Image © STFC Alan Ford

IRIS IAM

Federated Identity Management for IRIS

Thomas Dack

But what is IRIS?

- e**I**nfrastructure for **R**esearch and **I**nnovation for **S**TFC
- Collaboration between **Science Activities** and **Provider Entities**
  - Driven by the physics communities supported by UKRI STFC
- A coordinating body for the provision of STFC eInfrastructure
- IRIS does not run infrastructure **directly**
  - Commissions deployment of resources available to all science activities
- IRIS 4x4 is a capital project coordinated by IRIS
  - £4 million per year for 4 years
  - No money for operations
  - Can issue grants for equipment and grants to make things
    - Such as the IRIS IAM
- Identity management is required for IRIS resources to function as a coherent infrastructure

Science and Technology Facilities Council

IRIS Partner Examples

- IRIS Provider Entity examples:
  - STFC Scientific Computing Department
  - The Hartree Centre
  - The Ada Lovelace Centre (SLC)
  - DiRAC [HPC]
  - GridPP [HTC]
  - The DLS Computing Department
  - CCFE computing
- IRIS Science Activity examples:
  - ALMA
  - ATLAS
  - CCFE
  - CLF
  - CMS
  - CTA
  - DLS
  - DUNE
  - eMERLIN
  - EUCLID
  - GAIA
  - ISIS
  - LHCb
  - LIGO
  - LSST
  - Lux-Zepelin
  - SKA

Science and Technology Facilities Council

IRIS Background

- Need some common elements to support these communities working together:
  - Policy and Trust Framework
  - ***Identity Management***
  - Resource Accounting
  - Monitoring

Science and Technology Facilities Council

The IRIS IAM

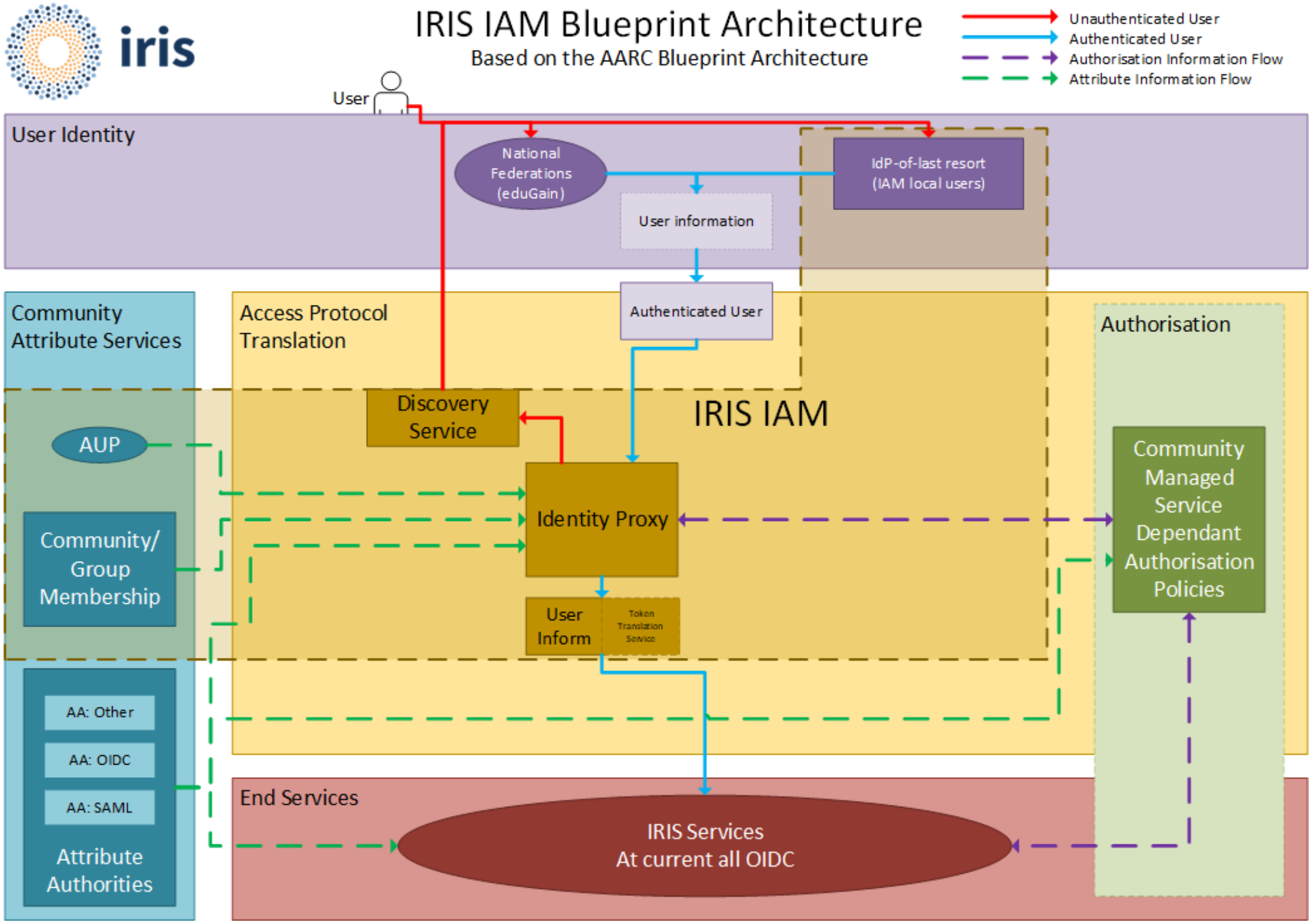
- INDIGO IAM selected for use due to existing capabilities and support
- Aims of the IRIS IAM:
  - Provide users with a consistent authentication experience across IRIS services
  - Provide science communities with central authorization through group management capability
- Observer in AEGIS, active participant in FIM4R

Current Status of the IRIS IAM

- Production standard service based on AARC blueprint
  - Primary authentication a number of IRIS services, including Accounting Portal, Dynafed, MISP Security Portal and OpenStack Clouds
  - Primary means of authorization for IRIS Users within the STFC SCD Cloud
- Small team supporting the service development and operations
  - Currently looking to expand effort in order to better serve community
- Close liaison with IRIS Policy and Trust Framework
  - Ensure that the IAM follows collaboration polices and policies reflect what is possible
  - additionally this is part of an effort to pull together all our experience in identity management, policy and operational security that David will mention later
- Testing IdP-of-last-resort usage with select science communities

IRIS IAM: AARC Blueprint based

- Federated Identities via eduGAIN
- SIRTFI compliant with REFEDS status asserted
- GÉANT COC compliant



Science and Technology Facilities Council

Challenges

- How to provide access to services which operate only over command line
- Assurance for users who do not have an eduGAIN IdP
  - Using the IRIS IAM as an IdP-of-last-resort
  - How best to ensure a registration approvals follow security policies
- Community and Client Buy In
  - The service is in production and serves some IRIS communities
  - Slow uptake from others – have a good service, but how to convince people it’s better than what they’ve got

Next Steps

- Integration of more IRIS services and communities
  - Including particular focus on Command Line services
- Investigating moving to a Kubernetes based deployment to support future growth
- Deploy instances of IAM to support specific communities within IRIS, allowing them more control over delegation and registration
- Adoption of FITSM
  - Service is operating fine, but adoption of FITSM would help with sustainability
- Adoption and Migration of INDIGO IAM 2.0 when available
  - Improved multi-tenancy support

Science and
Technology
Facilities Council

Questions?

UKRI Science and Technology Facilities Council

Thank you

Science and Technology Facilities Council @STFC_matters Science and Technology Facilities Council