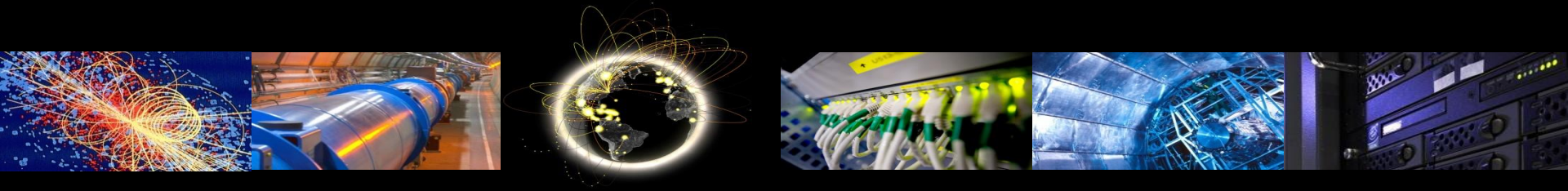
Authored by the WLCG AuthZ WG

IAM adoption at WLCG

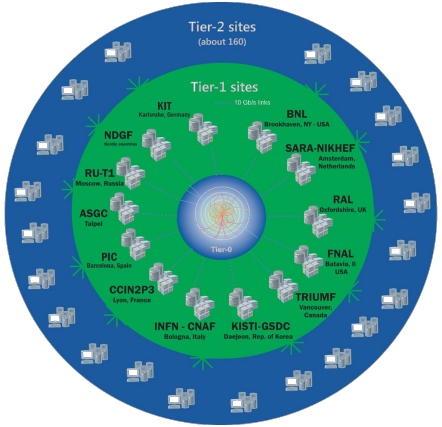
IAM Users Meeting

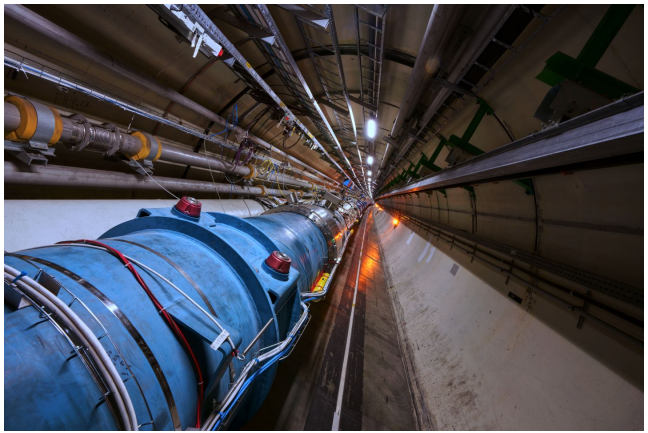
Jan 27th 2021



WLCG

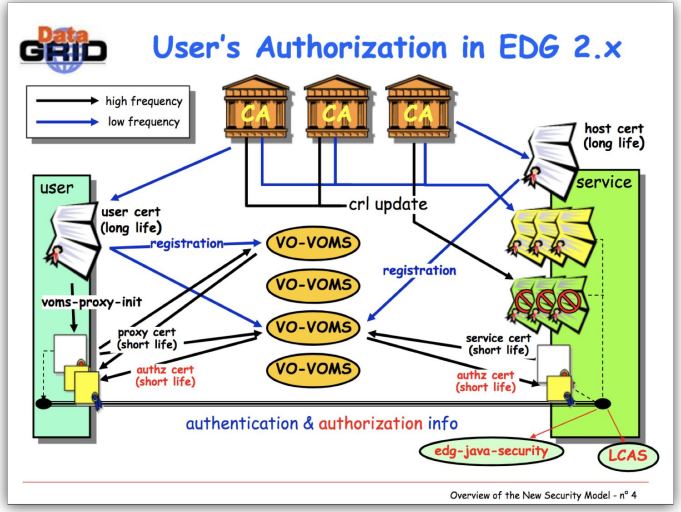
- Worldwide LHC (Large Hadron Collider) Computing Grid
- Used by physicists to perform analysis on data from the LHC
- Highly distributed, >170 organisations
- CERN provides 20% of storage & compute





WLCG AuthN & AuthZ

- Born in early 2000s
- Best solution at the time for AuthN and AuthZ was to use **X.509 certificates**, with proxy certificate extensions to convey groups/roles (VOMS)
- Has been working for 20 years but community is increasingly motivated to move to Tokens
- **IAM has been chosen as the future WLCG Token Issuer**



Why the move to Tokens?

- **Evolving Identity Landscape**
  - User-owned X.509 certificates -> federated identities (SAML & OpenID Connect)
- **Technology Readiness**
  - Increasing solutions for shielding users from the complexities of X.509 certificate management
  - Token-based authorization widely adopted in commercial services and increasingly by R&E Infrastructures
- **Data Protection**
  - Tightening of data protection (GDPR) requires fine-grained user level access control, certain provisioning practices may need to be adjusted

However, not all grid middleware supports token (OAuth2) based authorization (yet…!).

Objective: Understand & meet the requirements of a future-looking AuthZ service for WLCG experiments

WLCG AuthZ WG

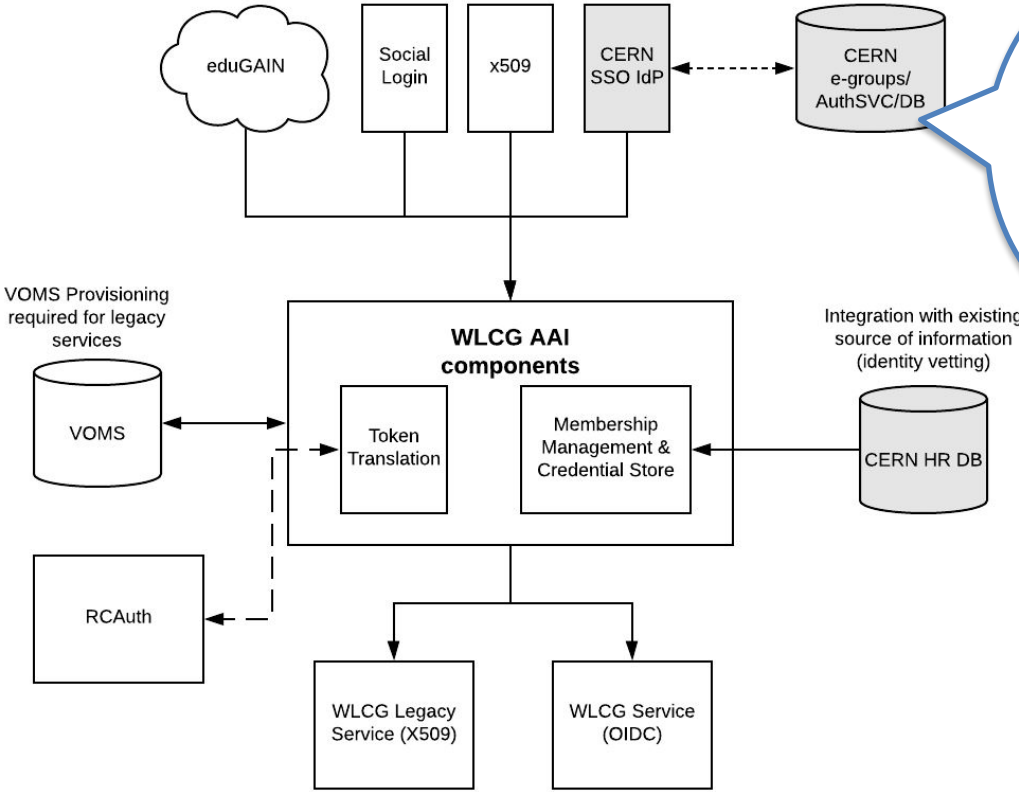
- Includes current major users of tokens in High Energy Physics
  - INDIGO IAM
  - EGI Check-in
  - SciTokens
  - dCache
  - ALICE
- Development work of pilot projects supported by:

- Priority to stick to industry and R&E standards wherever possible

AAI Design

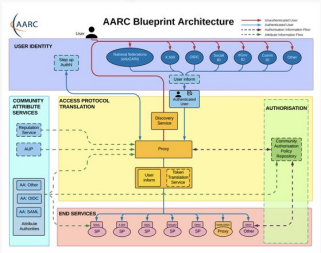
OpenID

eduGAIN



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/



WLCG Worldwide LHC Computing Grid

Token Claims

Common Claims	ID Tokens	Access Tokens
• sub • exp • iss • acr • aud • iat • nbf • jti • eduperson_assurance (REFEDS) • wlcg.ver (WLCG) • wlcg.groups (WLCG)	• auth_time • general OIDC Claims	• scope (RFC8693)

wlcg prefix added to avoid collisions

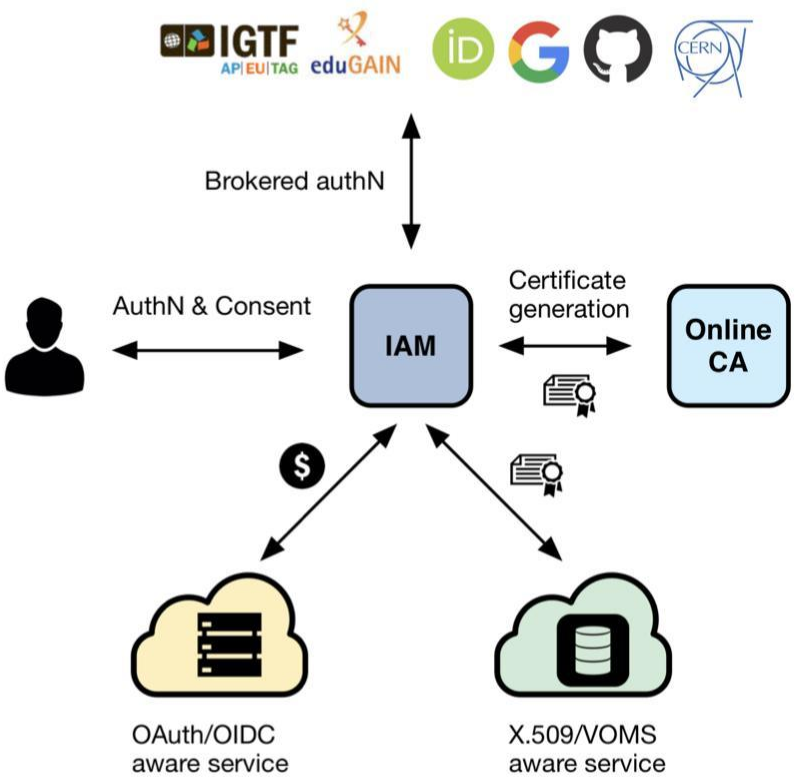
Access tokens should include at least scope or group

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

INDIGO Identity and Access Management Service

A **VO-scoped** authentication and authorization service that

- supports **multiple authentication mechanisms**
- provides users with a **persistent, VO-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**

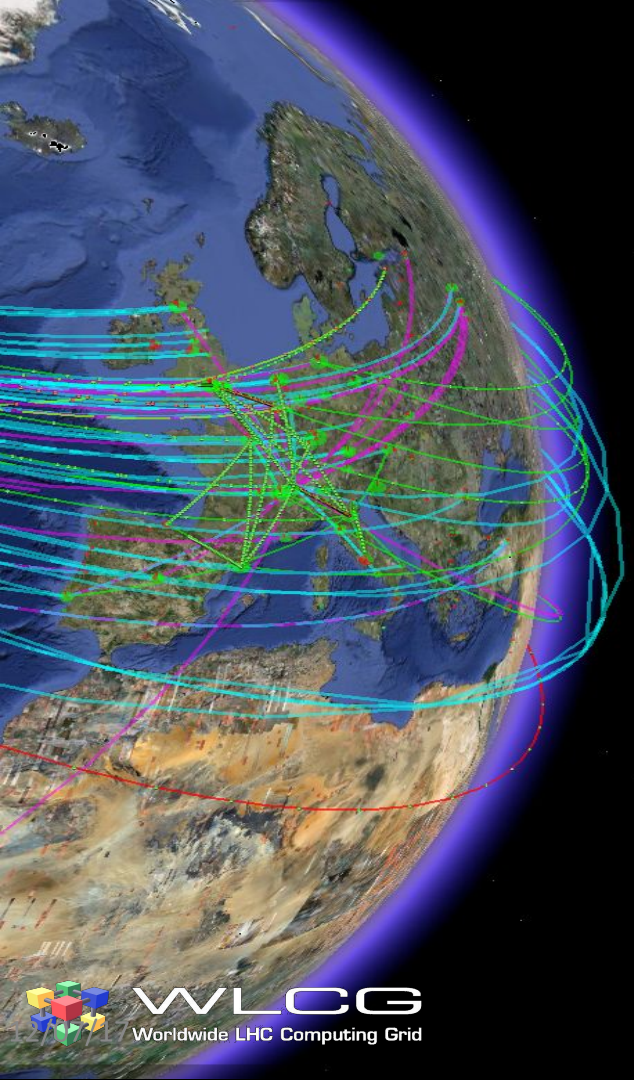


Easy integration with relying services

Standard OAuth/OpenID Connect enables **easy integration** with off-the-shelf services and libraries.

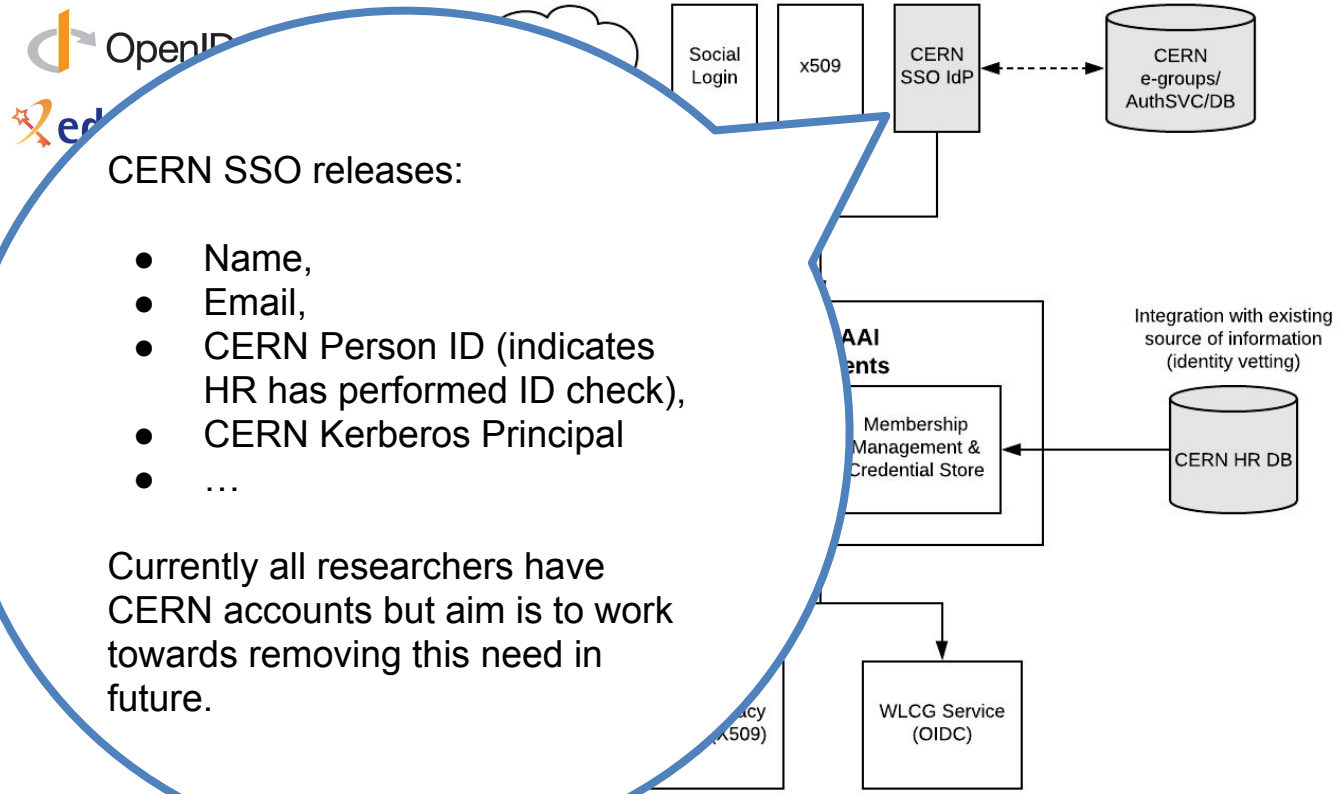
IAM has been successfully integrated with

- Openstack, Atlassian JIRA & Confluence, Moodle, Rocketchat, Grafana, Kubernetes, JupyterHub, dCache, StoRM, XRootD (HTTP), FTS, RUCIO, HTCondor



Integration with CERN & Certificates

AAI Design

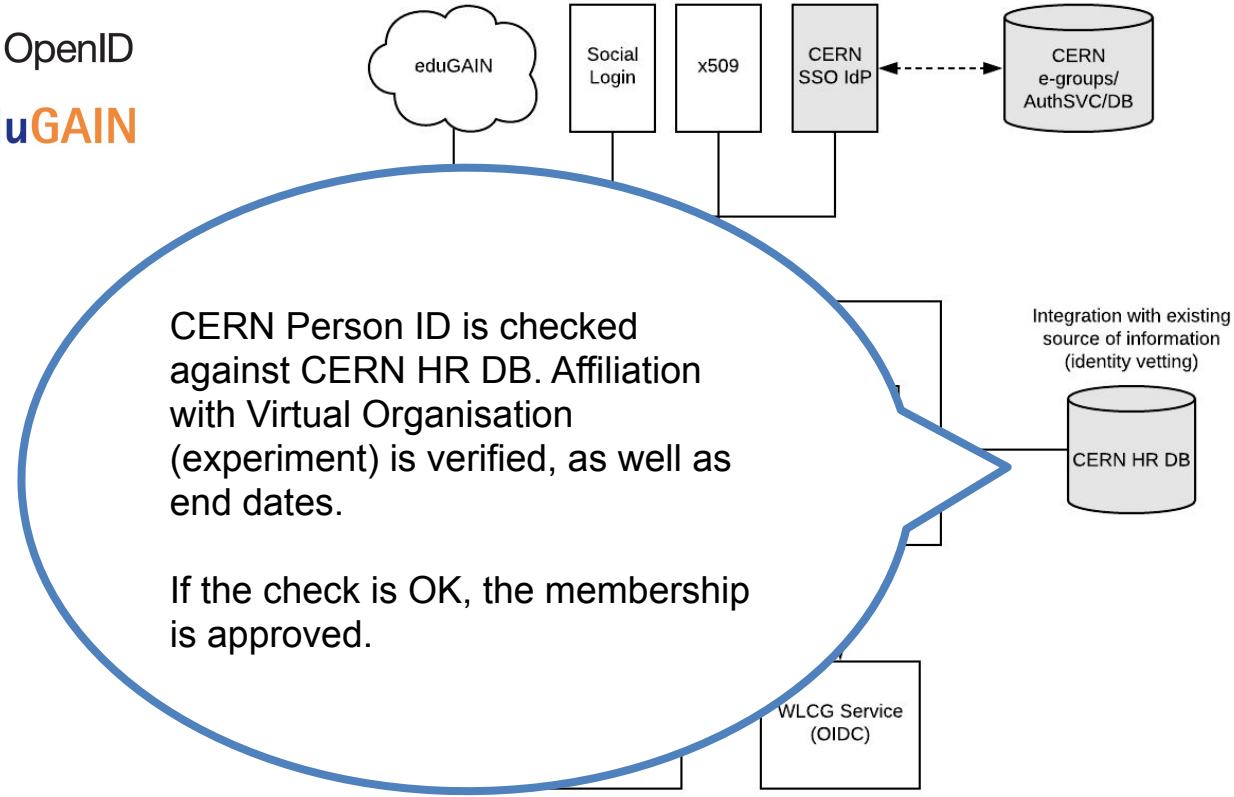


CERN SSO releases:

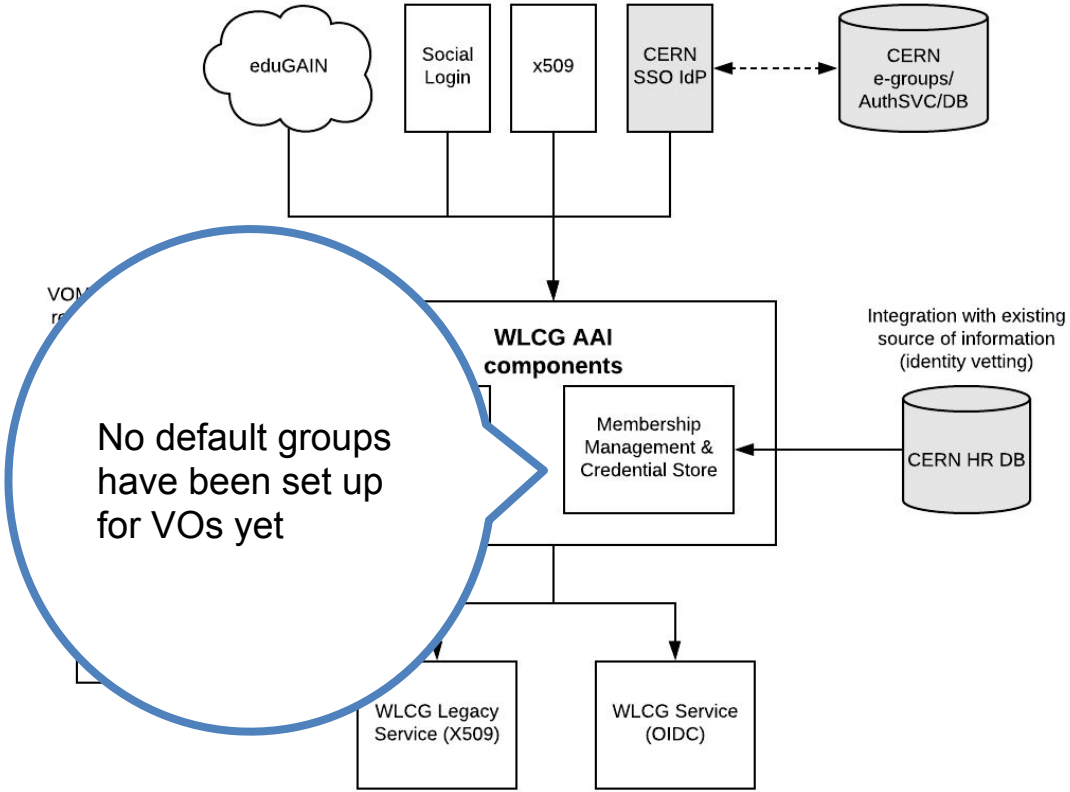
- Name,
- Email,
- CERN Person ID (indicates HR has performed ID check),
- CERN Kerberos Principal
- …

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

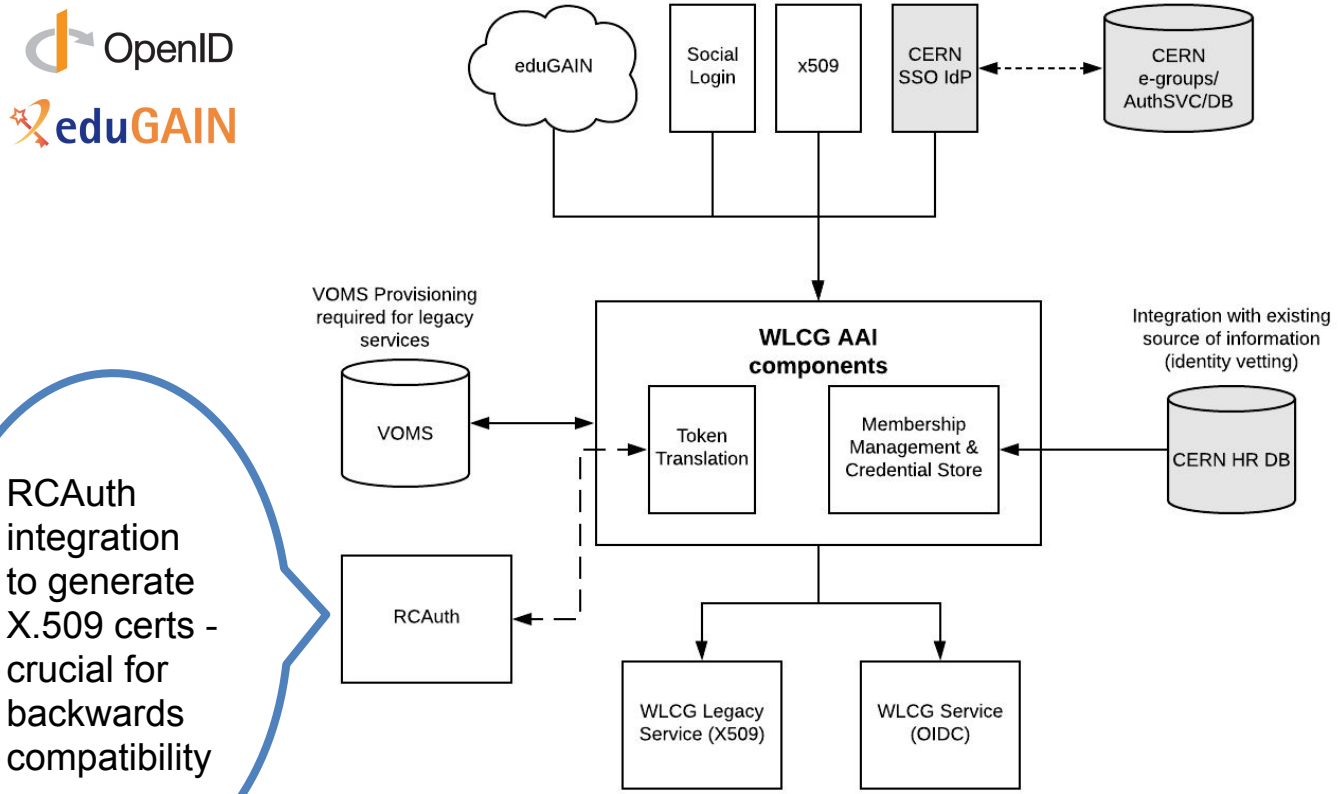
AAI Design


OpenID
eduGAIN
eduGAIN
Social Login
x509
CERN SSO IdP
CERN e-groups/ AuthSVC/DB
Integration with existing source of information (identity vetting)
CERN HR DB
WLCG Service (OIDC)
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

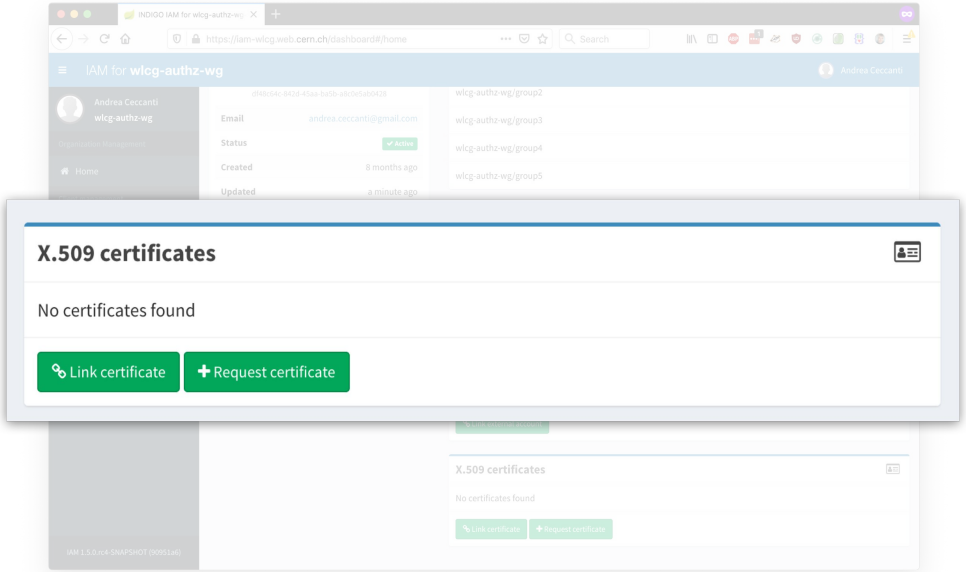

eduGAIN
Social Login
x509
CERN SSO IdP
CERN e-groups/ AuthSVC/DB
WLCG AAI components
Membership Management & Credential Store
Integration with existing source of information (identity vetting)
CERN HR DB
No default groups have been set up for VOs yet
WLCG Legacy Service (X509)
WLCG Service (OIDC)

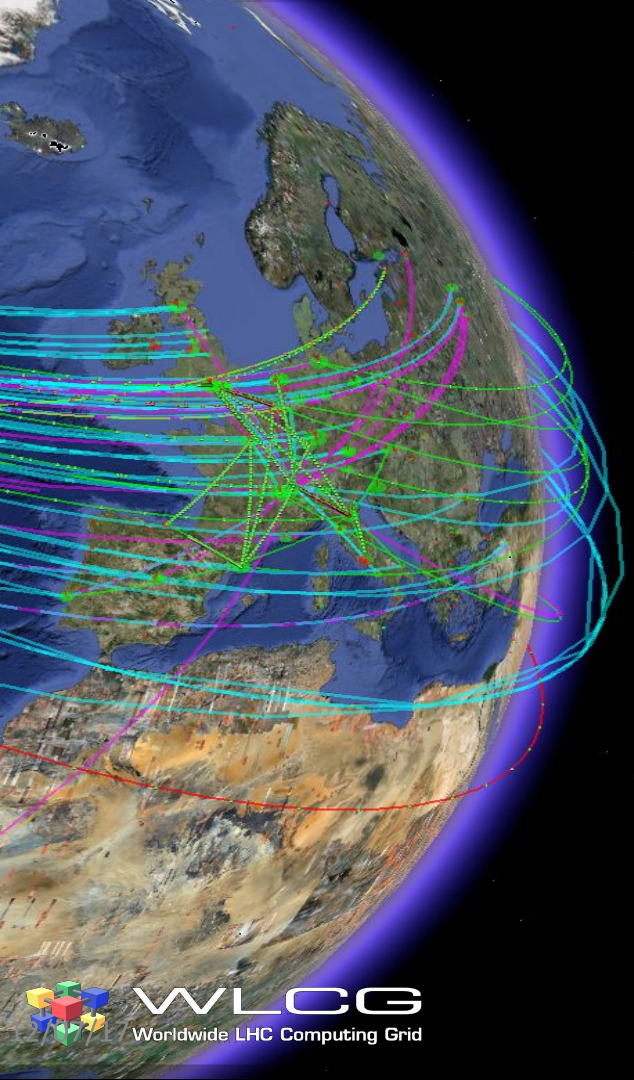
AAI Design


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)
RCAuth integration to generate X.509 certs - crucial for backwards compatibility

X.509 Compatibility

- X.509 certificate generated
- Long lived proxy cert generated and stored in IAM
- Available via authenticated REST API





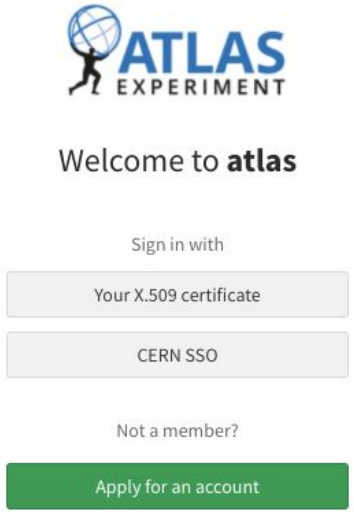
Deployment

Deployment

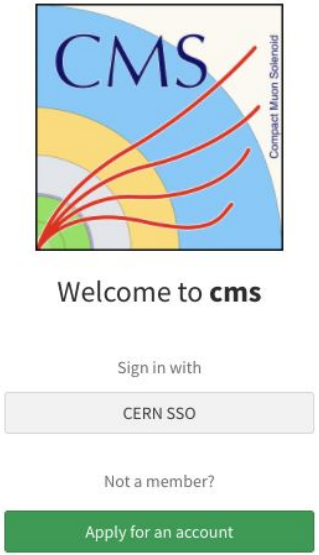
- Deployed on CERN's **Openshift** infrastructure
- IAM run as **Docker** container
- Configuration managed using CERN's **gitlab** https://gitlab.cern.ch/wlcg-iam-deployments
- Deployment managed by **Kubectl**

Current blocker is getting IGTF cert for openshift project - work in progress!

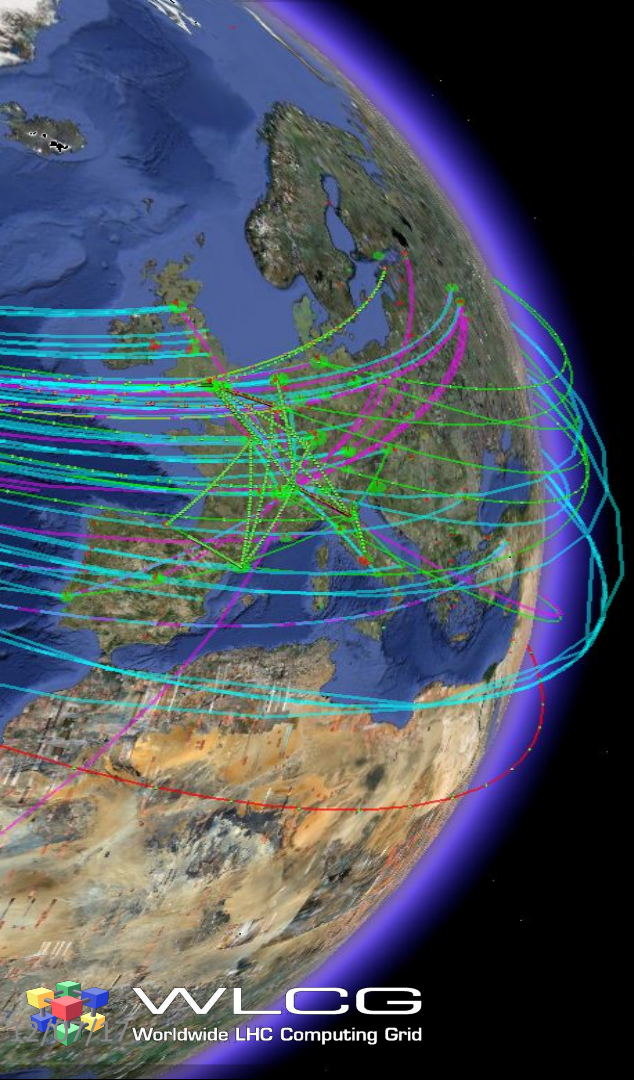
Deployments



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



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



Migration

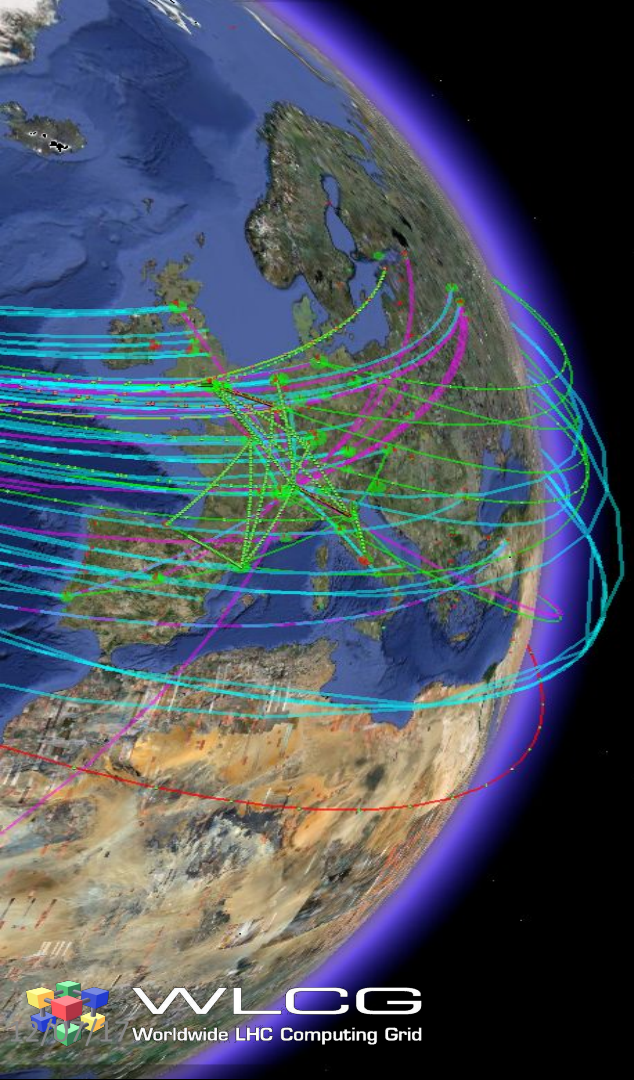
Overview

- X.509 will continue to play a vital role in our infrastructure as host certificates, but users will no longer need to manage the certificate lifecycle themselves
- VOMS records will be synchronised to IAM instances
- It is likely that power users, e.g. admins, may need to manage certificates for much longer

	2019	2020	2021	2022	2023
Integrate RCAuth.eu for on-demand IOTA X.509					
Migrate VOs to IAM, retire VOMS Admin					
Add Token support to Middleware					
Dual mode (IAM issues X.509/VOMS and Tokens)					
Privilege Tokens, analyse remaining X.509 use					
Begin removing X.509 User Certificate Support					

Tentative Milestones (TBC)

- **March 2021** - WLCG baseline services include HTTP-TPC endpoint
- **July 2021** - IAM services available (including VOMS endpoints)
- **October 2021** - physics job submission performed with tokens
- **December 2021** - previous membership management interface retired (VOMS Admin)
- **January 2022** - OSG ends support for Grid Community Toolkit
- **March 2022** - Services support tokens for HTTP endpoints
- **October 2022** - data transfers performed with tokens
- **March 2023** - experiment stageout performed with tokens
- **March 2024** - X.509 client auth becomes optional



Questions?