Science and Technology Facilities Council

Welcome

Image © STFC Alan Ford

UKRI Science and Technology Facilities Council

IAM Update

Token Technical Meeting
Tom Dack

INDIGO IAM Recap

- INDIGO IAM will replace VOMS(-Admin)

- Integrates federated identities through CERN SSO plugin
- Obtains LHC experiment membership details from the CERN HR DB
  - Just like VOMS-Admin

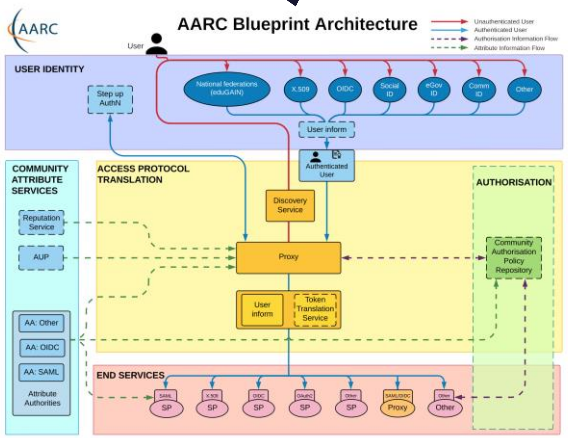
- Can issue fine-grained tokens to users and services
  - Details depend on the configuration per VO and per workflow

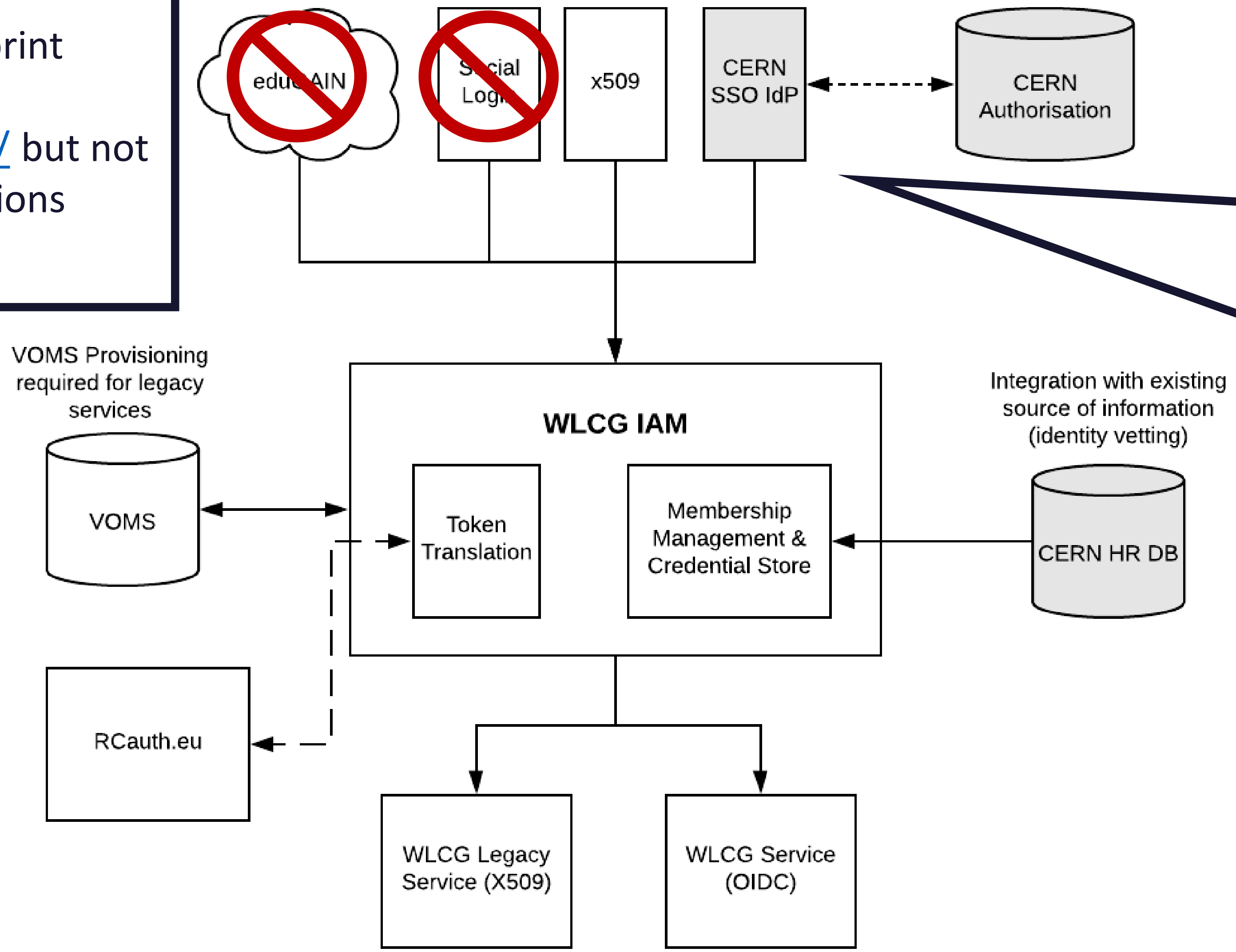
- Also has a VOMS endpoint for backward compatibility
  - Users will still have their X509 certificates linked for now

- It does **not** have a VOMS-Admin endpoint
  - Classic grid-mapfiles etc. have to be constructed using the IAM SCIM API
  - For any IAM instance, all SCIM API clients have to be **registered**

New AAI for WLCG

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




eduGAIN
Social Login
x509
CERN SSO IdP
CERN Authorisation
VOMS Provisioning required for legacy services
VOMS
WLCG IAM
Token Translation
Membership Management & Credential Store
Integration with existing source of information (identity vetting)
CERN HR DB
RCauth.eu
WLCG Legacy Service (X509)
WLCG Service (OIDC)

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

UKRI Science and Technology Facilities Council

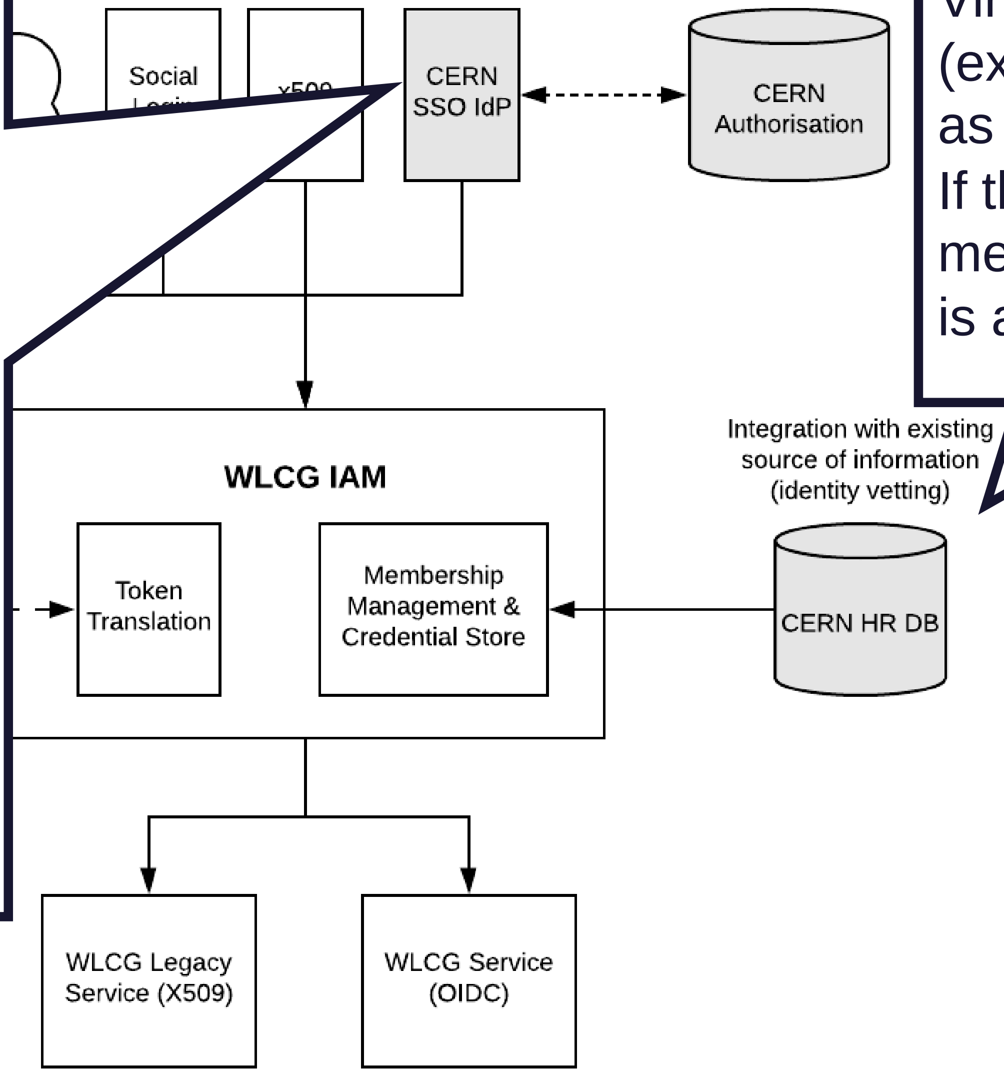
New AAI for WLCG

CERN SSO releases:

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

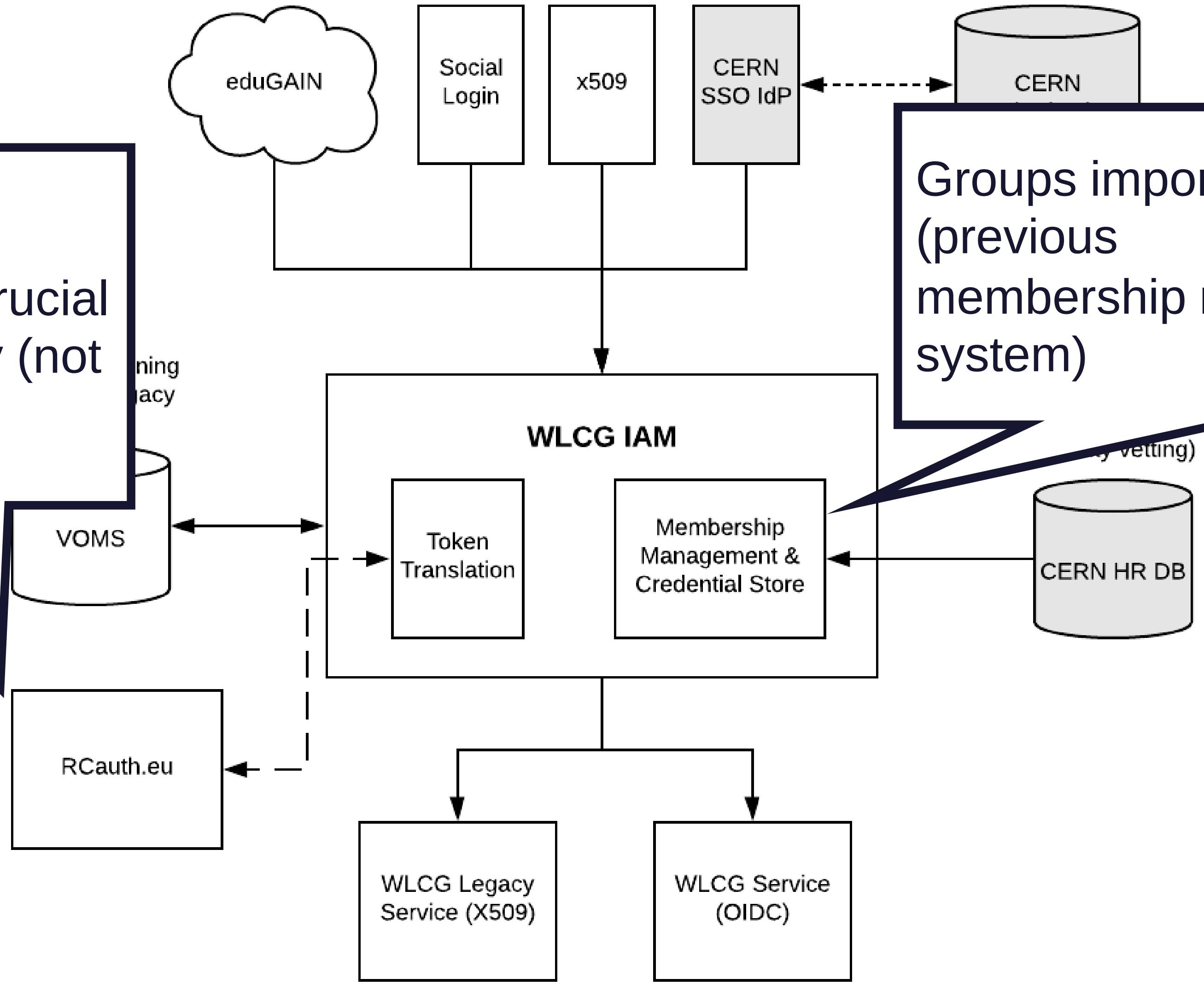
Currently all researchers have CERN accounts but aim is to work towards removing this need in future

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.



Social Login
x509
CERN SSO IdP
CERN Authorisation
WLCG IAM
Token Translation
Membership Management & Credential Store
Integration with existing source of information (identity vetting)
CERN HR DB
WLCG Legacy Service (X509)
WLCG Service (OIDC)

New AAI for WLCG

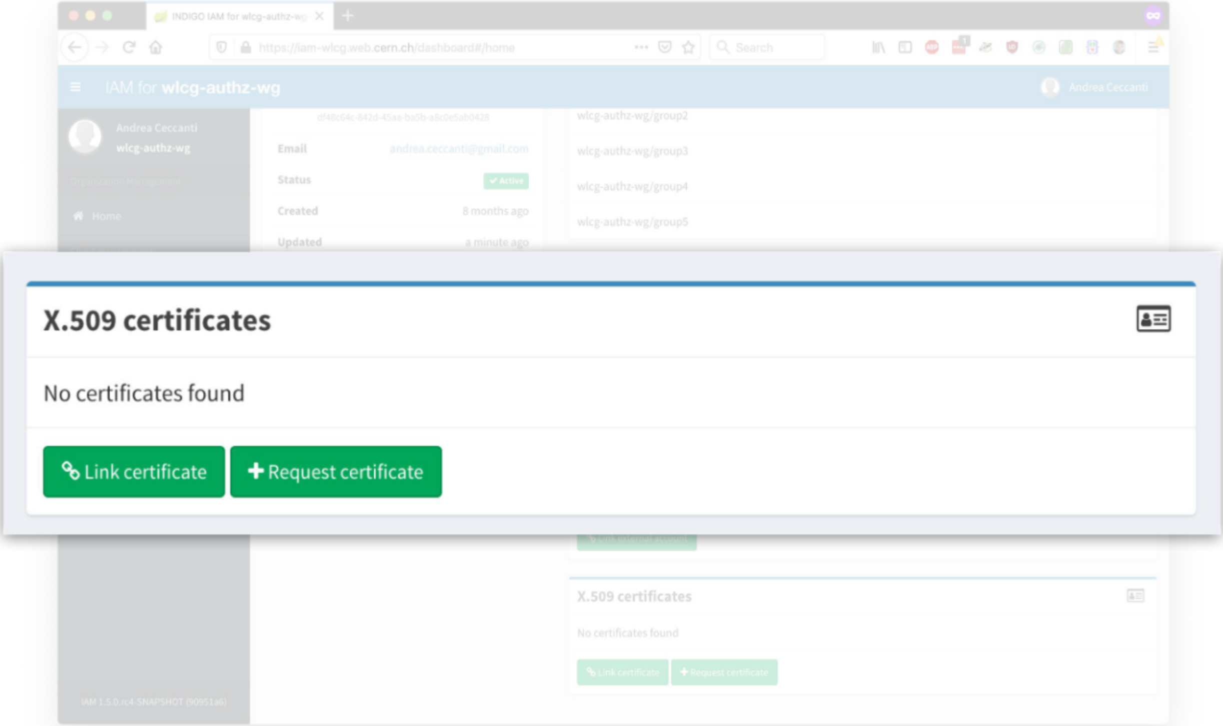


RCAuth integration
to generate X.509 certs - crucial for backwards compatibility (not currently used)

Groups imported from VOMS (previous
membership management system)

X.509 Compatibility

- X.509 certificate can be linked to an IAM account
- Long lived proxy cert can be stored in IAM
- Available via authenticated REST API (SCIM)
- IAM also can connect to RCAuth, however work is needed to understand status of RCAuth integration



X.509 certificates

No certificates found

Science and Technology Facilities Council

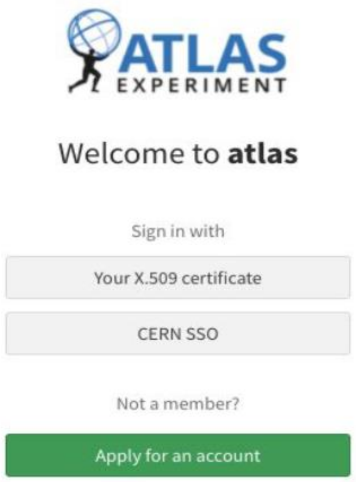
Deployment

- 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

GitLab OPENSHIFT

docker

Deployments



Welcome to **atlas**

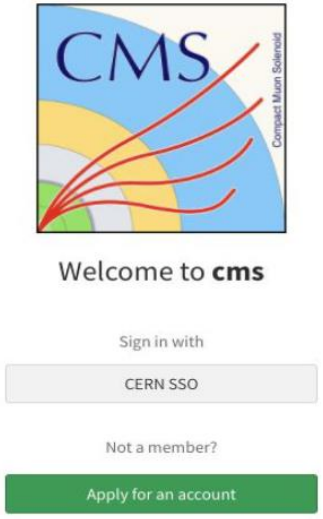
Sign in with

Your X.509 certificate

CERN SSO

Not a member?

Apply for an account



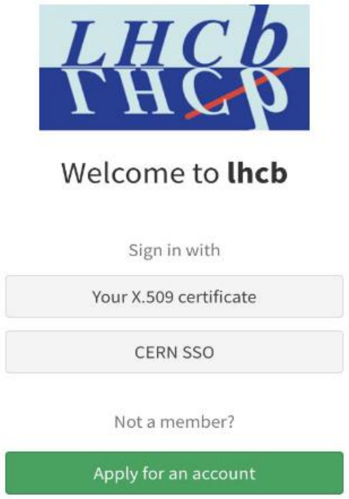
Welcome to **cms**

Sign in with

CERN SSO

Not a member?

Apply for an account



Welcome to **lhcb**

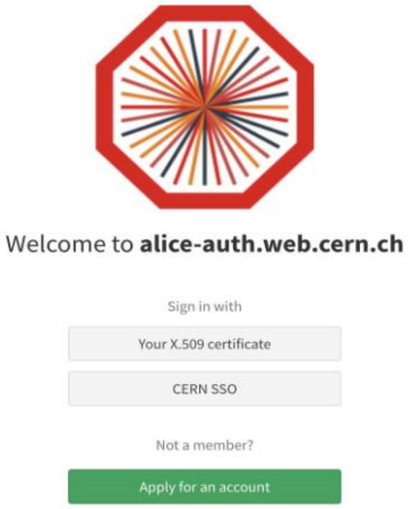
Sign in with

Your X.509 certificate

CERN SSO

Not a member?

Apply for an account



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

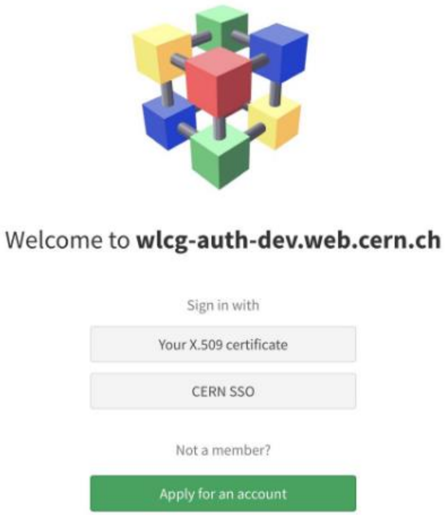
Sign in with

Your X.509 certificate

CERN SSO

Not a member?

Apply for an account



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

Sign in with

Your X.509 certificate

CERN SSO

Not a member?

Apply for an account

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

Supporters

- Operational support provided by INFN/CNAF IAM team and by CERN IT
  - CERN IT has recently confirmed a new recent-graduate starter, who will join the team 01/02/23
  - This will help provide further support in case of issues, such as the one on 31/10

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

Recent Issues: Oct 2022 Downtime

- At 07:02 31/10, after more than two days of smooth operation under vegeta stress test (~100 Hz, ~400 ms response time, ~0% error rate), IAM showed service degradation
- Likely issue was the K8S liveness probe took it down because it was not responding to the /health endpoint within the timeout
- Probable cause was IAM was stuck in some SQL query and was not able to make the /health endpoint available within the timeout
- Noticed large database tables (especially the one keeping the access tokens), which caused long completion times for SQL queries

- AuthZ postmortem review - includes links to ATLAS and Batch

IAM Dev Team General Considerations

- ~100 Hz sustained for more than two days is good news

- Scalability testing is on our roadmap, but to be effective it has to be done in a controlled environment, so that we can monitor relevant service parameters (memory, cpu, network, disk, database interaction, etc.)

- We have limited information about the IAM behaviour at the time when it became unavailable to know exactly what happened, so we can only/mostly speculate

Science and
Technology
Facilities Council

Questions?

Science and Technology Facilities Council

Thank you

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