



What to look for in an Identity management solution

UK Federation FAM 2026

Matthew Slowe
Solutions Architect

Matthew Slowe

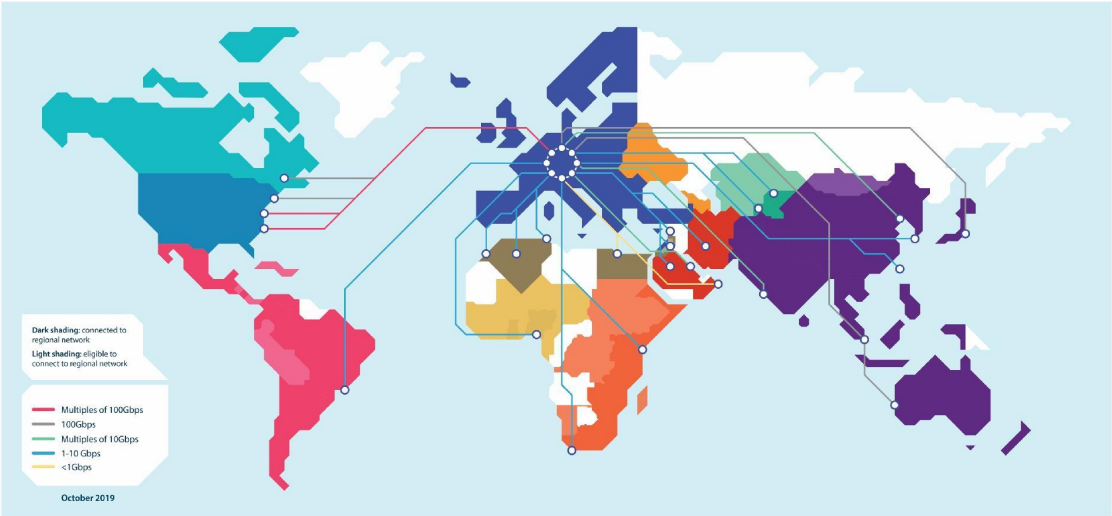
- Trust & Identity specialist who focuses on federated access, SAML/OIDC, and, previously, eduroam
- Formally of Jisc and University of Kent
- Now part of Core AAI team at GÉANT supporting MyAccessID and related services



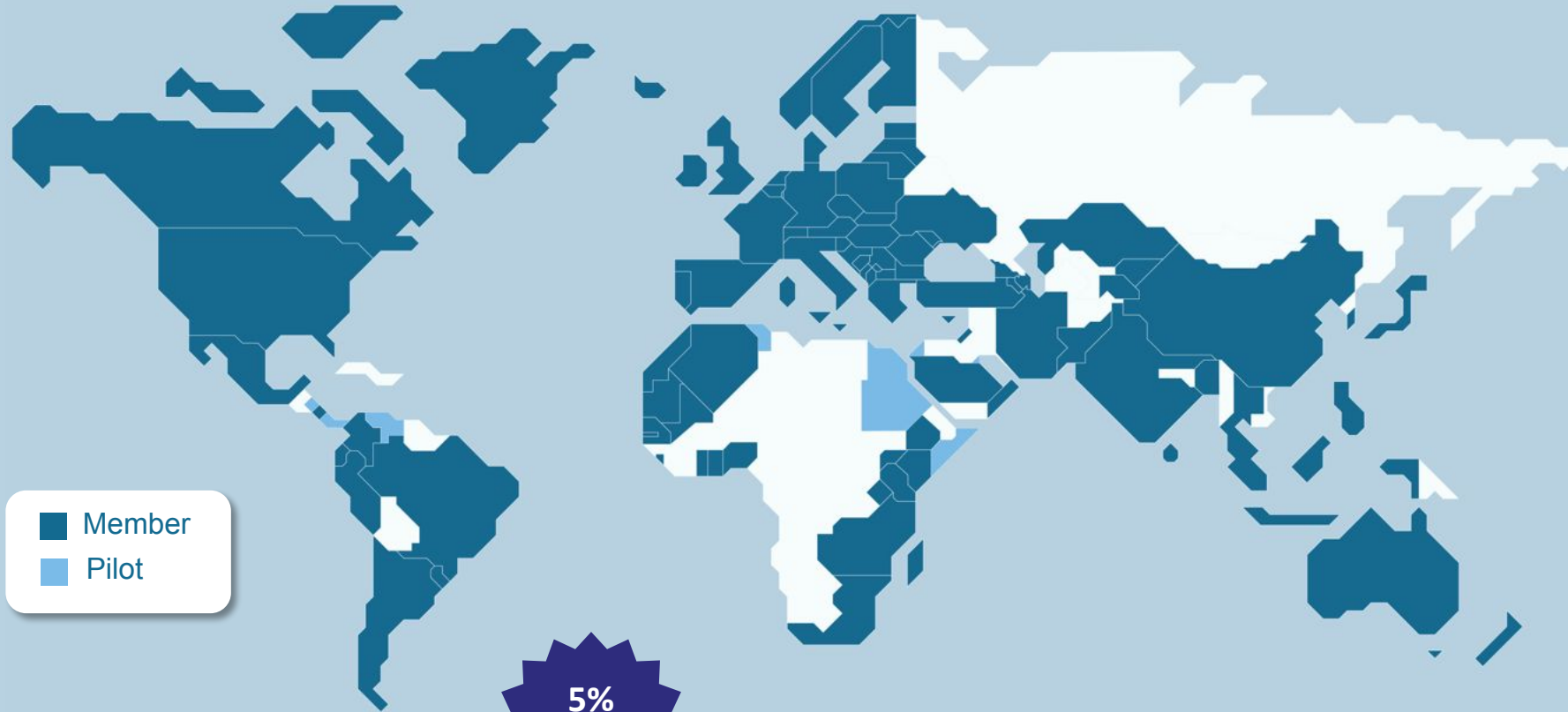


- Pan-European membership organisation similar in setup to Jisc
 - 37+ NRENs, and associates like CERN, ESA
- Connectivity
 - Connecting NRENs and others
 - eduVPN
 - eduMEET
- Trust & Identity
 - eduGAIN
 - eduroam
 - MyAccessID, MyAcademicID, eduTEAMS
- Much more

AT THE HEART OF GLOBAL RESEARCH
AND EDUCATION NETWORKING



eduroam



5%
growth

>106
Countries

10,500+
Institutions

44,600+
Service Locations

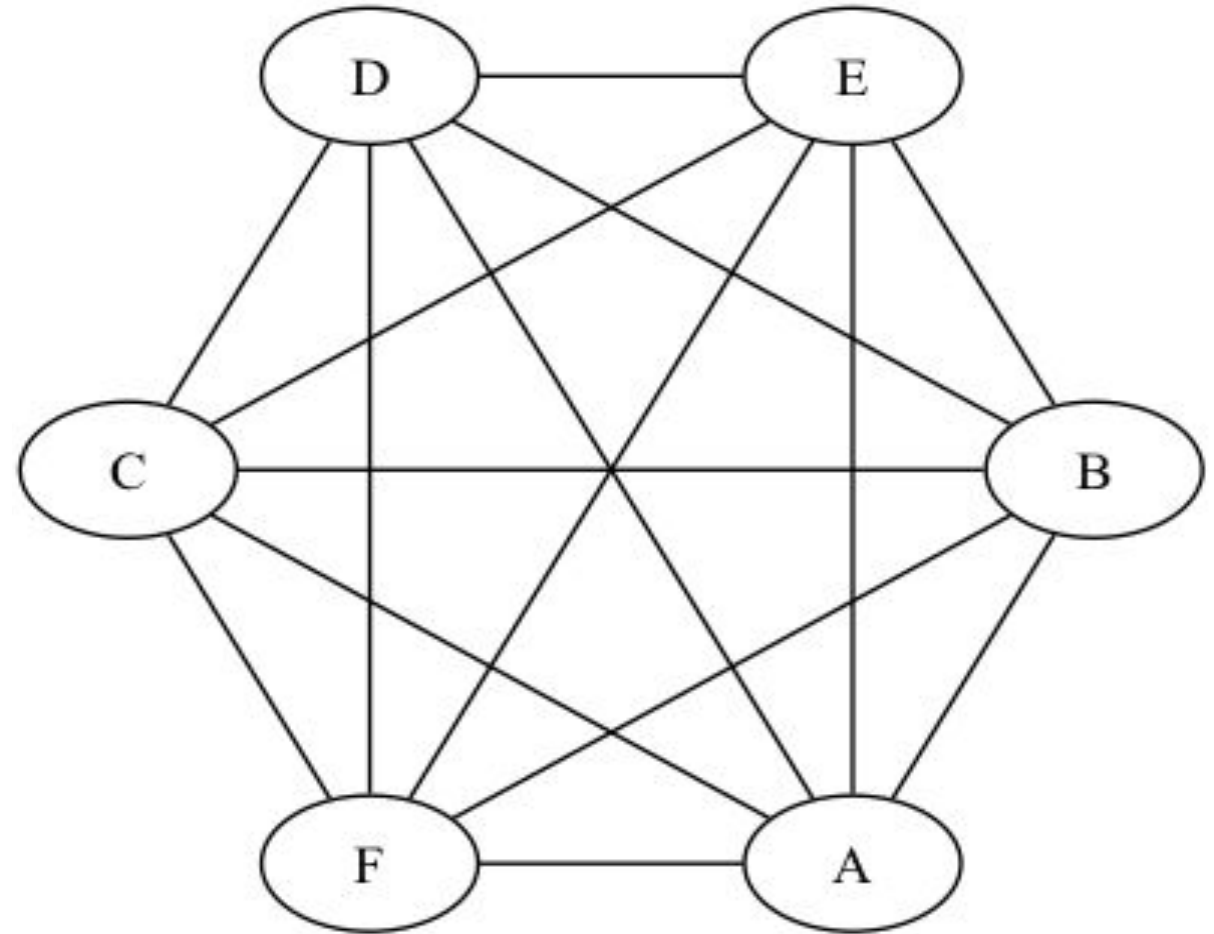
25,000,000+
Authentications per day

9.2
BILLION
TIMES



What is a federation?

- Collection of entities with common aims
 - Seamless authentication of users
 - Reducing friction for users
 - Widening access to services
- Common rulebook and framework for interoperability
- Robust frameworks for interoperability



Single Sign On: What has 20+ years of development got us?

- A cornucopia of standards (protocols, schema etc)
- Mostly consigned *Single Source of Sign On* to history
- A huge deployment base of SAML compliant services
- Various thriving ecosystems of resources
- Some walled-gardens (with or without gates)
- Organisational centralisation of authentication services has
 - Driven MFA adoption and improved the associated user experience
 - Laid the foundation for further improvements
 - Improved organisational security posture



Why should I care?



- Seamless access to resources for students, researchers, and other staff
- Student discounts
- Reduced *friction*

Why should I care? (2)



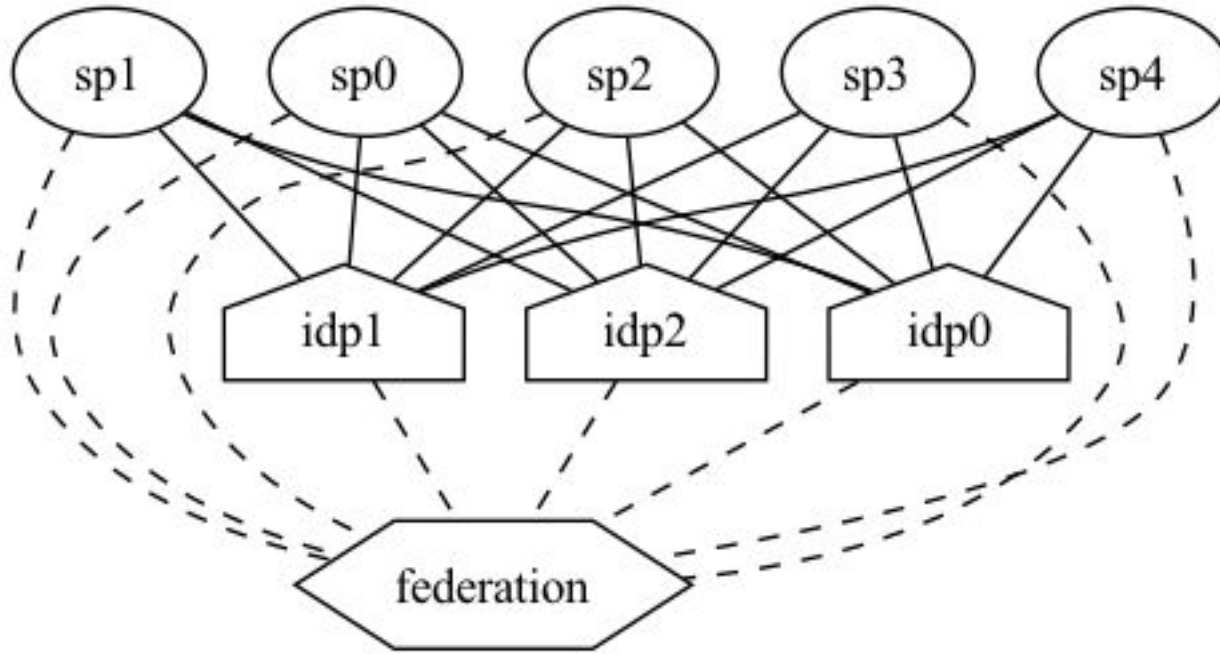
For Home organisations

- Reduced security attack surface
- Less Authentication fatigue for users
- Centrally applied controls

For Services

- No need to handle user credentials (less overhead)
- Happier users
- Less user data (less GDPR requirements)

Federation Reality in the UK



- Full mesh federation
- Some are “Hub & Spoke”
- Interfederation via eduGAIN
- Don't need to worry about most of this

Identity federations



A common identity layer



Requirements

- Protocol support
- Open Source vs Commercial vs Hybrid?
- Self-hosted or *Cloud*?
- Level of customisation
- Integration with existing services
- Support options

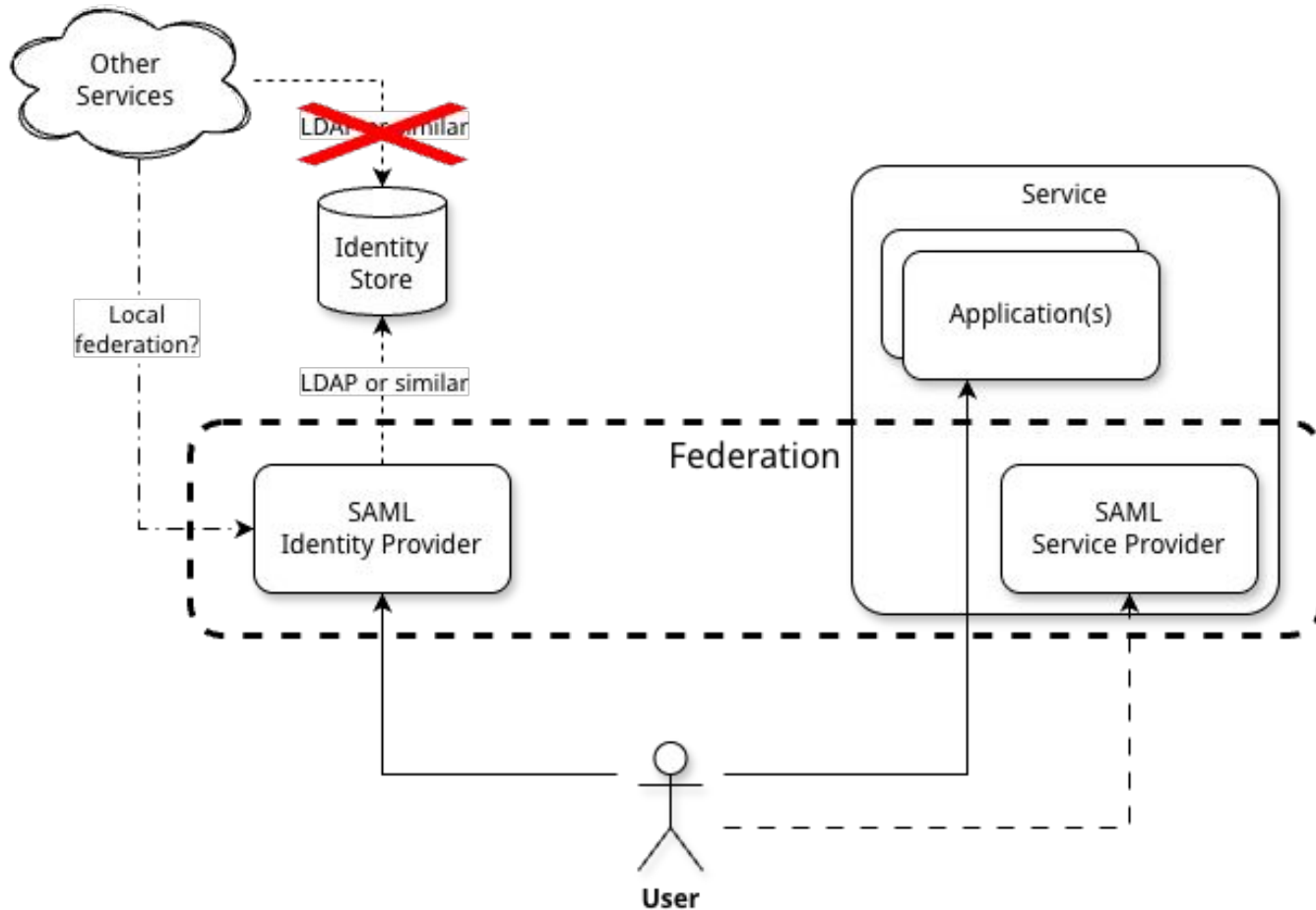
Federation participation options

- ~~Roll your own~~
- Self-host
- Self-hosted proxy
- Get help self-hosting
- Outsource proxy
- Outsource

Roll your own



Self host

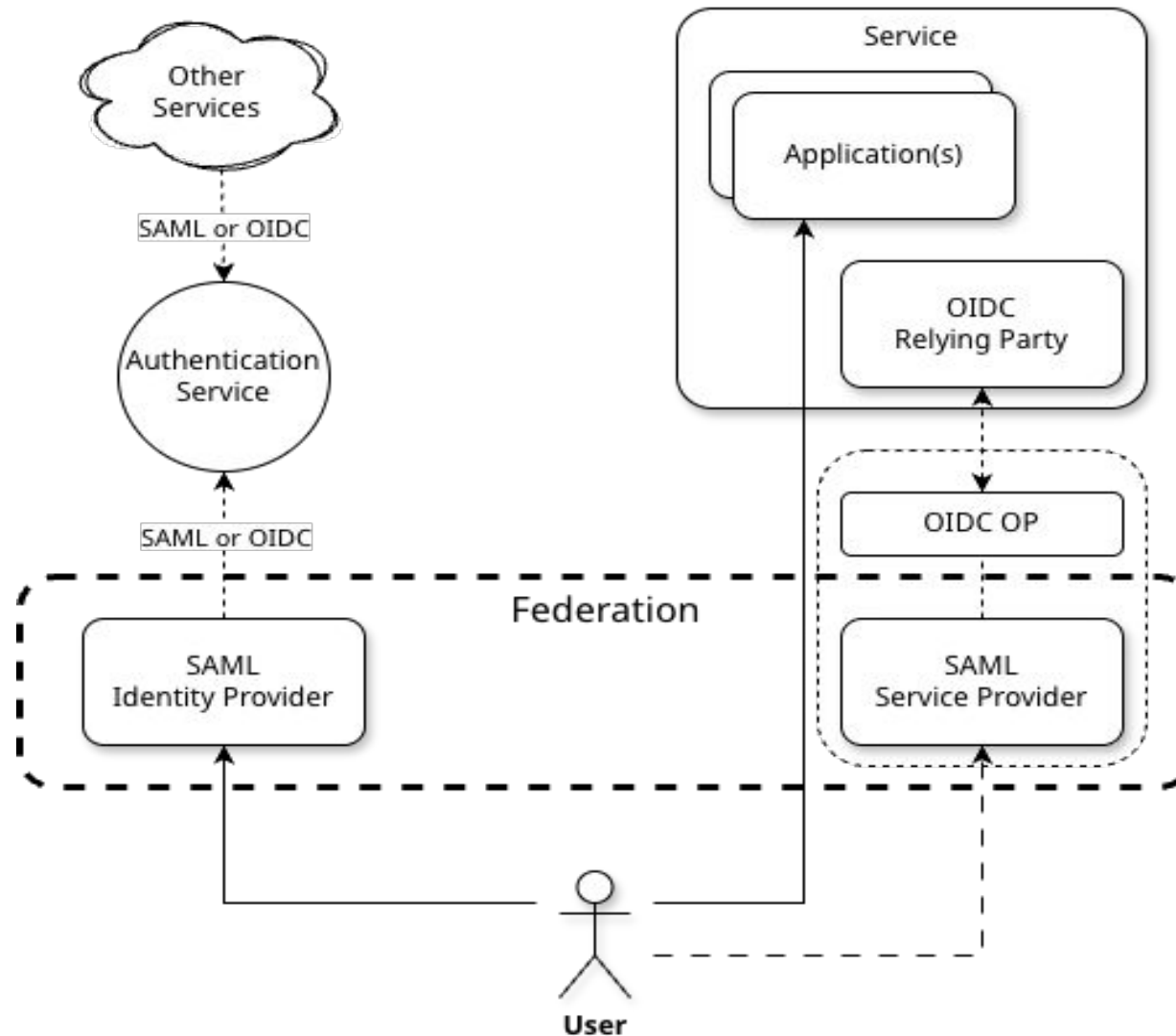


- Shibboleth Identity Provider
- Shibboleth Service Provider
- SimpleSAMLphp
- Other options may be available depending on deployment architecture

Software selection

- Not all software is created equal
- SAML is a huge specification (set of specifications)
- Many implementations do not implement enough to be compatible
 - Cryptography
 - Trust management
 - Protocol support
 - Discovery
- See also:
 - UK Federation Technical Recommendations for Participants (<https://docs.ukfederation.org.uk/trp/>)
 - SAML V2.0 Deployment Profile for Federation Interoperability (<https://kantarainitiative.github.io/SAMLprofiles/saml2int.html>)

Self host with proxy



Get help with Self-Hosting

ukfederation.org.uk/content/Documents/3rdPartySupport

Organisations offering support to inst

The following UK federation members have informed the federation operator cannot comment on their quality or suitability. Considering using a service must satisfy themselves, through their own requirements.

Any other organisations offering appropriate services who are not UK federation members can be found on the federation [helpdesk](#) .

- [Jisc](#) 
 - Jisc provides a [consultancy service](#)  for both Shibboleth and OpenAthens. Activities include installation, upgrade and sustainability advice and planning.
 - [OpenAthens](#)  (a Jisc enterprise) provides support to member countries
- [Overt Software Solutions](#) 
- [Highwire](#) 
- [Primary Technology](#) 
- [9Star Research](#) 
- [Digital Identity](#) 
- [Atypon Systems Incorporated](#) 
- [LibLynx](#) 
- [IDM Integration](#) 
- [ProofID](#) 
- [Essington Computer Consultancy](#) 
- [Sirius OpenSource](#) 

~~Outsource~~ Put it in the cloud

- Outsource what?
- To what extent?
- To whom?
- On what basis?
- Where does your data come from (and where does it go?)
- How does it get there?
- Exit strategy?
- Audit/security testing reports?
- Normal service review cycle...



Federation participation (again)

- ~~Roll your own~~
- Self-host
- Self-hosted proxy
- Get help self-hosting
- Outsource proxy
- Outsource

Future considerations

- Longevity of SAML
 - Post-quantum cryptography
 - Other challenges...?
- Coalescing around vendors
 - Entra/Google/Okta/Auth0...
- Other protocols
 - OpenID Connect?
 - OpenID Federation





Thank you

Any questions?