Image © STFC Alan Ford

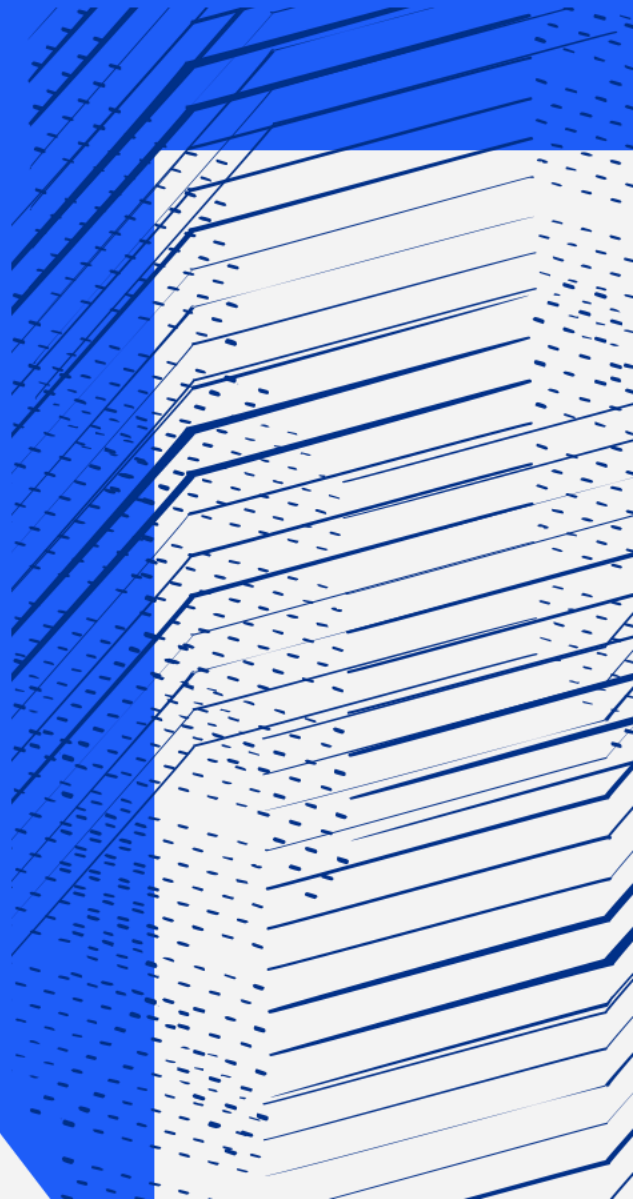
Science and Technology Facilities Council

Identity Management in GridPP7

Tom Dack, thomas.dack@stfc.ac.uk

GridPP49, Abingdon, 29 Mar 23

#translivesmatter



Transition to Tokens – Recap of Motivations

- OAuth and OIDC protocols have been adopted by a wide range of software and systems, thanks to their prevalence in industry – in particular within the social identity space
  - This prevalence enables developers to utilise developed libraries, and facilitates integration and interoperability

- User Certificates, whilst established within WLCG, are not familiar outside this context - and are often viewed as unintuitive. Conversely, Token-based flows are becoming increasingly commonplace, and can lead to a better user experience as a result

Identity Management in WLCG

- Token-based authentication and authorisation will arrive during GridPP7
- VOMs will be retired
- GridPP sites need to be prepared for token transition

Token Transition Milestones

From the Token Transition Timeline:

- M.2 (Dec 2022) DIRAC versions supporting job submission tokens deployed for concerned Vos
  - LHCb have upgraded to v8.0 and validated job submission to HTCondor and ARC CEs with tokens
  - Token configuration details to be communicated to the sites
- M.3 (Feb 2023) VOMS-Admin is switched off for one or more experiments
  - Pushed back, but good progress in CMS
- M.4 (Mar 2023) HTCondor installations at EGI sites have been upgraded to supported versions > 9.0.x
- M.5 (Mar 2023) End of HTCondor support for GSI Auth (link)
  - Postponed to May
- M.6 (Mar 2023) Some storage endpoints provide support for tokens
  - Pushed back, but steady progress in DOMA BDT WG

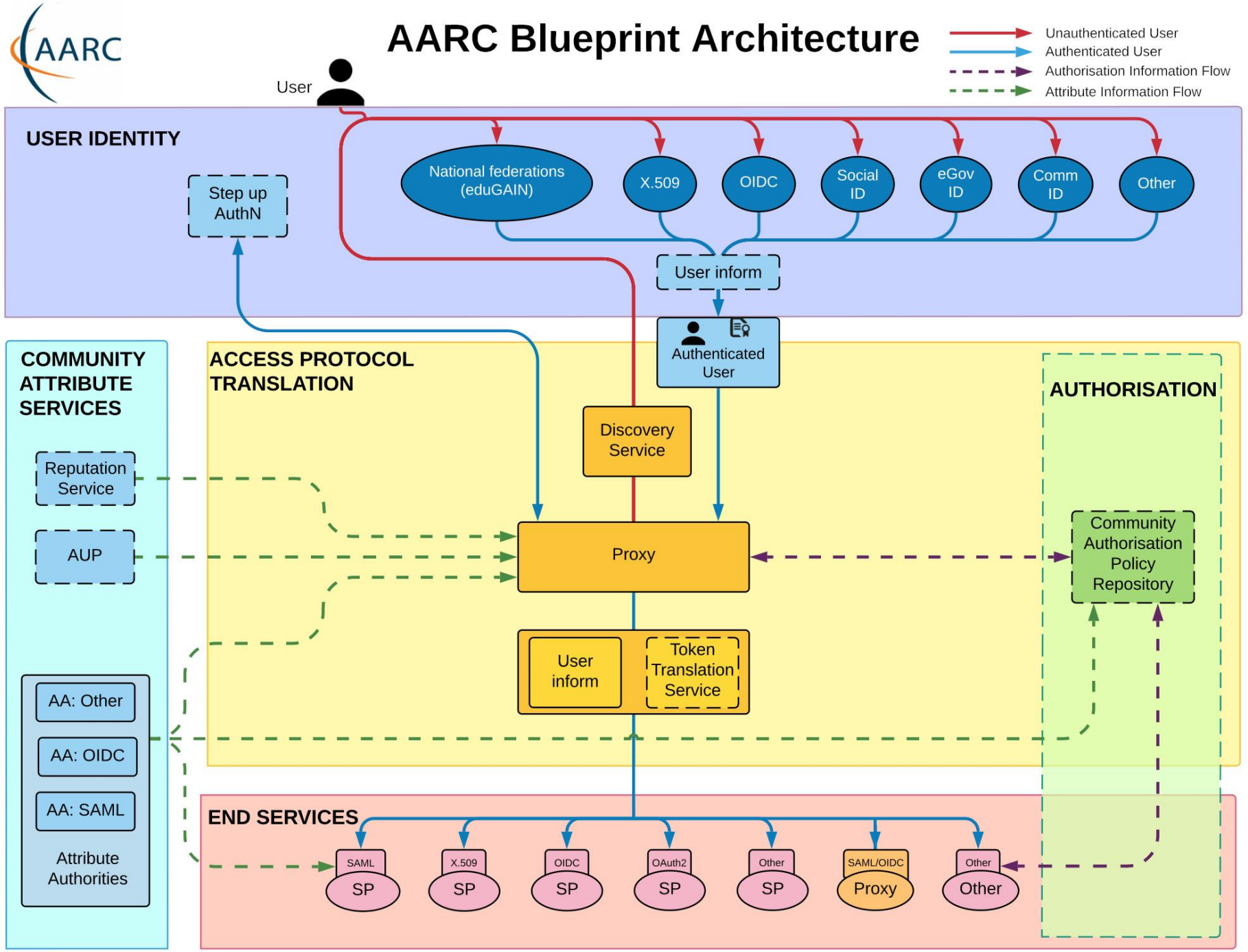
For further details on M.4 and M.5, see Maarten Litmaath's March GDB update

Science and Technology Facilities Council

Token Authentication and Authorisation Infrastructure

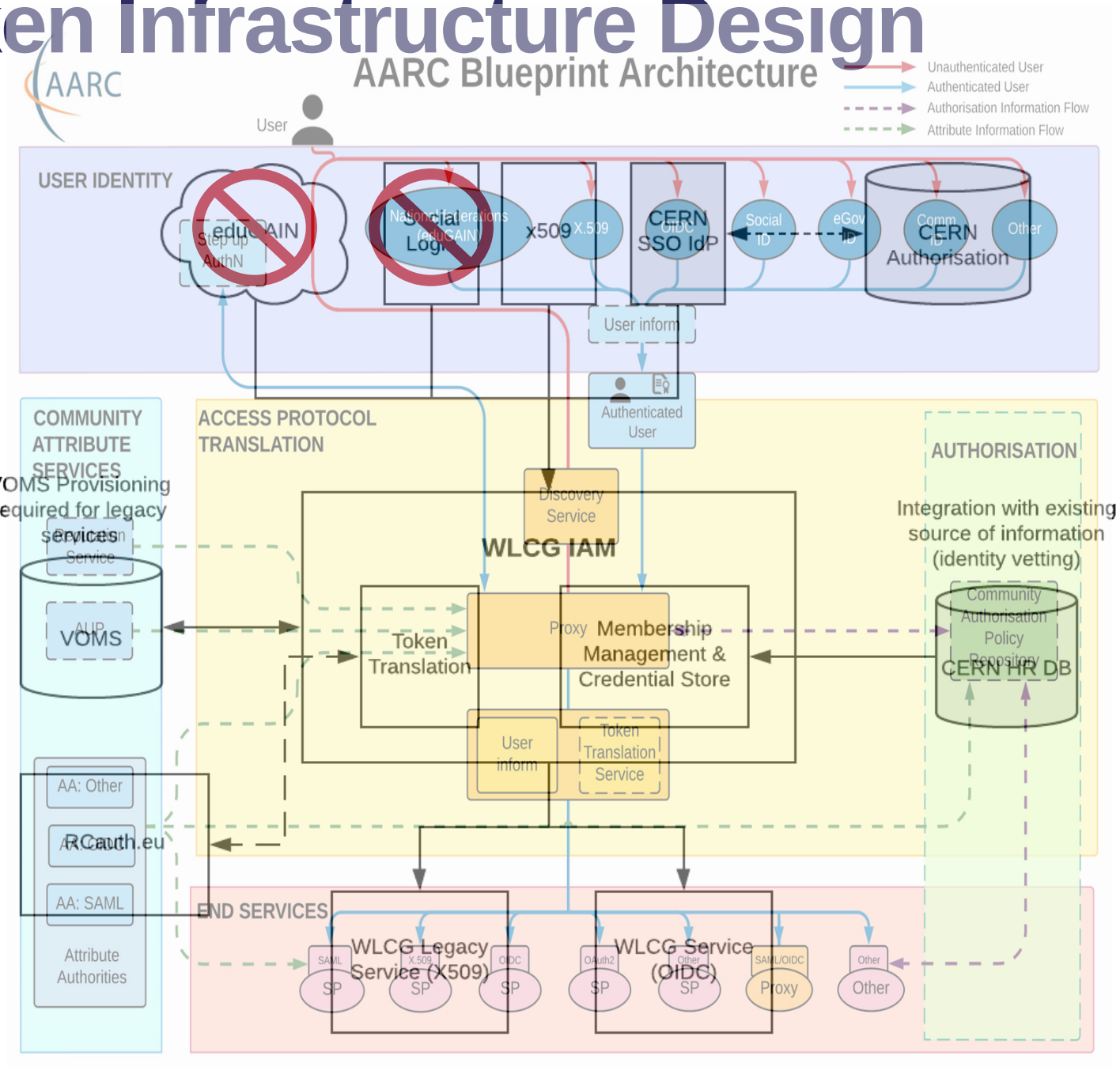
- In the planned WLCG infrastructure, there will be an OIDC Provider per VO, which users may access using their CERN Account
- This model unifies the IdP and Research community, with both being represented by the Token Issuer
- The Infrastructure design has been informed by the **AARC Blueprint architecture** - a set of software building blocks that can be used to implement federated access management solutions for international research collaborations

The AARC Blueprint



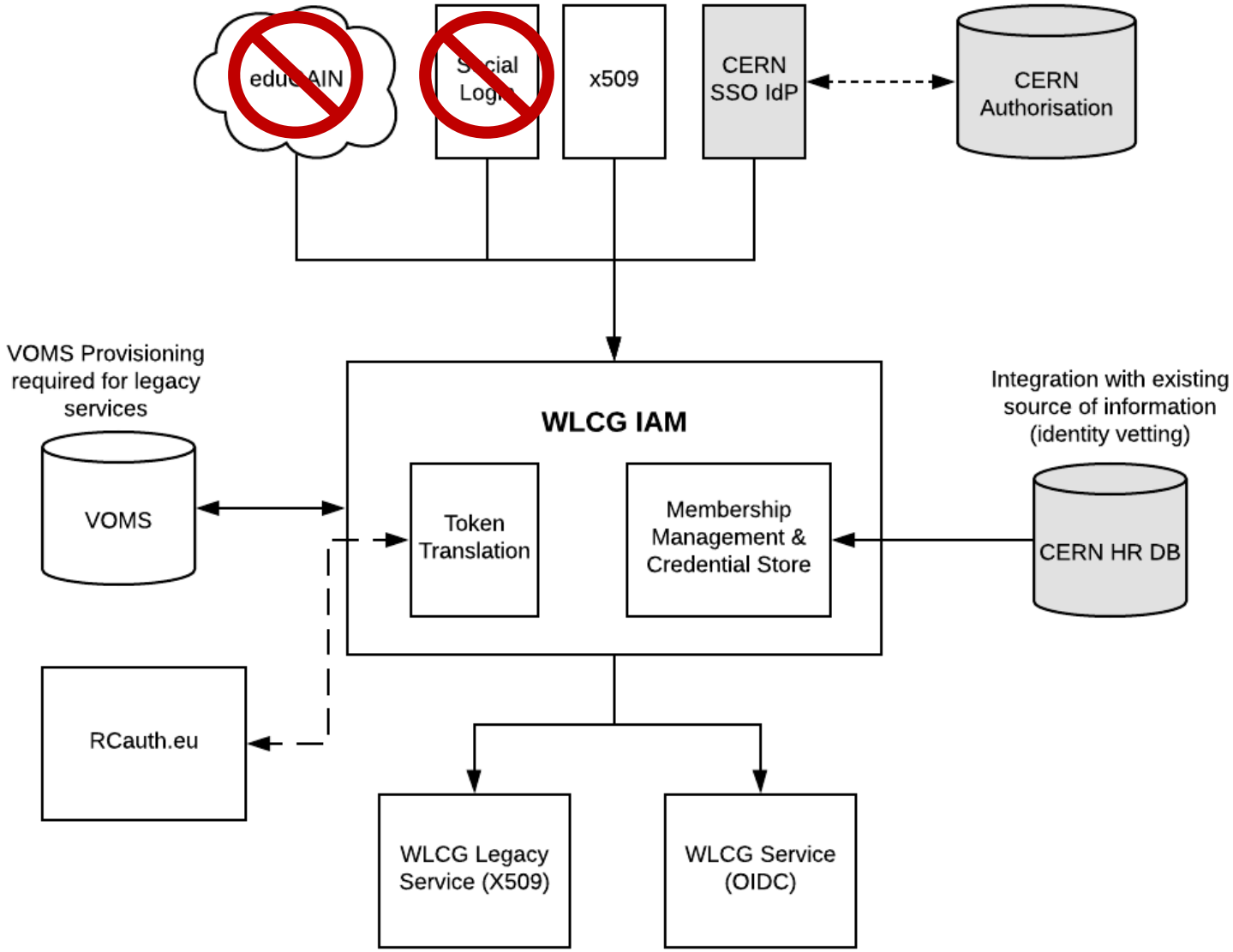
Science and Technology Facilities Council

WLCG Token Infrastructure Design



Science and Technology Facilities Council

WLCG Token Infrastructure Design



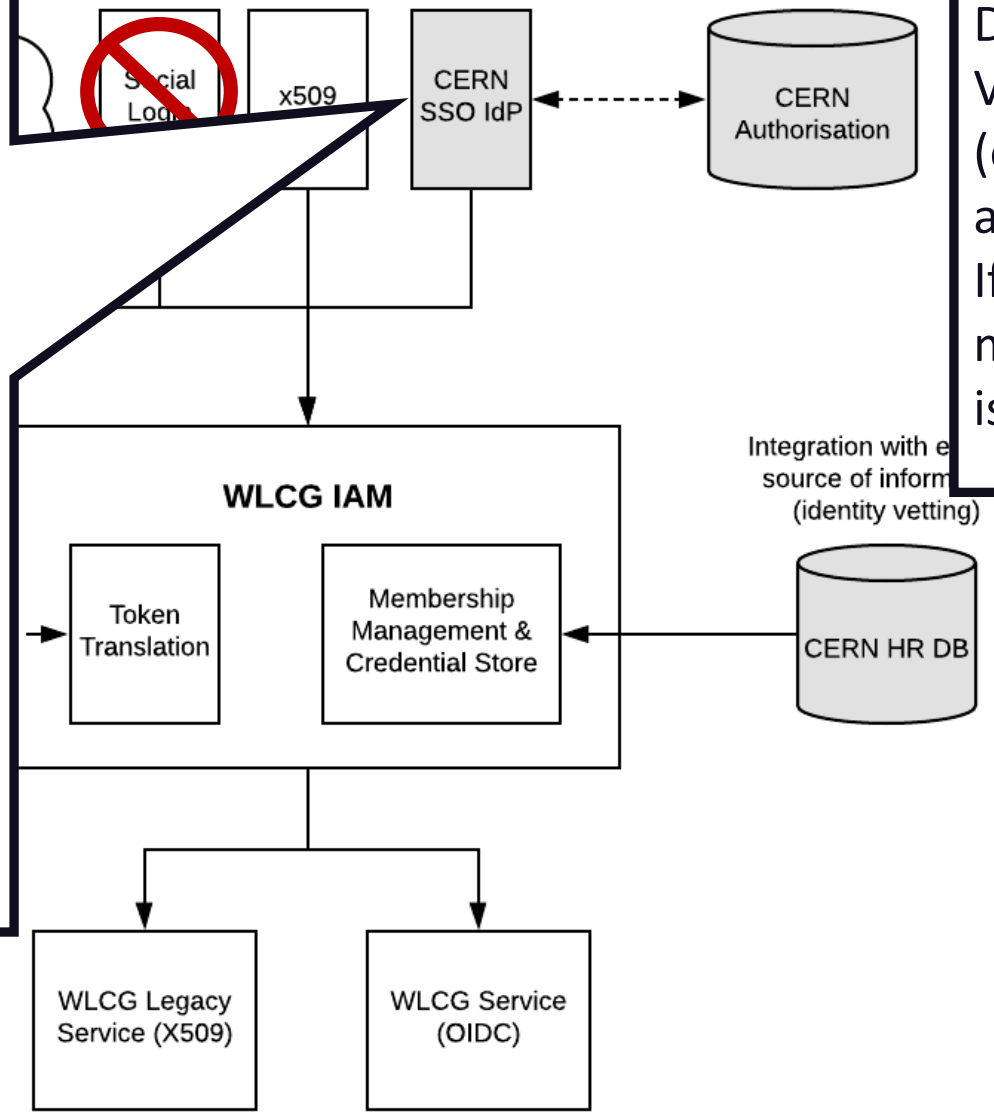
Science a
Technolog
Facilities C

WLCG Token Infrastructure Design

CERN SSO releases:

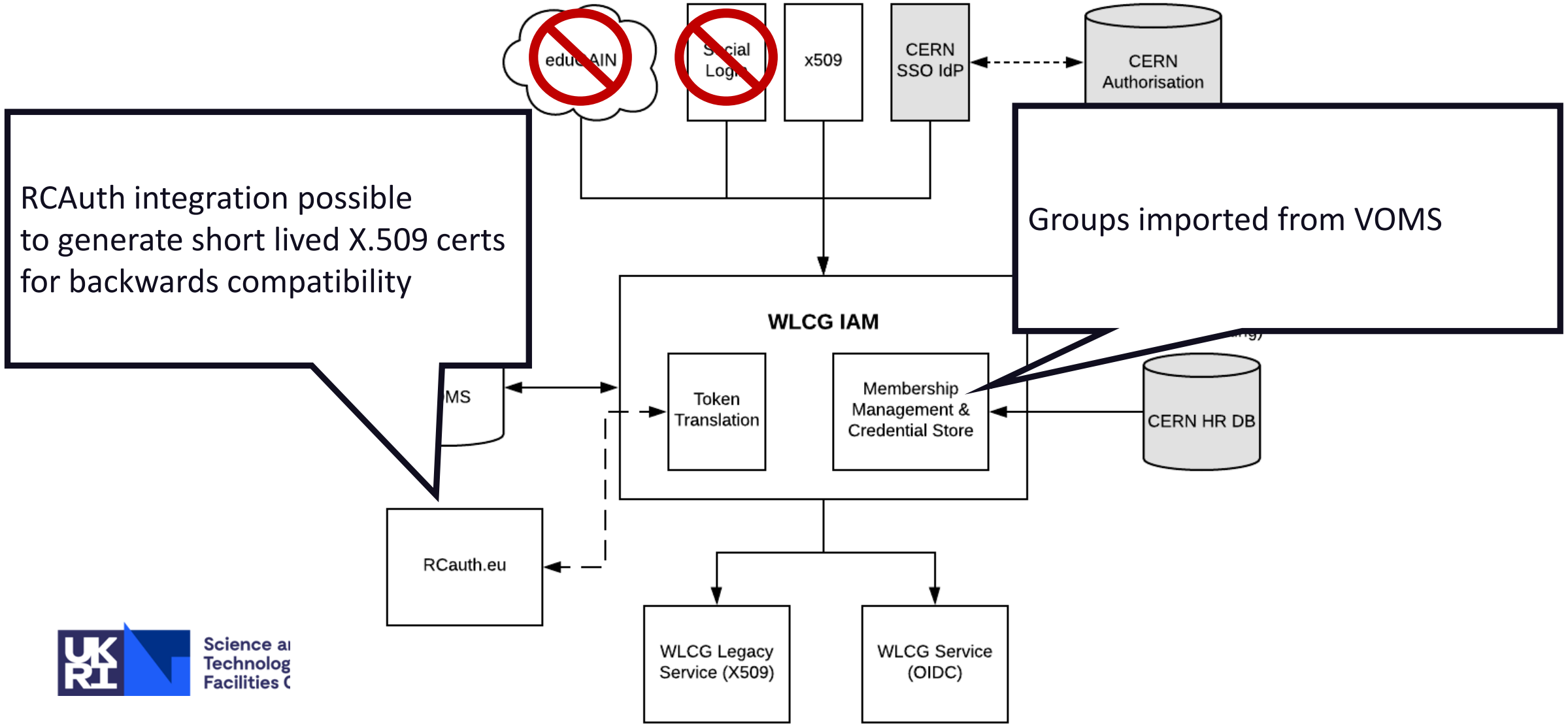
- Name,
- Email,
- CERN Person ID (indicates HR has performed ID check),
- CERN Kerberos Principal
- ...

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



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.

WLCG Token Infrastructure Design



Science a
Technolog
Facilities C

WLCG Token Schema

- In order to serve authorisation information a VO, the WLCG token schema definies extra claims – `wlcg.groups` for Group-based authorisation and `scopes` for Capability-based authorisation
- `wlcg.groups` semantics are equivalent to existing VOMS groups, and will be initially imported directly from VOMS
  - Eg: /atlas/production
- `scopes` is used to provide capability to a specific token, rather than permanent authorisation to a user
  - Format `$AUTHZ:$PATH` where `$PATH` is mandatory (may be '/' for *)
  - Eg: storage.read:/atlas
- For more details, you can see the published schema: https://zenodo.org/record/3460258#.Y-YqUxPMLVs

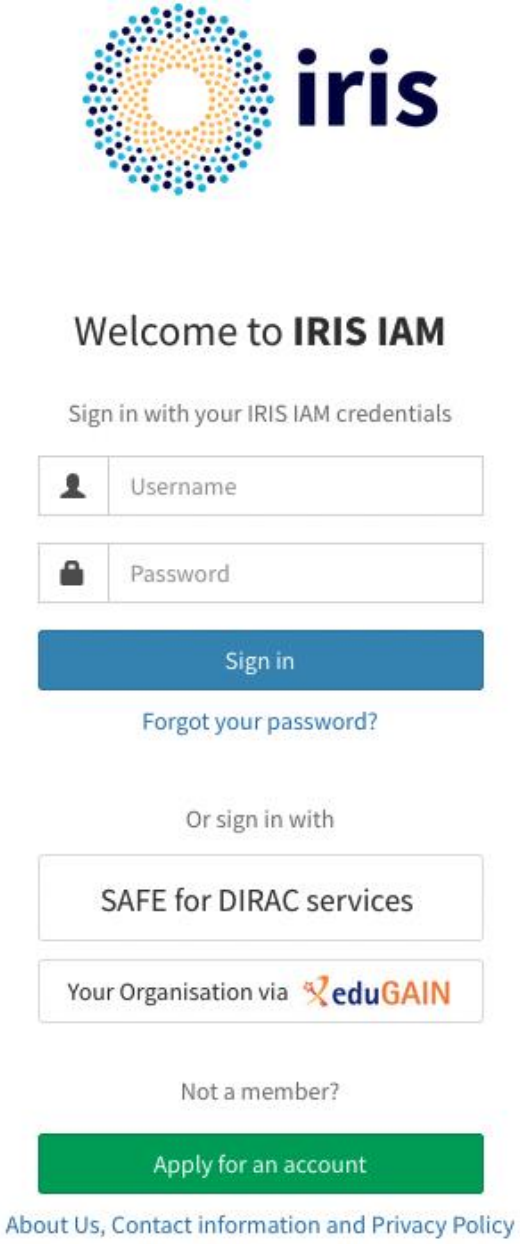
Science and Technology Facilities Council

Science and Technology Facilities Council

Identity Management for IRIS

Current Status of the IRIS IAM

- Primary authentication and authorization for IRIS services, including Accounting Portals, GocDB, and OpenStack Clouds
  - Integration with SCARF HPC soon to roll out
- Close liaison with IRIS Policy and Trust Framework
  - Ensure that the IAM follows collaboration polices and policies reflect what is possible
  - Community policy and risk assessments
- PAM module for authenticating with IAM for SSH
- Improved operational support
  - Now managed as part of STFC GridTools on-duty rota, alongside APEL and GocDB



Science and Technology Facilities Council

iris

IRIS IAM Group Management

- Recently updated with the IAM v1.8.1 rollout
  - Group managers now have full approval, removal, and view rights
  - Direct addition – likely through invite flows – to come in a later release
    - Wanted a solution which did not allow Managers to see all IAM users

What Next for IRIS IAM?

- High Availability – a priority for IRIS
  - Planned deployment of distributed high availability database – STFC Graduate placement, managed by Jens Jensen, to start soon
  - Similar work underway within the WLCG context – INDIGO IAM team has development work planned to support, planned for IAM v1.9.0 - https://github.com/indigo-iam/iam/projects/10#card-86093149
  - Planned to be one area of focus for an INDIGO IAM hackathon @ Coseners in July

What Next for IRIS IAM?

- Looking to grow the supporting team
  - Whilst IAM now has greater operational support from the GridTools team, technical development and deployment effort should be grown
  - Case to be made for further recruitment focussing on Identity Management

Science and
Technology
Facilities Council

Identity Roadmap For GridPP7

Areas for Focus

- Resource Trust – Host Certificates
  - Should be evaluated in light of new technologies in the space
    - Especially with development resources tight
  - Discussed at the recent EUGridPMA and within GDB
  - Further understanding of Cloud Workflows, so as to definitively understand trust environments
  - Fermilab are currently experiencing issues with their CA
    - Looking to see where UK CA can help

Science and
Technology
Facilities Council

Questions?

UKRI Science and Technology Facilities Council

Thank you

Science and Technology Facilities Council @STFC_Matters Science and Technology Facilities Council