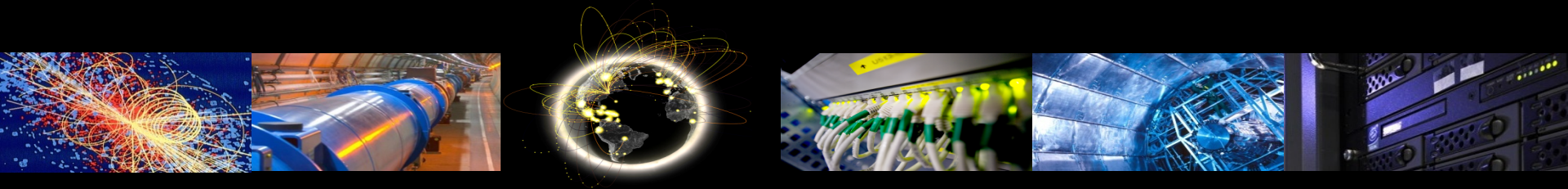


Presented by Hannah Short, Andrea Ceccanti, Brian Bockelman

WLCG Authorisation WG Update

Authored by the WLCG AuthZ Working Group

GDB Feb 2020



Key Updates

- Recap
- Authorisation Hackathon
- CHEP Paper
- Close Collaboration with Fermilab

Who? WLCG AuthZ WG

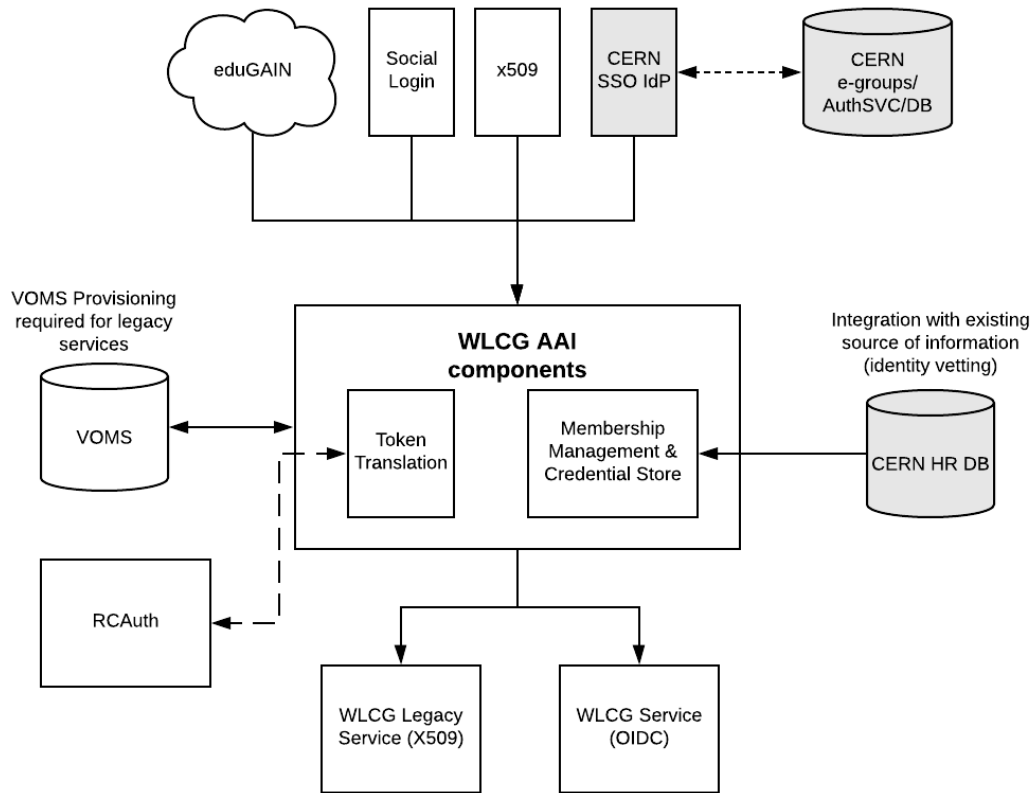
Representation from wide range of institutes and experiments. Development work of pilot projects supported by:



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

Solution Design



CERN components are optional configuration – technical solution is widely relevant!

WLCG Schema

- Published on Zenodo, September 25th 2019
- Allows middleware developers to enable token based authorization to an agreed schema
- Tests to be run within WLCG DOMA WG
- WLCG Token established at INFN for test bench purposes: <https://wlcg.cloud.cnaf.infn.it/>

September 25, 2019

Technical note Open Access

WLCG Common JWT Profiles

Altunay, Mine; Bockelman, Brian; Ceccanti, Andrea; Cornwall, Linda; Crawford, Matt; Crooks, David; Dack, Thomas; Dykstra, David; Groep, David; Igoumenos, Ioannis; Jouvin, Michel; Keeble, Oliver; Kelsy, David; Lassnig, Mario; Liampotis, Nicolas; Litmaath, Maarten; McNab, Andrew; Millar, Paul; Sallé, Mischa; Short, Hannah; Teheran, Jeny; Wartel, Romain

This document describes how WLCG users may use the available geographically distributed resources without X.509 credentials. In this model, clients are issued with bearer tokens; these tokens are subsequently used to interact with resources. The tokens may contain authorization groups and/or capabilities, according to the preference of the Virtual Organisation (VO), applications and relying parties.

Wherever possible, this document builds on existing standards when describing profiles to support current and anticipated WLCG usage. In particular, three major technologies are identified as providing the basis for this system: OAuth2 (RFC 6749 & RFC 6750), OpenID Connect and JSON Web Tokens (RFC 7519). Additionally, trust roots are established via OpenID Discovery or OAuth2 Authorization Server Metadata (RFC 8414). This document provides a profile for OAuth2 Access Tokens and OIDC ID Tokens.

Preview

Page: 1 of 35 Automatic Zoom:

WLCG Common JWT Profiles

Authored by the WLCG AuthZ Working Group

Version History:

Date	Version	Comment
------	---------	---------

<https://zenodo.org/record/3460258#.XacTni2Q01I>

Edit

New version

98

views

81

downloads

[See more details...](#)

Indexed in

OpenAIRE

Publication date:

September 25, 2019

DOI:

[DOI: 10.5281/zenodo.3460258](https://doi.org/10.5281/zenodo.3460258)

Keyword(s):

[jwt](#), [OIDC](#), [OAuth2.0](#), [wlcg](#)

License (for files):

[Creative Commons Attribution 4.0 International](#)

Token-based AuthN/Z Hackathon

<https://indico.cern.ch/event/870616/>

Objective:

- Demonstrate full-stack HTTP X509-free data transfer management with tokens issued by IAM and compliant with the WLCG JWT profile focusing on scope-based authZ
 - RUCIO-> FTS -> SEs

Accomplishments:

- Working fully token-based transfers managed by FTS against XRootD, StoRM, dCache
- Bug fixes/enhancements in token-based authn/z support in IAM, FTS, XRootD
- Initial support for WLCG profile and token-based authN/Z in DPM and EOS
- Knowledge exchange!
- And more .. See this [Google doc](#)



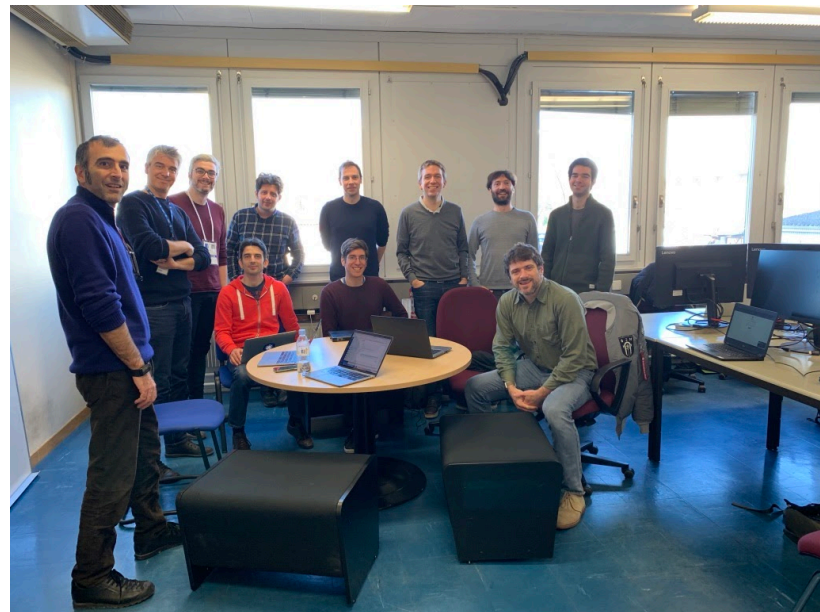
Token-based AuthN/Z Hackathon

Next steps:

- Integrate RUCIO, DPM, EOS, Echo in the chain
- Audience checks enforcement and group-based authZ support
- HTCondor and integration of pilot submission frameworks

Second token-based AuthN/Z Hackathon in Lund?

- Focusing on the topics above
- Room pre-booked on the Sunday afternoon and Monday morning before the WLCG workshop
- [Doodle](#) to collect interest
 - Please give feedback ASAP!



CHEP Paper

- Collaborative editing ongoing
- 11 Authors at the moment
- Deadline extended until March 14th (but we are almost done!)
- CHEP Slides at <https://indico.cern.ch/event/773049/contributions/3473383/>
- Proceedings being edited on Overleaf at <https://www.overleaf.com/read/cyphjnbjzhpq>

The screenshot displays the Overleaf collaborative editing environment. The main editor shows LaTeX code for a document titled "WLCG Authorisation from X.509 to Tokens". The code includes sections for "Introduction", "OpenID Connect (OIDC)", and "Access Tokens". The chat window on the right shows a discussion between "mischasalle" and "Thomas Dack" regarding the design of the WLCG IAM software. The document preview on the far right shows a diagram of the WLCG IAM software architecture.

Figure 2. Design of the WLCG IAM software architecture. Grey boxes represent configurable components, in this case based for the CERN environment.

The INDDO IAM [18] software was chosen as the core of WLCG's future, token based authentication and authorisation infrastructure. In Figure 2, we see the WLCG IAM is WLCG based on INDDO IAM in the center, providing multiple authenticators, OAuth2, OpenID Connect, and other protocols. It is connected to the X.509 and having a uniform token issuer for downstream WLCG Services. The Token Translation is performed using the WLCG IAM [12] which Certificate Authority and users can request a certificate from the WLCG IAM User Interface.

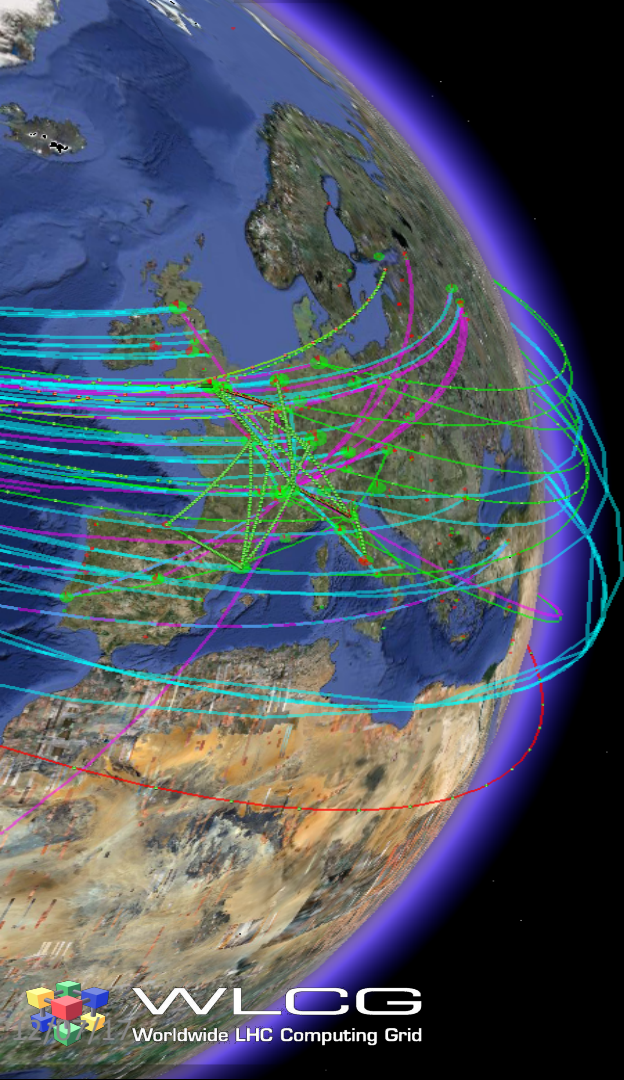
Figure 3. Anticipated Token Flow.

It is envisaged that there will be a small number of registered clients for WLCG and a much larger number of unregistered browsers.

1. A SAML [17] or OIDC [12] credential is sent from an Identity Provider to WLCG IAM.
2. WLCG IAM sends three OIDC tokens to a registered Client, the ID Token, Access Token and Refresh Token.
3. The Access Token is used to authorize access to downstream Resources (such as sites).
4. The Resource validates the token against known trust roots. The trust roots may be cached in advance or stored a high number of trusted roots on the client itself.
5. When the Access Token expires, the Client may use the Refresh Token to request a new Access Token.

Collaboration with Fermilab

- ****Very**** useful call held on January 28th
- Discussed topics such as
 - Command line
 - Token types (ID vs Access)
 - Audiences
 - Renewal
- Notes at <https://indico.cern.ch/event/881002/>
- Expecting close collaboration to continue, clarify roadmap for next few years



Questions?