draft-howlett-abfab-trust-router-ps

ABFAB, IETF83

Josh Howlett & Margaret Wasserman
Background

• ABFAB uses AAA infrastructure to connect RPs and IdPs

• AAA technologies currently use shared secret or certificate based mechanisms to establish trust

• We believe that these mechanisms impose barriers to the deployment and use of ABFAB

• We are proposing a complementary trust establishment mechanism

• Other documents describe the proposed mechanism; this document describes the motivations
Barriers that concern us

• Cost
  – The costs associated with a trust infrastructure should be bourn predominantly by those that benefit from it
  – This encourages adoption by actors that have less to gain
  – Shared secrets and certificates impose non-trivial costs on actors; e.g.
    • Purchase certificates from a commercial CA
    • Set up a special purpose CA
    • Configuration churn where there are many partners
    • Credentials should be selected for their intrinsic advantages in particular usage scenarios, and not for the convenience of the trust infrastructure
  – Credentialing is expensive and so should be minimised
Barriers that concern us

• Scaling
  – A trust infrastructure should be able to scale up, down and sideways
  – Scale up: An actor should bear the costs of connection to a trust infrastructure. Other actors that might also happen to be part of the same infrastructure should not.
  – Scale down: Communities come in all shapes and sizes. What works for the US Federal Government may not be practical for much smaller communities.
  – Scale sideways: Communities often become more inclusive or exclusive over time.
Terminology

• Partner
  – An organization that participates in an ABFAB federation as an IdP, an RP or both.

• Community
  – A group of IdPs and RPs that are associated with each other for a specific purpose.

• Community of Interest (CoI)
  – A community that is formed to share a set of resources and services.

• Community of Registration (CoR)
  – A community that provides registration and authentication services for its members.
Roles

• CoRs are responsible for asserting authentication of partners that it has registered (i.e., identified and credentialed)
• Cols are responsible for asserting a partner’s membership a community
• Partners apply for membership to one or more Cols, and register with those CoRs necessary to meet the requirements of the Cols.

→ Explicit separation of ‘technical trust’ (CoR) and ‘behavioral trust’ (Col)
"Dave’s Shoes"

CoI

Application

CoR

Registration (e.g., LoA 1)

Shoe Trade Association

Retailer

RP

Business interaction

DoD

Approved DoD Suppliers

Application

DoD

CoR

Registration (e.g., LoA 2)
Some goals

• Establishing a CoI should be sufficiently trivial that anyone can operate one (or out-source at negligible cost)
  – This is not generally true of public key based infrastructures
• Registration is non-trivial, and so it will always be expensive. So, a registration should be useful for interactions in many contexts
  – Public key based infrastructures bind policy (community) information to the public key. It can be difficult to persuade issuers to include policy identifiers that are not relevant to them
• The credential technology used within a trust infrastructure should be selected on the basis of business need, and not because the trust infrastructure requires it for interoperability
  – If the properties of your credential and my credential satisfy the abstract security requirements required by our use case, we should be able to use them to establish trust even if they are different technologies
• There are examples where trust infrastructures have been combined to achieve a separation of CoR (e.g., a vanilla PKI) and CoI (e.g., a SAML attribute authority or LDAP directory), but it would be cleaner if a single trust infrastructure supported both functions