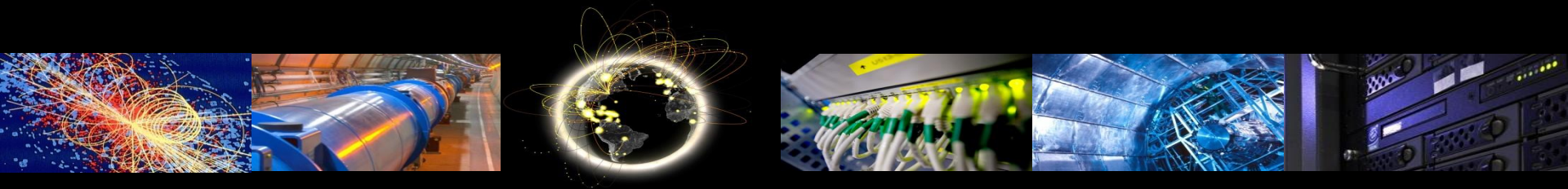


Tokens in WLCG - Introduction

WoTBAn&Az

October 18th 2021

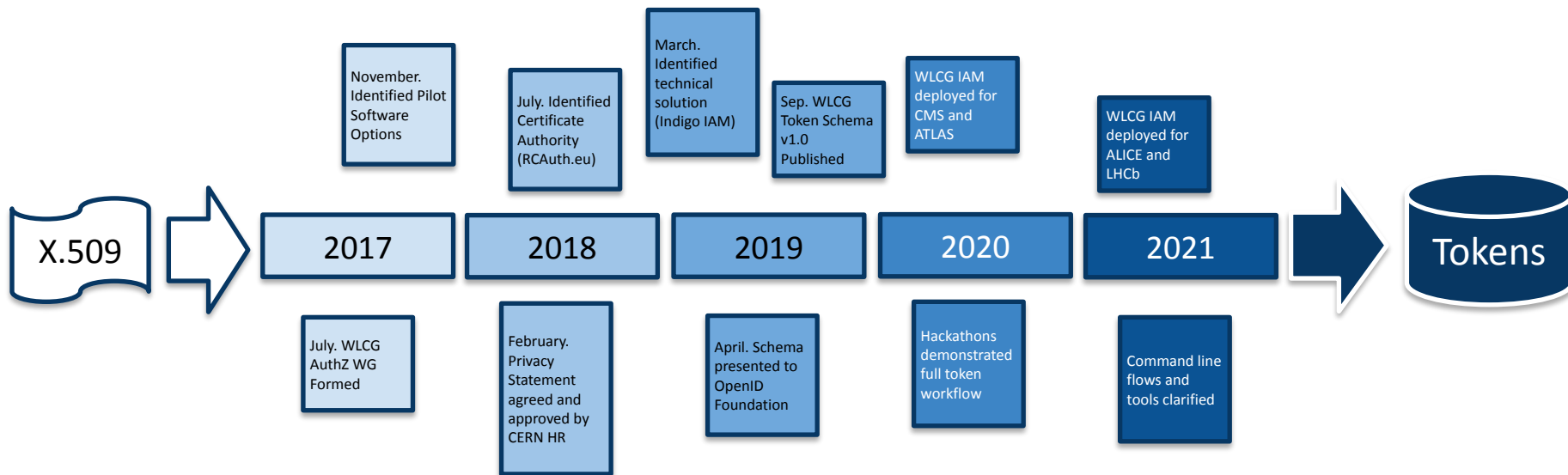


Overview

- WLCG (Worldwide LHC Computing Grid) used for high energy physics data analysis
- Since 2000s has relied on X.509 certificates for client and user authentication, and VOMS for authorization
- Since 2017 have been looking to move to JWT tokens over OAuth2.0
 - WLCG Authorization Working Group meets every 2 weeks



Towards Tokens



WLCG Token Schema V1.0

- Published on Zenodo, September 25th 2019
- Allows middleware developers to enable token based authorization to an agreed schema
- Working document at <https://github.com/WLCG-AuthZ-WG/common-jwt-profile>

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#.X8ED_i1Q1qs

Edit

New version

98

views

81

downloads

[See more details...](#)

Indexed in

OpenAIRE

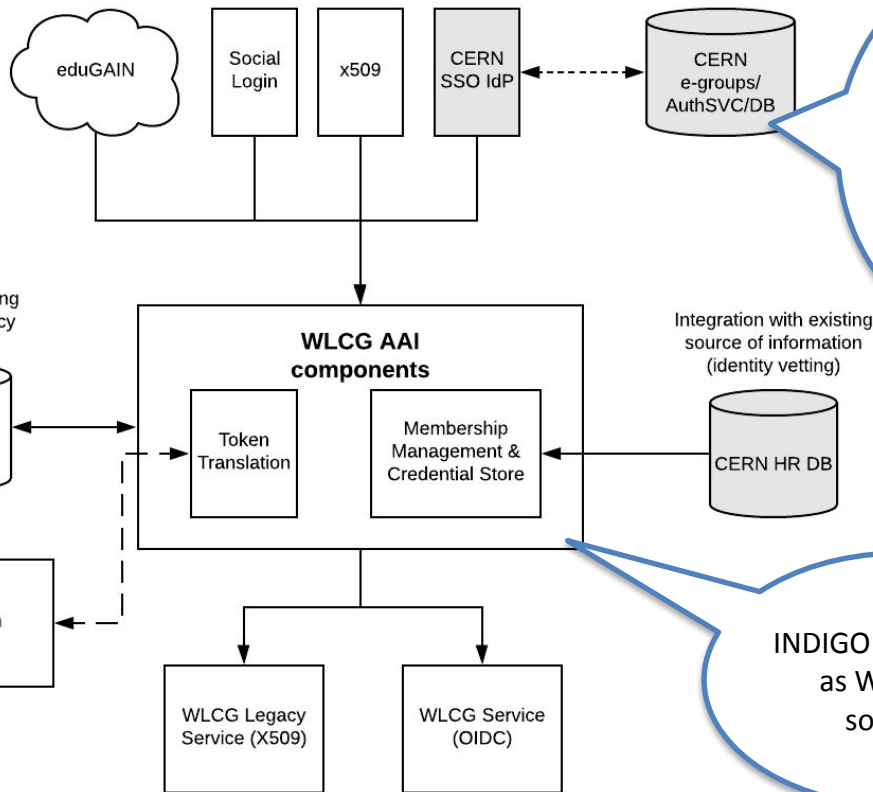
Publication date:
September 25, 2019

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

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

License (for files):
[CC Creative Commons Attribution 4.0 International](#)

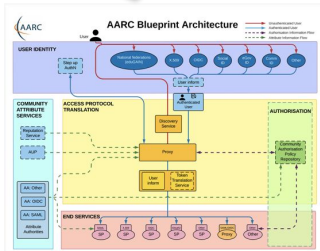
AAI Design



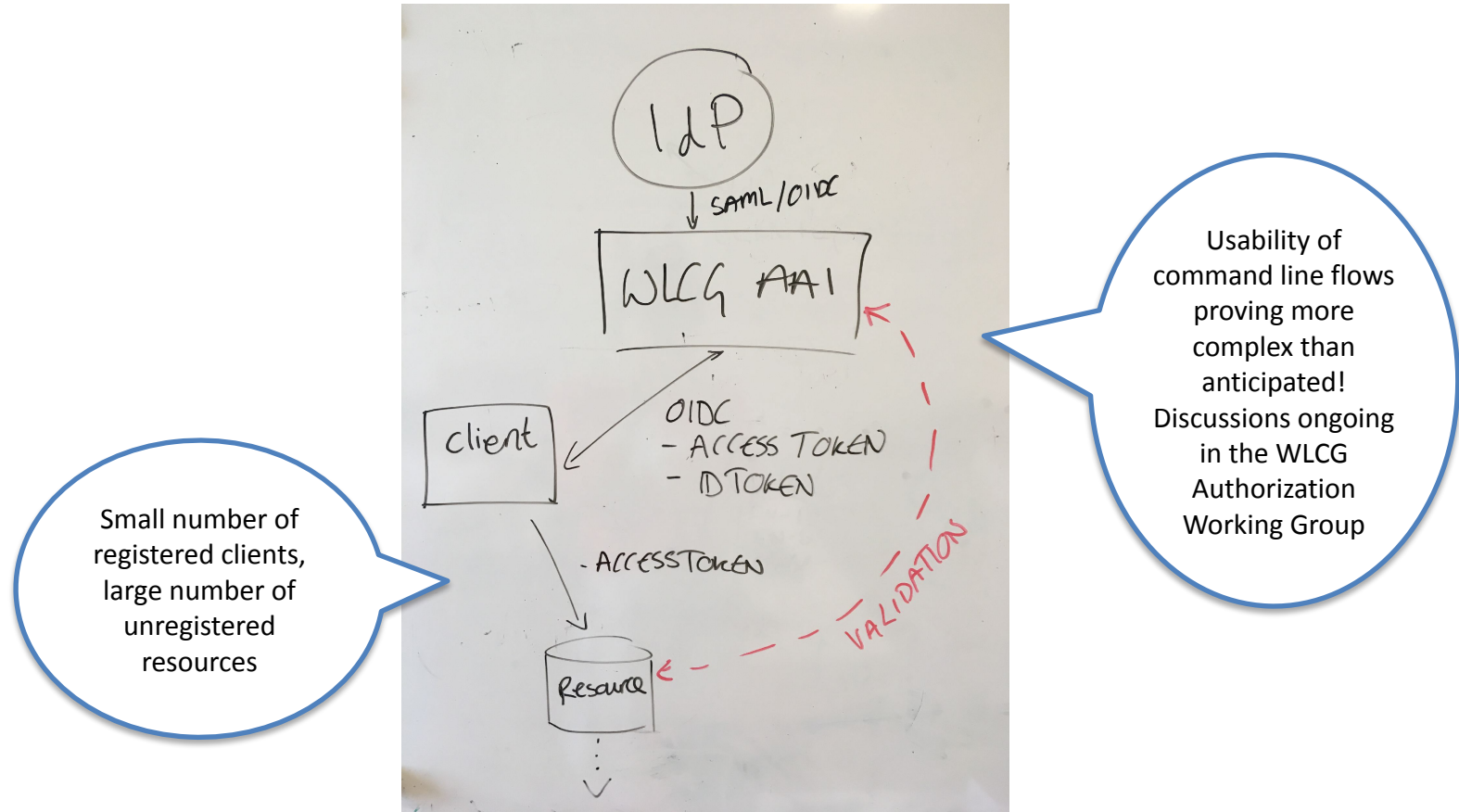
CERN SSO configured as sole Identity Provider, enables identity verification via HR DB (match CERN PersonID)

Follows the AARC Blueprint
<https://aarc-community.org/architecture/>

INDIGO IAM chosen as WLCG AAI software



Anticipated Token Flows



Certificate fadeout

- X.509 will continue to play a vital role in our infrastructure as host certificates, but users will no longer need to manage the certificate lifecycle themselves
- It is likely that power users, e.g. admins, may need to manage certificates for much longer
- This is a very early plan and significant changes are expected

| | 2019 | 2020 | 2021 | 2022 | 2023 |
|---|------|------|------|------|------|
| Integrate RCAuth.eu for on-demand IOTA X.509 | | | | | |
| Migrate VOs to IAM, retire VOMS Admin | | | | | |
| Add Token support to Middleware | | | | | |
| Dual mode (IAM issues X.509/VOMS and Tokens) | | | | | |
| Privilege Tokens, analyse remaining X.509 use | | | | | |
| Begin removing X.509 User Certificate Support | | | | | |

Today's Talks

| Time | Item | Speaker |
|------|--|---------------------------------------|
| 5m | Introduction | Hannah Short (CERN) |
| 20m | Lightning talk: Fermilab | Mine Altunay, Dave Dykstra (Fermilab) |
| | Lightning talk: CERN - WLCG IAM deployment | Hannah Short (CERN) |
| | Lightning talk: CiLogon and WLCG | Jim Basney (Uni Illinois) |
| | Lightning Talk: Condor with Vault | Dave Dykstra (Fermilab) |
| 10m | IAM Development Roadmap | Andrea Ceccanti (INFN) |



Questions?