# Federation Implementations

*Mwotil Alex*

*RENU Identity Federation (RIF)*

# Federation Architectures

- Identity Federations can be categorized into the following:
  - Full Mesh
  - Hub & Spoke
    - Centralized login
    - Distributed login
  - Hybrid (Full Mesh and Hub & Spoke)

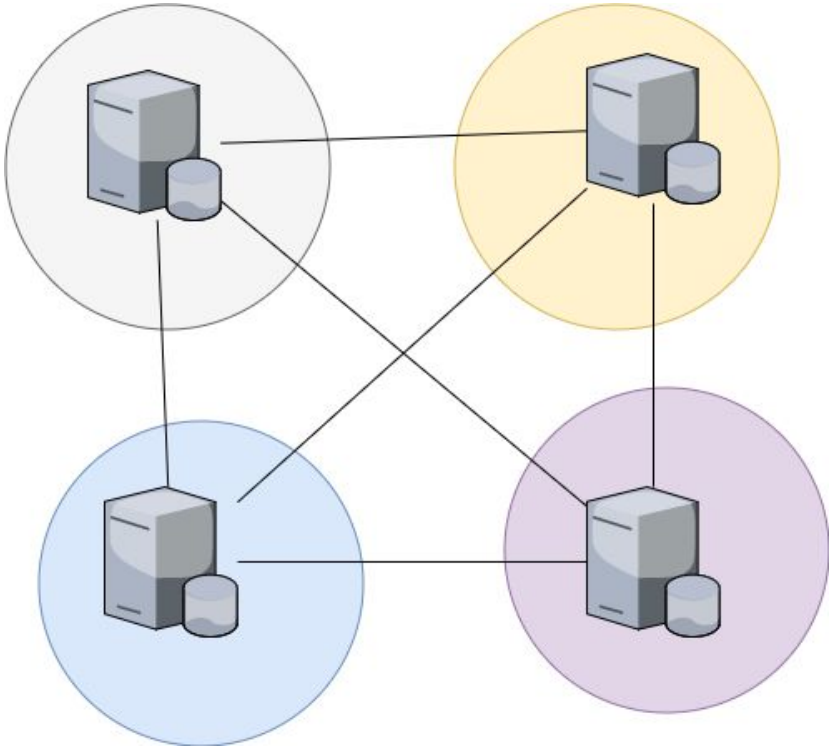
# Full Mesh

- Most federations employ this architecture
- No central components, all are distributed including failover
- Entities typically have more connections to other entities in the federation
- IdPs and SPs do more work
  - Configure attribute release
  - Maintain a discovery service
  - Protocol support
  - Manage entity connection

# Full Mesh

Example: *eduGain*

- *SWAMID*
- *SWITCHaai*
- *InCommon*
- *RIF*



# Full Mesh

| Pros | Cons |
| --- | --- |
| ● *Better User Experience*<br>● *Distributed Points of Failure*<br>● *Providers have full control of the data*<br>● *No single points of attribute intercept*<br>● *Simpler for the operator* | ● *Harder for new providers*<br>● *All providers have to agree to a standard protocol, and implement it*<br>● *Results into large metadata*<br>● *Harder to debug problems* |

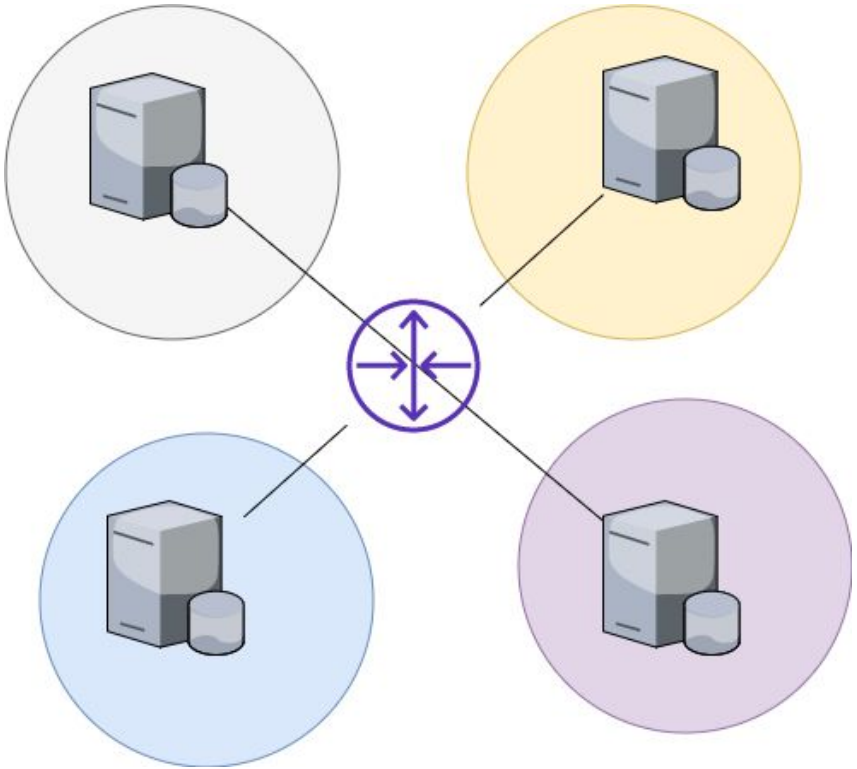
# Hub & Spoke

- A central hub exists between all IdPs and SPs
- Entities need a single connection to the central hub, and maintain it
- The hub manages connections between the entities
- Features can easily be rolled out given the central hub
- Login may be centralized or distributed

# Hub & Spoke

Example: *eduroam*

- *Distributed*
  - *SAFIRE*
  - *WAYF.dk*
- *Centralized*
  - *FEIDE*
  - *AAI@eduHr*



# Hub & Spoke

| Pros | Cons |
| --- | --- |
| ● *Onboarding simpler for providers*<br>● *Hubs can hide/solve interoperability problems*<br>● *Hub can extend or transform attributes* | ● *Complicates discovery*<br>● *Hub can be a single point of failure*<br>● *Privacy issues*<br>● *Individual providers lose control*<br>● *More complex to operate* |

# Hybrid

- Organizations represented as individual entities in the metadata
  - May run own Identity Providers
- A central hub
  - Does most of the heavy lifting just as hub and spoke
- May have a central login with customization options for organizations
- Provides best aspects of full mesh and hub & spoke worlds
  - Flexibility and agility