GNAP interaction with VC-HTTP API W3C work

Adrian Gropper
IETF 111 GNAP
July 26, 2011

Me

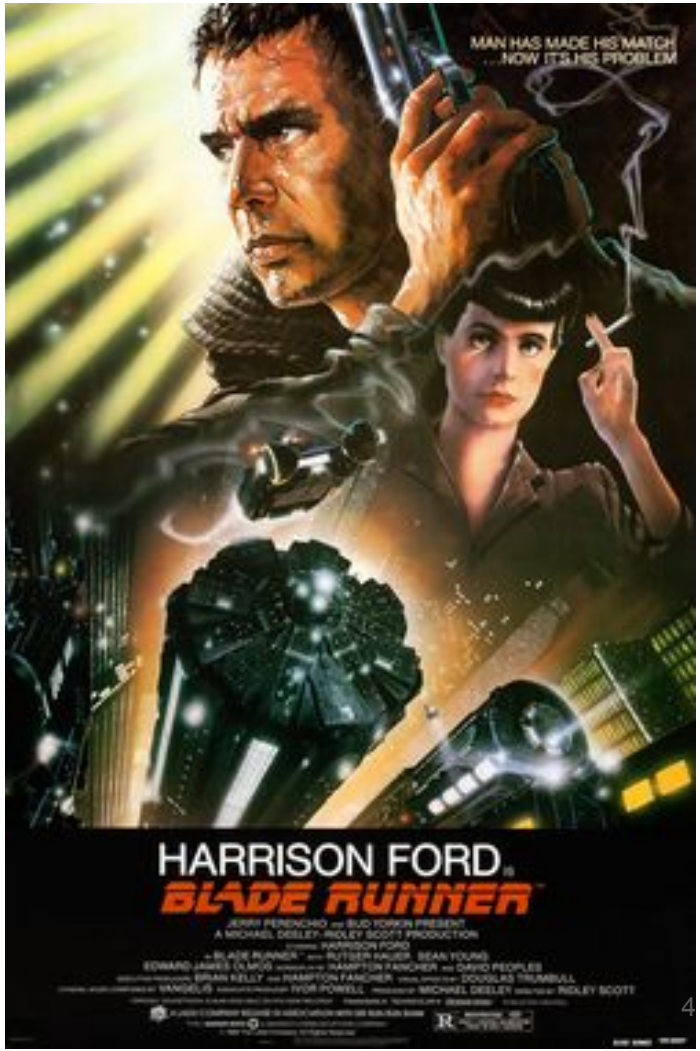
- **Invited expert on privacy** to many **SSI-related W3C and DIF** groups
- Core contributor to the transition from UMA 1 to **UMA 2**
- Volunteer CTO Patient Privacy Rights Foundation
- EPIC Advisory Board
- Lead the **HIE of One implementation** example of self-sovereign technology
- Engineer / Entrepreneur / Physician
- **New to IETF**

A Human Rights Perspective on Protocol Design

- Privacy is not enough
- Efficiency shifts power to the sovereigns
- Standardized data models are useful but **protocols are essential**
- What is Self-Sovereign Identity?
- Separation of Concerns - Controller or Processor (**not both**)
- Control Models and Protocols - (direct vs. delegated)
- W3C and DIF Protocol Work
- Discussion Points

Human Rights Concerns

- Ambient Authentication
- Non-repudiable Authentication
- Anonymity Barriers
- Strong Credentials
- Chain-of-Custody Protocols
- Lack of Agency
- Controls on Free Assembly
- Proprietary AI



https://en.wikipedia.org/wiki/File:Blade_Runner_(1982_poster).png

What is Self-Sovereign Identity?

- An identity only you **control**
  - DID and DID Method control the service endpoints - **public**
  - Service Endpoints - interfaces that can be dereferenced from a DID - **protected**
- Control Models
  - Direct
    - Possession (wallets, platforms, data brokers)
    - Messaging Address (email, SMS)
    - Mediator (Sign-in with Apple email proxy)
  - Delegated
    - Agent (Authorization Server, UMA2 or GNAP)
- Everything else is a (sovereign) processor
  - Nations and states
  - Courts and law enforcement
  - Hospitals
  - Schools
  - Vendors

Standardizing the (Digital) Sovereign

Verifiable Credential - Data Model

- Subject
- Attributes
- Issuer (processor, not a controller)
- Proof (security)

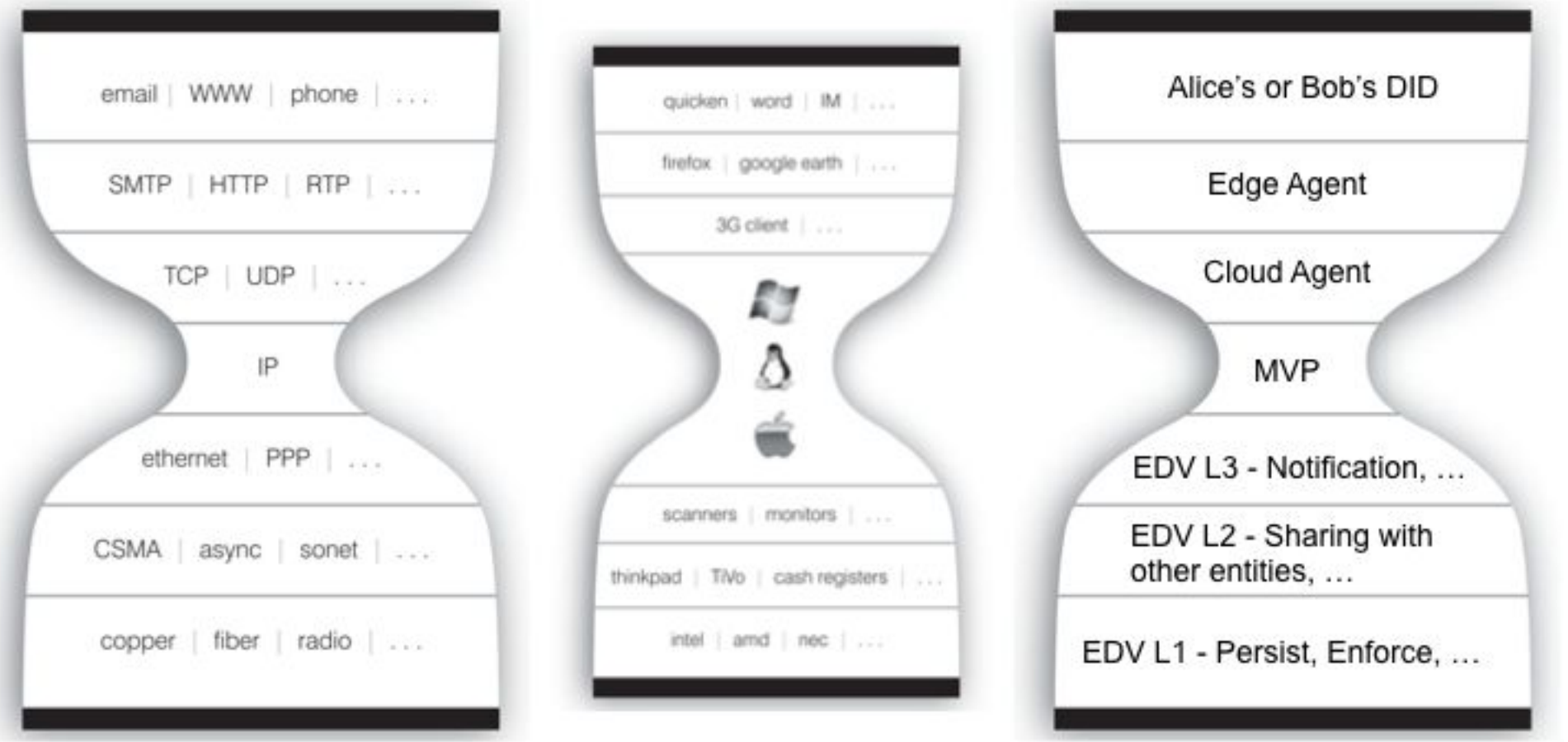
Resource Server - Protocol

- Subject / RO / (Registration)
- Attributes (scopes)
- Processor (not a controller)
- Authorization (who decides?)

The sovereign is the processor, so **where's the controller?**

Control Models and Protocols

- Direct
  - Authentication
  - Possession
  - Messaging Address
  - Mediator
- Delegated
  - Authorization
  - Agent
  - UMA 2
  - GNAP



Adapted from J. Zittrain The Future of the Internet and How to Stop It
https://dash.harvard.edu/handle/1/4455262

W3C and DIF Protocol Work

- VC-HTTP API - access to digital credentials
- Encrypted Data Vaults - blind storage can’t be censored
- Identity Hubs - person-centered storage
- DIDComm - message-level (not transport-level) security
- SIOP - self-issued OIDC OP

Is GNAP the “narrow neck” Minimum Viable Protocol**?**

Discuss Human-Centered Protocols

- How many authorization protocols does the Internet need?
- The problem with OAuth is lock-in and censorship (via client credentials)
- Self-sovereign and Fiduciary agents (both are important to human rights)
- How to detach “chain of custody” from verification (without biometrics)?
- Is GNAP the “narrow waist” of Self-Sovereign Identity?

PLEASE contact me to continue the discussion:
agropper@healthurl.com
HIE of One example implementation https://github.com/HIEofOne/Trustee-Community
NEED help implementing GNAP in FastAPI and Vue PWA https://github.com/agropper/OGNAP