Verifiable Credentials HTTP API

A Human Rights Perspective

Adrian Gropper

May (Day) 2021

Technology is neither good nor bad; nor is it neutral.

Kranzberg's First Law of Technology

https://www.cs.middlebury.edu/~candrews/classes/cs312-f19/5164996f8790fdccfad1d7379d0e4e23/lecture15-moral-developer.pdf

In this session, we will discuss:

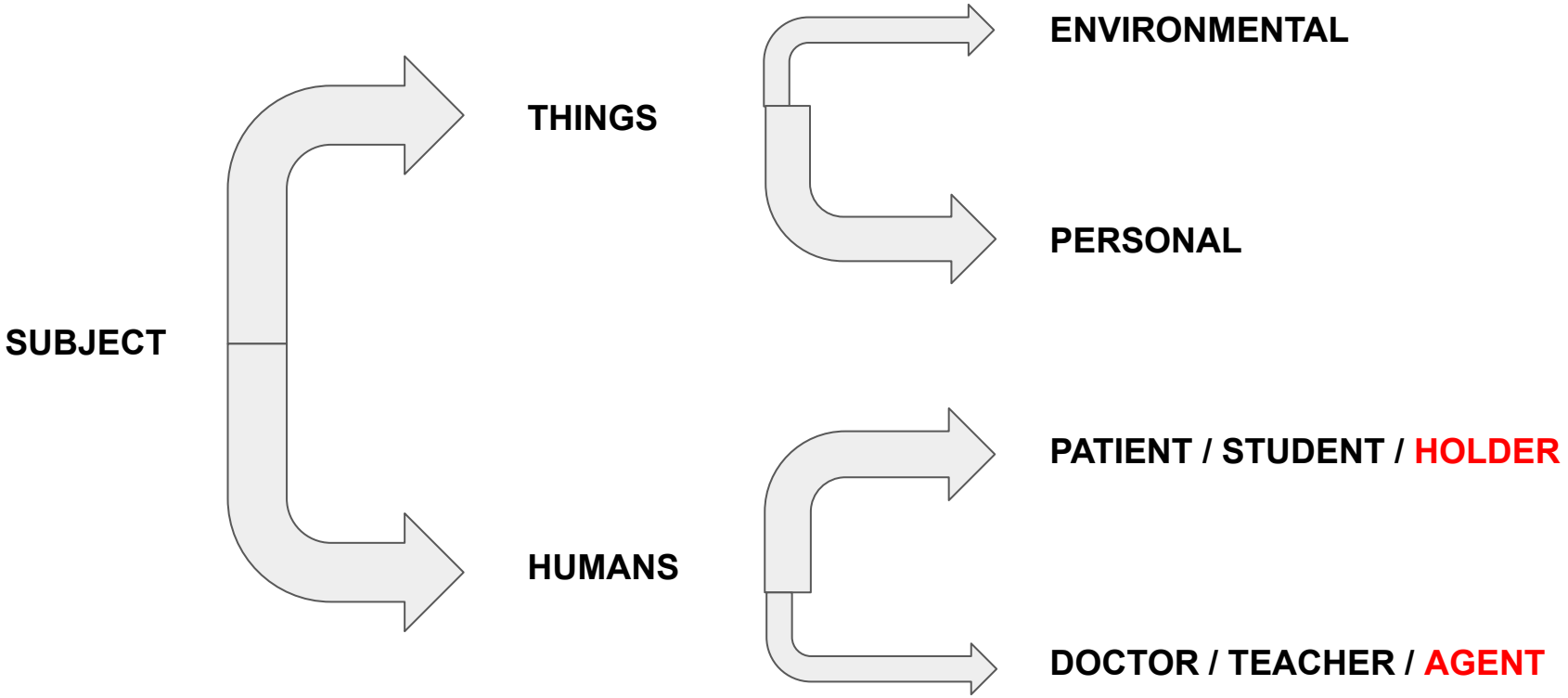
- Problem statement for the VC HTTP API
- Origin of the “learned intermediary” and Hippocratic Oath
- Implementation of the VC-HTTP API
- Use Cases and Current Challenges
- Next Steps

VC HTTP API Problem Statement

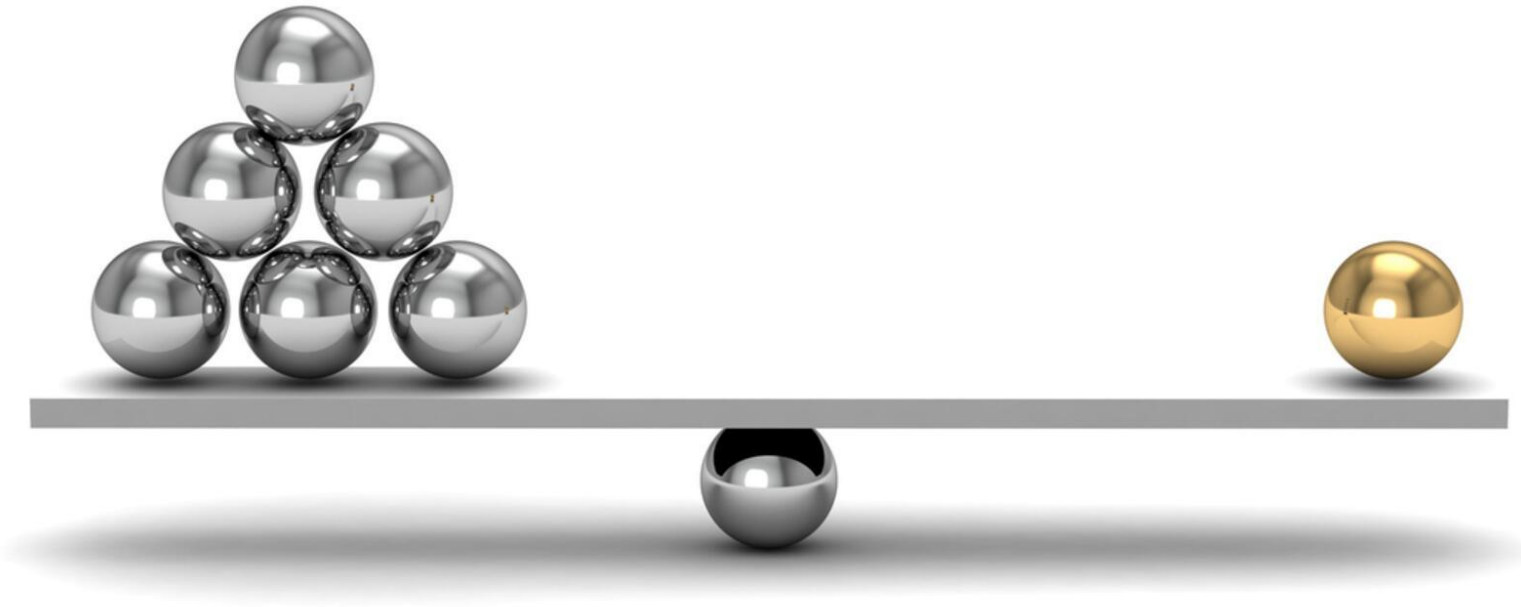
Provide an HTTP API to issue and verify data used in the Verifiable Credentials Ecosystem for use by servers and clients.

Examples of data include: Verifiable Credentials, Verifiable Presentations, Derived Credentials

VCs always have a Subject



The Asymmetry of Power

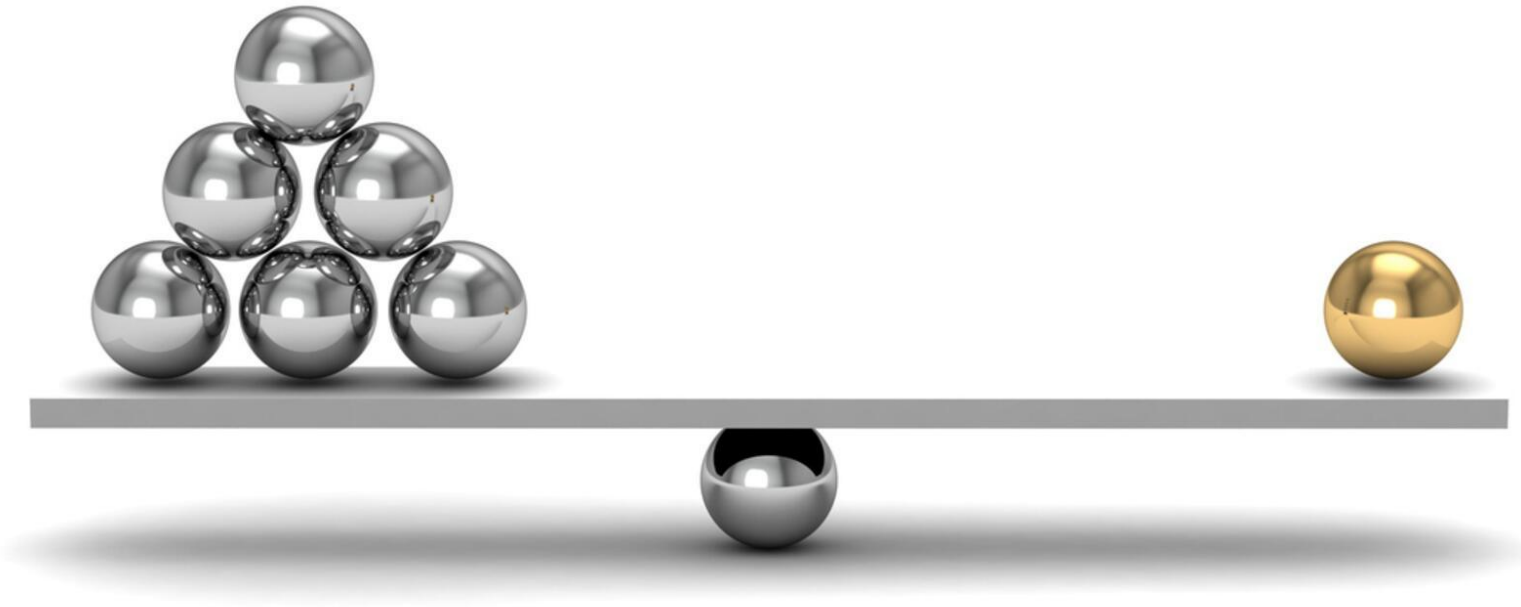


ISSUERS

VERIFIERS

HOLDERS

Control as Leverage for Human Rights



VC HTTP API

The Subject’s Levers: Choice and Delegation

- Choice
  - Issuers (limited or no competition)
  - Verifiers (limited or no competition)
  - Holders (a realistic choice only if acting as agents or delegates)
- Delegation
  - NOT the subject, a “learned intermediary”
  - Chosen by the Subject, not the Issuer or Verifier
  - Self-sovereign or Fiduciary
  - MUST NOT restrict choice of Issuers or Verifiers

Implementation of the VC HTTP API

- API Standard is Critical to Choice and Delegation
- Verifier is always the Requesting Party
  - Subject controls the request endpoint
  - Subject must be protected from spam and other attacks by requesting parties
- Subject can always:
  - choose a Holder or an Agent without Verifier prejudice
  - choose directed access from the Issuer vs. proxied via holder
  - introduce a Notary or Witness

Use Cases and Current Challenges

- SVIP Use Cases: the embodiment of asymmetric power
- Vaccination Credentials
- Prescription Credentials
- Revocation?
- Delegation?
- “Trust” Frameworks instead of Self-Sovereign Agency

Use Case: Vaccinating the Undocumented (among us)

Simultaneously:

- Detect fake certificates
- Provide paper versions
- Stratify eligibility
- Track disparities in access
- De-identify patients
- De-duplicate patients
- Track payment fraud
- Report adverse events
- Measure vaccine efficacy
- Promote both science and trust
- Global standards

Next Steps

- Issuers are just Resource Servers
- Verifiers are just Requesting Parties
- Holders may be:
  - User Agent (mobile wallet also capable of non-repudiable signature)
  - Resource Servers (custodial wallet)
  - Self- Sovereign Authorization Servers (process requests)
  - Fiduciary Authorization Server (process requests)
- Adopt the IETF GNAP terminology for the roles
- Define the VC HTTP API as a special case of GNAP

Designing SSI protocols to meet the SVIP requirements will have adverse human rights consequences.

I’m sure that’s not SVIP’s intent.

Resources

https://www.ietf.org/archive/id/draft-ietf-gnap-core-protocol-05.html

https://www.ietf.org/archive/id/draft-ietf-gnap-resource-servers-00.html

https://blog.fimbault.com/managing-authorization-grants-beyond-oauth-2

https://blog.petrieflom.law.harvard.edu/2021/04/27/vaccine-data-fake-cards/