A Look at

Token-Based

Authorisation

taking in

REQUIREMENTS AND EXPERIENCES

from

Communities and Projects

such as

ISIS, UKSRC, SKA SRCNet

and more

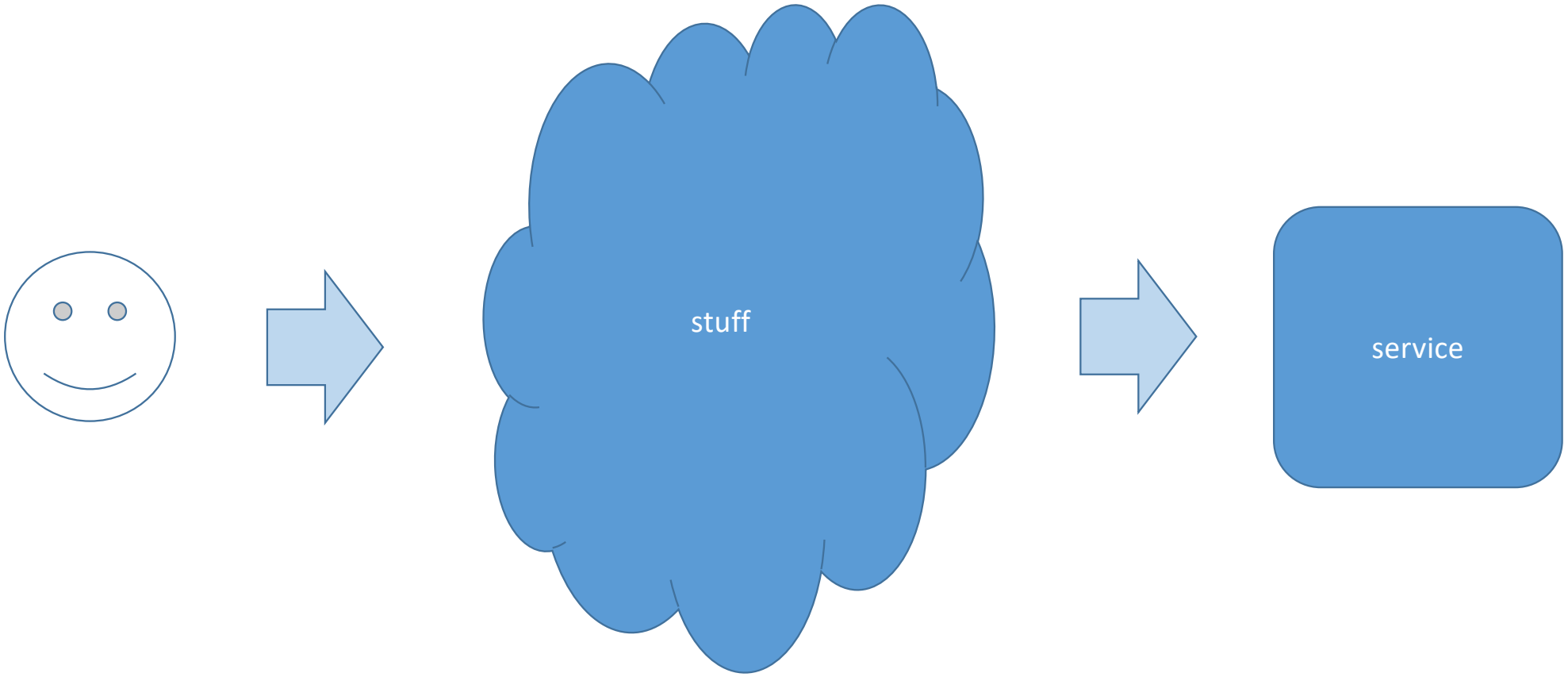
Abstract

this talk will ~~rant~~ discourse through a range of issues associated with doing authorisation with tokens, highlighting opportunities for further work

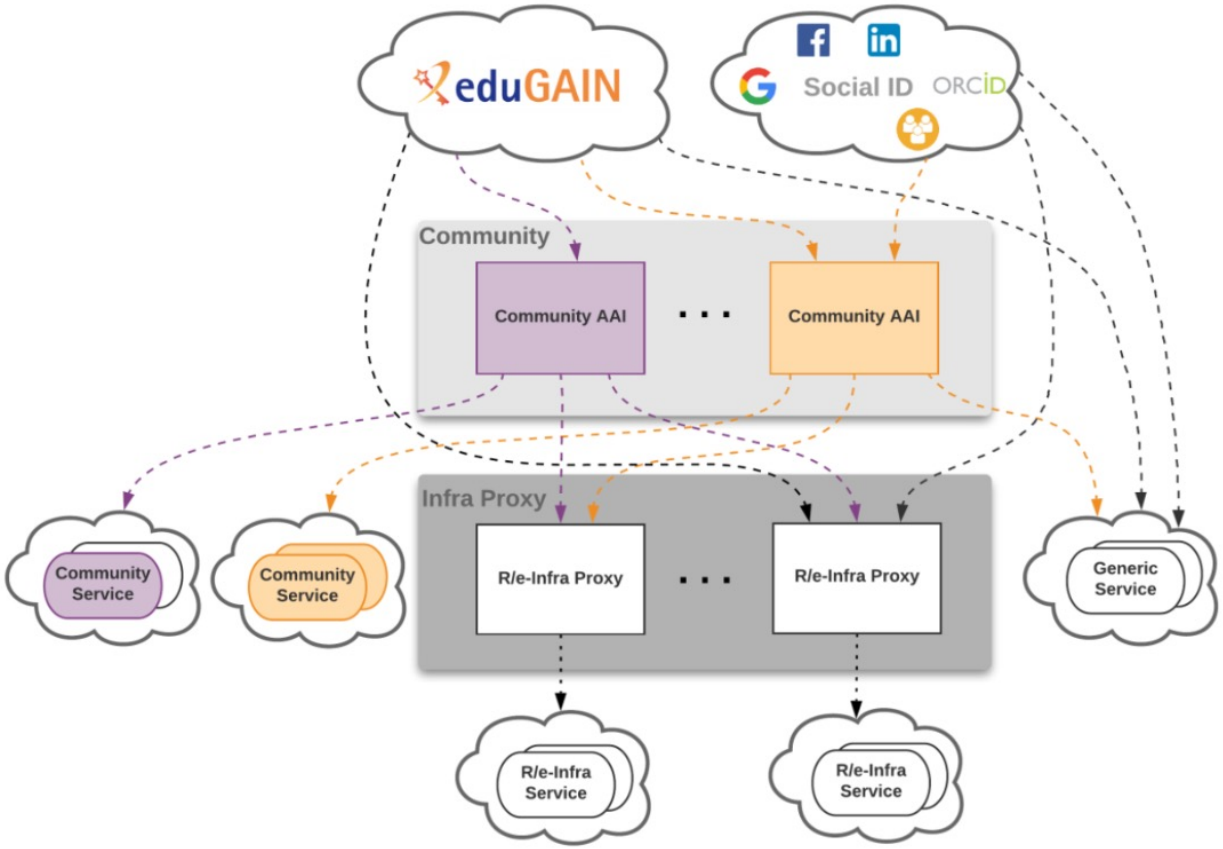
0000-0003-4714-184X

London X id. Mar. AD MMXXV

Service Access
High Level Architecture

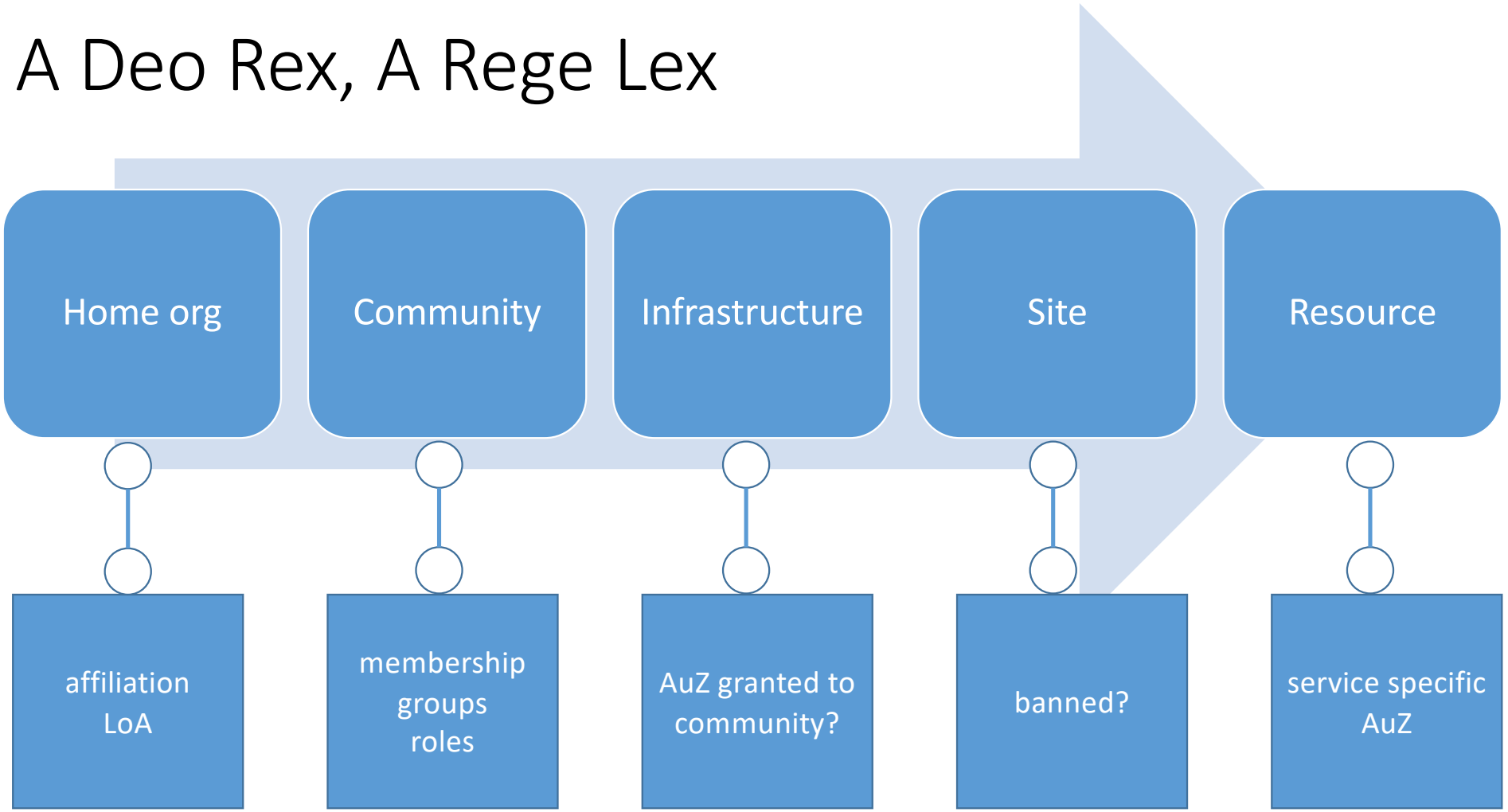


AARChitecture – Community AAI view



Community as source of (some) authorisation attributes

A Deo Rex, A Rege Lex



How to play along 0

Set up a Debian or Ubuntu system

- Demo will be using oidc-agent from KIT
- oidc-agent is packaged natively for Debian

How to play along 1

```
$ sudo apt install oidc-agent
…
$ eval $(oidc-agent-service start)
$ oidc-gen -w device
…iris-iam
…https://iris-iam.stfc.ac.uk/
…aarc openid profile entitlements offline_access
```

(follow instructions or QR for web login, see next slide)

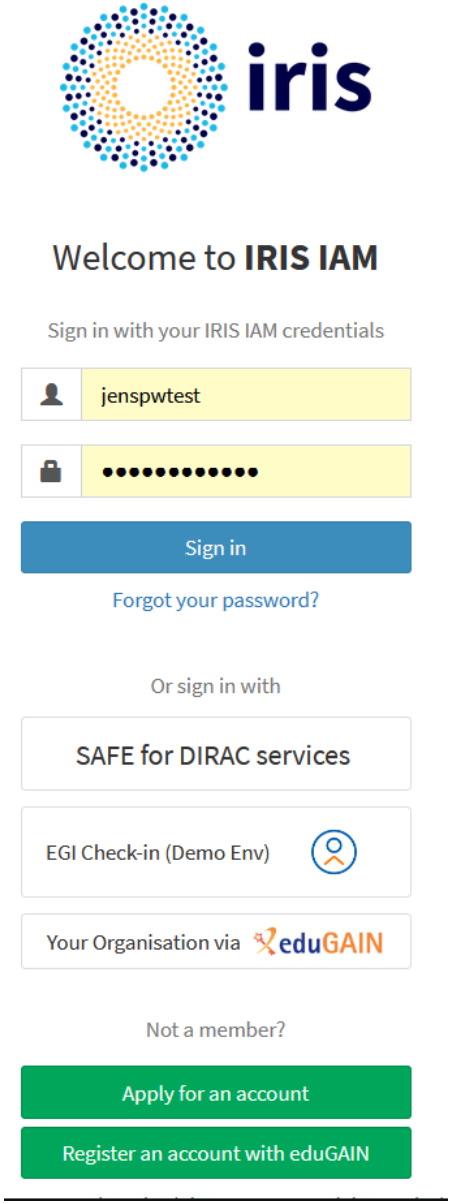
```
…**********
```

IRIS Login

- Poor layout of login screen
  - The basic assurance login-of-last-resort is most prominent
- The medium assurance login at the bottom of the page
- Login through SAFE currently isn't working in iris-iam
  - Though it used to
  - We think the client id changed?

Prominent default login low assurance

Required default login hidden away



Playing along 2

$ # (with the agent running and the iris-iam account created, it is already active)

```
$ eval $(oidc-token -c iris-iam)
$ # expiry in 1h
$ date -d @$OIDC_EXP
Tue Mar  4 11:02:44 UTC 2025
$ # Get userinfo
$ curl -s -H "Authorization: bearer $OIDC_AT" \
  https://iris-iam.stfc.ac.uk/userinfo | jq
```

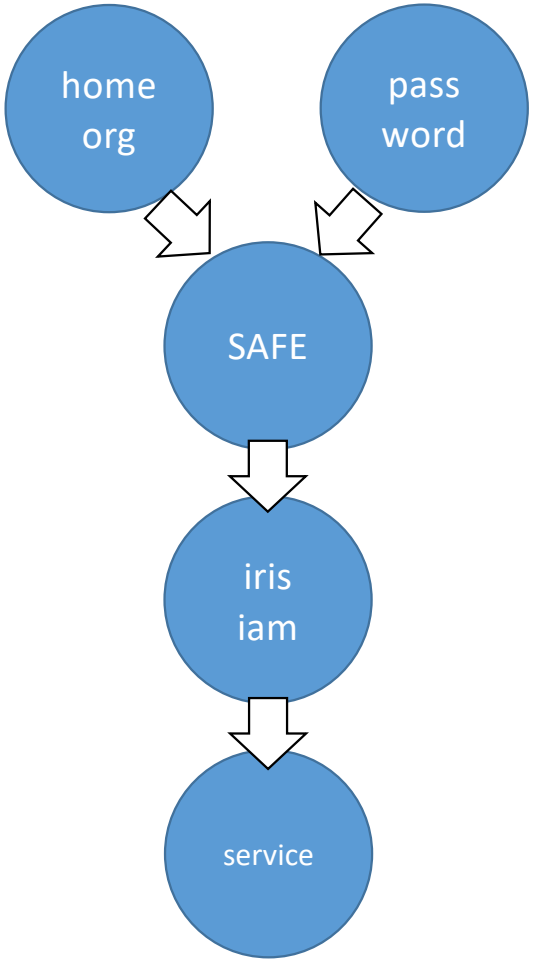
Playing along 3

Equivalent from CheckIn

```
$ curl -s -H "Authorization: bearer $OIDC_AT" https://iris-iam.stfc.ac.uk/userinfo|jq
{
 "sub": “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
 "name": "Jens Jensen",
 "preferred_username": "jens.jensen@stfc.ac.uk",
 "given_name": "Jens",
 "family_name": "Jensen",
 "updated_at": 1732193577,
 "entitlements": [
  "urn:geant:iam.example:group:stfc-cloud-prod",
  "urn:geant:iam.example:group:gridtools",
  "urn:geant:iam.example:group:stfc-cloud-dev",
  "urn:geant:iam.example:group:stfc-cloud-aai-test",
  "urn:geant:iam.example:group:gridtools:admins"
 ]
```

```
{
 "sub": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx@egi.eu",
 "voperson_id": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx@egi.eu",
 "voperson_verified_email": [ "jens.jensen@stfc.ac.uk" ],
 "email_verified": true,
 "name": "Jens Jensen",
 "eduperson_assurance": [
  "https://refeds.org/assurance/IAP/low",
  "https://aai.egi.eu/LoA#Substantial"
 ],
 "preferred_username": "jjensen",
 "given_name": "Jens",
 "family_name": "Jensen",
 "eduperson_entitlement": [
  "urn:mace:egi.eu:res:ggus.eu",
  "urn:mace:egi.eu:res:gocdb#aai.egi.eu",
  "urn:mace:egi.eu:res:rcauth#aai.egi.eu"
 ],
 "email": "jens.jensen@stfc.ac.uk"
}
```

Community Authorisation (example)



Your details | Service information | Projects | Login accounts | Help and Support

DiRAC

SAFE for DIRAC services
Service Administration by EPCC

Project: dr004 (Dirac Benchmarking)

Code	dr004
Status	Active
Description	Dirac Benchmarking
Start Date	2019-01-11
End Date	2026-04-01
PI	Rev Prof Jeremy Yates (ucapjay@ucl.ac.uk)
Grants	DiRAC Support
Funding Body	DiRAC
Project Class	Internal
Subject area	Support
Project notification list	ucapjay@ucl.ac.uk

Machines

- cosma: The Durham COSMA machine
- MI: Cosma7
- Cambridge_HPC
- Peta4-Skylake: Skylake system at Cambridge CS3D
- DlaL: DiRAC machines at the University of Leicester
- Wilkes2-GPU: GPGPU system at Cambridge CSD3
- cosma8: Cosma8
- DlaL3
- ES-Tursa
- tursa-ldap

DIRAC SAFE guide Accessibility statement

Using oidc-agent

- Can’t specify groups/roles
  - Problem for people with many group memberships
  - À la voms-proxy-init (but maybe fine grained)
  - Plan/Hope to have a demo (for SKA) this (Tuesday 11/03/2025)
- Doesn’t renew tokens

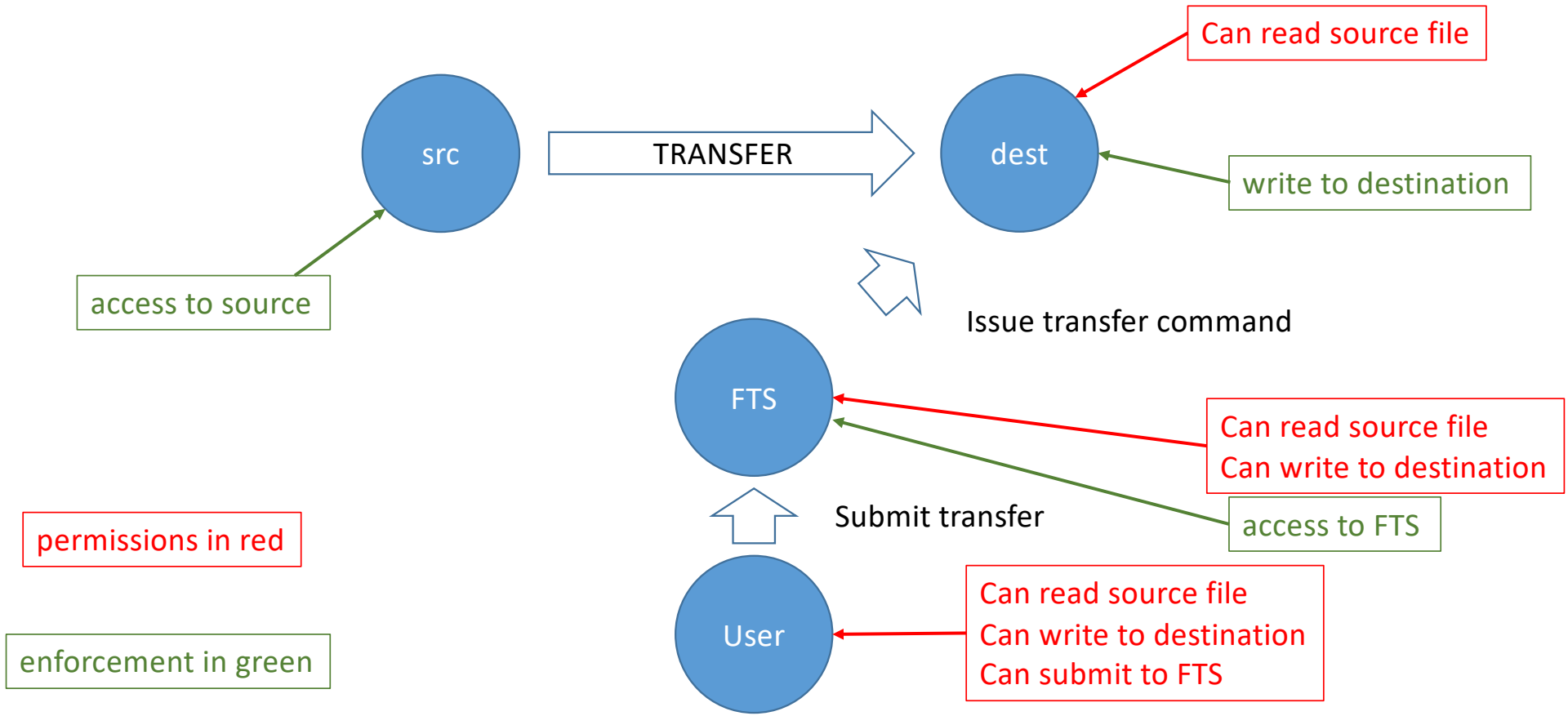
G069 compliance

- What?
  - https://aarc-community.org/guidelines/aarc-g069/
  - RFC 8141 (URNs)
  - E.g. `urn:geant:iam.example:group:stfc-cloud-prod`
  - Should be `urn:geant:iris.ac.uk:group:stfc-cloud-prod`
  - Note Indigo IAM uses `entitlements`; CheckIn uses `eduperson_entitlement`
- Why?
  - Enable interoperation between infrastructures
  - All groups & roles are “safe”
    - Not stepping on each other’s (virtual) toes
    - “Owner” of attribute is immediately evident (IRIS in this example)
- How?
  - Easy – turn on the `aarc` scope?

General authorisation issues

- Group names get longer…
  - Tokens get bigger… or do they?
- Allowing users to assert groups
  - (Can’t do negative selection)
- Push or Pull? Foreground or Background?
  - Planning a demo for SKA
- Still need PKI
  - Host certificates for endpoint protection
  - Signatures on tokens

Fine grained authorisation (FTS example)



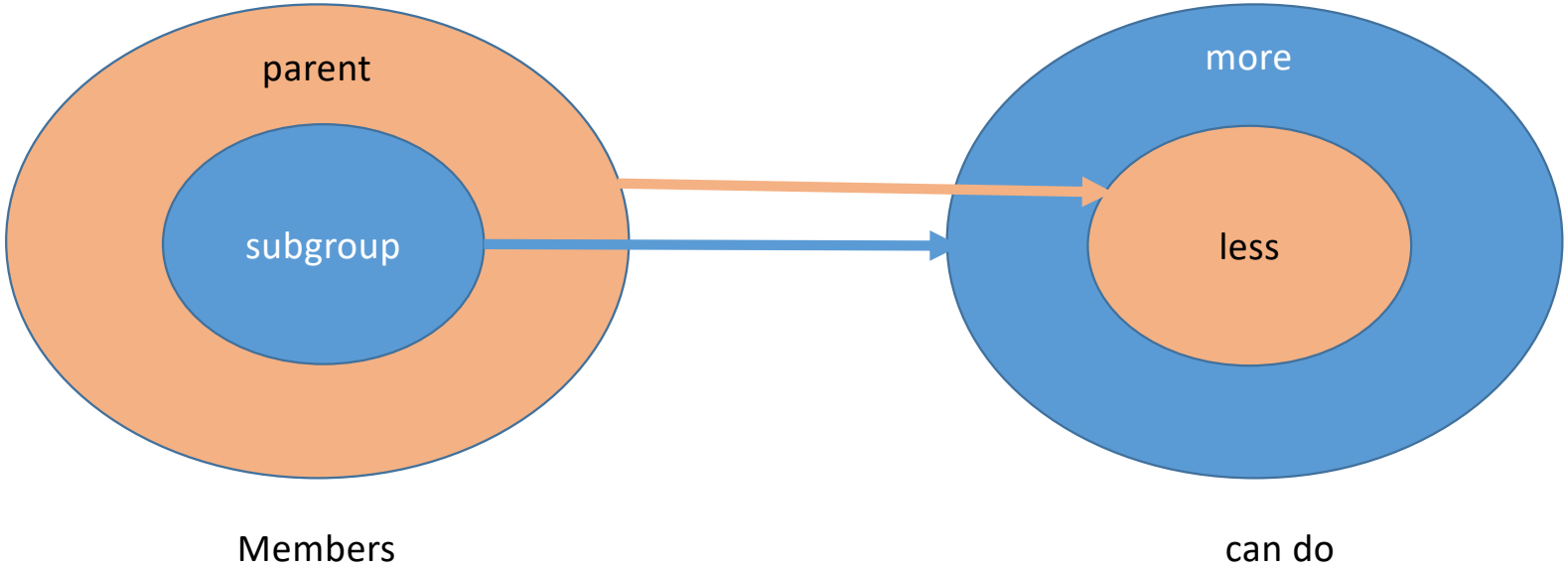
Subgroup membership implies group membership?

- Indigo IAM uses the same semantics:
  - Joining `foo/bar/baz` also adds membership of `foo/bar` and `foo`
  - Subsequently leaving `foo` also removes `foo/bar` and `foo/bar/baz`
  - All are published: "groups":["foo", "foo/bar", "foo/bar/baz"]
- CheckIn seems to manage all independently
  - A user can be in a subgroup but not in the parent
  - A user can be in the parent but not the subgroup
- Not completely straightforward
  - But could reduce number of groups published
  - In the above example, publish only "groups":["foo/bar/baz"]

Subgroup membership implies group membership?

Makes sense when:

The authorisations associated with the *subgroup* are a *superset* of the authorisations of the *parent*



Subgroup membership implies group membership?

Counterexample:

- As a PI, I want to share data with some group members
  - Give a *subgroup* read-only permissions
  - Everyone else can write
  - Negative selection (as in “not in the subgroup”) should be done with caution

Relying Parties need to substring match, not string match:

```
# python 3.11
authorised_group="urn:group:foo"
user_group="urn:group:foo:baz"
if user_group.startswith(authorised_group):
    print("user is authorised\n")
```

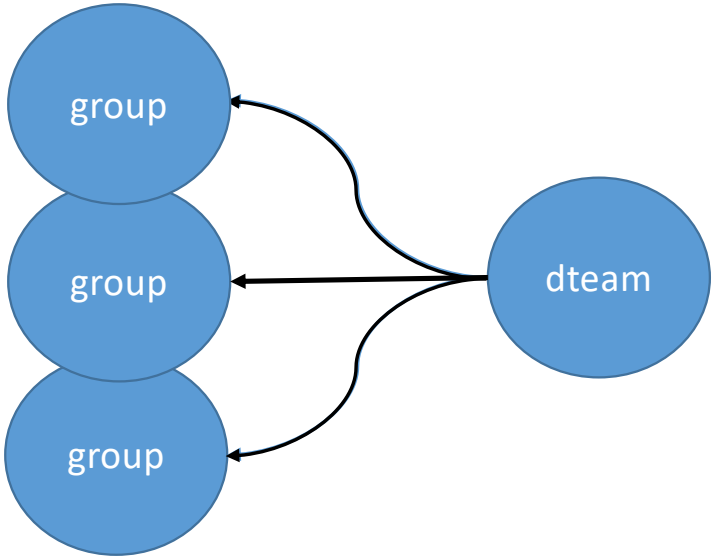
See also: https://github.com/aarc-community/architecture-guidelines/issues/25

Federated ssh (DiRAC case primarily)

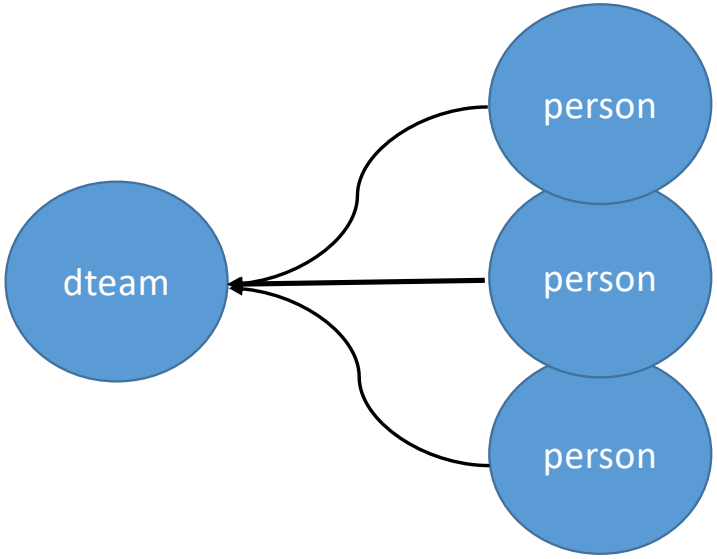
- Lots of ways to do ssh logins with federated credentials
  - ssh is very flexible in its use of PAM and GSSAPI
  - Each method has its own {,dis}advantages
  - Little interoperation between methods
- XXX PAM module
- Account {,de}provisioning
  - Synchronise with the proxy?
    - Privacy issue – can read user data
    - Scalability issue – not everyone needs an account so needs to evaluate authorisation without user attributes?!
  - Generate accounts on the fly?
    - But persist, account remains at the next login

dteam

- Need to move a team as if it were a person



Team can be added to/removed from groups



Team itself works as a group

Token Exchange (RFC 8693)

FTS use cases for token exchange

- Drop privileges from tokens (à la GSI delegation, RFC 3820)
- Obtain refresh tokens (for long running transfers, restart, retry)
  - More generally, change token type
- Delegation (tracking *subject* and *actor*)
- Multi-OP support

Problems

- Multi-OP support not well understood in community
- How to specify *useful* policies for exchange
  - (beyond allowing drop privs)

Usability

- Federations are also for the users
- Not all users will be compute experts
- Some will have low tolerance for Complicated Things™
  - Things that are not directly relevant to the work they want to do
- We *never ever* do UX testing

Gaps identified in today's demo/talk

- General
  - The full benefit of tokens – not delivered yet (eg too much use of bearer tokens (RFC6750)
  - Tokens were supposed to be simpler than SAML
  - UX testing
  - Specifying policies for token exchange
- Indigo IAM (and other proxies…)
  - eduGAIN should be default login
  - Who can request a client – some restrictions on scopes
    - Command line requires dynamic client registration
    - CheckIn tightens rules
  - Passing community (upstream) entitlements to the service (downstream)
  - Selecting relevant groups as opposed to all groups
  - Subgroup membership implies group membership
  - Managing a group as if it were a person ("dteam")
- oidc-agent
  - Refreshing tokens
  - Some usability issues (e.g. values checked late)
- SPs
  - Subgroup membership implies group membership

But Wait, There's More!

Future gaps to worry about… not covered today ☺

- Authorisation beyond groups and roles
  - Capabilities were not much used (G006)
- Usage control (cf XACML 3) – token revocation is not sufficient
- Caching (authorisation) attributes
- Authorisation attribute metadata
  - (Origin, Time asserted, Expiry, …)
- Community based evidence
  - Like Mike Jones' FOAF experiment; AARC1-JRA1.4 for social media
  - ELIXIR researcher
- Implementing OIDC Fed
  - Trust marks, trust chains (they work a lot like X.509 certificates' trust chains)
- Expressing authorisation policies
  - E.g. allow access to members of IRIS who have been members for more than a year and they've used organisational id and they have signed an extended AUP and are physically in the office
- Service hints to proxy
  - Support multi-policy environments

Advertisement

Workshop Reading 04/04/2025

Dear colleagues,

As part of growing and developing UKRI's Trust and Identity strategy for the UK's Digital Research Infrastructure, we would like to invite you or a nominated colleague to a workshop which will take place at the University of Reading on 4th April 2025.

The workshop will provide an opportunity to discuss recent developments in Authentication, Authorisation, Accounting and Identity Management such as the evolution of Identity Federations to include cloud native approaches like OpenID Connect, and best practice integrating higher assurance applications such as Trusted Research Environments.

Workshop participants will include:

- Identity service providers in the UK and internationally
- Established identity federations and digital research infrastructures
- Representatives of key projects and initiatives such as EuroHPC Federation Platform, DARE UK, GÉANT, AI Research Resources, UKRI Federation NetworkPlus
- Technologists, funders and policymakers

We hope that the workshop will be instrumental in helping to build a community of participants and stakeholders recognising the significant changes in landscape in recent years including entire new communities, and the range of UKRI investments in DRI.

Workshop outputs will feed into UKRI's Trust and Identity strategy and wider UKRI Digital Research Infrastructure initiatives to support more effective access and collaboration across the whole range of DRI facilities and resources.

Registration and logistical information can be found at https://cvent.me/2Z9qNG

TIIME (Trust and Internet Identity Meeting Europe - https://time-unconference.eu) which precedes the workshop at the same venue may also be of interest.

If you have any questions please contact Ian Collier - Ian.collier@stfc.ac.uk

Acks

Shout outs to

- Donald Chung, Thomas Dack (STFC) for contributions to Indigo IAM
- Rose Cooper (STFC) for sherlockholmesing the FTS stuff
- Nicolas Liampotis (GRNET) for assistance with CheckIn