WLCG Tokens Update

18th FIM4R Workshop
30th January 2024

Tom Dack
STFC UKRI

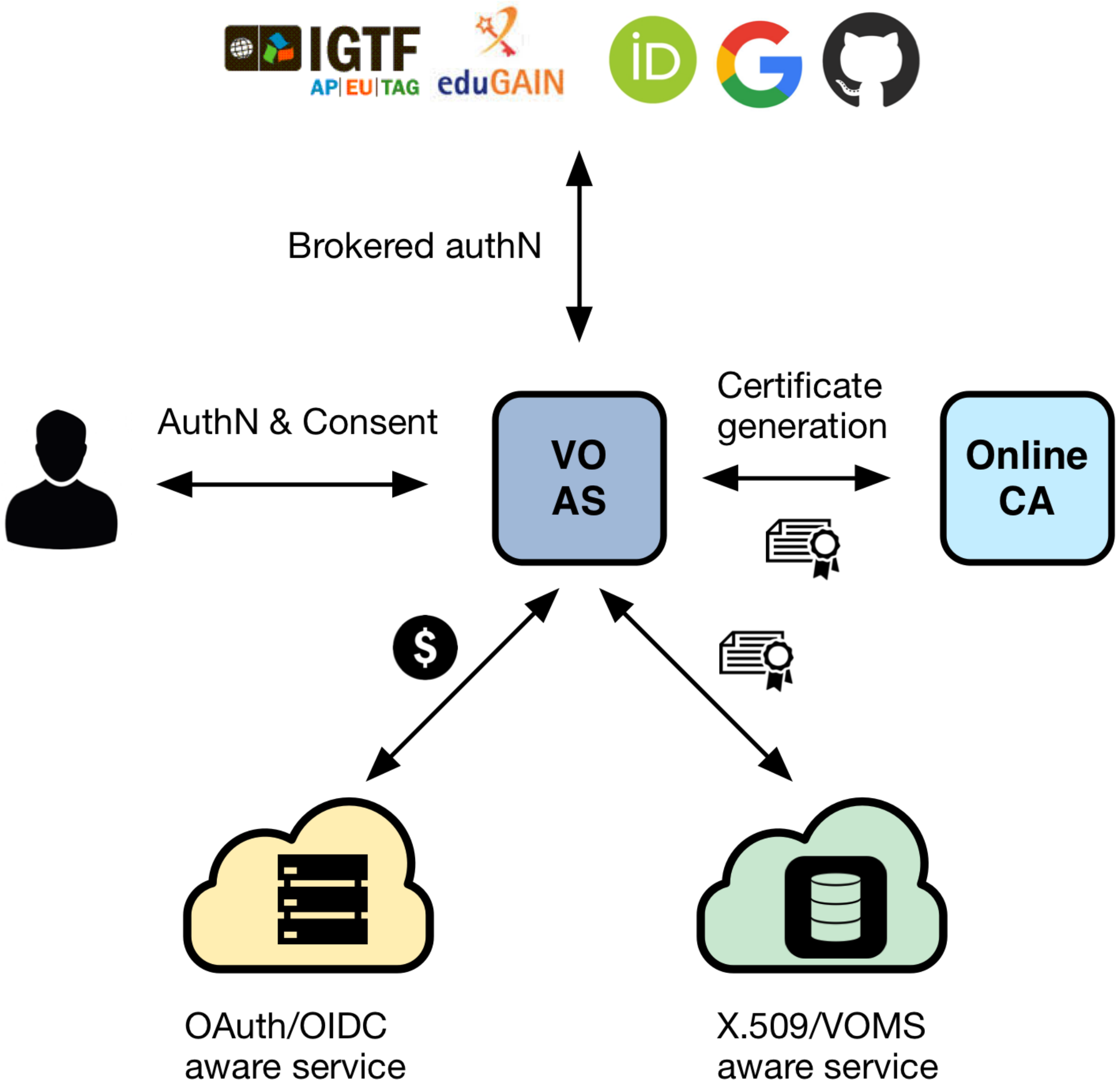
On behalf of the

WLCG Authorisation Working Group

Token Based AAI for WLCG

- VO Scoped Token issuers, which can:
  - Support multiple authentication mechanisms
    - Currently supporting CERN SSO or X.509
  - Provide users with a persistent VO-Scoped identity
  - Expose identity information, attributes and capabilities to services via JWT tokens and standard OAuth & OpenID Connect protocols
  - Integrate with existing VOMS-aware services
  - Support both Web and non-Web access, delegation, and token renewal

- WLCG uses **INDIGO IAM** as its token issuer



Status

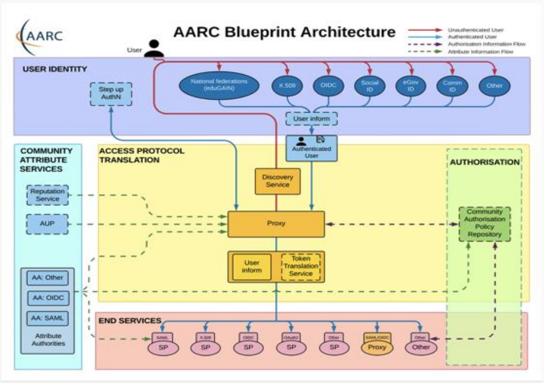
- ATLAS and CMS moved to HTCondor 10 in Summer 2023, and support tokens from respective IAM instances
- ALICE
  - Token deployment campaign done, for HTCondor CE sites only
  - VOMS proxies will continue being used with ARC CEs for now
    - And with HTCondor CEs *in addition*, because APEL currently expects that
    - ALICE jobs do not need that proxy anymore
- LHCb
  - Token deployment campaign mostly done, for HTCondor CE sites only
- RUCIO token support in place for upcoming data challenge, with sufficient integration with FTS/gfal
  - RUCIO interaction non-standard at current, using the client credentials flow to request a token with a specific scope and audience

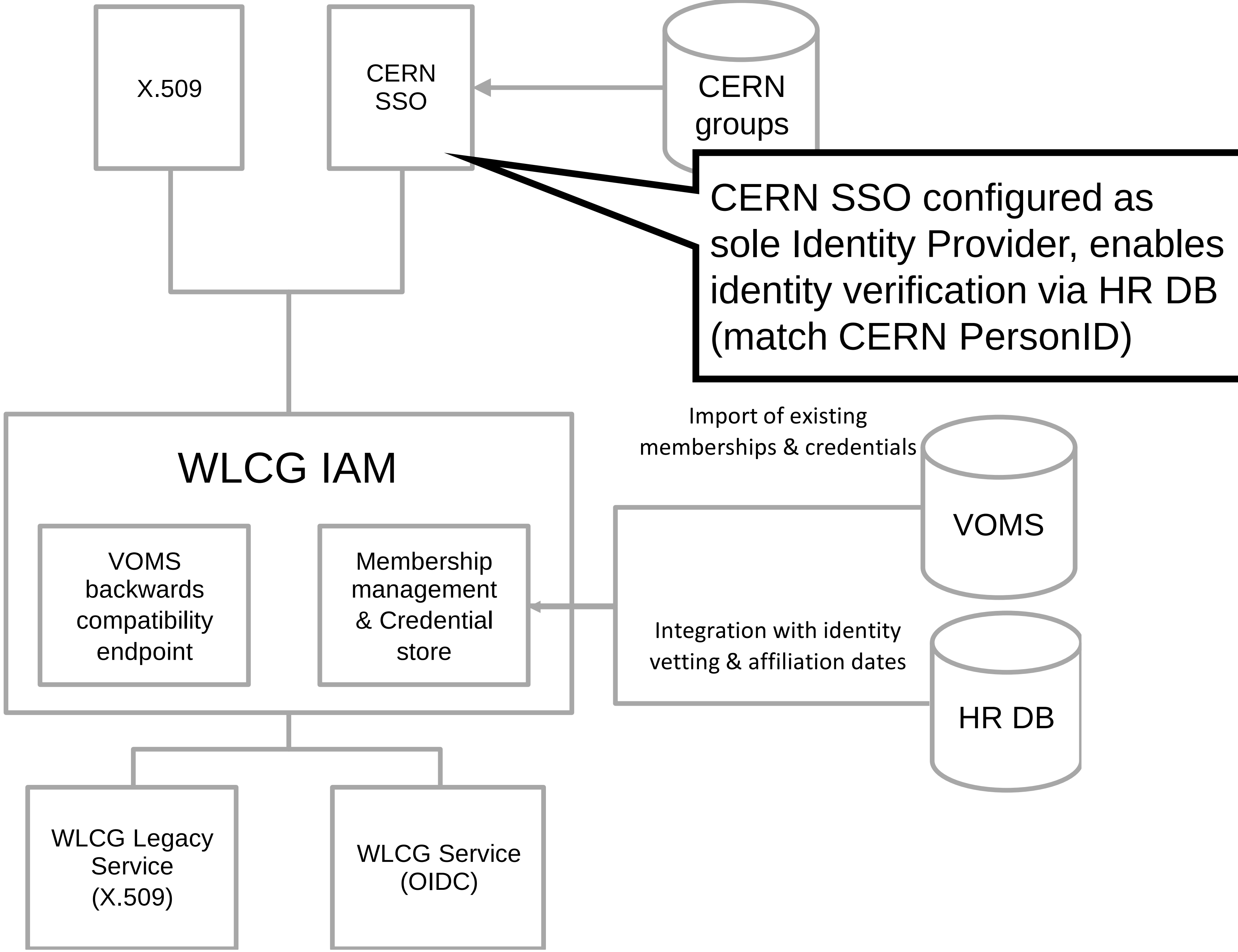
Status

- First HTCondor CE token campaign on EGI done
  - HTCondor CE v5 + condor-9.0.x
- Second EGI Campaign was launched Nov 3 and updated Nov 17
  - HTCondor CE v5 + condor **v9.0.20**
  - A stepping stone towards next phase
- Third EGI campaign to be launched in the spring of this year
  - HTCondor CE >= **v23** with condor >= **v23**

WLCG Token Infrastructure Design

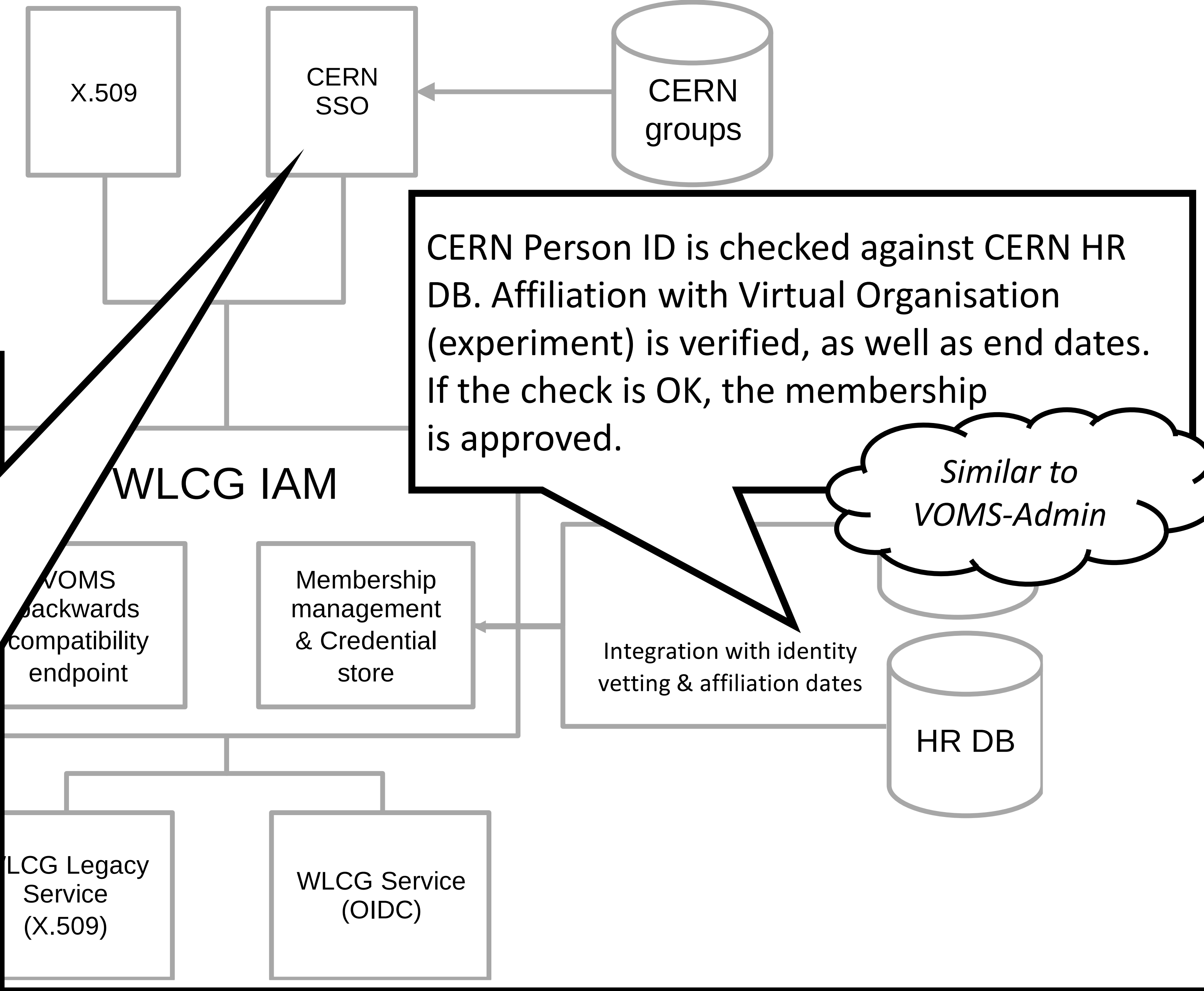
Follows the AARC Blueprint: https://aarc-community.org/architecture/ but not all AEGIS recommendations




X.509
CERN SSO
CERN groups
WLCG IAM
VOMS backwards compatibility endpoint
Membership management & Credential store
Import of existing memberships & credentials
VOMS
Integration with identity vetting & affiliation dates
HR DB
WLCG Legacy Service (X.509)
WLCG Service (OIDC)

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

WLCG Token Infrastructure Design


X.509
CERN SSO
CERN groups
WLCG IAM
VOMS backwards compatibility endpoint
Membership management & Credential store
Integration with identity vetting & affiliation dates
HR DB
LCG Legacy Service (X.509)
WLCG Service (OIDC)

CERN SSO releases:

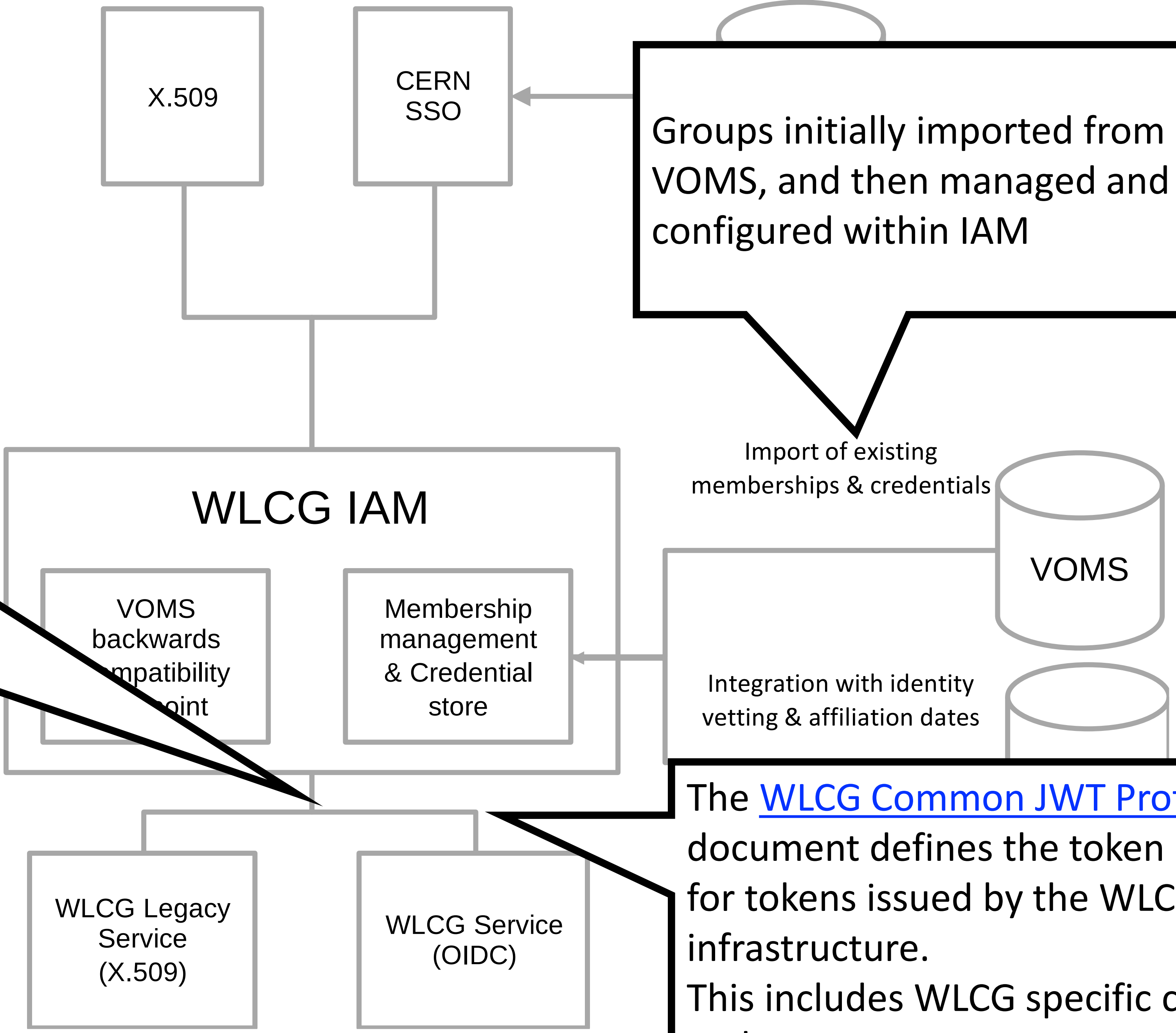
- Name,
- Email,
- CERN Person ID (indicates HR has performed ID check),
- CERN Kerberos Principal
- ...

Currently LHC experiment members can have CERN accounts, and so all access is via CERN SSO or Linked X.509, 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.

Similar to VOMS-Admin

WLCG Token Infrastructure Design


X.509
CERN SSO
WLCG IAM
VOMS backwards
mpatibility
oint
Membership management & Credential store
Import of existing memberships & credentials
VOMS
Integration with identity vetting & affiliation dates
WLCG Legacy Service (X.509)
WLCG Service (OIDC)

Groups initially imported from VOMS, and then managed and configured within IAM

Outbound communication of user information to end services, which can be used to establish authorization.

VOMS proxies can still be used for as long as they are needed.

The WLCG Common JWT Profiles document defines the token profile for tokens issued by the WLCG infrastructure.
This includes WLCG specific claims and scopes.

Current Focus

- Required updates to the WLCG Common JWT Profiles
  - Discussion and experience since the v1.0 release, Sept 2019, means there are a number of areas where re-writing and updating is required.
  - WLCG intends to collaborate closely with the “Grand Unified Token Profile” work, to best facilitate interoperability with other issuers.

- Operational Experience to be gained from DC24
  - Token authorised data transfers should take part during DC24 using production infrastructure components
  - This will provide vital operational expertise and help identify areas of improvement

AuthZ WG selected discussion topics

- How to determine the VO for various kinds of tokens?
  - Needed e.g. by APEL for accounting
  - Differences between how things are defined in the WLCG profile vs other issues, such as EGI Check-In

- Use of `scope` vs. `wlcg.groups`
  - Groups are primarily foreseen to provide *context* information, but may also be used for AuthZ decisions by services that have been configured to use groups *instead of* capabilities, as agreed between a VO and those services
  - WLCG token profile to be updated accordingly

- Token rates and lifetimes
  - Avoid IAM being the bottleneck
  - High rates vs. transparent service downtimes
  - Mitigate through longer lifetimes and/or less fine-grained scopes
  - Impacts IAM, FTS, Rucio, DIRAC
  - Different treatments of read / create vs. modify (delete)
  - Today no such distinctions with VOMS proxies!
  - We hence do not need a perfect system right from the start

We will gain operational experience in **DC24** (Feb 12-23)

Token **Trust** and ***Traceability*** (TTT) WG

- Instantiated in August, intended to fill a role similar to that of the previous Traceability and Isolation WG.
  - And drawing from the findings of that group.
  - Working alongside members of the AuthZ WG, meetings within the Security Group in Indico.

- Meeting approximately once a month, no regular slot yet.

- Aiming to bring together collaborators from a range of communities
  - WLCG, EGI, DUNE, SKA, others

- Intended to cover the Token side of the AuthZ coin - Federated Identity provision is important but mostly out of scope.
  - As is the user-side experience.

- Goal is to produce tangible outputs
  - Policy: Consider what is Best Practice. Risk Identification and Analysis. Building Trust in Tokens.
  - Documentation: Write down the above. And also produce “How-Tos”, guides and manuals.
    - E.g. “Understanding Token Flows for Admins”, “Token Job Tracing”, “Incident Response and Forensics in a Token-based environment.”

- Want to know more? Contact **Matt Doidge m.doidge@lancaster.ac.uk**
  - Or look up the CERN e-group token-trust-and-traceability-wg

Conclusions and outlook

- The main token *development*, *deployment* and *testing* objectives at this time are about:
  - Computing – HTCondor CE versions that no longer support GSI
  - Data transfers – preparations for DC24

- Work is underway to resolve issues with the existing WLCG token profile
  - As well as participation in the GUT Profile activity

- The *trust* and *traceability* of token workflows are to be served by various kinds of documentation to be produced by the TTT WG