
Image © STFC Alan Ford

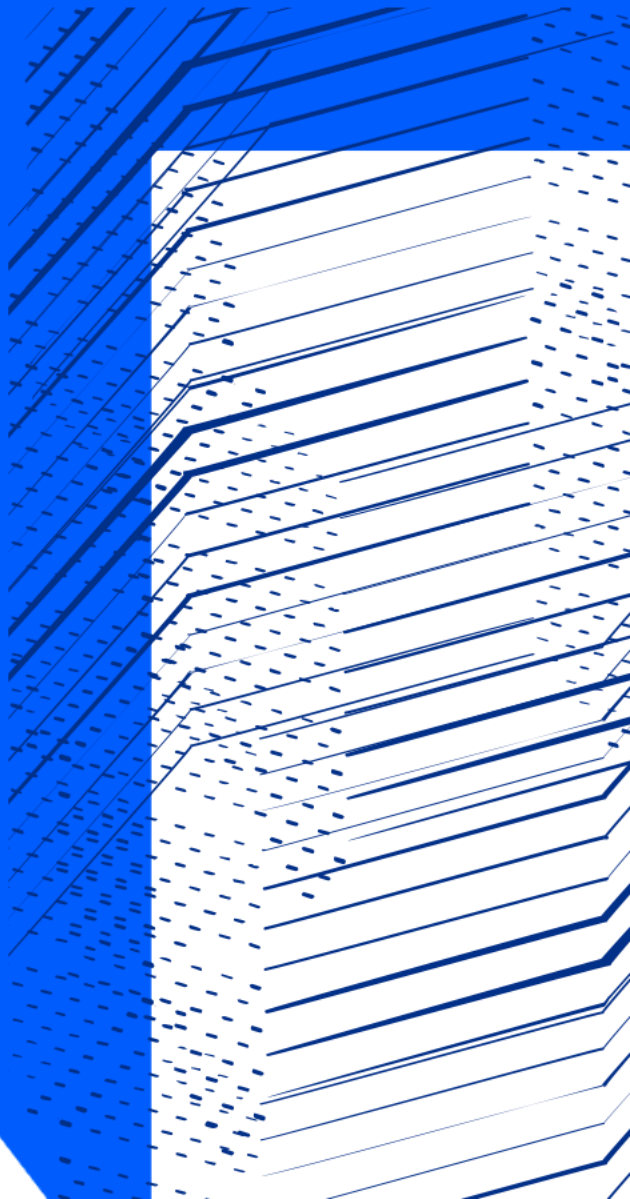
Science and Technology Facilities Council

iris

# IRIS-IAM

Dec’ 19  Status Update

Tom Dack



# Agenda

## 1 Project Overview

An overview of the IRIS identity project and the INDIGO IAM application it utilises.

## 2 Status Update

Update as to the current status and progress of the IRIS IAM digital asset, including challenges and issues encountered.

## 3 Next Steps

The next steps and goals for the Identity Project in 2020.




Science and Technology Facilities Council

Science and Technology Facilities Council

# IRIS IAM Overview

# IRIS IAM Overview

## INDIGO Identity and Access Management

This is the service utilised by IRIS as its AAI solution

- Initially developed as part of INDIGO DataCloud by INFN
- Supported through EOSC pilot and EOSC hub projects
- Selected for use due to existing capabilities and support
  - Previous experience with the IAM within the department
  - Has been selected as the AAI solution for the WLCG authorization project
- IAM provides most required capabilities in its current version

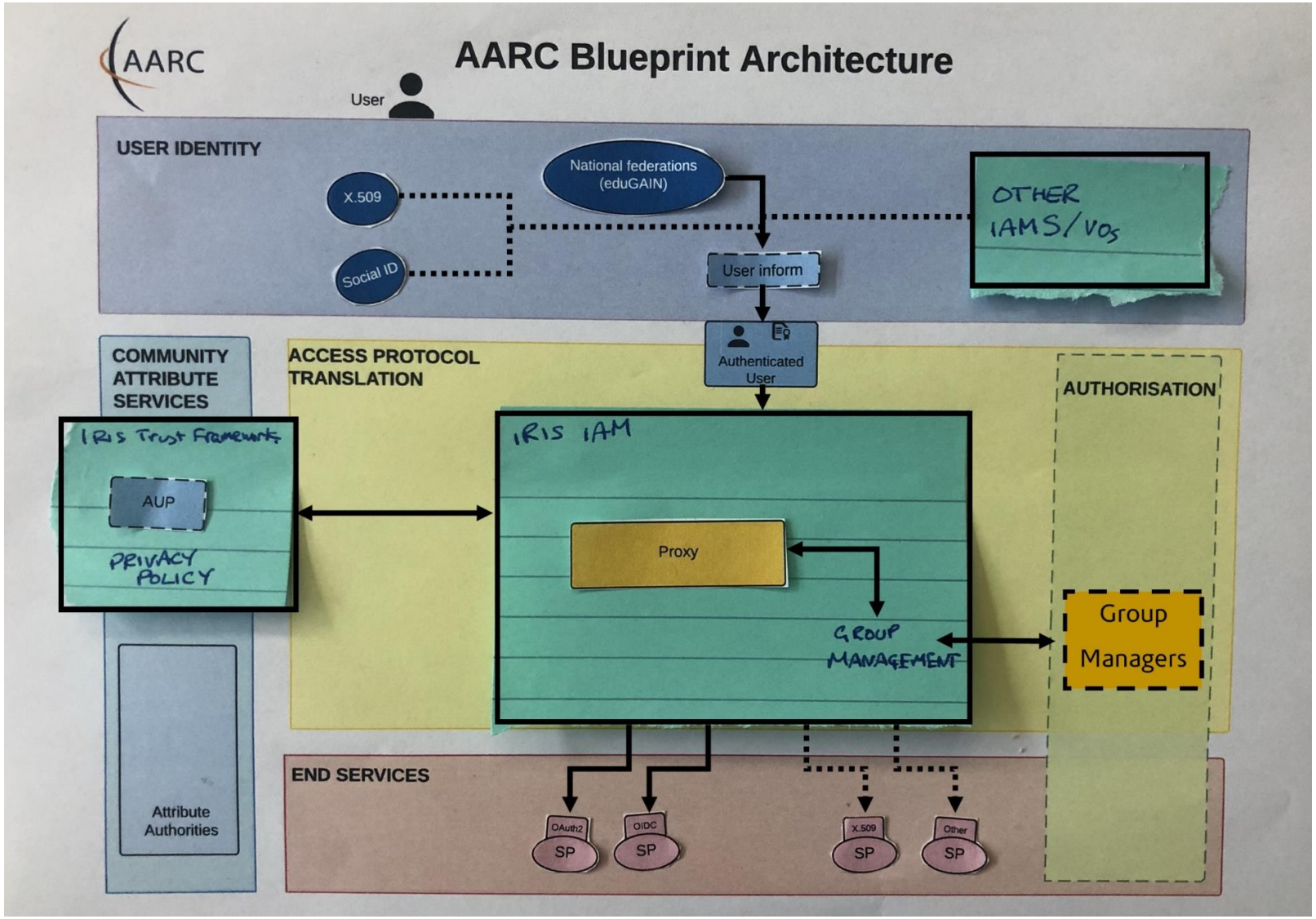
Science and Technology Facilities Council

iris

# IRIS IAM Overview

## IRIS IAM Blueprint

- The IAM service takes a user identity and maps the required authorization to it.
- This then allows access to IRIS end services behind IAM




Science and Technology Facilities Council

iris

# The IRIS Identity Project

## Implementation

- Service is online and available, hosted at: https://iris-iam.stfc.ac.uk
- IAM deployed via Docker
- Service is hosted on a VM managed by the RAL Tier 1
  - host fully configured using Tier 1 configuration management (aquilon)
- Utilises existing service tools ran within SCD
  - RequestTracker for ticketing
  - Icinga for service health monitoring
  - Telegraf monitoring for metrics & usage
  - IAM backed database managed by Database Services

Science and Technology Facilities Council

iris

# Status Update

# Current Status

## Federation Membership

- IAM has been successfully registered as a service provider within the UK Access Management Federation
  - This enables registration and authentication through any IdP which is an eduGAIN member
- Asserting SIRTFI compliance and REFEDS Research and Scholarship entity status
- Compliance with GÉANT Data Protection Code of Conduct
- IAM has its own SAML implementation, meaning we do not need to run Shibboleth

## Glossary:

SIRTFI:
Security Incident Response Trust Framework for Federated Identity

REFEDS:
Research and Education FEDerations group

Science and Technology Facilities Council

iris

# Current Status

## Policy Work

- working closely with the IRIS Trust Framework digital asset
  - IRIS policy and IRIS IAM capability closely interconnected, and IAM procedures and processes need to follow these policies
- Draft privacy and acceptable use policies are in place
  - AUP is hosted at https://iris-iam.stfc.ac.uk/aup/
  - Privacy Policy hosted at https://iris-iam.stfc.ac.uk/privacypolicy/
- A draft group management procedure has been written and is being revised to align to policy

# Current Status

## Access to Services

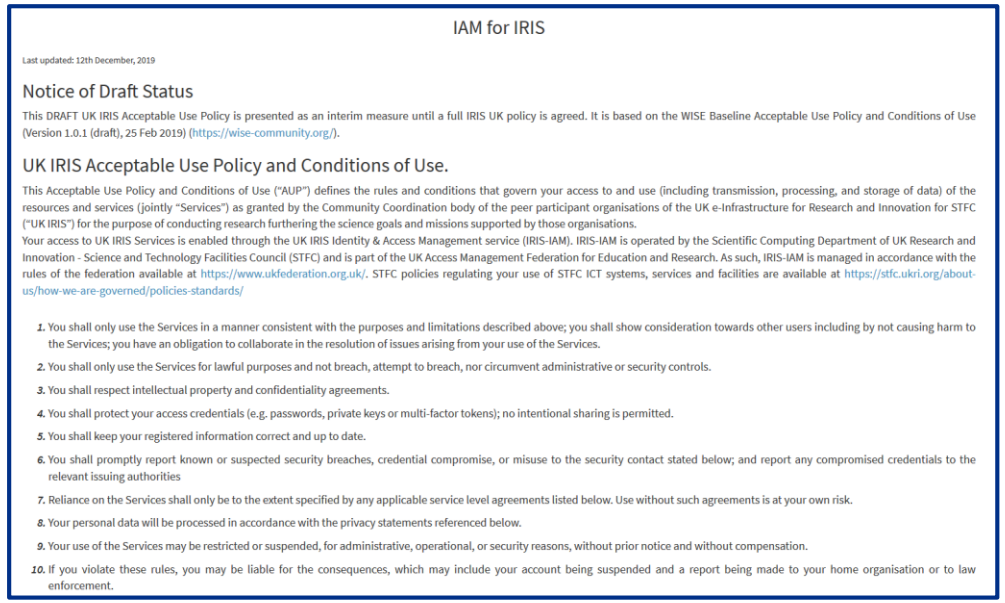
- IAM can provide authorized access to SCD Cloud, Cambridge IRIS Openstack and IRIS Accounting Portal Beta
  - Soft launched with SCD OpenStack and IRIS users (CCFE primarily)
- Development work underway for access to Dynafed (storage)
- Working on implementing test connection to Rucio

# Current Status

## Challenges and Issues

- Acceptable usage policy formatting
  - AUP implementation is a single line of text – no formatting
  - Mitigated hosting AUP at a fixed URL
  - IAM v1.6.0. will include a direct link to the AUP, rather than the text field currently used

- Operational funding questions
  - Options and possibilities are being discussed
  - IAM was recently reviewed by SCD services committee



IAM for IRIS

Last updated: 12th December, 2019

Notice of Draft Status

This DRAFT UK IRIS Acceptable Use Policy is presented as an interim measure until a full IRIS UK policy is agreed. It is based on the WISE Baseline Acceptable Use Policy and Conditions of Use (Version 1.0.1 (draft), 25 Feb 2019) (https://wise-community.org/).

UK IRIS Acceptable Use Policy and Conditions of Use.

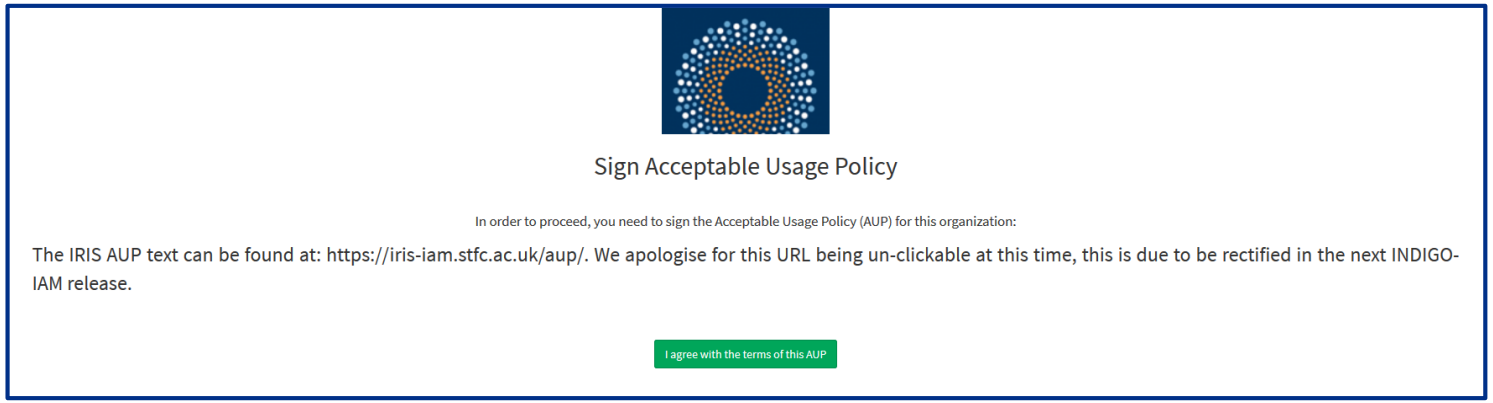
This Acceptable Use Policy and Conditions of Use ("AUP") defines the rules and conditions that govern your access to and use (including transmission, processing, and storage of data) of the resources and services (jointly "Services") as granted by the Community Coordination body of the peer participant organisations of the UK e-Infrastructure for Research and Innovation for STFC ("UK IRIS") for the purpose of conducting research furthering the science goals and missions supported by those organisations.
Your access to UK IRIS Services is enabled through the UK IRIS Identity & Access Management service (IRIS-IAM). IRIS-IAM is operated by the Scientific Computing Department of UK Research and Innovation - Science and Technology Facilities Council (STFC) and is part of the UK Access Management Federation for Education and Research. As such, IRIS-IAM is managed in accordance with the rules of the federation available at https://www.ukfederation.org.uk/. STFC policies regulating your use of STFC ICT systems, services and facilities are available at https://stfc.ukri.org/about-us/how-we-are-governed/policies-standards/

1. You shall only use the Services in a manner consistent with the purposes and limitations described above; you shall show consideration towards other users including by not causing harm to the Services; you have an obligation to collaborate in the resolution of issues arising from your use of the Services.
2. You shall only use the Services for lawful purposes and not breach, attempt to breach, nor circumvent administrative or security controls.
3. You shall respect intellectual property and confidentiality agreements.
4. You shall protect your access credentials (e.g. passwords, private keys or multi-factor tokens); no intentional sharing is permitted.
5. You shall keep your registered information correct and up to date.
6. You shall promptly report known or suspected security breaches, credential compromise, or misuse to the security contact stated below; and report any compromised credentials to the relevant issuing authorities
7. Reliance on the Services shall only be to the extent specified by any applicable service level agreements listed below. Use without such agreements is at your own risk.
8. Your personal data will be processed in accordance with the privacy statements referenced below.
9. Your use of the Services may be restricted or suspended, for administrative, operational, or security reasons, without prior notice and without compensation.
10. If you violate these rules, you may be liable for the consequences, which may include your account being suspended and a report being made to your home organisation or to law enforcement.

**Acceptable Usage Policy (AUP)**

The IRIS AUP text can be found at: https://iris-iam.stfc.ac.uk/aup/. We apologise for this URL being un-clickable at this time, this is due to be rectified in the next INDIGO-IAM release.

By submitting this registration request, you agree to the terms of this organization Acceptable Usage Policy (AUP).



Sign Acceptable Usage Policy

In order to proceed, you need to sign the Acceptable Usage Policy (AUP) for this organization:

The IRIS AUP text can be found at: https://iris-iam.stfc.ac.uk/aup/. We apologise for this URL being un-clickable at this time, this is due to be rectified in the next INDIGO-IAM release.

I agree with the terms of this AUP

Science and Technology Facilities Council

iris

Science and Technology Facilities Council

iris

# Next Steps

# Next Steps

## IAM Deployment

- When available migrate to IAM 2.0 – built on keycloak
- In preparation we are planning to deploy a keycloak test instance in order to prepare for IAM 2.0 release

## Policy and Documentation

- Produce/finalise and circulate IAM user guides, ensuring these follow policy
- Finalise group management process and implement this with IRIS services
  - Some draft documents have been written, but will need to be aligned with outputs from the Trust Framework DA

# Next Steps

## Identify Solutions for running IAM in Production

- Continued investigation for operational funding sources
- Undertake tasks to ensure IAM has the service management systems in place to run as a production service
  - Eg: SLA's, Change Management processes, etc

## On-boarding of IRIS Services

- Ongoing work with other IRIS services
  - Discussions to be had this afternoon to look at which services/DA's can utilise IAM.

## Aim is to have the IAM in a production-ready state by q1 2020

UKRI Science and Technology Facilities Council

iris


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