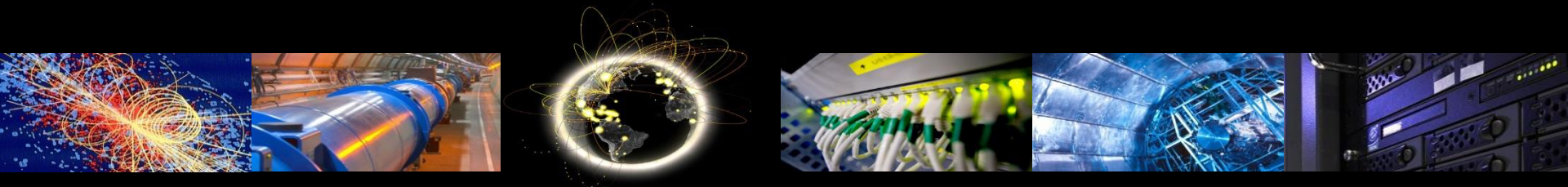


Presented by Hannah Short, Andrea Ceccanti, Brian Bockelman

# WLCG Authorisation WG Update

Authored by the WLCG AuthZ Working Group

GDB September 2020



# Key Updates

- Bearer token discovery published
- Current discussions
- Announcements

# Who? WLCG AuthZ WG

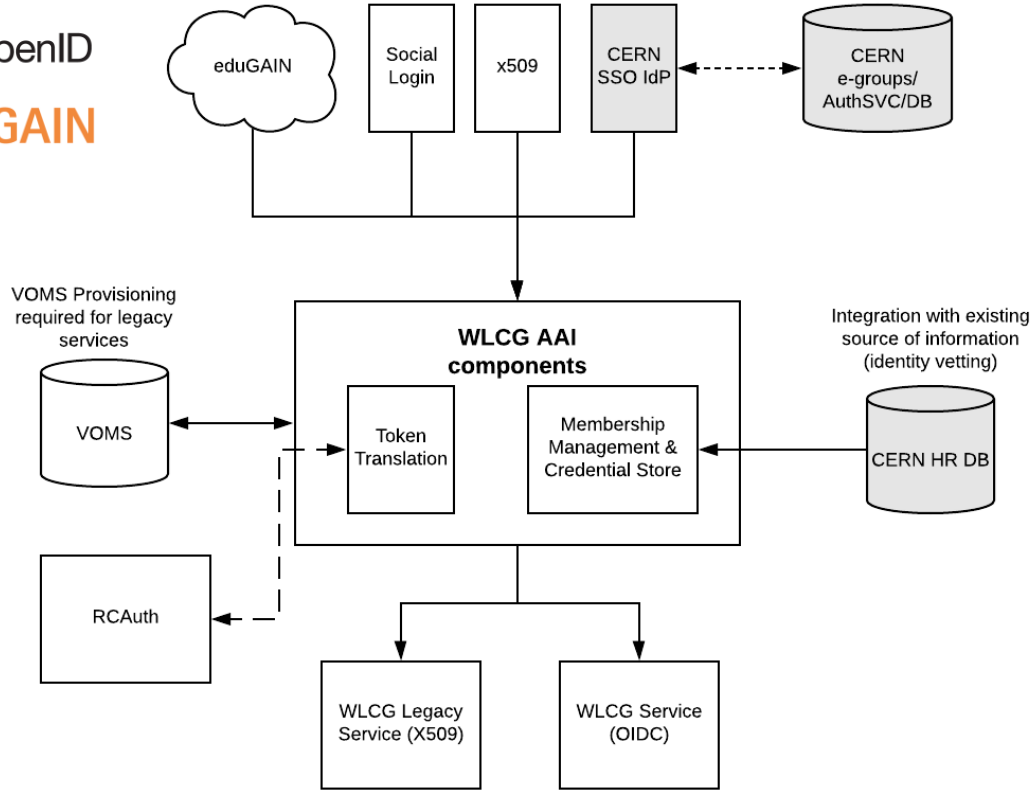
Representation from wide range of institutes and experiments. Development work of pilot projects supported by:



## What are we improving?

- Usability
  - Removing need for users to manage user-certificates
  - Ability to authenticate with home organisation credentials
- Membership Management
  - Smoother alternative to VOMS Admin
- Simplified integration
  - Adopting widely accepted technologies (OAuth2 and OIDC)
  - Priority to stick to standards

# What? Solution Design



Now deployed for CMS at <https://cms-auth.web.cern.ch>



Welcome to **cms**

Sign in with

CERN SSO

Not a member?

Apply for an account

# Bearer Token Discovery

- Working document at <https://github.com/WLCG-AuthZ-WG/bearer-token-discovery>
- Published document at <https://zenodo.org/record/3937438#.X1dqnC2w0UE>
- Specifies location for token discovery:
  - BEARER\_TOKEN env var
  - BEARER\_TOKEN\_FILE env var
  - If XDG\_RUNTIME\_DIR env var is set\*, then \$XDG\_RUNTIME\_DIR/bt\_u\$ID\*.
  - Otherwise, take the token from /tmp/bt\_u\$ID.

The screenshot shows the Zenodo website interface. At the top, there is a blue header with the Zenodo logo, a search bar, and links for 'Upload' and 'Communities'. Below the header, the date 'July 9, 2020' is displayed on the left, and 'Technical note' and 'Open Access' labels are on the right. The main title is 'WLCG Bearer Token Discovery' by the 'WLCG Authorization Working Group'. The abstract states: 'This document defines a specification for the discovery of WLCG bearer tokens by client tools. Client tools that rely on a bearer token for authenticating themselves need a mechanism for receiving the tokens from their environment. While the browser is a monolithic user agent (and can internally manage tokens), the terminal environment involves a number of independently-developed tools; the environment needs a way to communicate the token to be used to Unix processes. To the best of our knowledge, there's no previously defined standard about how a Unix tool should discover a token from its environment.' Below the abstract, there is a 'Proposal' section with a detailed description of the discovery process. At the bottom, a file list shows 'wlog-bearer.pdf' (85.6 kB) with 'Preview' and 'Download' buttons.

<https://zenodo.org/record/3937438#.X1dqnC2w0UE>  
published in new WLCG Community

# Current Discussions

- Access token audiences (mechanism to restrict which tokens are accepted by which clients)
  - Does our software stack support them?
  - How to request them?
  - What should they be?
- Personal data availability in UserInfo endpoint

# Announcements

- Authorisation Hackathon #2 Sep. 16 - 18  
<https://indico.cern.ch/event/953075/>
- CHEP Paper accepted
- Calls resumed from September onwards  
<https://indico.cern.ch/category/68/>
- Docs prepared in support of the DOMA TPC WG  
<https://wlcg-authz-wg.github.io/wlcg-authz-docs/>



# Questions?