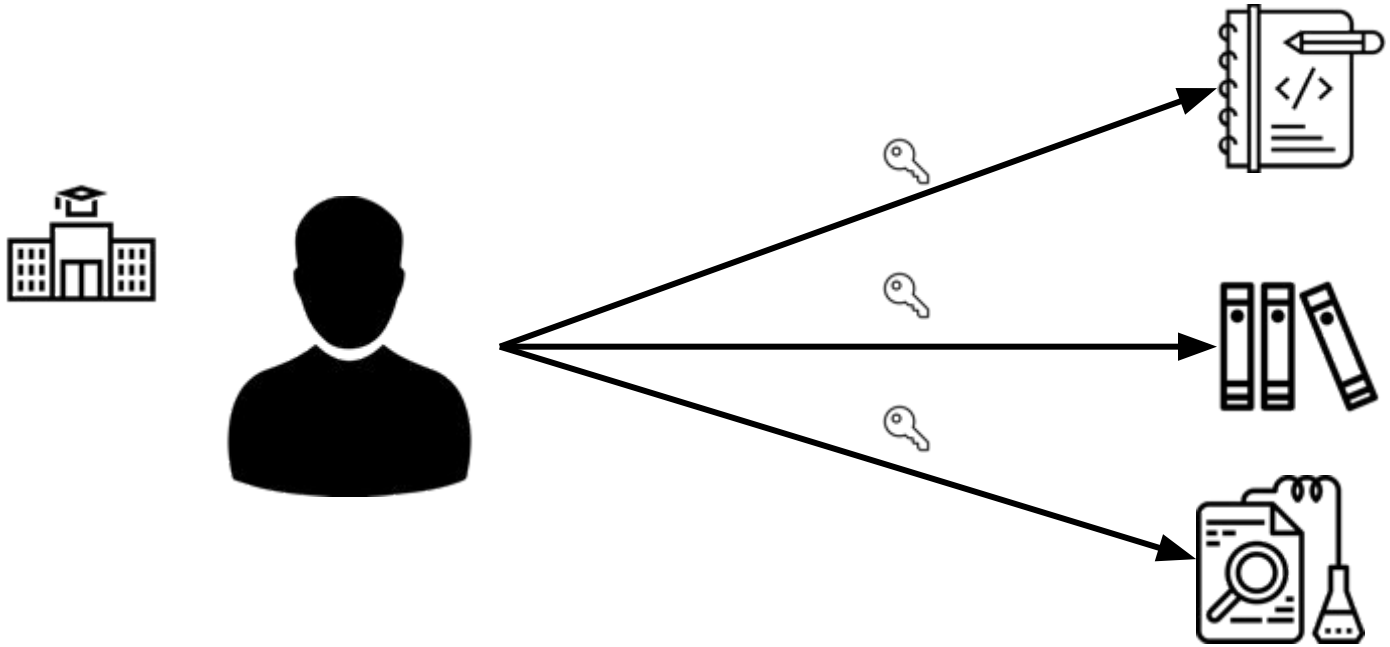
Identity Federations

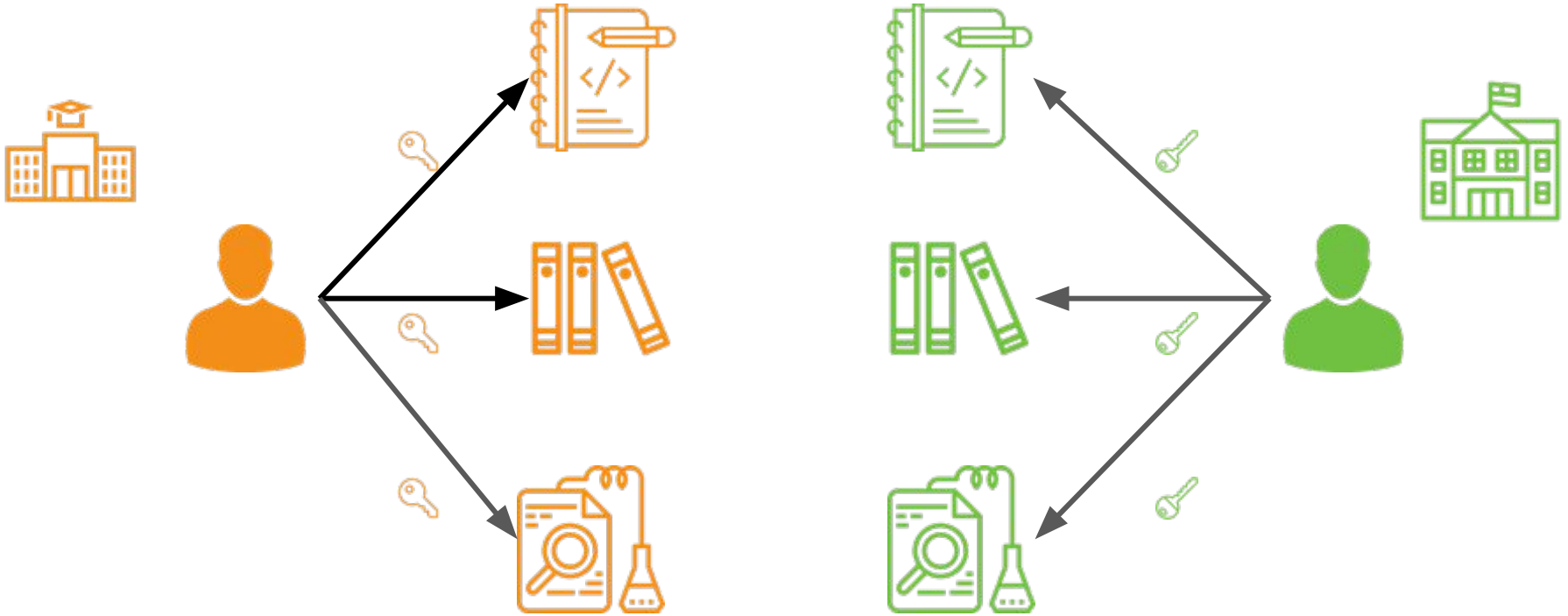
High Level Concepts

In the beginning...

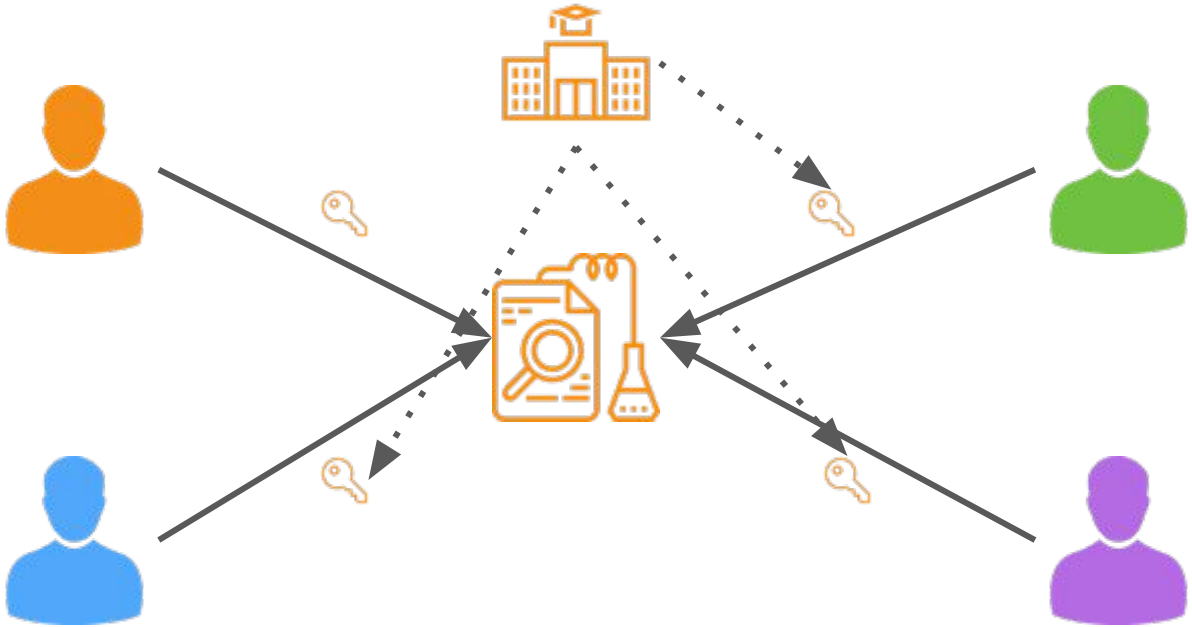
Traditional Identity Management



Traditional Identity Management



Traditional Identity Management



Traditional Identity Management

Traditional Identity Management

- Each organization must provision identity
  - High overhead for some organizations
  - Research organizations for example may just want to provide services

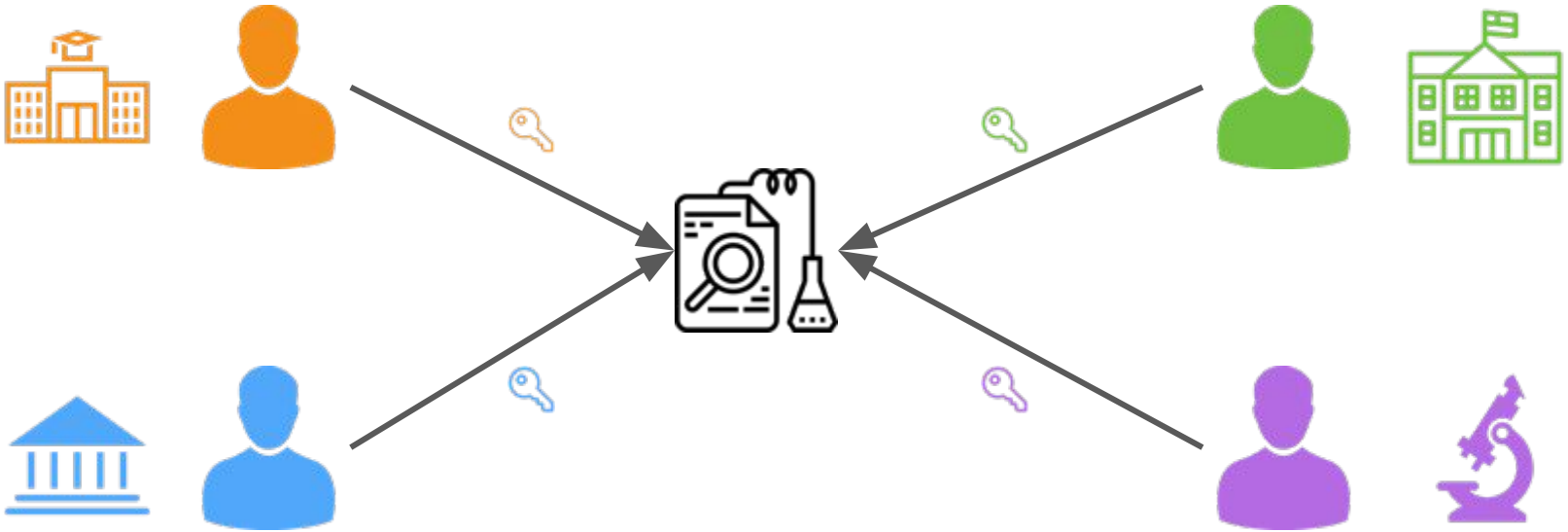
Traditional Identity Management

- Services only consume identity provisioned by service owner organization
  - Allows services to make assumptions about user identities and credentials
  - Assumptions become hardened into service over time
  - Burdens service owner when external users need access

Traditional Identity Management

- Collaboration across organizations demands...
  - Each organization provisions identities for non-members
  - Users manage multiple identities, each with a single purpose
    - Often results in users using same login/password for multiple sites

Federated Identity Management



Federated Identity Management

- Only identity providers provision identities
  - Not all organizations need to provision identities
  - Some organizations (campuses) well suited to provision and curate identities
  - Other organizations (research projects) focus on delivering services

Federated Identity Management

- Services consume identities provisioned by other organizations
  - No longer able to make assumptions about identity and credentials
  - Initially may take more time to deploy and bring into production
  - Over time results in more flexible services

Federated Identity Management

- Collaboration across organizations is facilitated:
  - Identity providers focus on provisioning well curated and managed identities
  - Service providers focus on delivering flexible and useful services
  - Users manage a single well curated identity

Foundation of Federated Identity is Trust

Foundation of Federated Identity is Trust

- Service provider must trust the identity provider to **appropriately**:
  - Vet user's real identity at enrollment or registration
  - Manage credential stores to protect secrets
  - Assert details about authentication events
  - Assert user identifiers and attributes (if any)

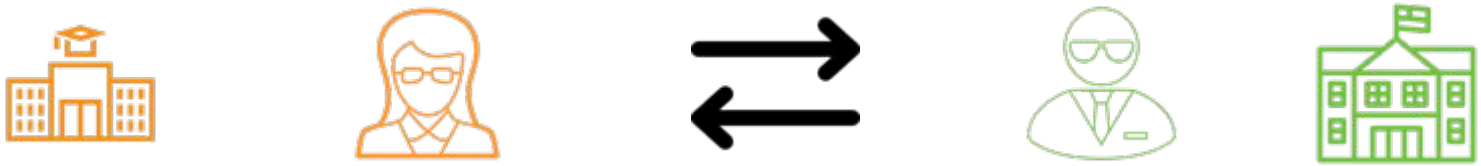
Foundation of Federated Identity is Trust

- Identity provider must trust the service provider to **appropriately**:
  - Consume assertions about authentication events
  - Consume user identifiers and attributes (if any)
  - Store user identity information
  - Protect user privacy

Establishing Trust

How do a service provider and an identity provider establish trust?

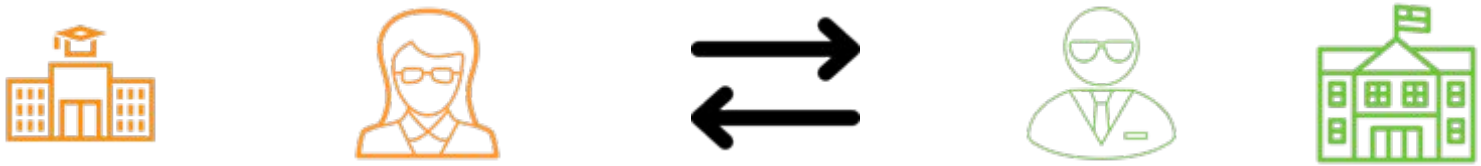
Bilateral Trust



Identity provider and service provider must agree on

- Technical details
  - Which protocols used to assert and consume identity?

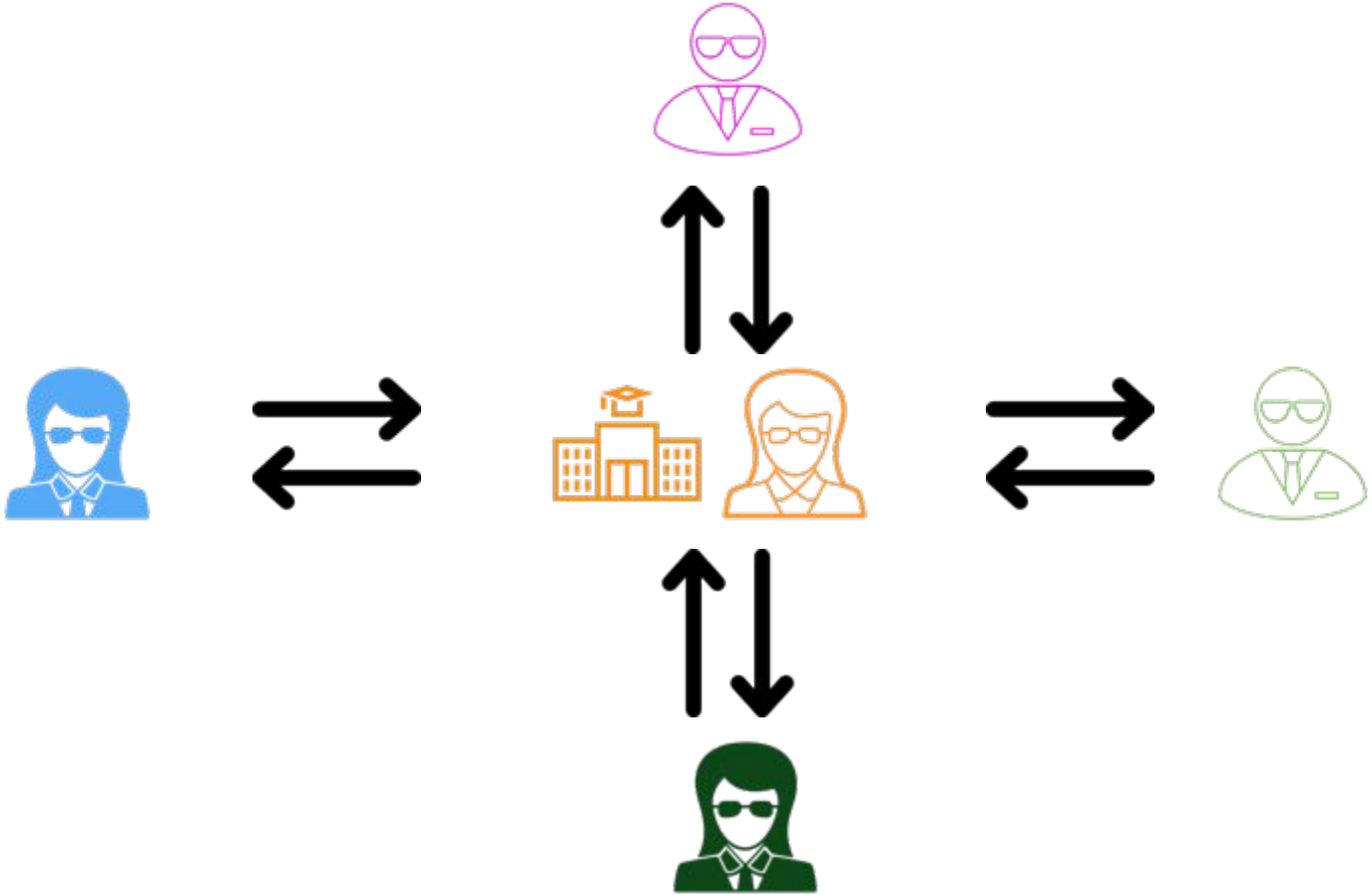
Bilateral Trust



Identity provider and service provider must agree on

- Policy
  - Which users? How are they vetted? What identity details will be asserted? Which will be consumed? How will it be stored? Who will have access to it? Will it be deleted? When?

Bilateral Trust Does Not Scale



Establishing Trust

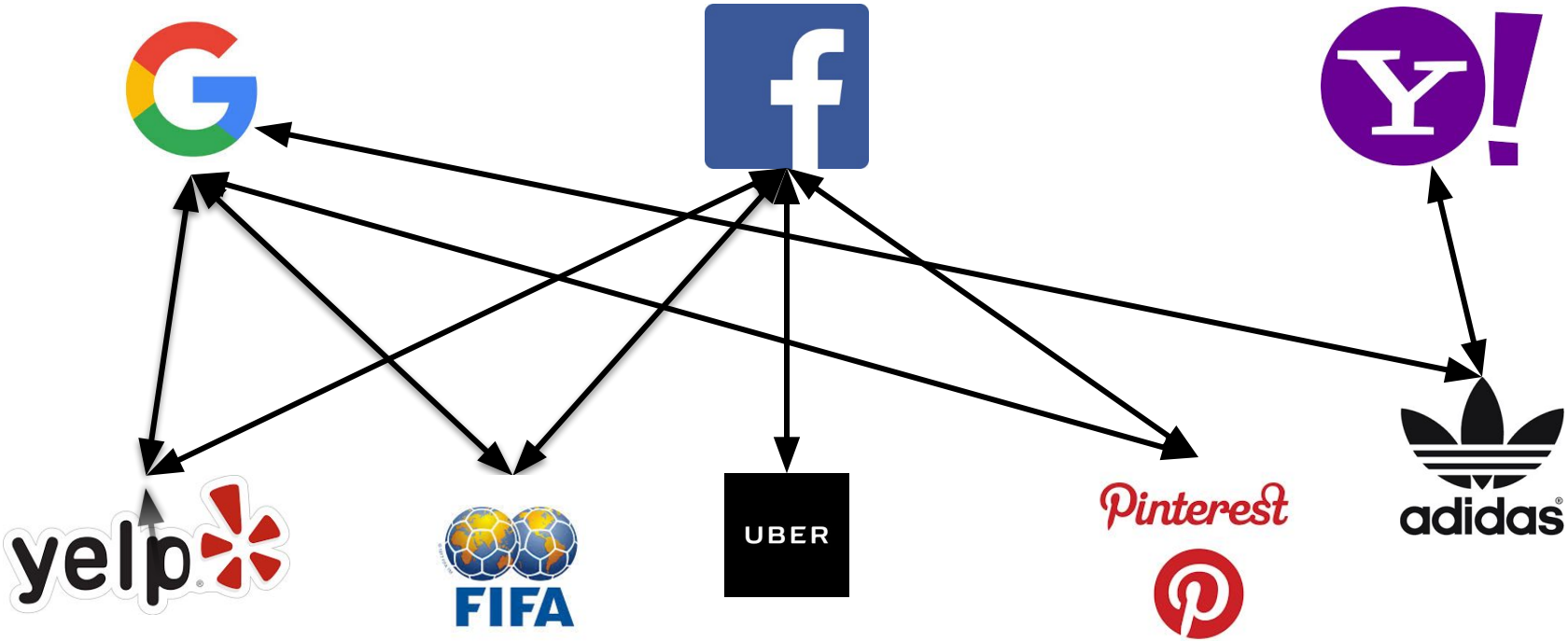
What if a group of identity providers and service providers came together and established a common set of policies and baselines for technical interoperability to **scale** trust and **facilitate collaboration**?

What would we call such a group?

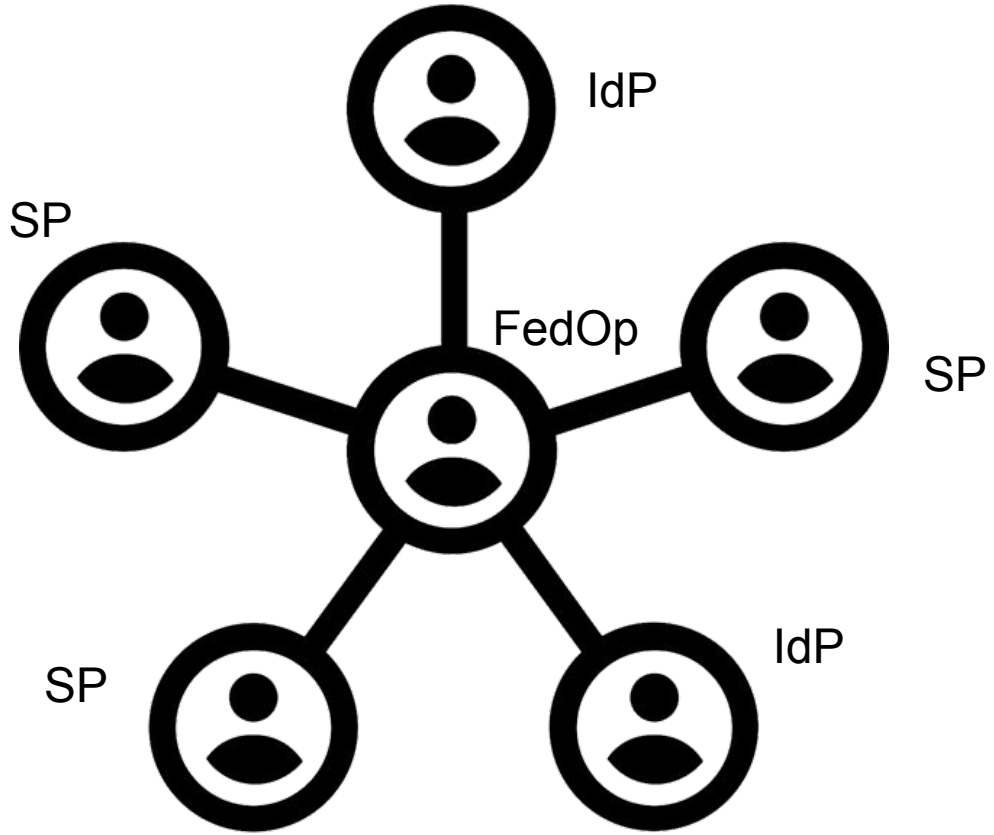
Identity Federation

Identity providers and service providers establishing **scalable trust** through a common set of policies and technical interoperability baselines.

Commercial Identity Federations



Higher Education & Research Identity Federations



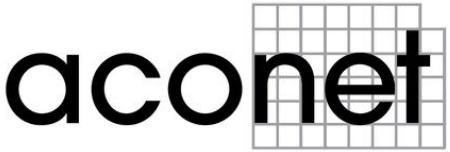
Higher Education & Research Identity Federations

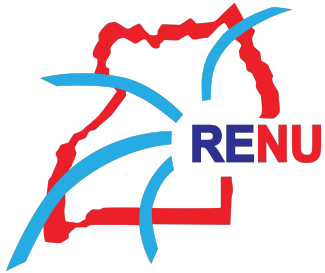
- Accessing Networks
- RADIUS

Higher Education & Research Identity Federations

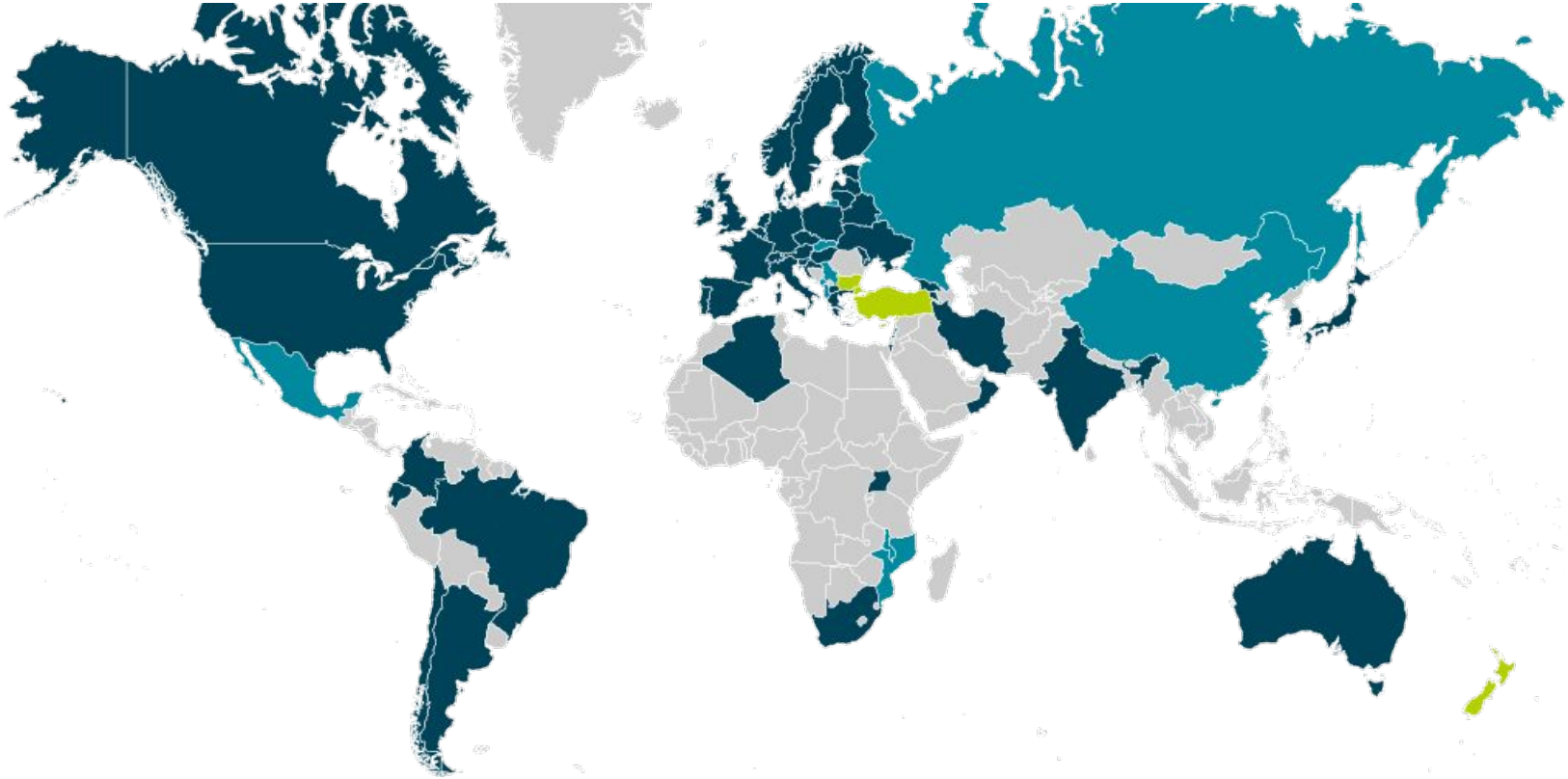
eduID
- Accessing Applications & Services
- SAML/WebSSO (Shibboleth)

Higher Ed & Research Identity Federations





eduGAIN Federation of Federations



Foundation of Federated Identity is Trust

As each organization matures its federated identity practice, it is tempting to focus on the minutiae of technical and policy detail and lose site of the big picture:

Higher Education and Research federations exist to facilitate and streamline collaboration, research, and scholarship across organizations and are built on a foundation of mutual trust.