Science and
Technology
Facilities Council

Towards Tokens for Research

Token Based Authentication and Authorisation Infrastructure at STFC

Tom Dack,
STFC Scientific Computing

Authentication vs Authorisation

- Authentication
  - *Verifying the identity of a user*
  - *AuthN*
- Authorisation
  - *Controlling what access a specific user has*
  - *AuthZ*

Moving away from User Certificates

- There is a landscape shift away from X.509 user certificates
  - *Security impact if compromised (and frequently compromised)*
  - *Not user friendly*
  - *Mobility issues*
- Shift towards OAuth2 and OpenID Connect (Tokens)
  - *Tokens widely accepted*
  - *Easy to implement – used by major industry players*
  - *Links directly to home institutions*

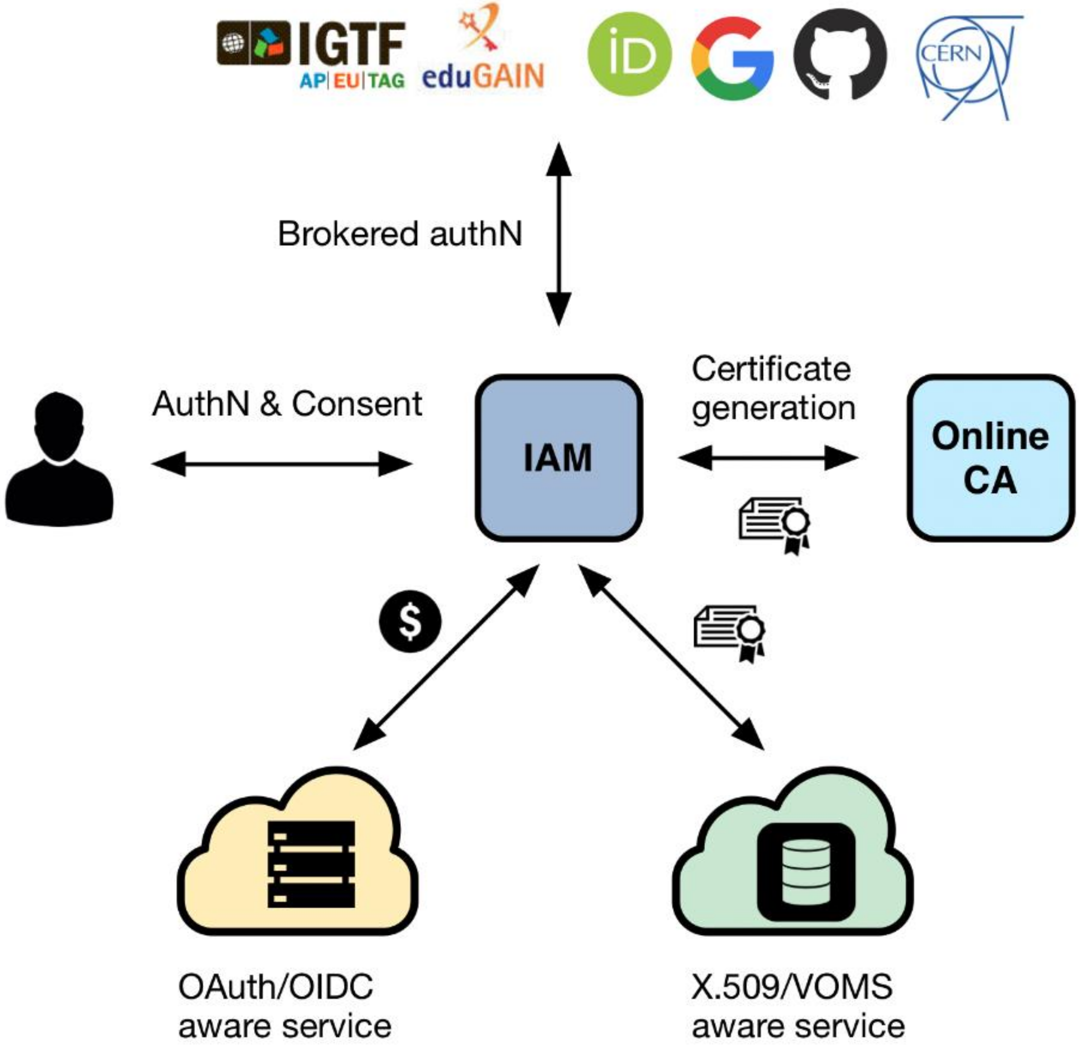
Token based work underway within…

- IRIS
  - *e*_**I**_*nfrastructure for* _**R**_*esearch and* _**I**_*nnovation for* _**S**_*TFC*
  - IRIS IAM service
- WLCG
  - _**W**_*orldwide* _**L**_*HC* _**C**_*omputing* _**G**_*rid*
  - Design and development of a token-based AAI service for WLCG
- SKA SRCNet
  - _**S**_*quare* _**K**_*ilometre* _**A**_*rray* _**S**_*cience* _**R**_*esource* _**C**_*entre* _**N**_*etwork*
  - AAI Prototyping work within the SRCNet

STFC uses INDIGO IAM

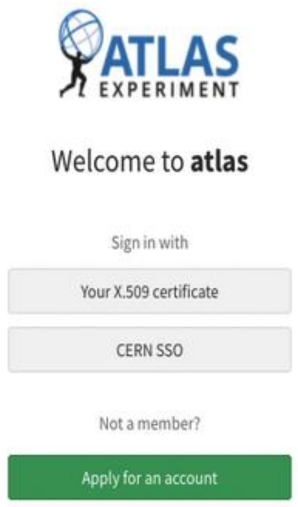
An authentication and authorization application that

- supports **multiple authentication mechanisms**
- provides users with a **persistent**, **organization scoped** identifier
- exposes **identity information**, **attributes** and **capabilities** to services via **JSON Web 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

… as will WLCG, and the SKA Prototype



Welcome to **atlas**

Sign in with

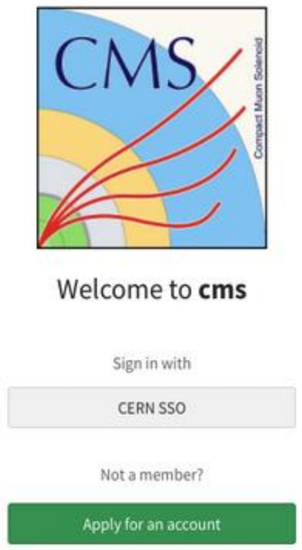
Your X.509 certificate

CERN SSO

Not a member?

Apply for an account

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



Welcome to **cms**

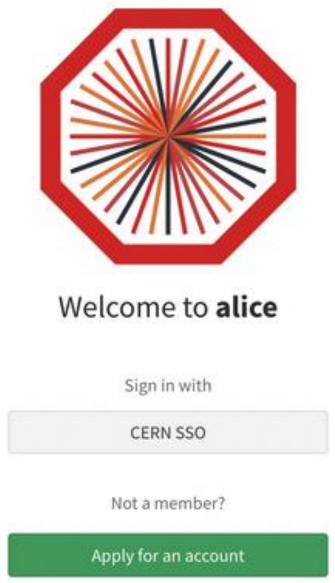
Sign in with

CERN SSO

Not a member?

Apply for an account

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



Welcome to **alice**

Sign in with

CERN SSO

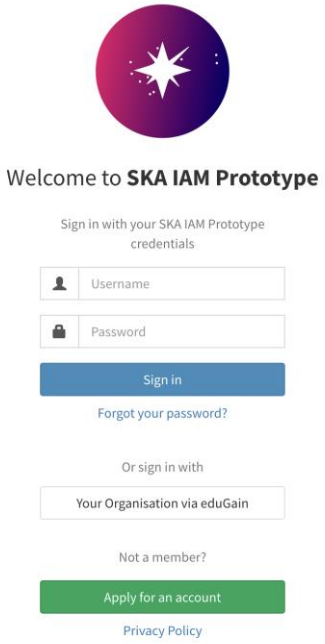
Not a member?

Apply for an account

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

TBC

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



Welcome to **SKA IAM Prototype**

Sign in with your SKA IAM Prototype credentials

Username

Password

Sign in

Forgot your password?

Or sign in with

Your Organisation via eduGain

Not a member?

Apply for an account

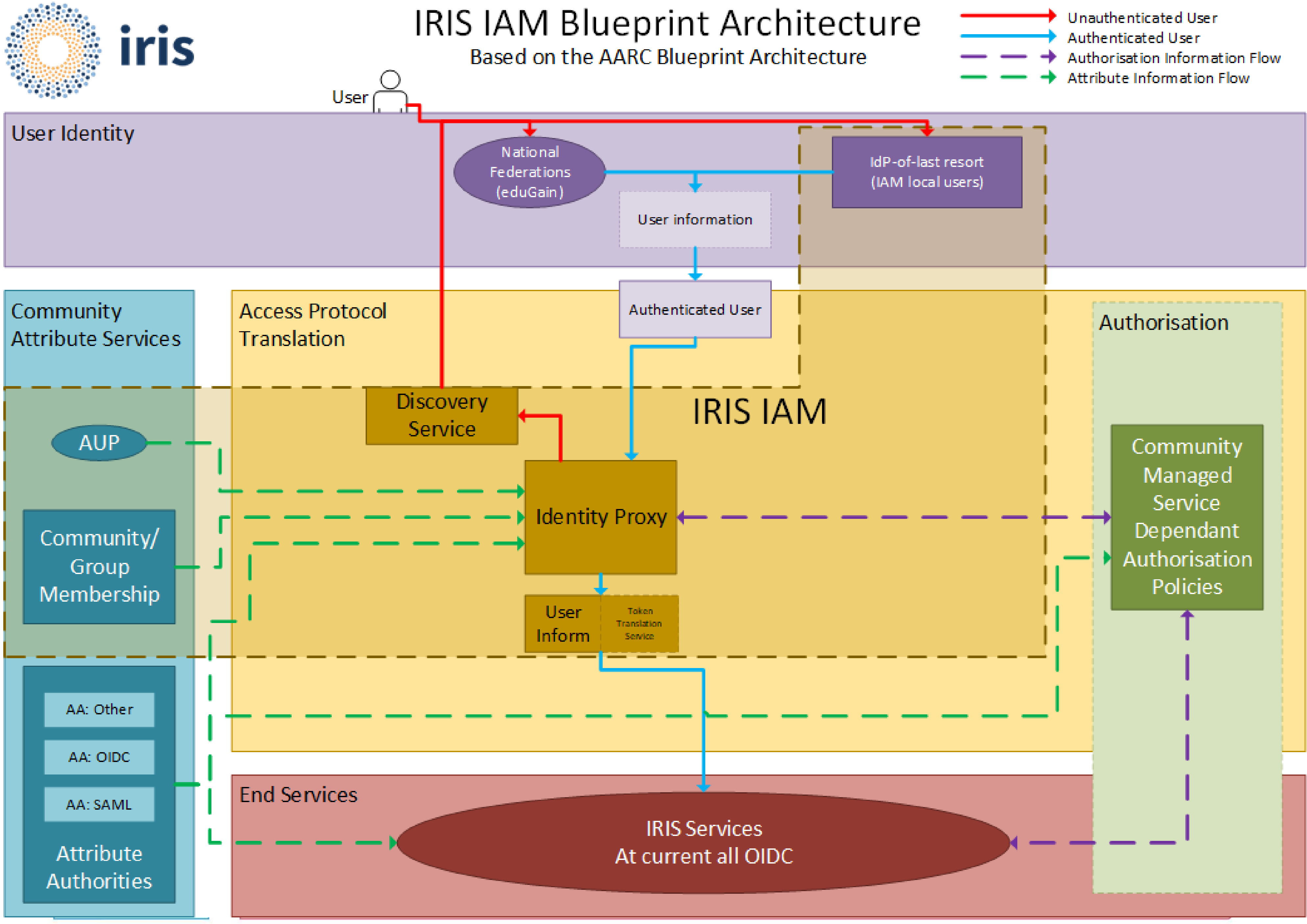
Privacy Policy

https://ska-iam.stfc.ac.uk

Science and Technology Facilities Council

INDIGO IAM and the AARC Blueprint Architecture for Infrastructures

Authentication and Authorisation for Research and Collaboration (AARC)



IRIS IAM Blueprint Architecture

Based on the AARC Blueprint Architecture

iris
Unauthenticated User
Authenticated User
Authorisation Information Flow
Attribute Information Flow
User
User Identity
National Federations (eduGain)
IdP-of-last resort (IAM local users)
User information
Authenticated User
Community Attribute Services
Access Protocol Translation
Authorisation
IRIS IAM
Discovery Service
AUP
Identity Proxy
Community/ Group Membership
Community Managed Service Dependant Authorisation Policies
User Inform
Token Translation Service
AA: Other
AA: OIDC
AA: SAML
Attribute Authorities
End Services
IRIS Services
At current all OIDC

Science and Technology Facilities Council

Challenges with Token Transition

- 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 AAI platform as an Identity-Provider-of-last-resort*
  - *"Community" IAM instances with local credentials acting as IdPs*
- Tokens and long-running jobs
  - *Token lifetime is typically short for security reasons – what happens with a job longer than the token*
  - *Refresh Tokens – Security Concerns*

Want to know more?

- Attend the WLCG Pre-GDB (Grid Deployment Board) Meeting in October – **WLCG AuthZ and IAM Workshop**
  - *Afternoons of 10th & 11th October at CERN*
  - *https://indico.cern.ch/event/1185598/*
  - *Maybe see you there and have a CSC catch-up drink?*
- Check out the WLCG Token Transition Timeline to get an idea of how things will shape up
  - *https://zenodo.org/record/7014668#.YxkaxCFBzVE*
- If you're interested in the topic - good content to be found in the slides from the Thematic School on Security:
  - *https://indico.cern.ch/event/1106023/*

Thank you for listening!

Any Questions?

UKRI Science and Technology Facilities Council

Science and Technology Facilities Council

Thank you

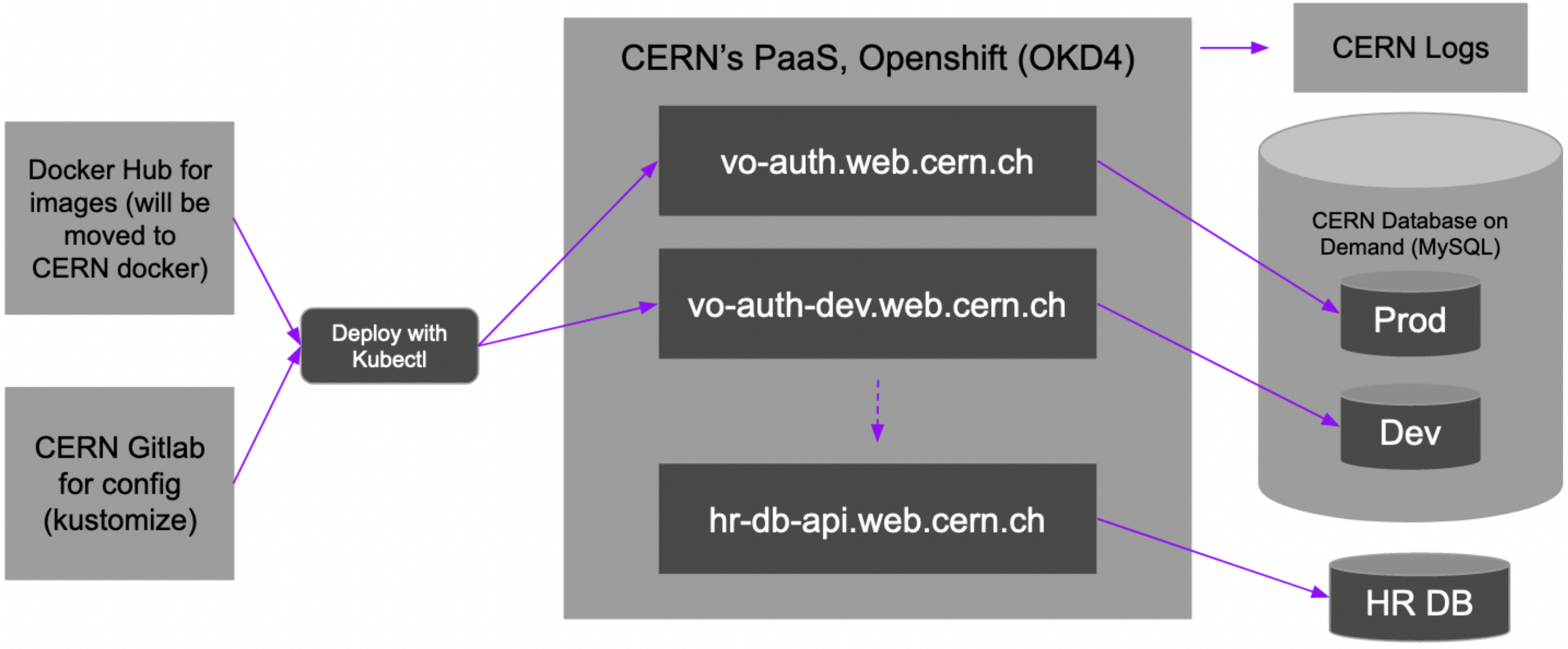
Science and Technology Facilities Council @STFC_matters Science and Technology Facilities Council

Science and
Technology
Facilities Council

Backup

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


Docker Hub for images (will be moved to CERN docker)
CERN Gitlab for config (kustomize)
Deploy with Kubectl
CERN's PaaS, Openshift (OKD4)
vo-auth.web.cern.ch
vo-auth-dev.web.cern.ch
hr-db-api.web.cern.ch
CERN Logs
CERN Database on Demand (MySQL)
Prod
Dev
HR DB

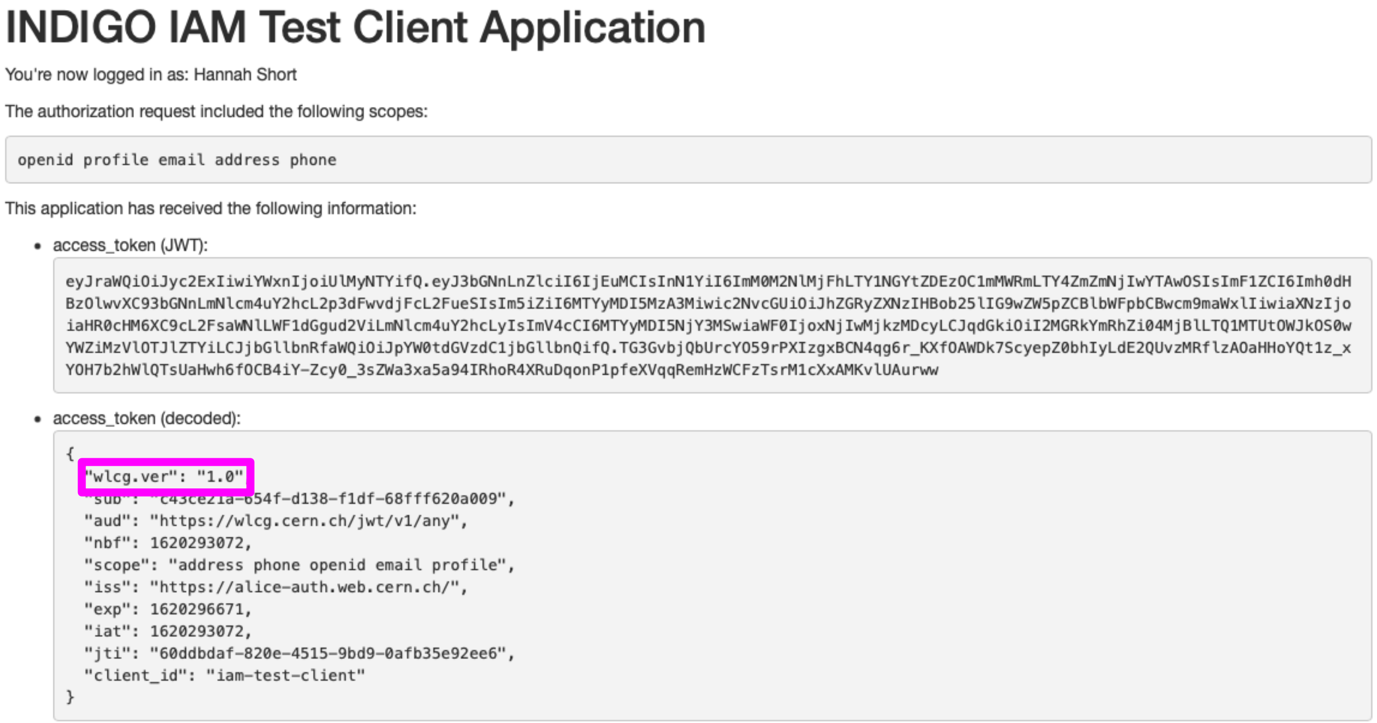
Leveraging CERN's infrastructure as far as possible.
Scalable deployment on Openshift.

WLCG IAM - Authentication

- Each 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.eyJ3bGNnLnZlciI6IjEuMCIsInN1YiI6ImM0M2NlMjFhLTY1NGYtZDEzOC1mMWRmLTY4ZmZmNjIwYTAwOSIsImF1ZCI6Imh0dH
BzOlwvXC93bGNnLmNlcm4uY2hcL2p3dFwvdjFcL2FueSIsIm5iZiI6MTYyMDI5MzA3Miwic2NvcGUiOiJhZGRyZXNzIHBob25lIG9wZW5pZCBlbWFpbCBwcm9maWxlIiwiaXNzIjo
iaHR0cHM6XC9cL2FsaWNlLWF1dGgud2ViLmNlcm4uY2hcLyIsImV4cCI6MTYyMDI5NjY3MSwiaWF0IjoxNjIwMjkzMDcyLCJqdGkiOiI2MGRkYmRhZi04MjBlLTQ1MTUtOWJkOS0w
YWZiMzVlOTJlZTYiLCJjbGllbnRfaWQiOiJpYW0tdGVzdC1jbGllbnQifQ.TG3GvbjQbUrcYO59rPXIzgxBCN4qg6r_KXfOAWDk7ScyepZ0bhIyLdE2QUvzMRflzAOaHHoYQt1z_x
YOH7b2hWlQTsUaHwh6fOCB4iY-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

Token Claims

Common Claims

- sub
- exp
- iss
- acr
- aud
- iat
- nbf
- jti
- eduperson_assurance (REFEDS)
- wlcg.ver (WLCG)
- wlcg.groups (WLCG)

iss+sub used to uniquely identify a user, e.g. for blocking

wlcg prefix added to avoid collisions with other schemas

ID Tokens

- auth_time
- general OIDC Claims

Access Tokens

- scope (RFC8693)

Access tokens should include at least scope (capabilities) or group for authorization

Note: Where unspecified, the origin is RFC7519 or OpenID Connect core

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

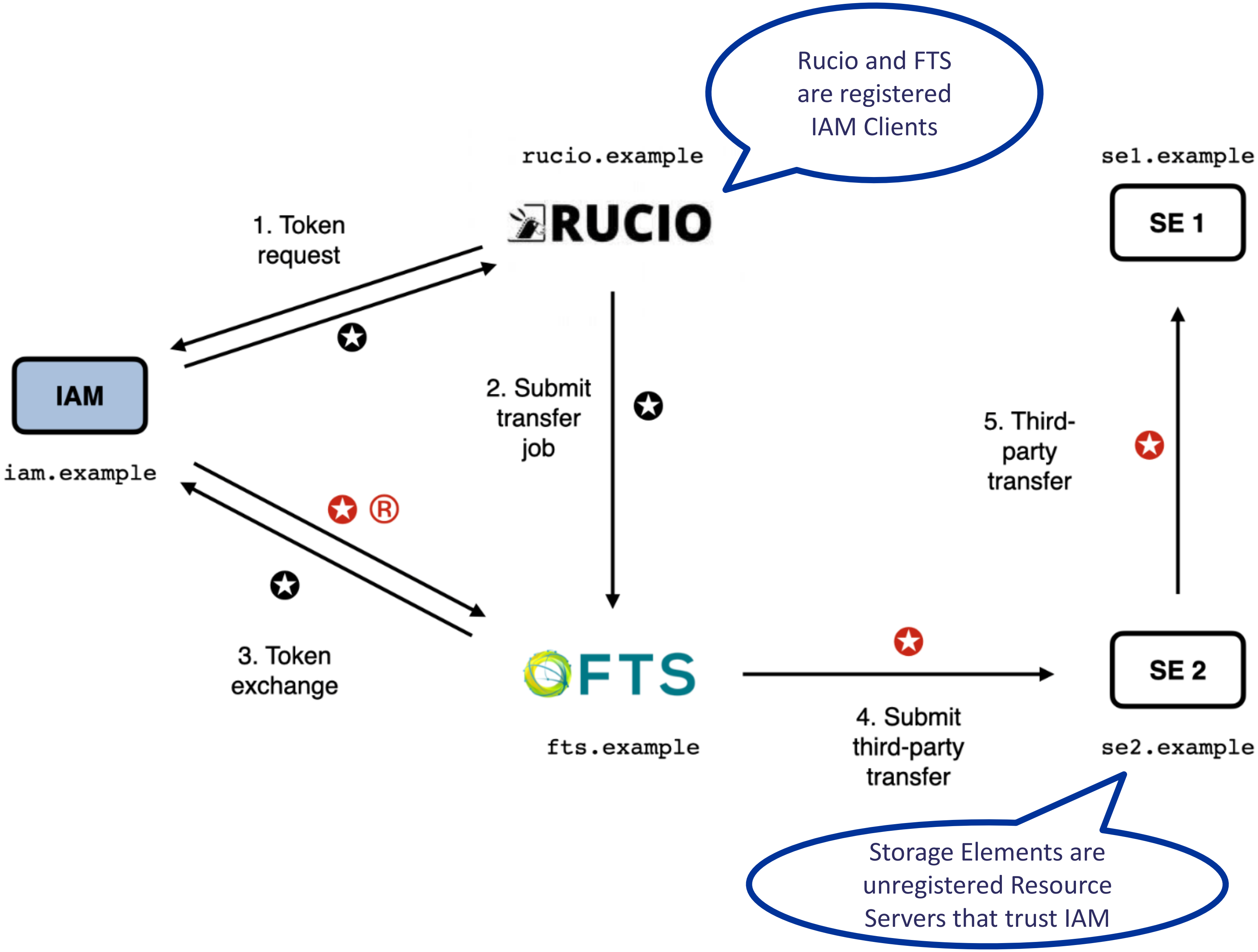
If a tool needs to authenticate with a token and does not have out-of-band WLCG Bearer Token Discovery knowledge on which token to use, the following steps to discover a token MUST be taken in sequence, where $ID below denotes the process's effective user ID:

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

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



Rucio and FTS are registered IAM Clients

Storage Elements are unregistered Resource Servers that trust IAM

Science and Technology Facilities Council

Lifetimes

Token Type	Recommended Lifetime	Minimum Lifetime	Maximum Lifetime	Justification
Access Token & ID Token	20 minutes	5 minutes	6 hours	Access token lifetime should be short as there is no revocation mechanism. The granted lifetime has implications for the maximum allowable downtime of the Access Token server.
Refresh Token	10 days	1 day	30 days	Refresh token lifetimes should be kept bounded, but can be longer-lived as they are revocable. Meant to be long-lived enough to be on a "human timescale".
Issuer Public Key Cache	6 hours	1 hour	1 day	The public key cache lifetime defines the minimum revocation time of the public key. The actual lifetime is the maximum allowable downtime of the public key server
Issuer Public Key	6 months	2 days	12 months	JWT has built-in mechanisms for key rotation; these do not need to live as long as CAs. This may evolve following operational experience, provision should be made for flexible lifetimes.