



**National Federated  
Compute Services**  
NetworkPlus

**Autumn Conference  
22-23 September 2025**

# **Federated IAM for existing infrastructures**

**Stephen Booth**



**Project will explore a bottom-up approach to Identity and Access Management federation growing incrementally and organically out of the existing landscape.**





# Challenges and opportunities

- Diversity of approach and technology stack
  - Existing community definitions in variety of places: Institutions, Facilities, existing federations
  - Established expectations from existing users.
- Existing IAM solutions use industry standard protocols e.g. SAML/OIDC
  - AARC blueprint provides flexible federation architecture to work towards
  - Can look for requirements and use-cases from existing user base.



# The project

## Project staffing from EPCC

- Community building
- Requirement gathering; Both from existing users and existing service operators.
- Exploratory investigations.



# Initial thoughts – group exchange

Existing communities could have definitions in lots of places

- Home institutions, GitHub, HPC centers.
- Would be useful if communities could re-use these definitions elsewhere without needing to re-create them manually.
- Export, distribution and consumption of group and role information (ie AARC-G069 and AARC-G003)
- How easy is it to add support for these kind of operations into existing software and processes?



# Initial thoughts – offline access

Users have an impact even when not logged in

- Provisioned accounts,
- Stored data,
- long running processes/VMs/Containers

Academics move jobs/institutions quite frequently.

- Identity federation helps with this, as information updates whenever user logs in via the federation.
- What if they don't log-in?
- Many sites require users to check-in regularly.



# Initial thoughts – offline access

Would be better user experience if service providers could access information without login

- OpenID Connect can support offline access (BS ISO/IEC 26131:2024 - Section 11) this uses refresh tokens so is consented, revokable and would work with pairwise-ids.
- SAML has attribute servers but without a built-in consent/revoke attribute release needs more negotiation.