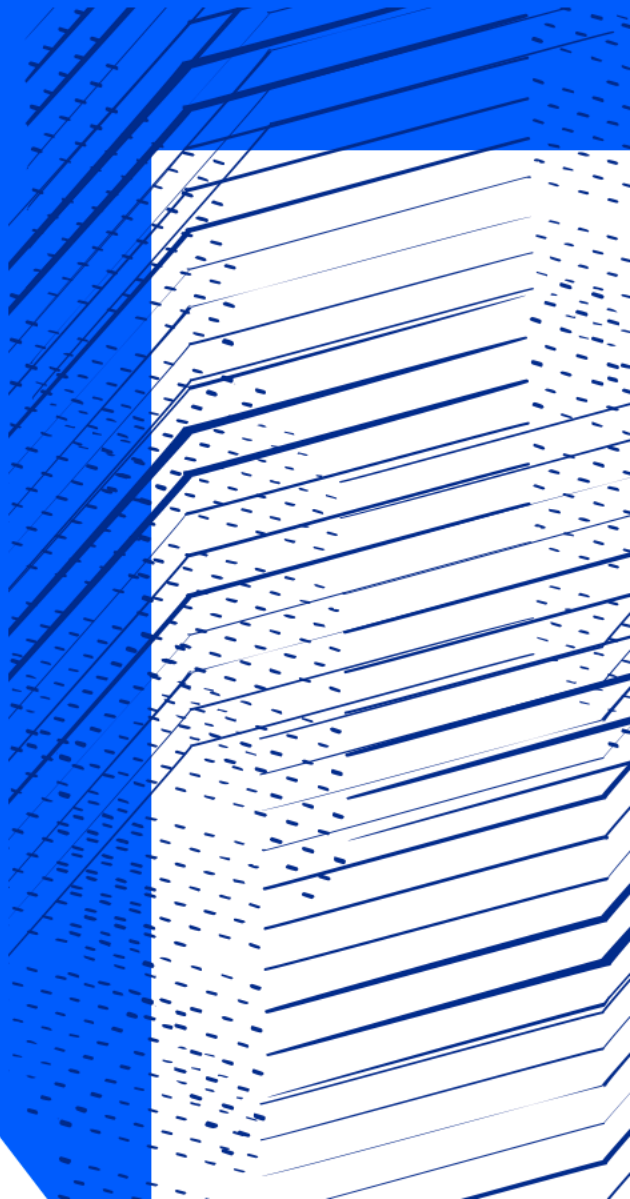
Science and Technology Facilities Council

INDIGO IAM and its Application within Research Communities

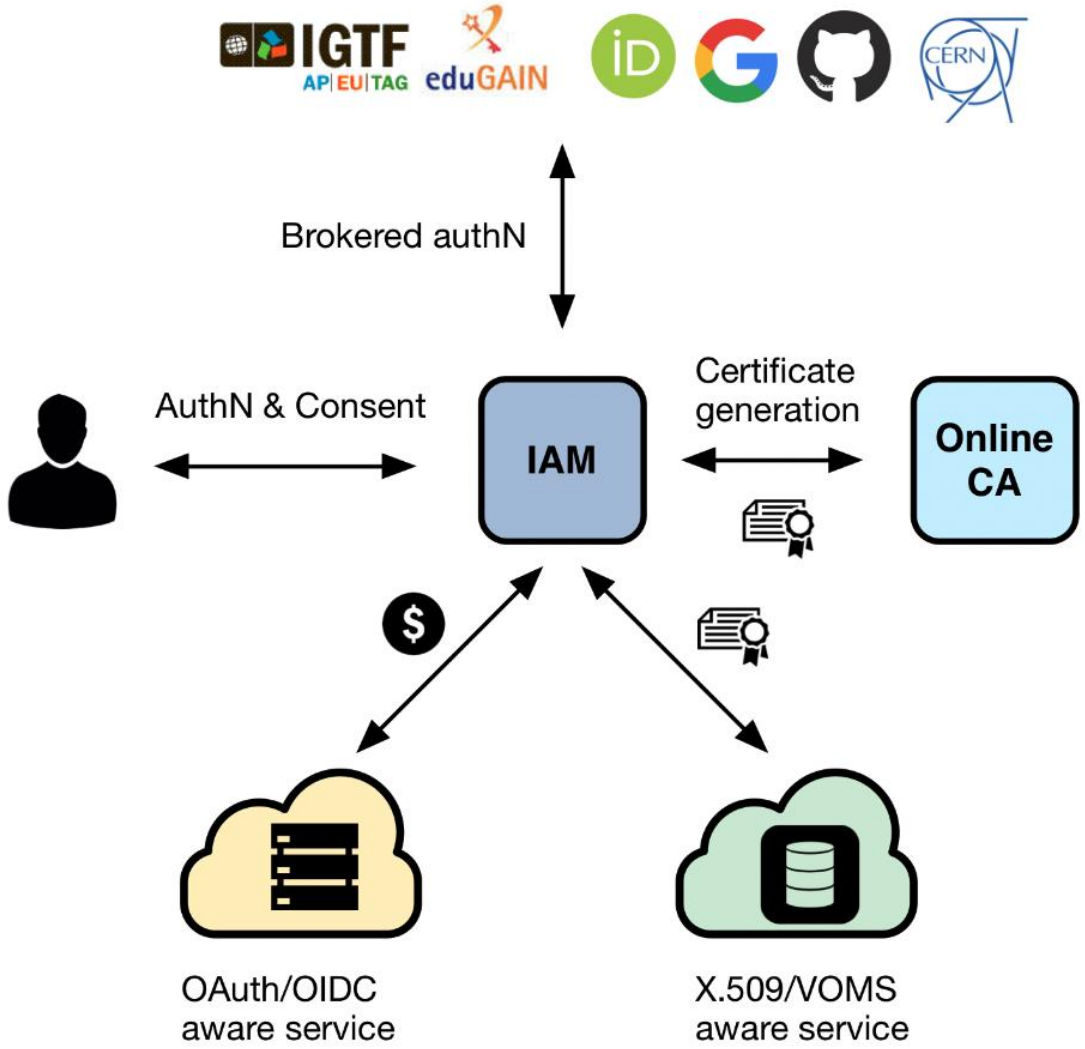
Tom Dack



What is INDIGO IAM

An authentication and authorization service that

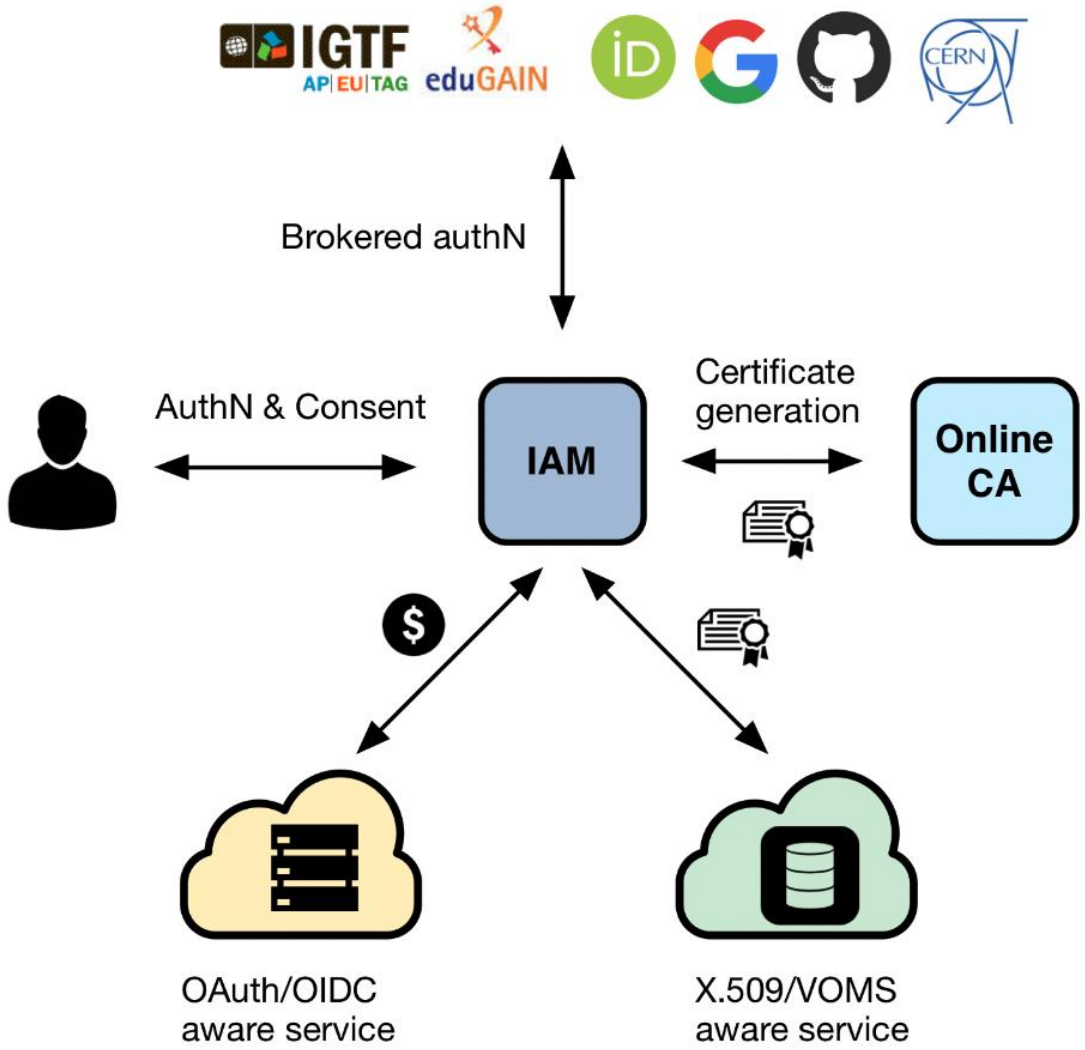
- supports **multiple authentication mechanisms**
- provides users with a **persistent**, **organization scoped** identifier
- exposes **identity information**, **attributes** and **capabilities** to services via **JWT** tokens and standard **OAuth & OpenID Connect** protocols
- can integrate existing **VOMS**-aware services
- supports **Web** and **non-Web access**, delegation and **token renewal**



Science and Technology Facilities Council

What is INDIGO IAM

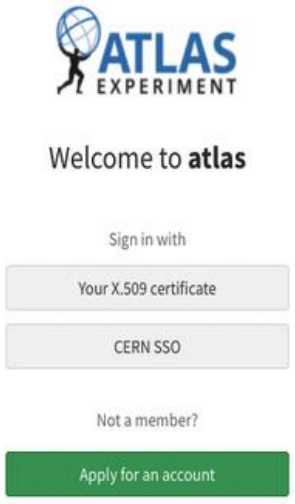
- First developed in the context of the **H2020 INDIGO DataCloud** project
- Sustained by INFN for the foreseeable future
- **Selected by the WLCG management board** to be the core of the future, token-based WLCG AAI
- In use within the **U.K. IRIS community** as their identity-management solution



Science and Technology Facilities Council

WLCG IAM

WLCG IAM - Deployments



https://atlas-auth.web.cern.ch

https://cms-auth.web.cern.ch

https://alice-auth.web.cern.ch

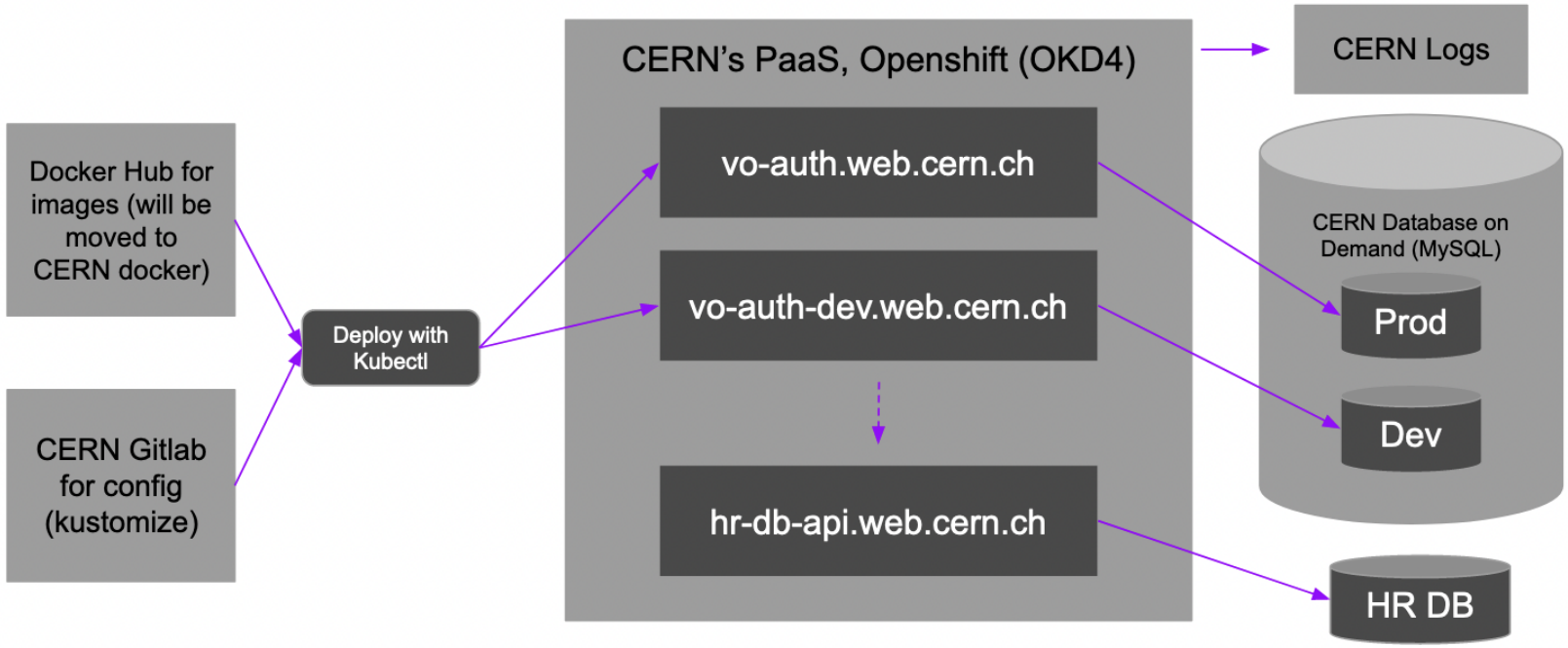
TBC

https://lhcb-auth.web.cern.ch

Science and Technology Facilities Council

WLCG IAM - Infrastructure

- Utilises the CERN shared infrastructure, using standard services and tools
- One project for each VO on CERN Openshift
- Will also have a Dev instance for each VO
- Openshift also hosts an API for interfacing with CERN HR DB
- Logs are pushed to the CERN Logs service, giving Kibana and E-Search
- CERN Database on Demand for backend



Leveraging CERN's infrastructure as far as possible.
Scalable deployment on Openshift.

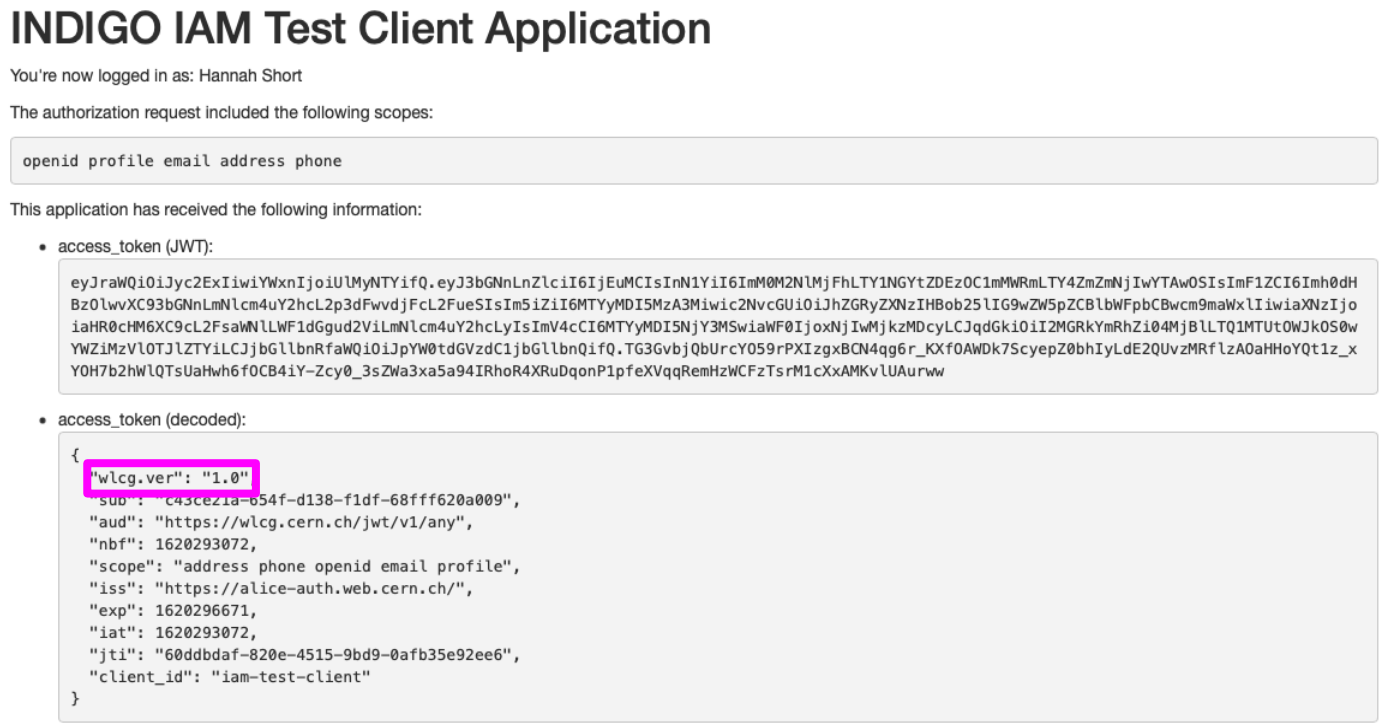
Science and Technology Facilities Council

WLCG IAM - Authentication

- Each of the LHC VOs have two login options
  - CERN SSO
  - Certificate Login
- Expected that a user will register with the CERN SSO and then may add a certificate later
- The CERN SSO ID token is used to validate VO membership
- Additional admin login (username/password) hidden for normal workflows

WLCG Token Schema

- Contains identity and authorisation information from issuer (VO)
  - Groups and/or Capabilities
- Follows the WLCG Token Schema (https://zenodo.org/record/3460258)



INDIGO IAM Test Client Application

You're now logged in as: Hannah Short

The authorization request included the following scopes:

```
openid profile email address phone
```

This application has received the following information:

- access_token (JWT):


```
eyJraWQiOiJyc2ExIiwiYWxnIjoiUlMyNTYifQ.eyJ3bGNnLnZlciI6IjEuMCIsInN1YiI6ImM0M2NlMjFhLTY1NGYtZDEzOC1mMWRmLTY4ZmZmNjIwYTAwOSIsImF1ZCI6Imh0dHBzOlwvXC93bGNnLmNlcm4uY2hcL2p3dFwvdjFcL2FueSIsIm5iZiI6MTYyMDI5MzA3Miwic2NvcGUiOiJhZGRyZXNzIHBob25lIG9wZW5pZCBlbWFpbCBwcm9maWxlIiwiaXNzIjoiaHR0cHM6XC9cL2FsaWNlLWF1dGgud2ViLmNlcm4uY2hcLyIsImV4cCI6MTYyMDI5NjY3MSwiaWF0IjoxNjIwMjkzMDcyLCJqdGkiOiI2MGRkYmRhZi04MjBlLTQ1MTUtOWJkOS0wYWZiMzVlOTJlZTYiLCJjbGllbnRfaWQiOiJpYW0tdGVzdC1jbGllbnQifQ.TG3GvbjQbUrcYO59rPXIzgxBCN4qg6r_KXfOAWDk7ScyepZ0bhIyLdE2QUvzMRflzAOaHHoYQt1z_xYOH7b2hWlQTsUaHwh6fOCB4iY-Zcy0_3sZWa3xa5a94IRhoR4XRuDqonP1pfeXVqqRemHzWCFzTsrM1cXxAMKvlUAurww
```


- access_token (decoded):


```
{
  "wlcg.ver": "1.0"
  "sub": "c43ce21a-654f-d138-f1df-68fff620a009",
  "aud": "https://wlcg.cern.ch/jwt/v1/any",
  "nbf": 1620293072,
  "scope": "address phone openid email profile",
  "iss": "https://alice-auth.web.cern.ch/",
  "exp": 1620296671,
  "iat": 1620293072,
  "jti": "60ddbdaf-820e-4515-9bd9-0afb35e92ee6",
  "client_id": "iam-test-client"
}
```


Example token from the IAM Test Client

Science and Technology Facilities Council

WLCG Token Discovery

- Many tools will rely on tokens being stored in the local environment
- Token discoverability specification v1.0 published https://zenodo.org/record/3937438

If a tool needs to authenticate with a token and does not have out-of-band WLCG Bearer Token Discovery knowledge on which token to use, the following steps to discover a token MUST be taken in sequence, where $ID below denotes the process's effective user ID:

1. If the **BEARER_TOKEN** environment variable is set, then its value is taken to be the token contents.
2. If the **BEARER_TOKEN_FILE** environment variable is set, then its value is interpreted as a filename. The contents of the specified file are taken to be the token contents.
3. If the **XDG_RUNTIME_DIR** environment variable is set1, then take the token from the contents of $XDG_RUNTIME_DIR/bt_u$ID2.
4. Otherwise, take the token from **/tmp/bt_u$ID**

Logic of where to search for (or place) tokens locally

Science and Technology Facilities Council

WLCG IAM – Next Steps

- Complete full development infrastructure
  - Ideally with automatic deployment with Gitlab CI
- High Availablity IAM
- Improvements to support capabilities

IRIS IAM

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

Science and Technology Facilities Council

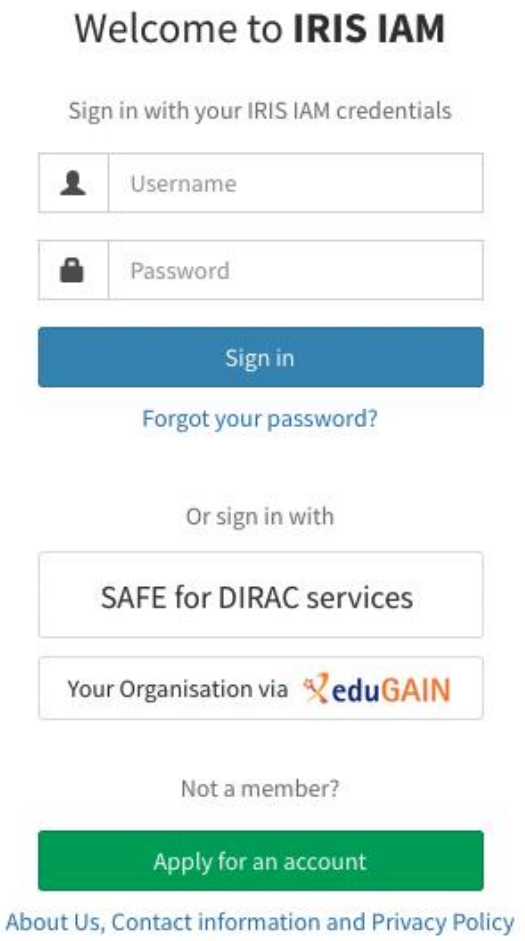
The IRIS IAM

- INDIGO IAM selected for use due to existing capabilities and support
- Multi-tenancy Identity Management Platform – serves multiple IRIS communities
- 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

Science and Technology Facilities Council

Current Status of the IRIS IAM

- Primary authentication a number of IRIS services, including Accounting Portals, IRIS DynaFed (Storage), MISP Security Portal and OpenStack Clouds
- Close liaison with IRIS Policy and Trust Framework
  - Ensure that the IAM follows collaboration polices and policies reflect what is possible



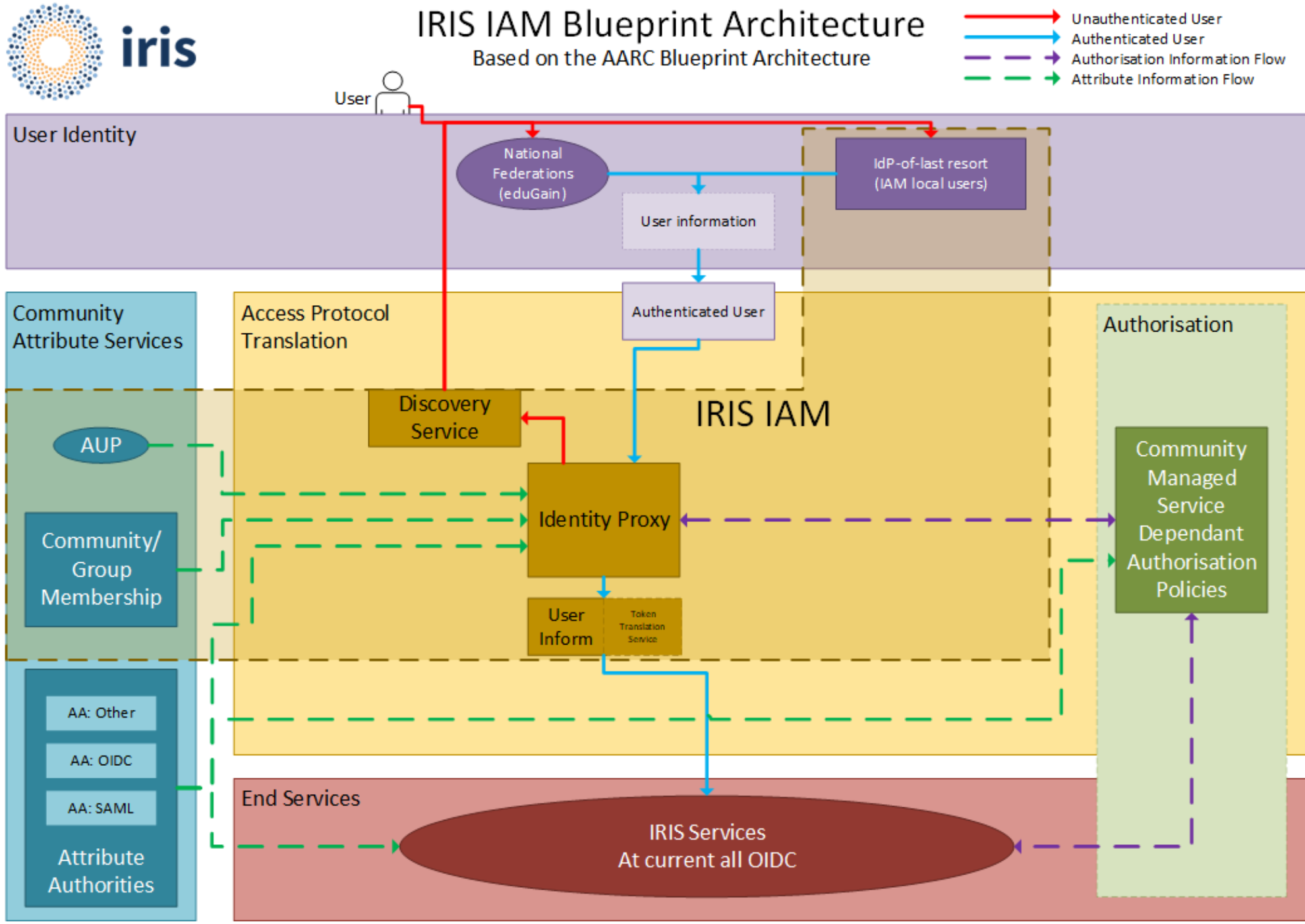
Science and Technology Facilities Council

The IRIS IAM - Authentication

- Remote eduGAIN authentication primary means of account creation
- Offers local credential registration to partners without eduGAIN identities
  - Acting as an IdP of last resort
- Recently added support for registration with SAFE for DiRAC HPC accounts

Science and Technology Facilities Council

IRIS IAM: AARC Blueprint based



Science and Technology Facilities Council

IRIS IAM – Challenges

- How to provide access to services which operate only over command line
  - OAuth Device Code PAM with Group Authorization
  - https://github.com/stfc/pam_oauth2_device
- Assurance for users who do not have an eduGAIN IdP
  - Using the IRIS IAM as an IdP-of-last-resort
  - Deploying community IAM instances which can be used to authenticate to IRIS IAM

IRIS IAM – Next Steps

- High-Availability IAM
  - Distrubuted resilient Database with IRIS partners
  - Front-end failover solution
- IAM community instances
  - Providing user communities with direct user approval control

UKRI Science and Technology Facilities Council

Thank you

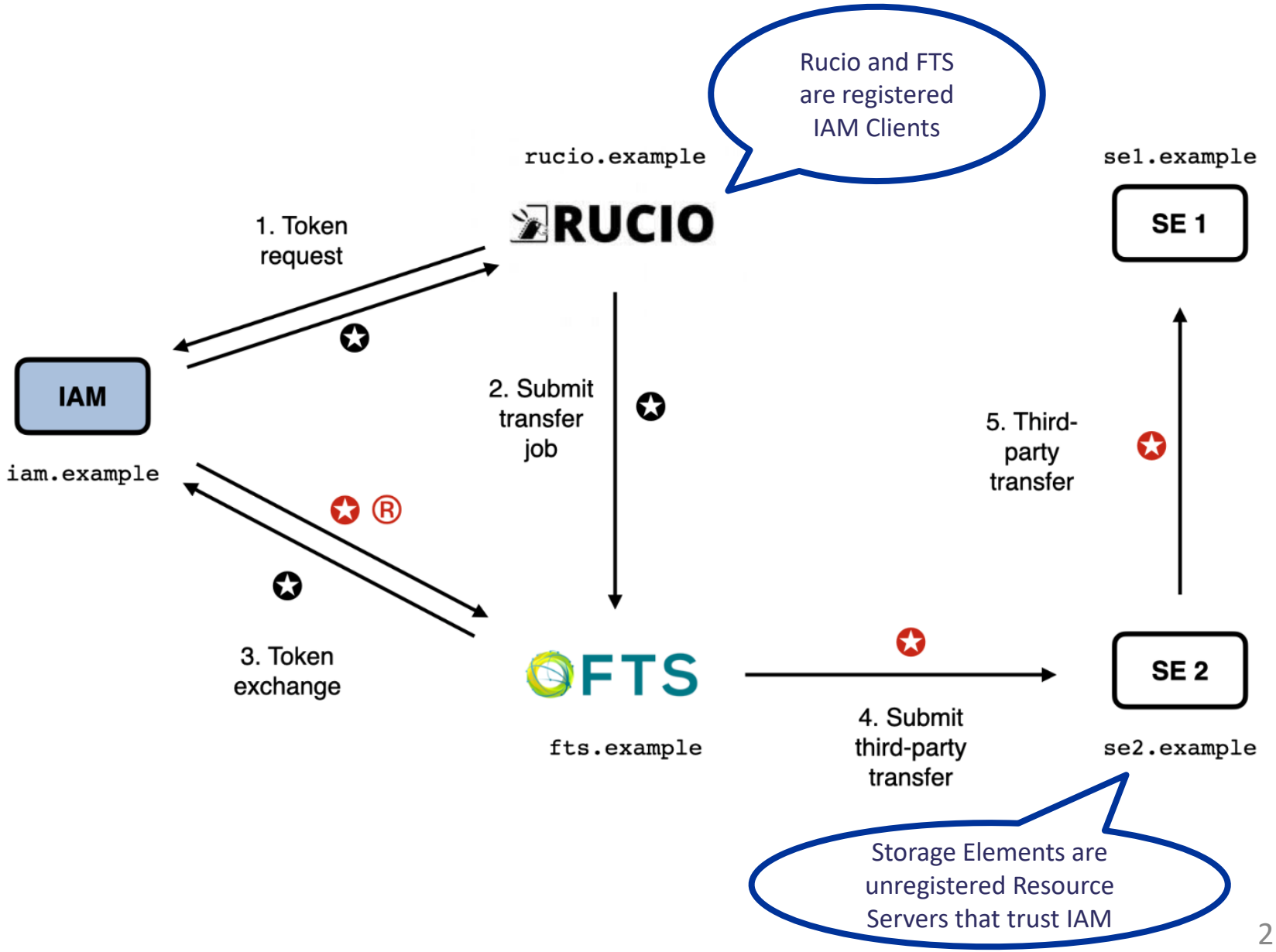
Science and Technology Facilities Council @STFC_matters Science and Technology Facilities Council

Science and
Technology
Facilities Council

Questions?

Rucio-FTS-SEs flow

1. Rucio requests token for FTS from IAM
2. Rucio submits job to FTS and includes token
3. FTS exchanges token for one for target third-party
4. Third-party transfer submitted along with new token
5. Token can be reused among instances of third-party



Science and Technology Facilities Council