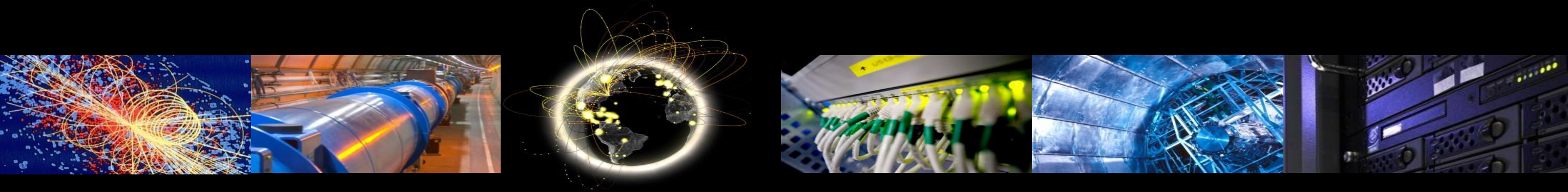
Authored by Hannah Short

IAM adoption at WLCG

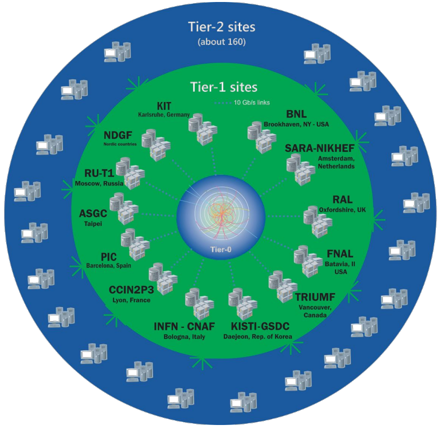
IAM Users Meeting

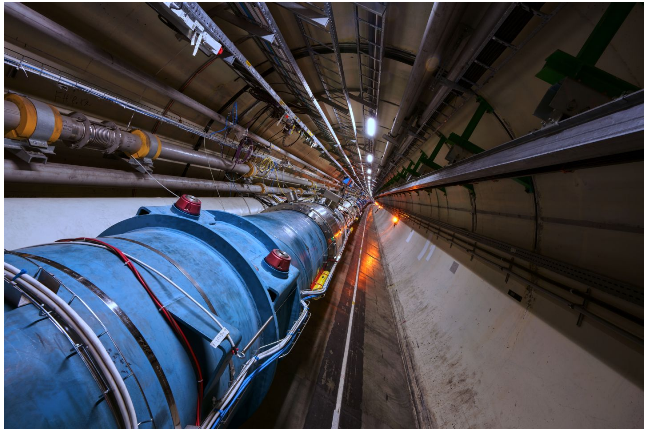
Oct 11th 2022



WLCG

- Worldwide LHC (Large Hadron Collider) Computing Grid
- Used by physicists to perform analysis on data from the LHC
- Highly distributed, >170 organisations
- CERN provides 20% of storage & compute

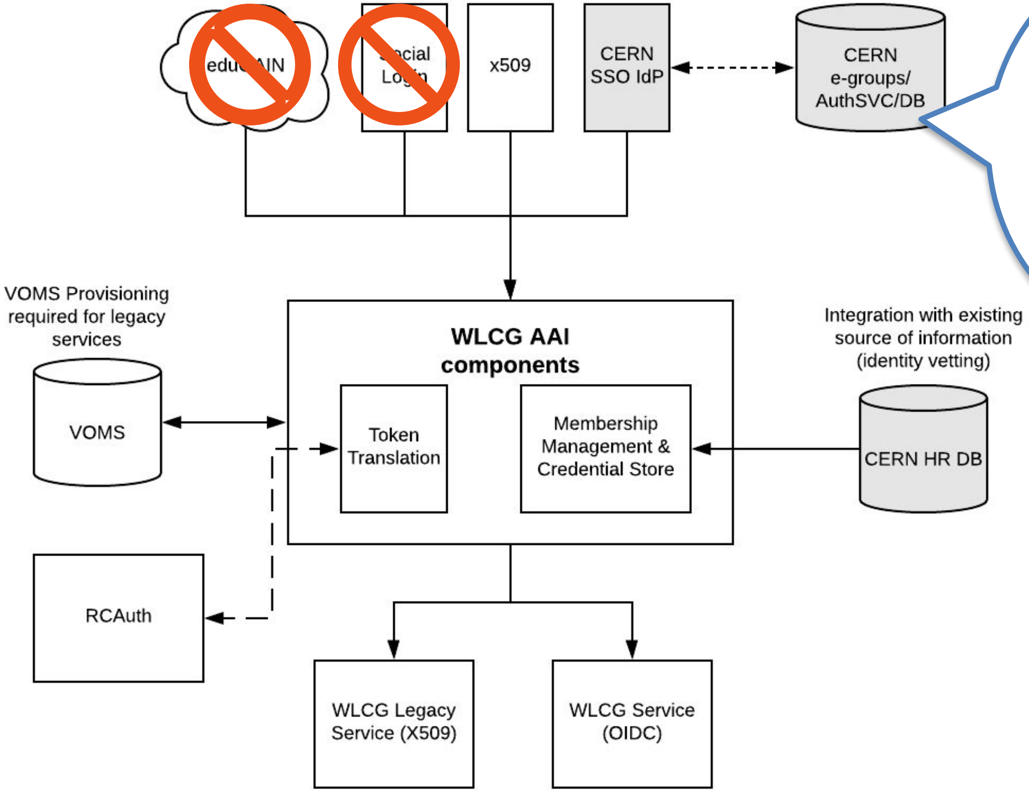




AAI Design

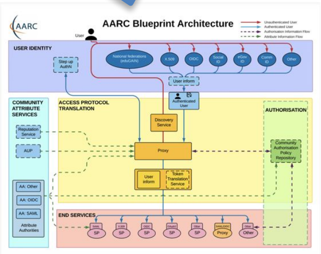
OpenID

eduGAIN


eduGAIN
Social Login
x509
CERN SSO IdP
CERN e-groups/ AuthSVC/DB
VOMS Provisioning required for legacy services
VOMS
WLCG AAI components
Token Translation
Membership Management & Credential Store
Integration with existing source of information (identity vetting)
CERN HR DB
RCAuth
WLCG Legacy Service (X509)
WLCG Service (OIDC)

CERN SSO configured as sole Identity Provider, enables identity verification via HR DB (match CERN PersonID)

Follows the AARC Blueprint https://aarc-community.org/architecture/ but not all AEGIS recommendations



WLCG Worldwide LHC Computing Grid

AARC

WLCG Token Claims

Common Claims

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

wlcg prefix added to avoid collisions

ID Tokens

- auth_time
- general OIDC Claims

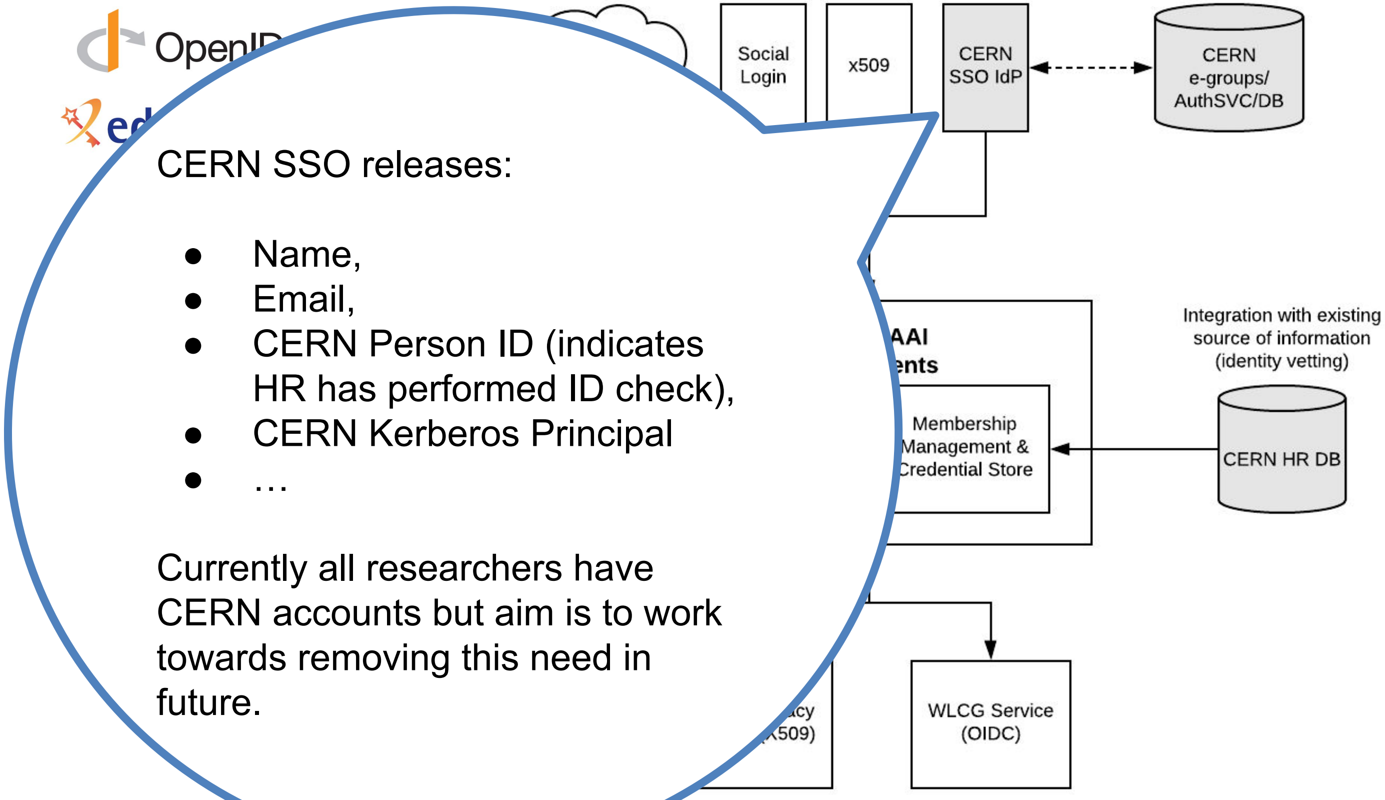
Access Tokens

- scope (RFC8693)

Access tokens should include at least scope or group

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

AAI Design

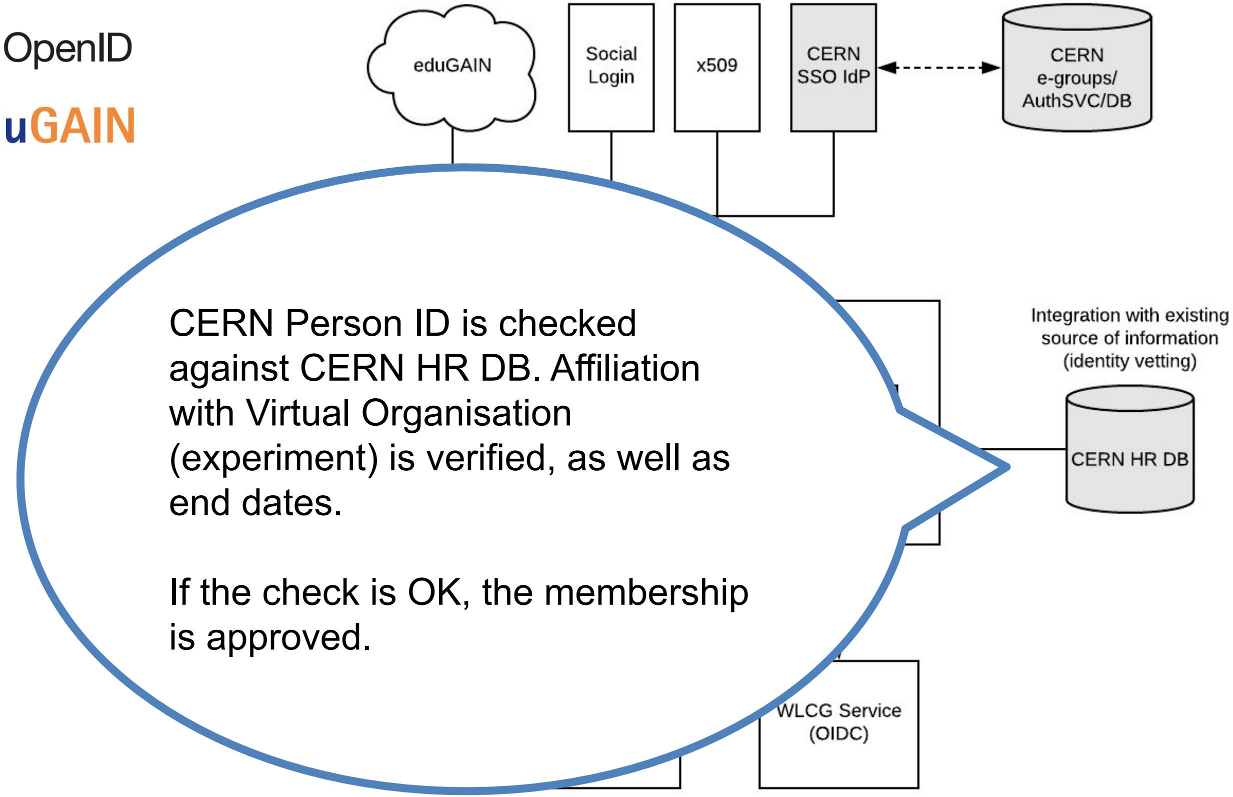

OpenID
ed
Social Login
x509
CERN SSO IdP
CERN e-groups/ AuthSVC/DB
AAI
ents
Integration with existing source of information (identity vetting)
Membership Management & Credential Store
CERN HR DB
acy (x509)
WLCG Service (OIDC)

CERN SSO releases:

- Name,
- Email,
- CERN Person ID (indicates HR has performed ID check),
- CERN Kerberos Principal
- …

Currently all researchers have CERN accounts but aim is to work towards removing this need in future.

AAI Design

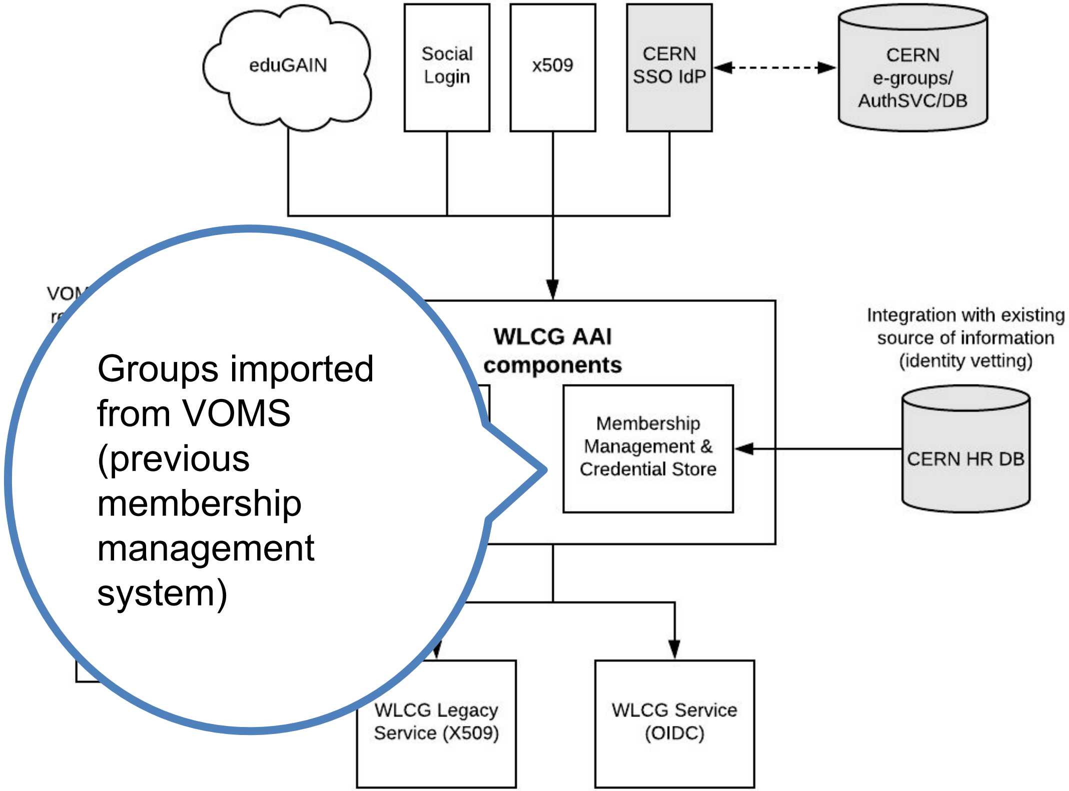


Integration with existing source of information (identity vetting)

CERN Person ID is checked against CERN HR DB. Affiliation with Virtual Organisation (experiment) is verified, as well as end dates.

If the check is OK, the membership is approved.

AAI Design

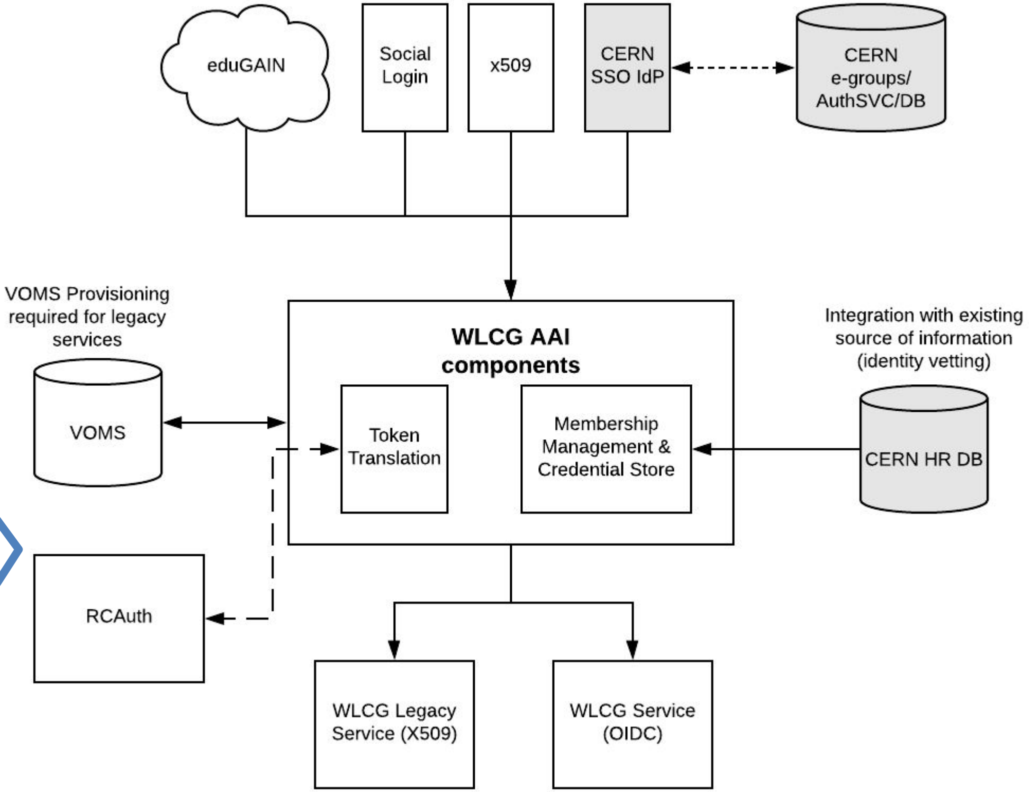


eduGAIN
Social Login
x509
CERN SSO IdP
CERN e-groups/ AuthSVC/DB
VOM
re
WLCG AAI components
Membership Management & Credential Store
Integration with existing source of information (identity vetting)
CERN HR DB
WLCG Legacy Service (X509)
WLCG Service (OIDC)

Groups imported from VOMS (previous membership management system)

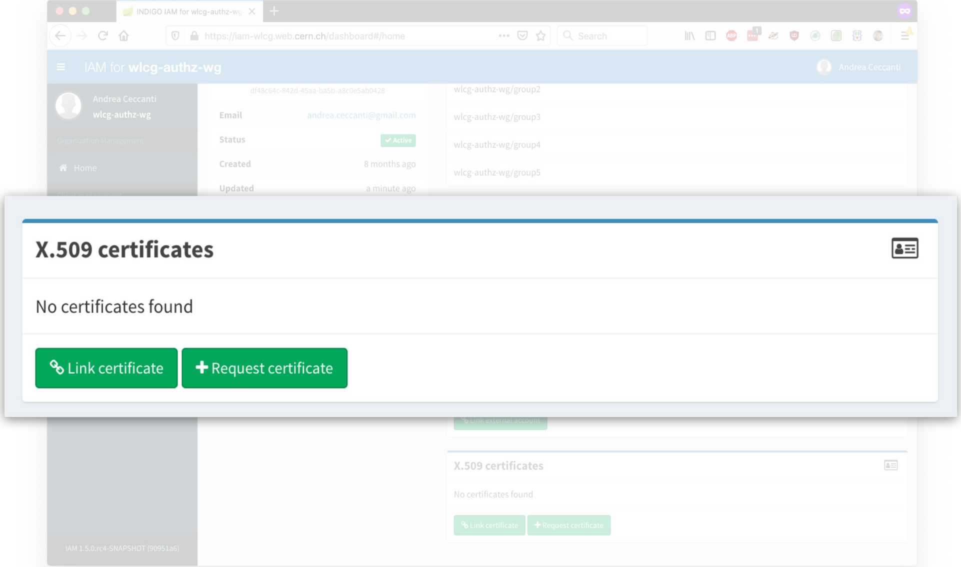
AAI Design

RCAuth integration to generate X.509 certs - crucial for backwards compatibility (not currently used)


eduGAIN
Social Login
x509
CERN SSO IdP
CERN e-groups/ AuthSVC/DB
VOMS Provisioning required for legacy services
VOMS
WLCG AAI components
Token Translation
Membership Management & Credential Store
Integration with existing source of information (identity vetting)
CERN HR DB
RCAuth
WLCG Legacy Service (X509)
WLCG Service (OIDC)

X.509 Compatibility

- X.509 certificate can be linked
- Long lived proxy cert can be stored in IAM
- Available via authenticated REST API (SCIM)
- *Need to understand status of RCAuth integration*



df48c64c-842d-45aa-ba5b-a8c0e5ab0428

Email andrea.ceccanti@gmail.com

Status ✓ Active

Created 8 months ago

Updated a minute ago

wlcg-authz-wg/group2

wlcg-authz-wg/group3

wlcg-authz-wg/group4

wlcg-authz-wg/group5

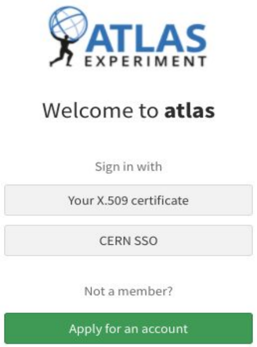
X.509 certificates

No certificates found

Deployment

- Deployed on CERN’s **Openshift** infrastructure
- IAM run as **Docker** container
- Configuration managed using CERN’s **gitlab**
- Logs sent to elastic search
- Deployment managed by **Kubectl**
- Sectigo certificate for IAM dashboard
- CERN Grid Host Certificate for VOMS endpoint
  - CERN’s CP/CPS was updated to allow this with EUGridPMA approval

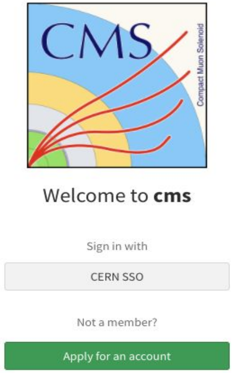
Deployments



Welcome to **atlas**

Sign in with

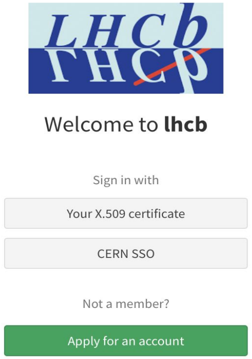
Not a member?



Welcome to **cms**

Sign in with

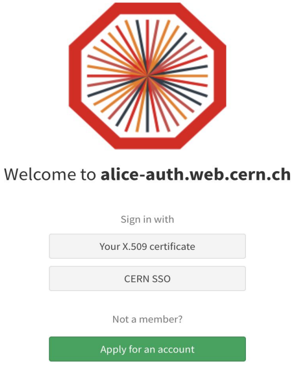
Not a member?



Welcome to **lhcb**

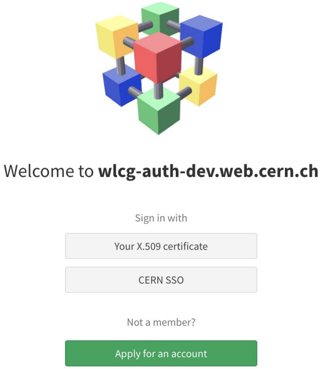
Sign in with

Not a member?


Welcome to **alice-auth.web.cern.ch**

Sign in with

Not a member?


Welcome to **wlcg-auth-dev.web.cern.ch**

Sign in with

Not a member?

IAM Dashboard: https://<experiment>--auth.web.cern.ch
VOMS endpoint: https://voms-<experiment>-auth.app.cern.ch

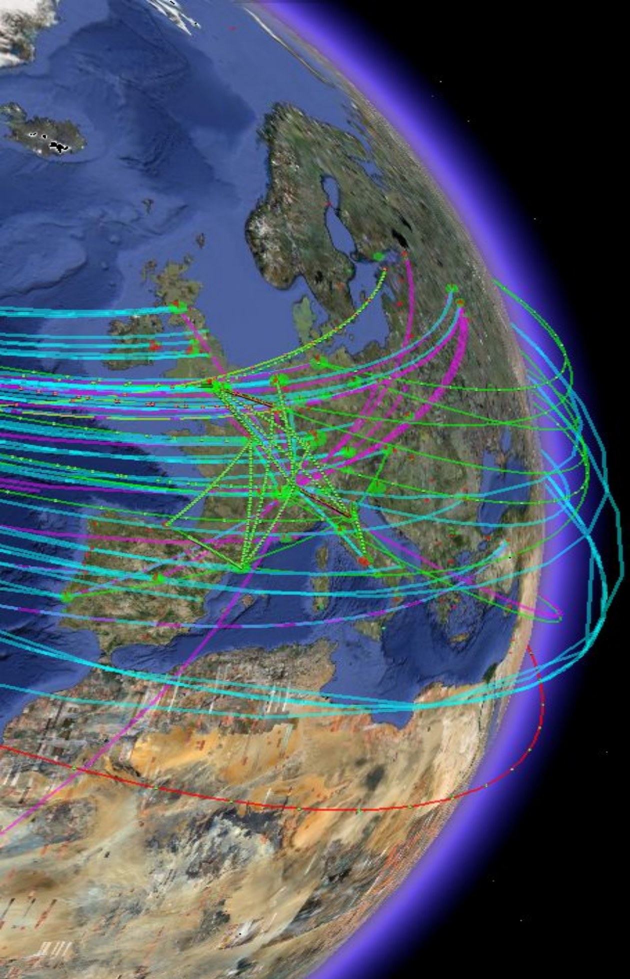
Supporters

We will be recruiting a (recent) graduate ASAP :)

know anyone good?? Let me know!

Policy

- Aiming to comply with AEGIS approved *"AARC-G071 Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities"* https://doi.org/10.5281/zenodo.5927799
- Known issues with current deployment e.g. segregation of openshift containers, secret storage
- Many policies r.e. lifecycle management do not change from previous X.509 based system



Questions?