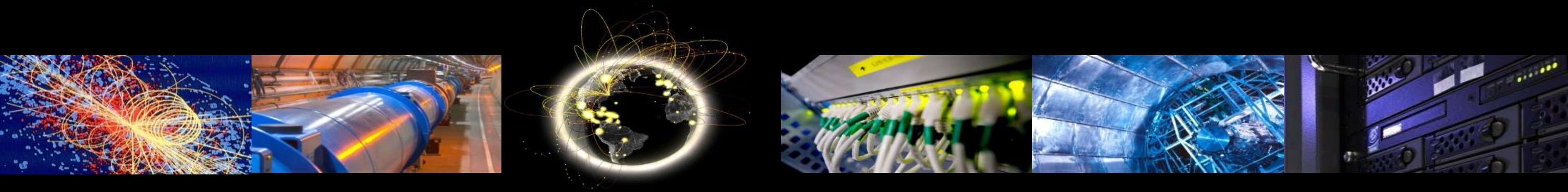
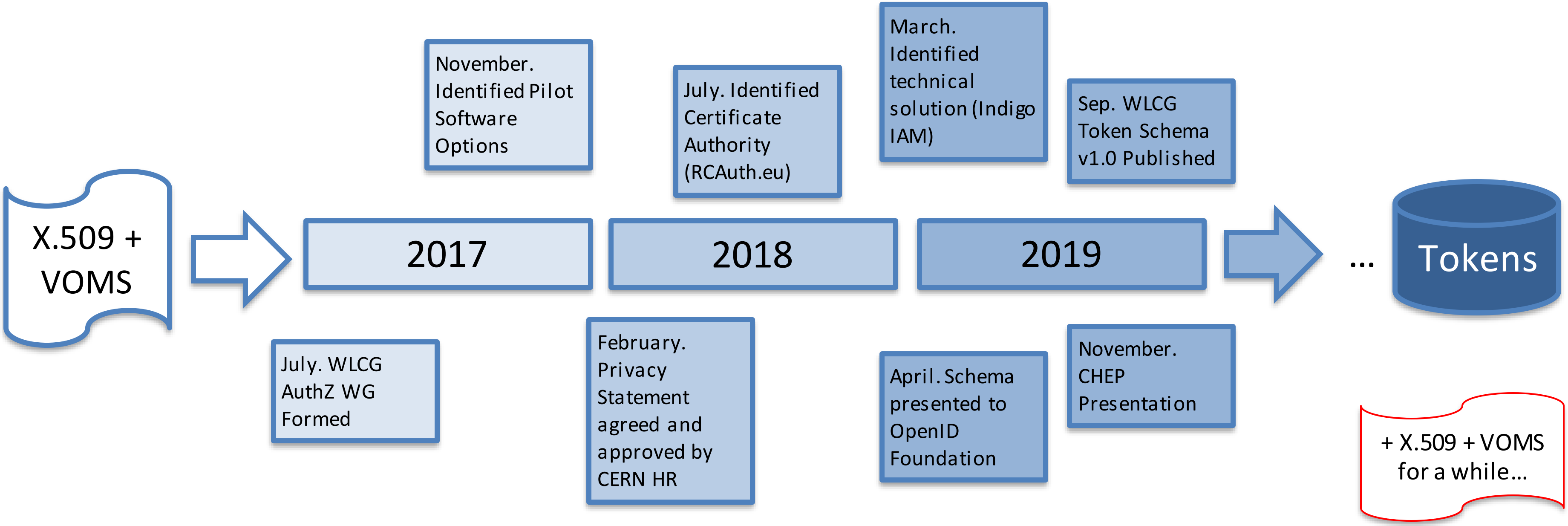
WLCG Authorization: from X.509 to Tokens

Authored by the WLCG AuthZ Working Group

PRACE-CERN-GÉANT-SKAO workshop on HPC, 29th September 2020



HEP Moving to Tokens



X.509 + VOMS

2017

July. WLCG AuthZ WG Formed

November. Identified Pilot Software Options

2018

February. Privacy Statement agreed and approved by CERN HR

July. Identified Certificate Authority (RCAuth.eu)

2019

March. Identified technical solution (Indigo IAM)

April. Schema presented to OpenID Foundation

Sep. WLCG Token Schema v1.0 Published

November. CHEP Presentation

…

Tokens

+ X.509 + VOMS for a while…

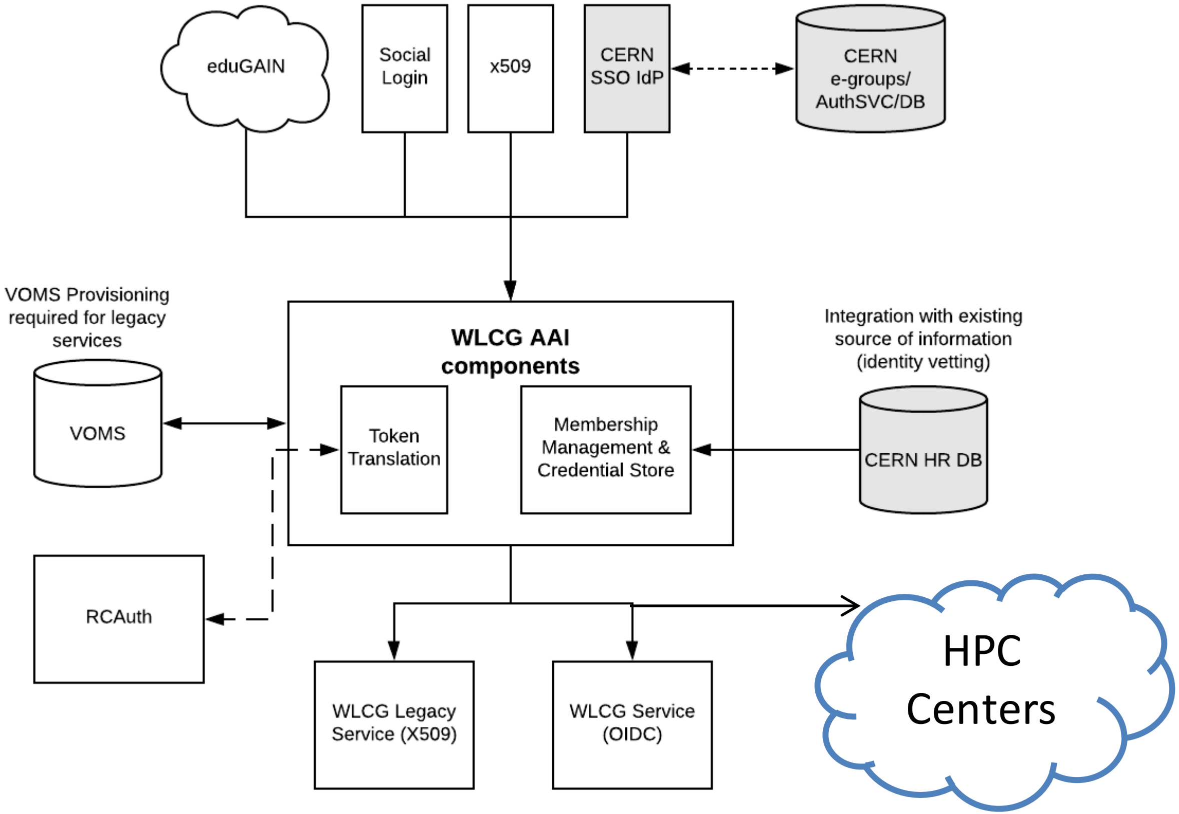
Why? Motivation

- **Evolving Identity Landscape**
  - User-owned X.509 certificates come with difficulties and significant support effort
  - Better alternatives now exist → JWT Tokens over OAuth2 and OpenID Connect
- **Technology Readiness**
  - Increasing solutions for shielding users from the complexities of X.509 certificate management
  - Token-based authorisation widely adopted in commercial services and increasingly by R&E Infrastructures

Much work is ongoing to enable token based authorization in HEP infrastructure, with WLCG leading the way

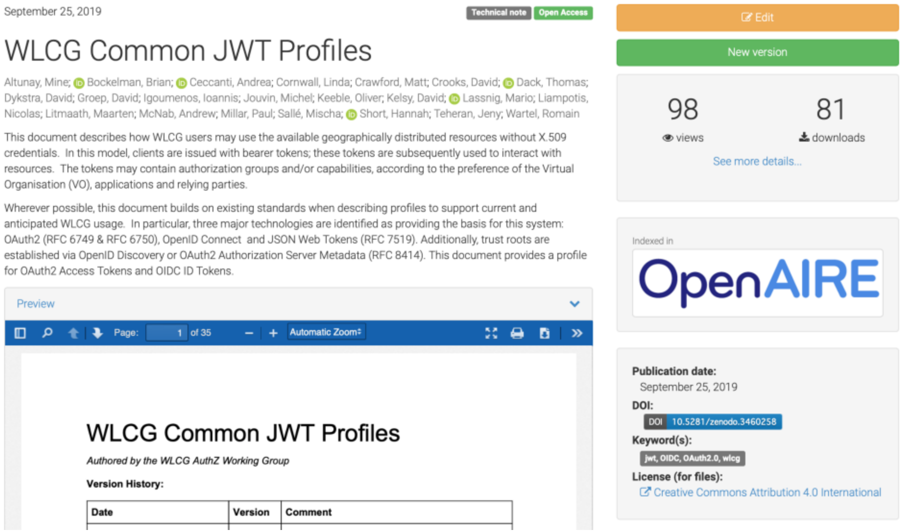
WLCG Worldwide LHC Computing Grid

What? Solution Design


eduGAIN
Social Login
x509
CERN SSO IdP
CERN e-groups/ AuthSVC/DB
VOMS Provisioning required for legacy services
VOMS
WLCG AAI components
Token Translation
Membership Management & Credential Store
Integration with existing source of information (identity vetting)
CERN HR DB
RCAuth
WLCG Legacy Service (X509)
WLCG Service (OIDC)
HPC Centers

Token Schema

- Published on Zenodo, September 25th 2019
- Allows middleware developers to enable token based authorization according to an agreed schema



September 25, 2019

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.

98 views

81 downloads

See more details...

Publication date: September 25, 2019

DOI: DOI 10.5281/zenodo.3460258

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

License (for files): Creative Commons Attribution 4.0 International

WLCG Common JWT Profiles

Authored by the WLCG AuthZ Working Group

Version History:

Date	Version	Comment

https://zenodo.org/record/3460258

Token Claims

Common Claims

- sub
- exp
- iss
- acr
- aud
- iat
- nbf
- jti
- eduperson_assurance (REFEDS)
- wlcg.ver (WLCG)
- wlcg.groups (WLCG)

ID Token Claims

- auth_time
- general OIDC Claims

Access Token Claims

- scope (inspired by OAuth token exchange draft)

Note: Where unspecified, the origin is RFC7519 or OpenID Connect core

Two forms of Authorization

Tokens Assert **Group Membership**

- Similar to VOMS Groups
- VOMS Roles are modeled as optional Groups

Tokens Assert **Authorized Actions**

- Called “Capabilities/scopes”
- Specific ability to perform an action (optionally, at a specific path) e.g. **storage.create /dir-1/dir-2/my-file** (under the root directory of the given VO)

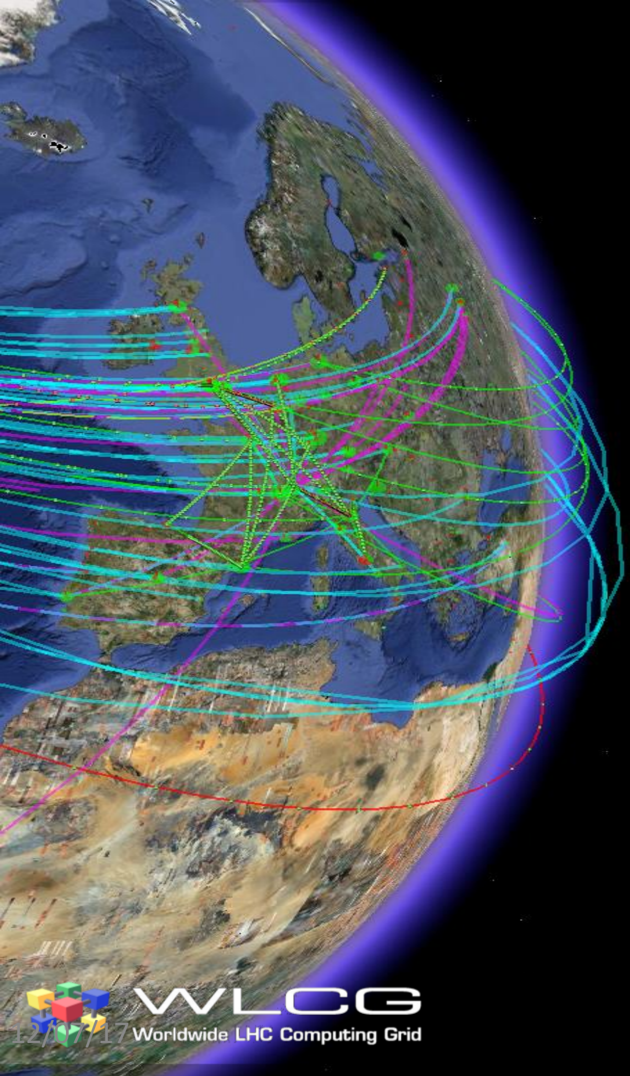
Capabilities are used by SciTokens (a sub-schema of WLCG Schema)

WLCG Worldwide LHC Computing Grid

HPC Integration

- HPC centers would need to **accept WLCG OAuth2 bearer tokens** for authorization
  - Trust the few, closely guarded WLCG Token issuers
  - Support authorization mechanisms through groups and/or capabilities

- Possibly depending on the timescale, while not every supported VO has switched to tokens: support VOMS authorization as being used today



Questions?