Science and Technology Facilities Council

AAI and Security

David Crooks
david.crooks@stfc.ac.uk

IRIS Collaboration Meeting
November 2020

Science and Technology Facilities Council

iris

Topics

1 AAI

2 Security

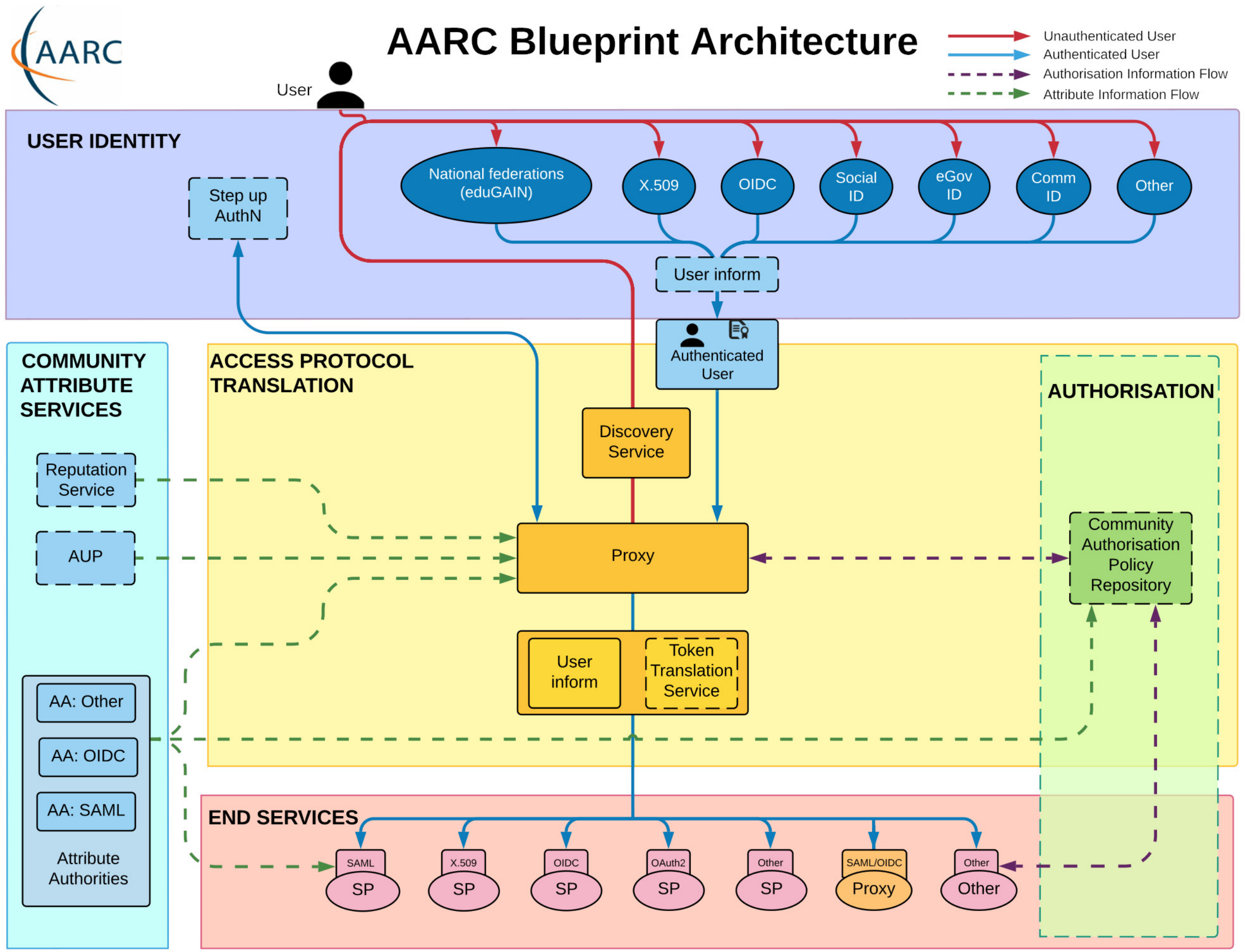
3 Distributed Research Trust and Security

AAI and Security

- Focus on our high level requirements and our current status

- Identity Management
  - Authentication of our users with an appropriate level of assurance
  - Coupled with appropriate service authorisation mechanisms
- Policy
  - Rules of engagement and expectations for participation in the infrastructure
- Operational security
  - Supporting the prevention of incidents and coordinating incident response

AARC Blueprint Architecture



Science and Technology Facilities Council

iris

Identity Management: IRIS-IAM

- IRIS-IAM is very successfully operating as an AARC Blueprint Architecture identity proxy

- Part of UK Access Management Federation and eduGAIN
  - Provides access to global network of identity providers (IdPs)
  - Authentication by users' home institutions

- Capability to act as Identity Proxy of last resort
  - For users that don't have a suitable eduGAIN Identity Provider

IRIS-IAM

- IRIS-IAM now backs a number of services, including
  - IRIS Accounting Portal
  - OpenStack Clouds
  - JupyterHub
- In development
  - Rucio
  - Dynafed
  - S3/CEPH
- Development of auth workflow for command line clients
  - DiRAC

IRIS-IAM: Research lifecycles

- With these pieces in place or in development, consider broad picture
  - Complete research lifecycles
  - Prototyping, processing, data access, result retrieval
  - Important to demonstrate complete workflow

- Development of IRIS-IAM takes place in the context of development of token-based federated authentication both in the UK and for other projects
  - WLCG
  - Opportunity to demonstrate complete exemplars

Policy

- Policy underpins all other security activity
- Acts to engender trust both within an infrastructure, but also with neighbours
  - AARC PDK is an excellent starting point for this
- IRIS Infrastructure Policy now approved
  - Opens door to other policies
- Review of AUP and Privacy Notice in light of approval
  - IRIS-IAM users sign AUP
  - Present AUP to other users
    - Work with services to facilitate this

Policy

- Next policies in preparation
    - Service Operations Security Policy
    - Community Security Policy

- In draft, work in collaboration with WISE towards new PDK templates
    - Consultation within IRIS to best match our topology

Assurance

- How well do we need to assure the identities of our users?
  - Depends on services
  - Informs requirements on vetting processes of users
  - Couple to identity management workflows

- Risk assessment for IRIS to inform this discussion
  - In parallel to similar work being done for WLCG

Operational Security

- Operating a secure infrastructure
  - Depends on and works alongside Identity Management and Policy
- Capabilities and processes
  - Risk management
  - Patching
  - Vulnerability management
  - Security tools and monitoring
  - Access controls
  - Traceability (who, what, where, when, how)
  - Incident response

IRIS Operational Security capability

- IRIS Security Team
  - Membership from GridPP, Cloud, HPC
  - Common understanding of IRIS technology stacks
  - All active members agree to CSIRT Code of Practice
  - Share sensitive information appropriately within team
  - Key contact point with other CSIRTs
    - Jisc/Institutions/Other CSIRTs
- Communication channels
- Security contact information
  - GOCDB

IRIS Operational Security capability

- Next steps
  - Communications challenge
  - Additional workshops and training materials
  - Build on access to threat intelligence for IRIS sites

- In the future
  - Service security challenge
  - Evaluate our procedures
  - IRIS-IAM is a vital part of this process
    - Also backs MISP threat intelligence

Distributed Research Trust and Security

- Within STFC in SCD and PPD we have people working on all areas of distributed security
  - Security Coordination
  - Identity Management
  - Trust and Policy
  - Operational Security
- Collectively many years of experience
  - National and international contacts
- Working to bring together a new team representing all these areas
  - Single point of contact to support communities in a distributed federated landscape

Science and
Technology
Facilities Council

Questions?