internet2.edu

FIM4L and Attributes for Access Control

Ken Klingenstein, Internet2

AGENDA

- FIM4L milestones
- FIM4L upcoming
  - use cases for managed access
  - open science and libraries (curation)
- Attributes redux
  - attribute providers in federations
  - attribute providers in VDC
  - authority trees and forests

FIM4L Milestones and Goals

- A working group under Liber
  https://libereurope.eu/working-group/liber-fim4l-working-group/
- Recommendations on federated identity, use of attribute entity categories for privacy and functionality https://zenodo.org/records/7313371
- Herding librarians

==========

- Gathering managed access use cases
- FIM and open science and libraries – curation, etc.

Federated identity and access control

- The original federated use cases were access control
  - Scalability, privacy, flexibility key design goals
- But we took a 20 year detour into authentication
  - What the marketplace (the federal government) wanted
  - Levels of Assurance, multifactor authentication, etc.
- Access control capabilities engineered but modestly implemented
  - Attributes exist but semantics and management lag

Open Access is actually “managed” access

- Many open access instances are gated communities
  - By citizenship
  - By age
  - By privacy considerations
  - By cultural restrictions
- Consortial relationships
- Sensitive data
- Special collection restrictions
- Protecting privacy
- Answer for privacy-preserving authorization lies in effective use of attributes

Liber post from FIM4L on managed access use cases

Processing stage (Data processing and conducting science)

- Open Science collaboration infrastructure
- Citizen sciences user identification and authentication
- University Press pre-publications, pre-prints, etc.

- **Published stage (Data, articles/journals, eBooks etc.)**
- Institutional repositories – Repositories may need to implement a number of controls, such as time and geo embargoes, restrictions on copyright such as photographs, domain specific licenses, etc.
- Data repositories – Sensitive data needs access controls; data sets for some domains are restricted to researchers in those domains; the integrity of the data needs to be protected by its owners.
- University Press publications – Copyright such as photographs, domain specific licenses, citizenship limitations, etc. need to be deployed.
- Open Educational Resources – Copyright and licensing issues the need to measure usage to establish the value and demographics of the resources.
- If the Open Access platform allows for reviews and comments, it is important to know the author of such contributions.

- https://libereurope.eu/article/managed-access-use-cases-for-open-science/

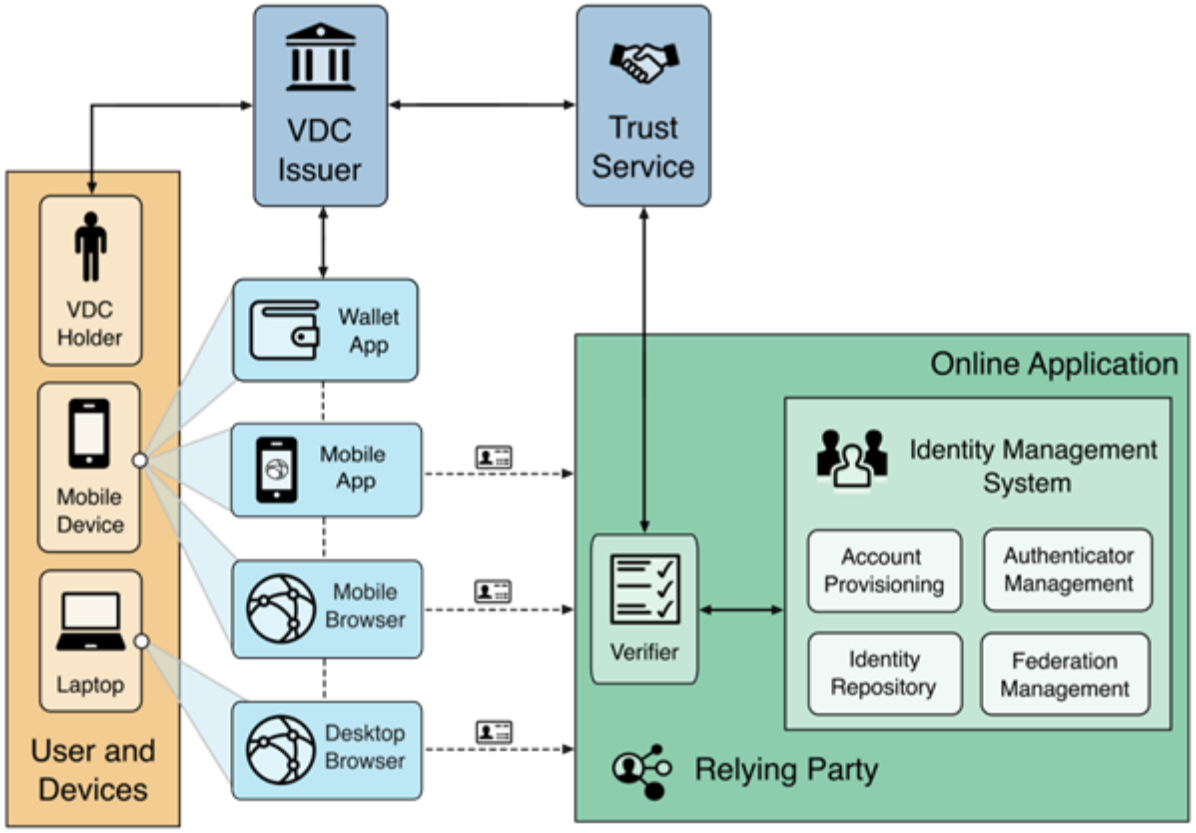
Attributes Redux

- The original federated model has attribute providers hidden inside the IdP
  - Overpowered by authentication
- Leveraged institutional trust for authority.
- Lessons of the Tao of Attributes
- Verifiable Digital Credentials and attribute providers
- Joe’s Credential Shack

The Tao of Attributes

- Legendary workshop at NIH circa 2008
- Identified many of the issues associated with the federated use of attributes
- which to face: e.g. standard semantics and syntax, extensibility, source, etc.
- which to avoid: currency, revocation, storage/security, other complexities
- Important to remember the Tao as we head in

Verifiable Credential Ecosystem



Users may present VDCs online to relying parties through a mobile application or through a browser.

NIST Blog 11/13/24

Attribute Providers and Authority Trees

- Authority to issue a credential depends on:
  domain authority - expertise
  institutional authority – role
- Often many authorities can issue equivalent credentials
  e.g. pipetting – from a class, a professional nursing association, public health clinic
- Authority forests – for now, assume trees issues equivalent credentials in the forest – e.g. aspen

Useful NIST Resources

Attribute Validation Services for Identity Management: Architecture, Security, Privacy, and Operational Considerations

https://csrc.nist.gov/pubs/ir/8480/ipd

https://www.nist.gov/blogs/cybersecurity-insights/digital-identities-getting-know-verifiable-digital-credential-ecosystem