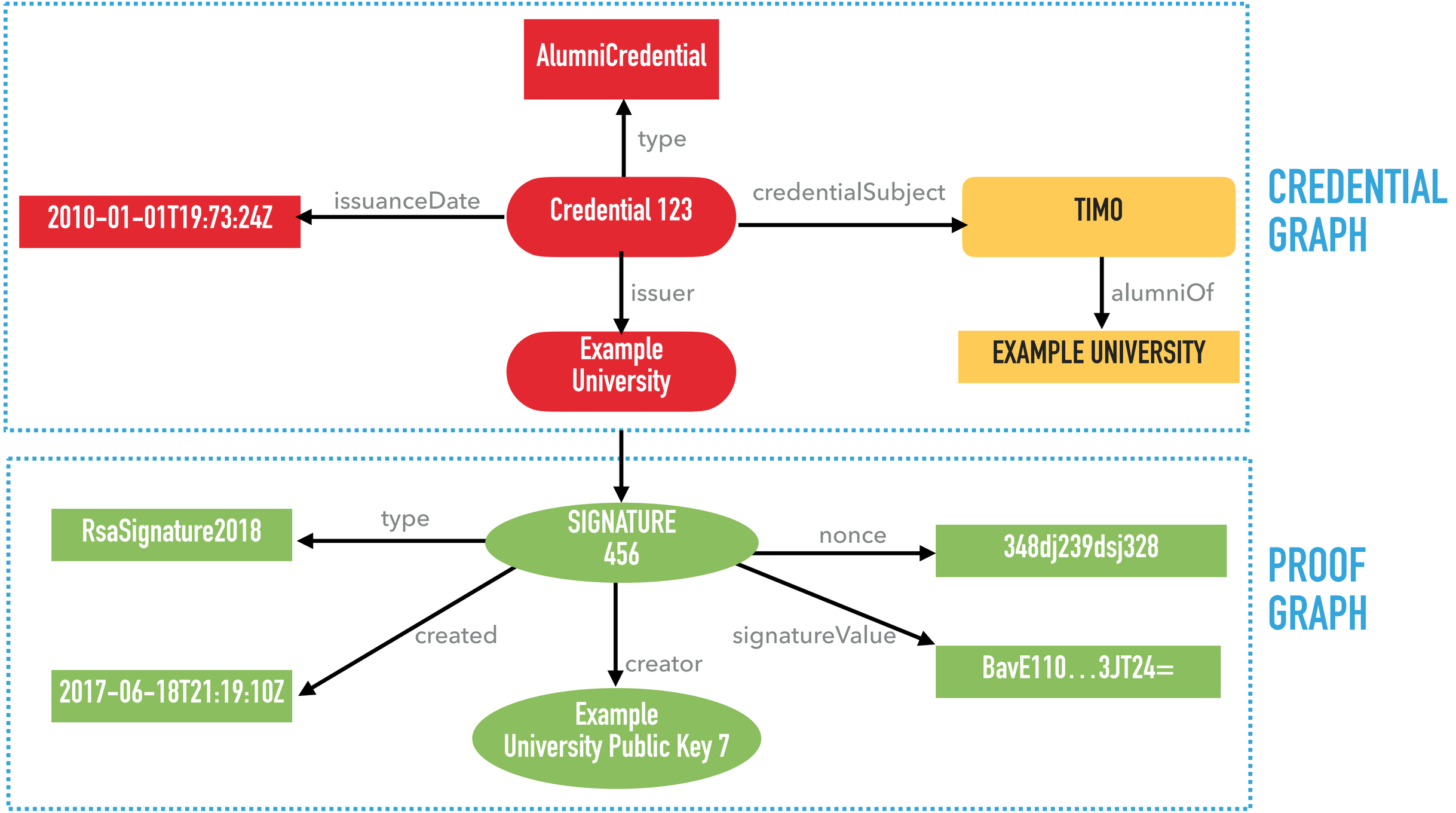
- A DID is a simple text string consisting of three parts:
  - The URL scheme identifier (did)
  - The identifier for the DID method
  - The DID method-specific identifier

did:example:123456789abcdefghi

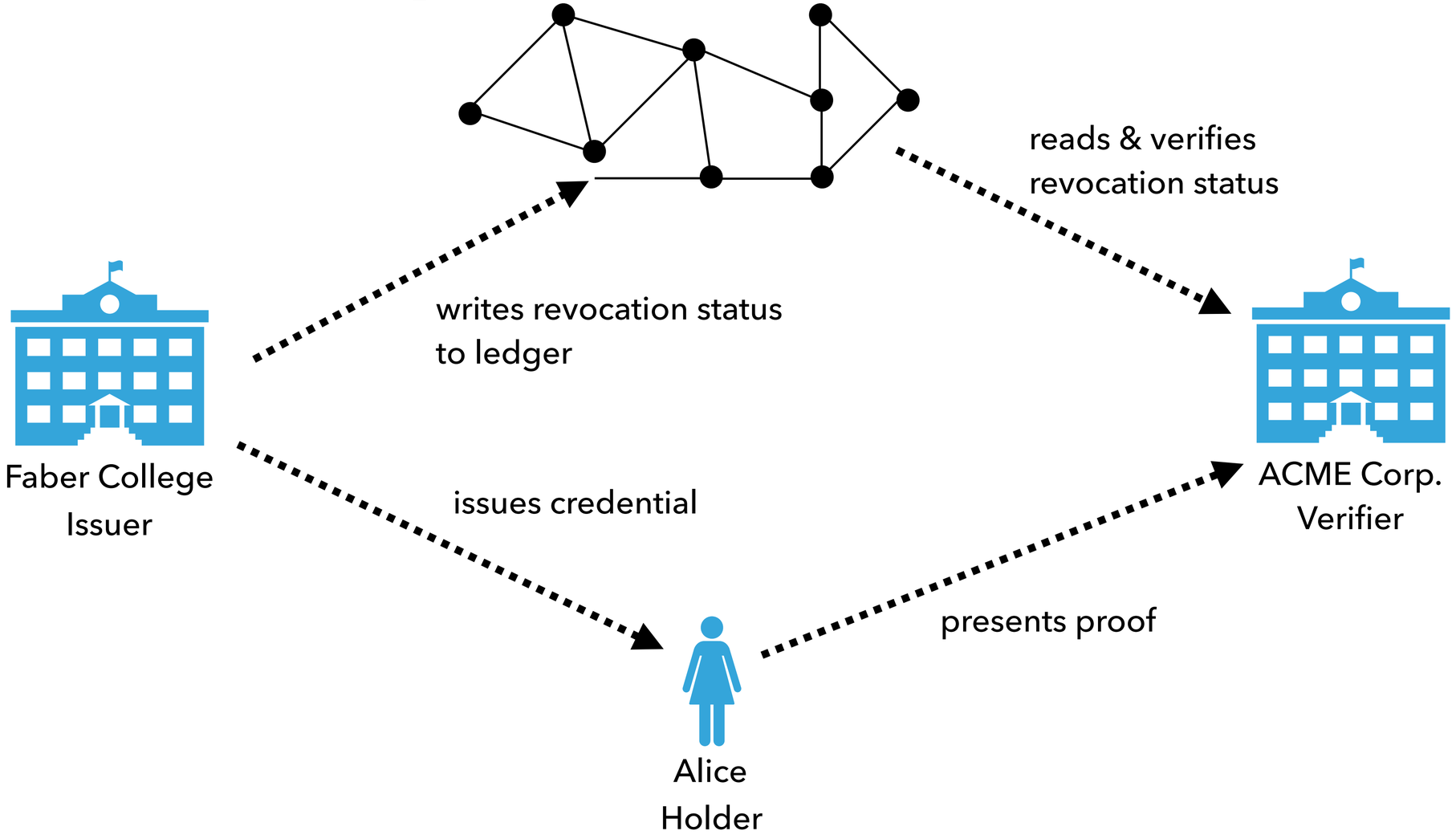
W3C standards - verifiable credentials

**“A verifiable credential is a tamper-
evident credential that has authorship that can be cryptographically verified.”**



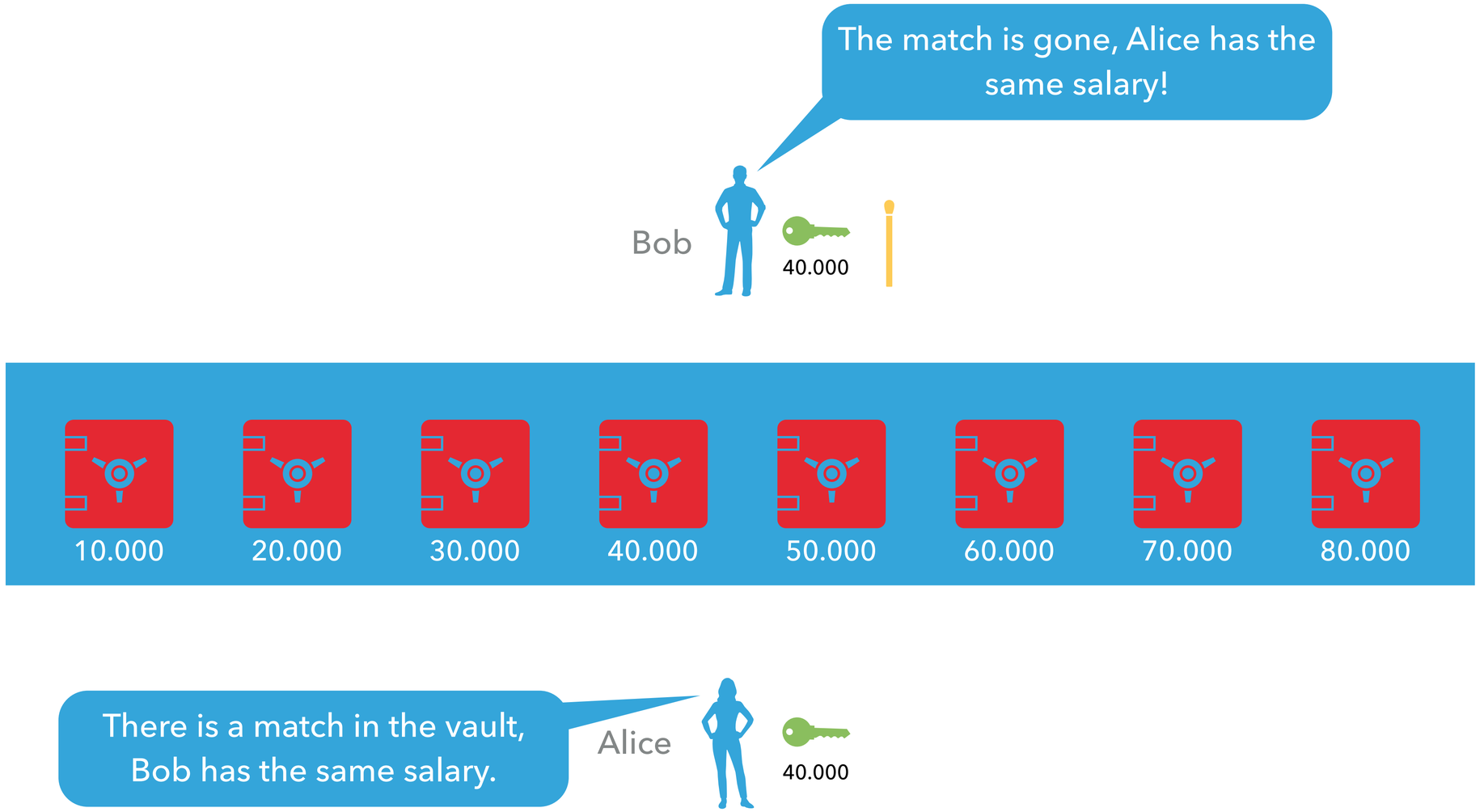

AlumniCredential
type
2010-01-01T19:73:24Z
issuanceDate
Credential 123
credentialSubject
TIMO
issuer
alumniOf
Example University
EXAMPLE UNIVERSITY
CREDENTIAL GRAPH
RsaSignature2018
type
SIGNATURE 456
nonce
348dj239dsj328
created
creator
signatureValue
2017-06-18T21:19:10Z
Example University Public Key 7
BavE110...3JT24=
PROOF GRAPH

Practical example



Selective disclosure

Zero-knowledge proof



Relevant questions

For the final presentation

- How does the technology handle identity?
- Does the technology incorporating some form of identity verification?
  - If so, what model do they use?
  - If not, is there any potential to be unlocked by incorporating it?
- What are the advantages of the identity model that is used (if any)
- What are potential risks of the identity model that is used (if any)