FEDERATION ARCHITECTURES

Mr. Terry Smith, Australian Access Federation
A brief discussion on the different type of federation architectures that have been deployed globally. We will identify their strengths and weaknesses, the effort involved in deploying and maintaining and their future directions. Architectures include Mesh, Hub and Spoke, Hybrid and Multi-Protocol.
Hub and Spoke v Mesh

A federation can be built according to the hub-and-spoke or mesh principle. In short:

- in a mesh federation, each entity is responsible for its connections to other entities,
- whereas in a hub-and-spoke federation, all entities connect to the hub and the hub manages connections between entities on a central location.
Mesh

Most federations employ the mesh principle. In a mesh federation, there is no central "hub" through which connections between entities flow. Thus, Identity Providers and Service Providers must create and maintain connections to each other themselves.

Contrary to a hub-and-spoke federation, entities typically have multiple technical connections to other entities.

In a mesh federation, Identity Providers and Service Providers must typically do more work themselves that could otherwise be done by the central hub. Examples are configuring attribute release, maintaining a discovery service, supporting multiple protocols and software and managing connections between entities.

Full Mesh Federation

~80% of all NREN Federations (June 2013)
E.g InCommon, UKAMF, SWITCHaai, SWAMID, HAKA, AAF
Hub and Spoke

In a hub-and-spoke federation, a central "hub" exists between all connected Identity Providers and Service Providers.

The main advantage of this principle is that all entities only need to create and maintain a single technical connection to a single entity: namely the central hub of the federation.

The hub manages and passes through individual connections between entities. Due to this design with a central hub, extra features can be rolled out easily and centrally, such as strong authentication and user consent.

SURFconext is an example of a hub-and-spoke federation.

Downsides: The Hub must always be available. It is a central point of attack. All user data flows through the hub.
Hub and Spoke with centralized login

Hub & Spoke federations with central login are a special case in the sense as there is only one single Identity Provider in the federation.

Instead of operating individual Identity Providers at each organisation, in this architecture all user databases are connected to a central Identity Provider. Users enter their organisation credentials on the central Identity Provider. Therefore, the organisation operating this Identity Provider needs to be especially trusted by all organisations.

Also the central Identity Provider is a single point of failure and it must be highly available. Depending on the number of logins, scalability issues may arise. On the other side, it is very easy to support new authentication protocols on the hub thanks to the central login. In an interfederation context, there are however similar usability problems like with the distributed login.

This is generally how a University will operate.
Hybrid

- Generally starts as a Mesh federation
- Small hubs of services start appearing
  - Authentication Proxies / Bridges
  - Services start to pool around these proxies / bridges
    - Protocol translation
    - Shared unique Identifiers
    - Additional attributes added at the hub
    - MFA at the hub
    - Social logins
- Can be operated by the federation or service provider
References

**Federation Architectures** -
https://wiki.geant.org/display/eduGAIN/Federation+Architectures

**Federation architecture: hub-and-spoke vs. mesh** -
https://wiki.surfnet.nl/display/surfconextdev/Federation+architecture%3A+hub-and-spoke+vs.+mesh
REVIEW #2