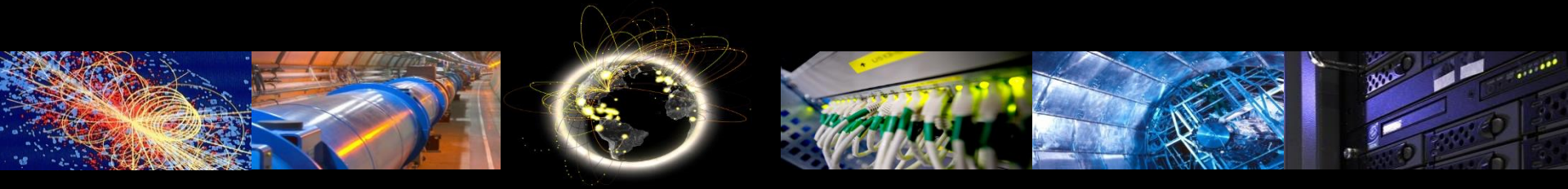
WLCG AuthZ WG

GDB Update

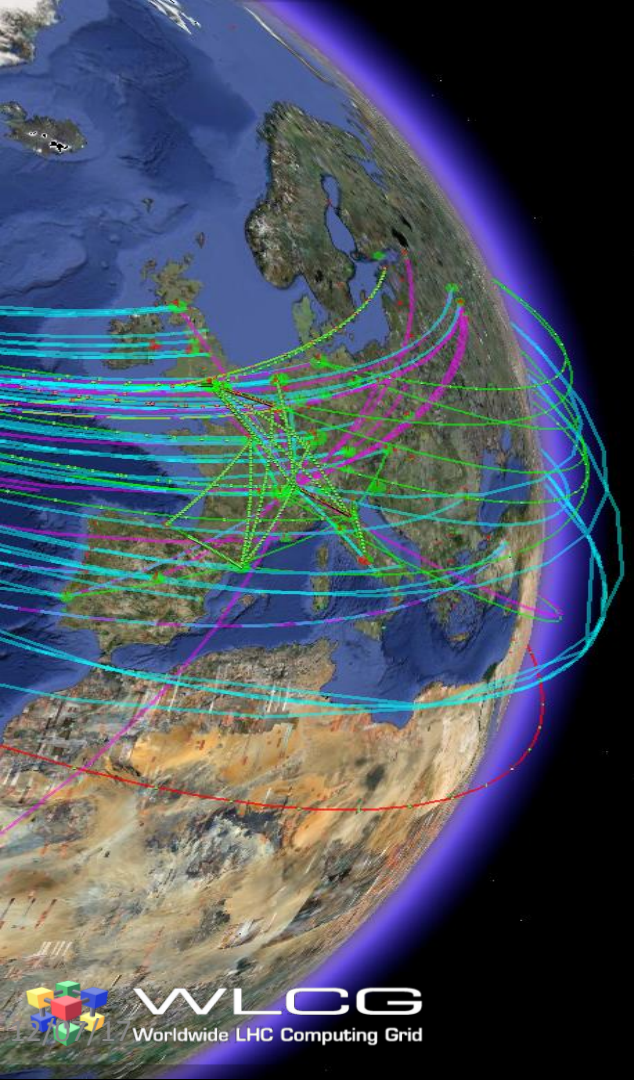
GDB, October 17th 2018



Agenda

- WG Background
- Status
- Next Steps

All information is available on the Twiki:
https://twiki.cern.ch/twiki/bin/view/LCG/WLCGAuthorizationWG



WG Background

Motivation

- Evolving Identity Landscape
  - User-owned x.509 certificates -> federated identities
  - Current grid middleware does not support federated identities
  - How can we shield users from the complexities of X.509 certificate management ?
  - Token-based (JWT) authorization widely adopted in commercial services and increasingly by R&E Infrastructures
- Data Protection
  - Tightening of data protection (GDPR) requires fine-grained user level access control, certain provisioning practices may need to be adjusted

Objective: Understand & meet the requirements of a future-looking AuthZ service for WLCG experiments

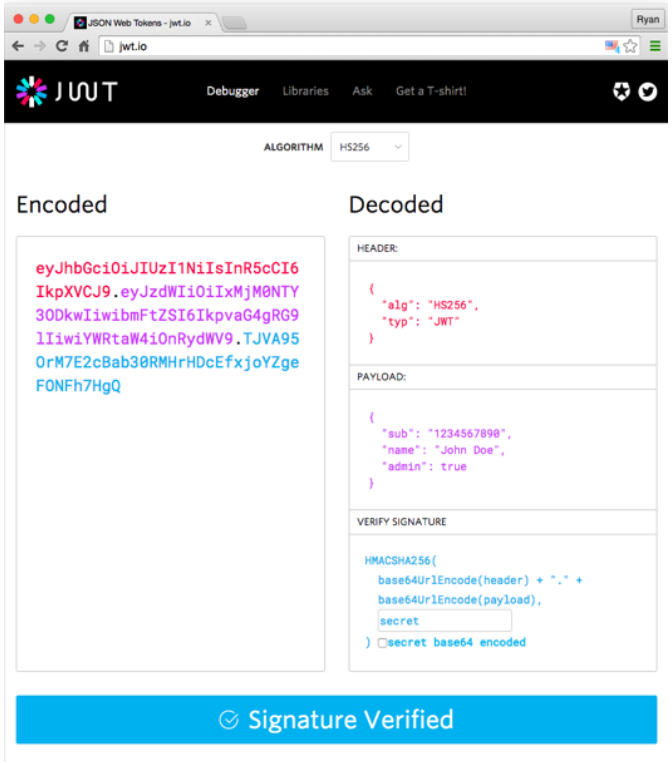
WG Objectives

1. Design and pilot a Token Based Authentication and Authorisation Infrastructure (AAI) for WLCG
2. Produce a v1 schema for these tokens

Principle throughout is to maximise use of common standards and shared software.

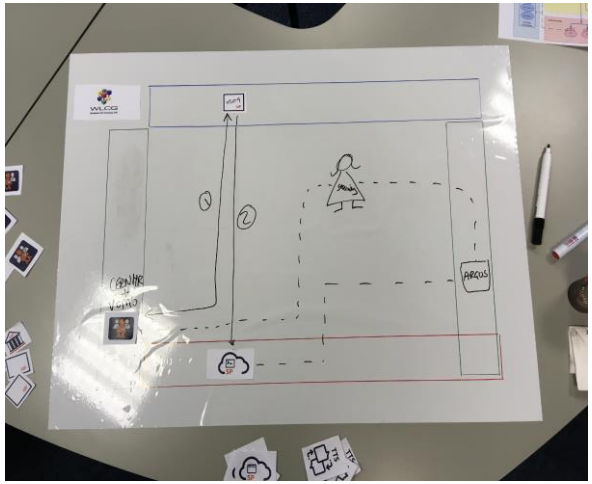
What is a JSON Web Token?

- What are they? "**JSON Web Tokens are an open, industry standard RFC 7519 method for representing claims securely between two parties.**"
- Computing services are increasingly turning to token based authentication & authorization
  - particularly used by the **OIDC** and **OAuth2** protocols
- Multiple infrastructure projects already using/supporting token based authorization but with diverging schemas or technologies
  - INDIGO IAM
  - EGI Check-in
  - SciTokens
  - dCache
  - ALICE tokens



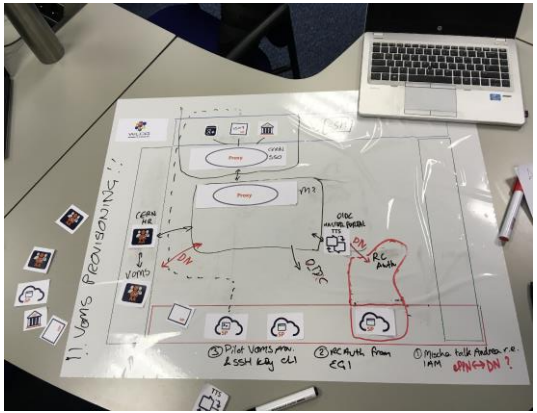
https://jwt.io/introduction/

What does the future look like?



Current infrastructure allows access based on X509, including VOMS, CERN HR DB and Argus

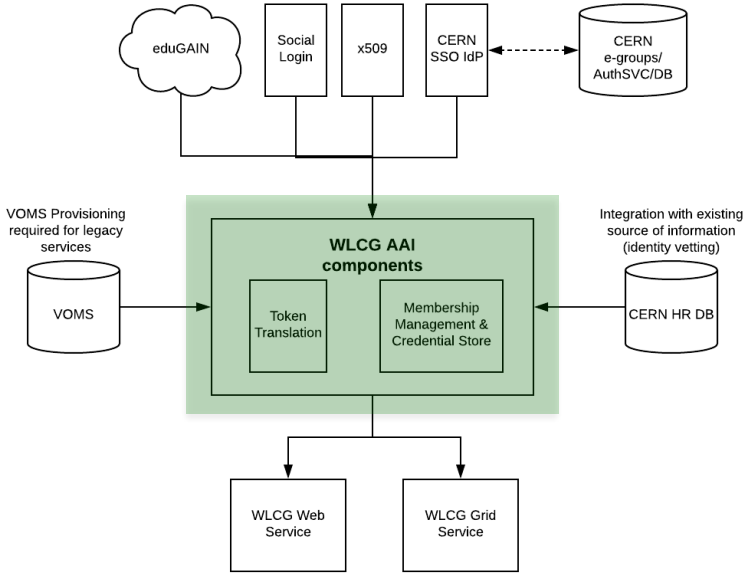
Future infrastructure will support a range of credential types for users and services and provide a user friendly experience

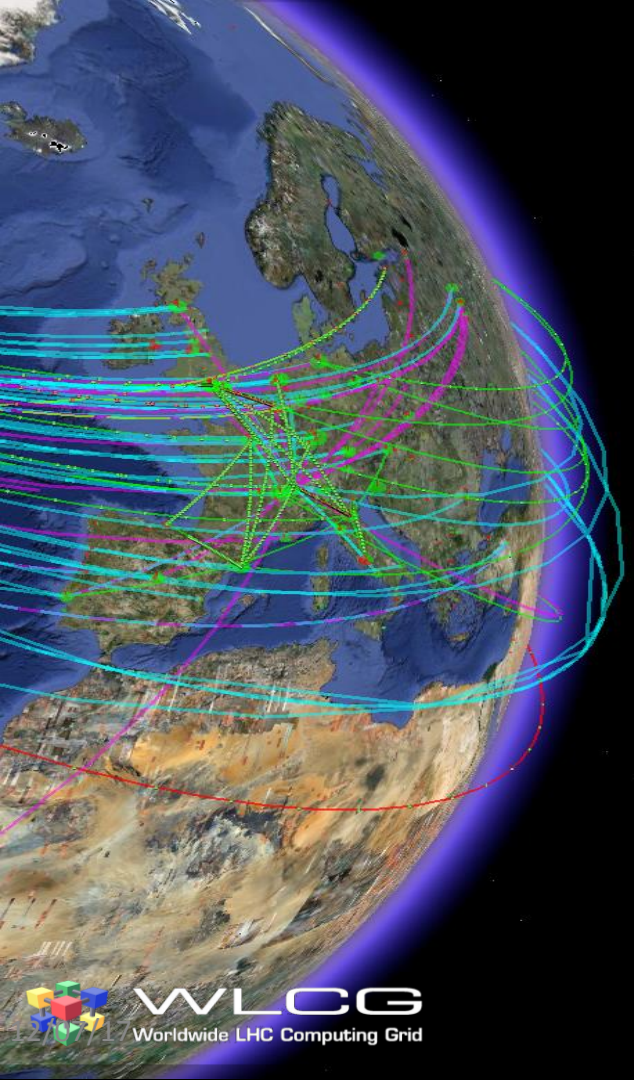


Supporting information available at:
https://hackmd.web.cern.ch/s/rkyic3vtm

Overlap with CERN?

- 2 modes for the AAI solution
  - CERN Mode = integration with CERN SSO, CERN HR DB
  - Standalone Mode = configurable authentication and identity vetting source
- In parallel CERN will be moving to a token based infrastructure
  - Likely on a longer timeline
  - Opportunity for convergence
  - see HEPiX Talk by Paolo Tedesco https://indico.cern.ch/event/730908





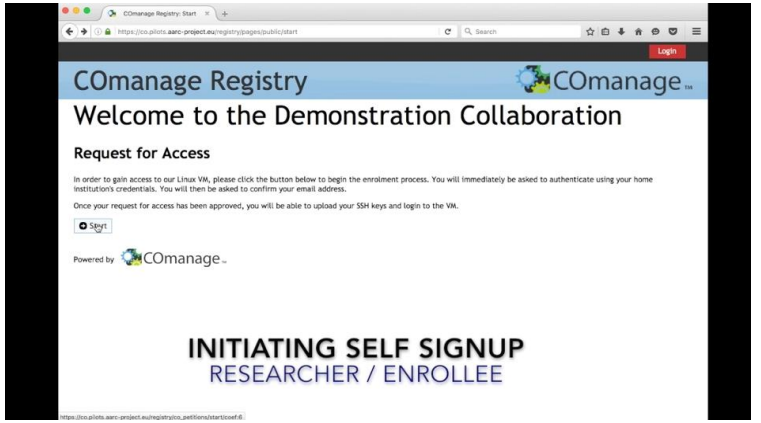
Status

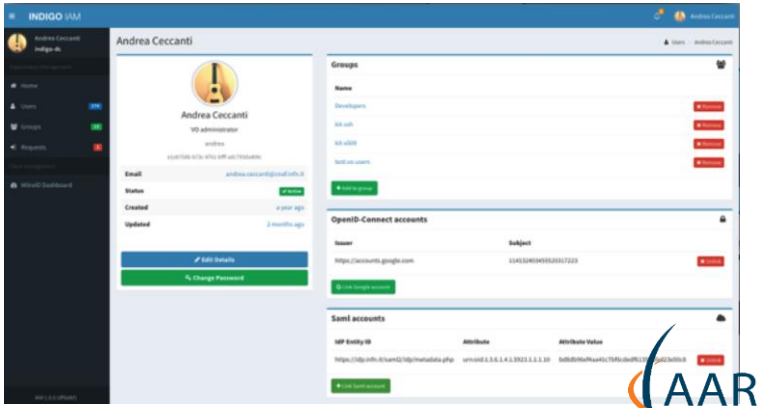
Status

Item	Status	Date
Document Current Token Usage	Final Draft	October 2018
Publish Requirements Document	Done	September 2018
Identify Pilot AAI Implementations	Done	November 2017
Enhance Pilot AAIs to meet requirements	Ongoing	December 2018
Define Token Schema	Ongoing	January 2019
Align with VO workflows (VO Interviews)	Ongoing	November 2018
HR approval of privacy policies for HR DB data release (name, experiment affiliation etc)	Ongoing	December 2018
Assess Pilots in pre-GDB		December 2018
Provide feedback to WLCG Management Board		February 2019

AAI Pilot Projects

- Two solutions appear to meet the majority of requirements
  - EGI Check-in & COmanage
  - INDIGO IAM
- Additional integration required for
  - VOMS provisioning & lookup
  - CERN HR DB integration (postponed until autumn)
  - AUP re-signing
- RCAuth.eu for x509 generation
  - High availability setup in progress



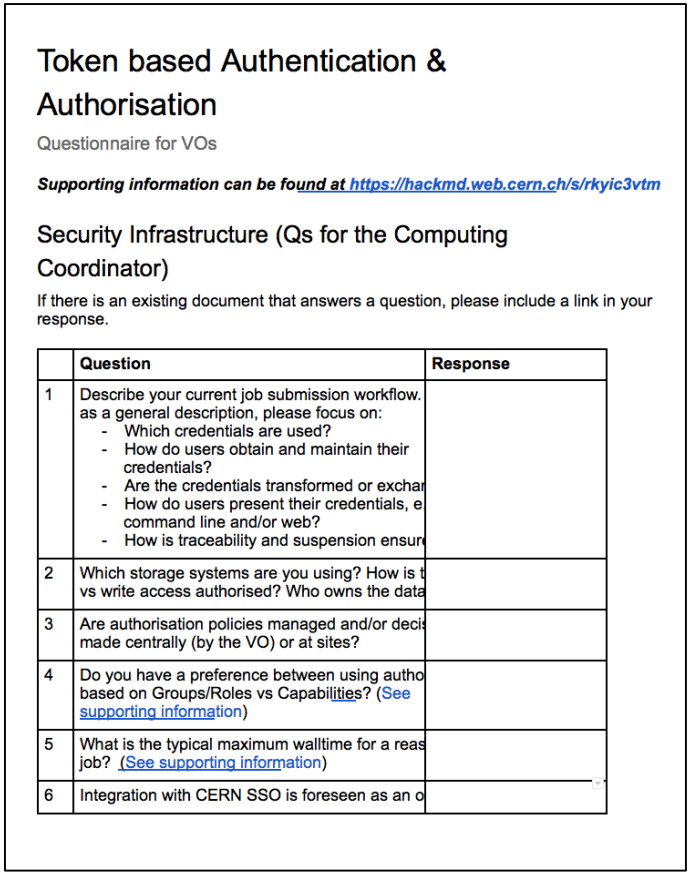


This software exists. We do not want to re-invent the wheel!

VO Interviews

- Questionnaire compiled by WG aimed at VO Computing Coordinators and VO Managers
- Supporting material produced to provide an overview of the technology **https://hackmd.web.cern.ch/s/rkyic3vtm**
- Offer to go through in face-to-face interview if needed
- Sent to first VO last week

Many thanks in advance for filling the questionnaire!



Token based Authentication & Authorisation

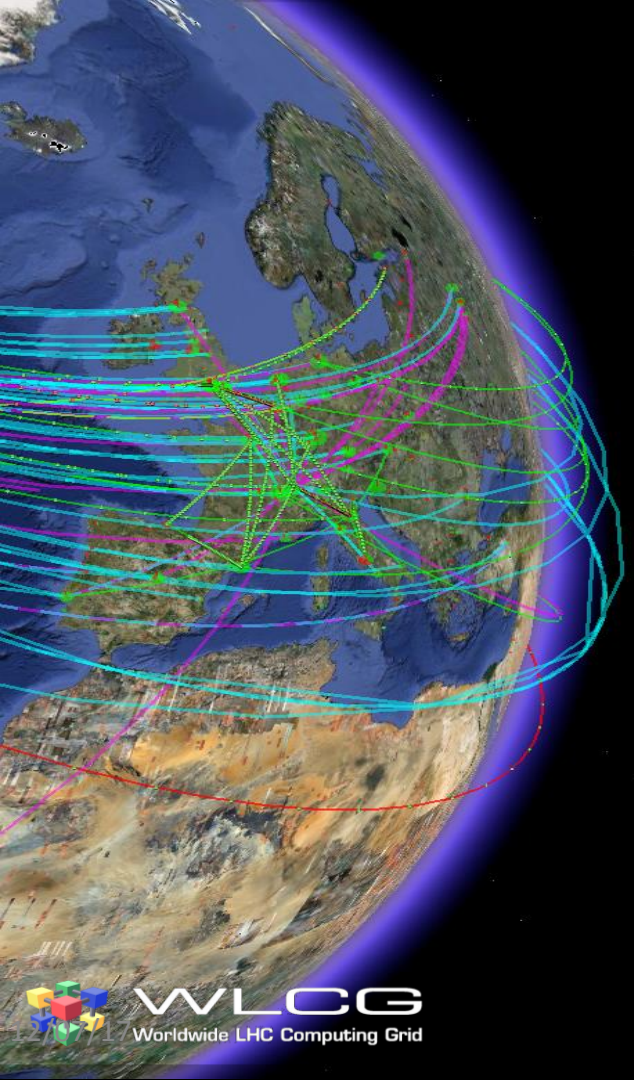
Questionnaire for VOs

Supporting information can be found at https://hackmd.web.cern.ch/s/rkyic3vtm

Security Infrastructure (Qs for the Computing Coordinator)

If there is an existing document that answers a question, please include a link in your response.

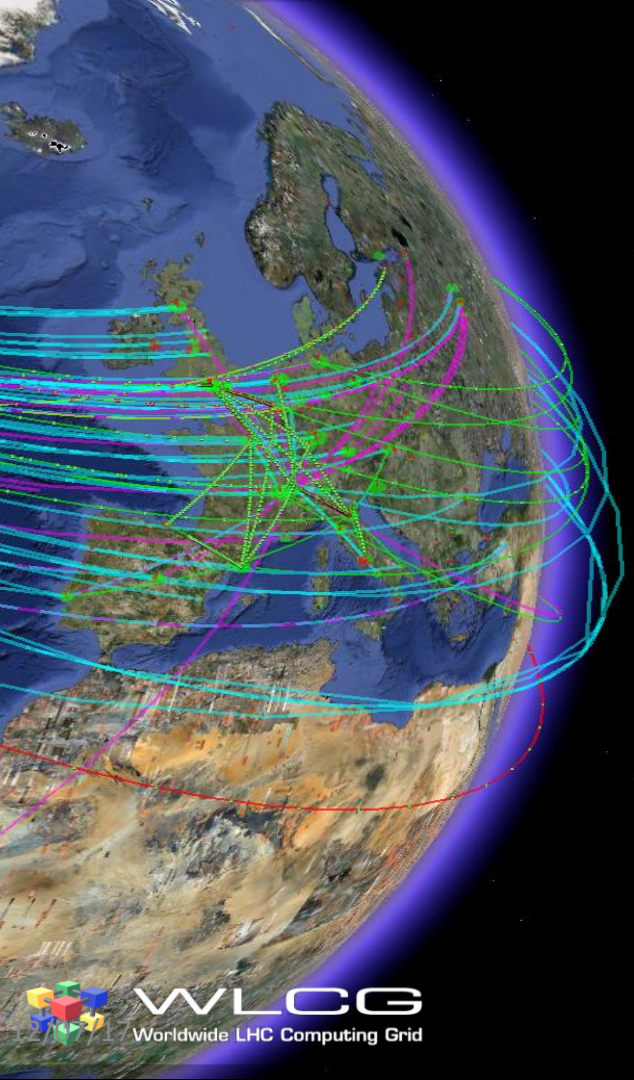
	Question	Response
1	Describe your current job submission workflow. as a general description, please focus on: - Which credentials are used? - How do users obtain and maintain their credentials? - Are the credentials transformed or exchar - How do users present their credentials, e command line and/or web? - How is traceability and suspension ensur	
2	Which storage systems are you using? How is t vs write access authorised? Who owns the data	
3	Are authorisation policies managed and/or deci made centrally (by the VO) or at sites?	
4	Do you have a preference between using autho based on Groups/Roles vs Capabilities? (See supporting information)	
5	What is the typical maximum walltime for a reas job? (See supporting information)	
6	Integration with CERN SSO is foreseen as an o	



Next Steps

Next Steps

- Gather input from LHC VOs
- Much work needed to confirm token schemas, e.g.
  - Input from VOs will be essential, e.g. for token lifetimes
  - Clarification on level of assurance, difference between attribute vs authorisation tokens
- Deploy Pilot AAIs at CERN (required for data transfer)



Questions?