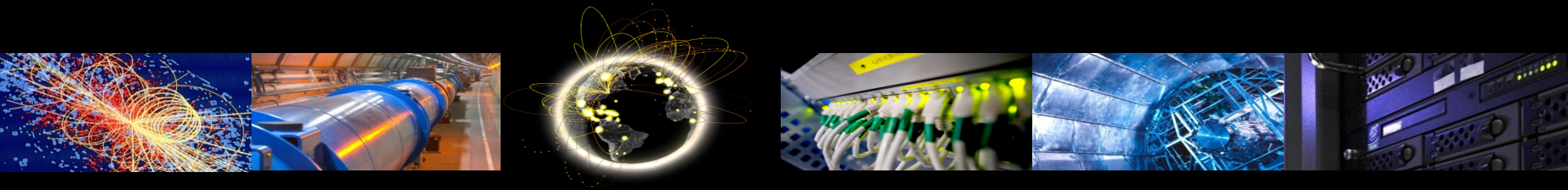
Presented by Andrea Ceccanti

WLCG Authorisation; from X.509 to Tokens

Authored by the WLCG AuthZ Working Group

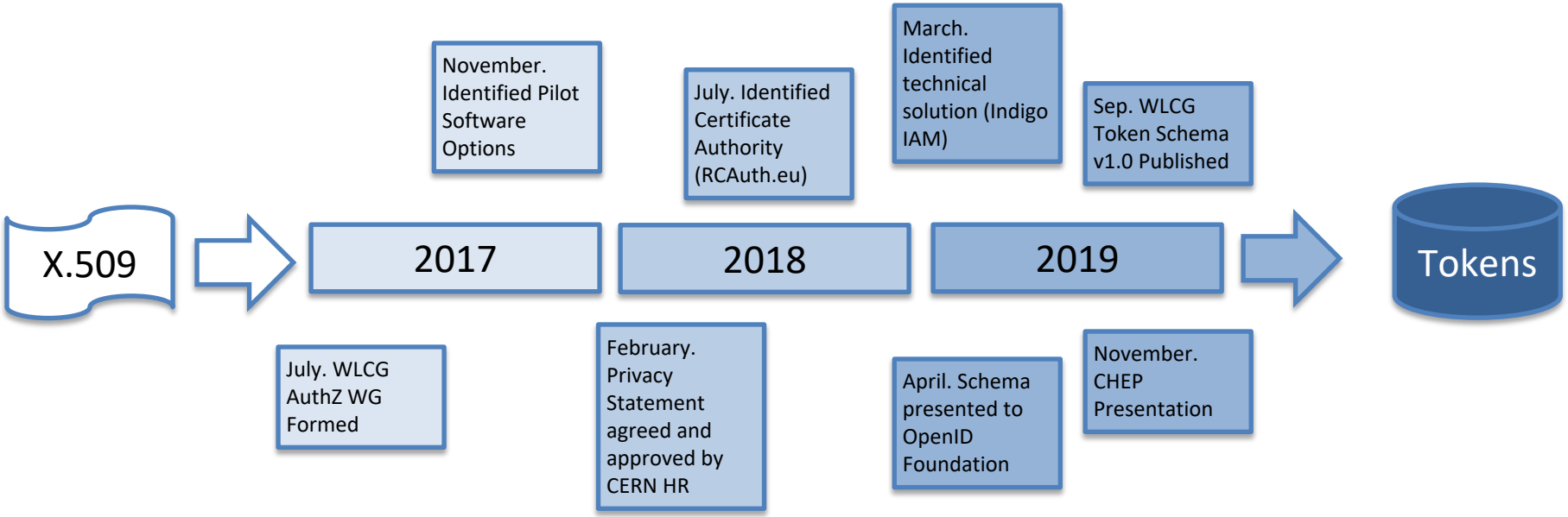
CHEP, Adelaide, November 5th 2019



WLCG
Worldwide LHC Computing Grid

CERN

Towards Tokens



Why? Motivation

- **Evolving Identity Landscape**
  - User-owned X.509 certificates -> federated identities (SAML & 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
- **Data Protection**
  - Tightening of data protection (GDPR) requires fine-grained user level access control, certain provisioning practices may need to be adjusted

However, current grid middleware does not support token (OAuth2) based authorisation.

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

Who? WLCG AuthZ WG

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

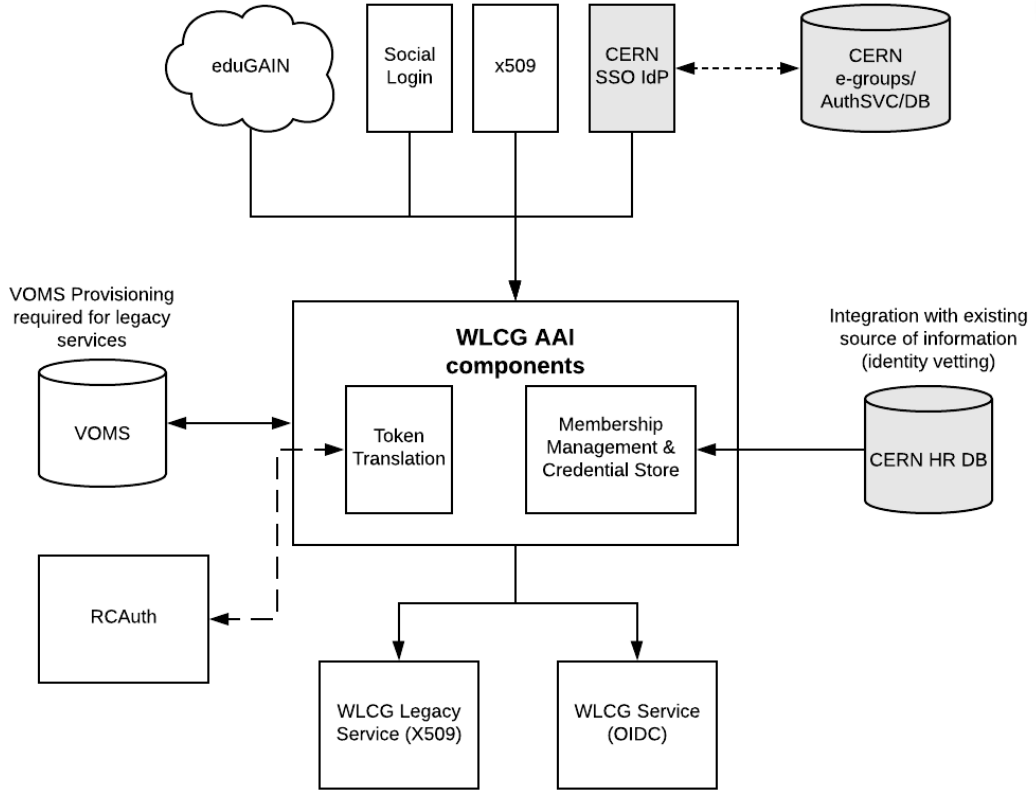
Work tracked in the [WLCG AuthZ WG wiki page]

What are we improving?

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

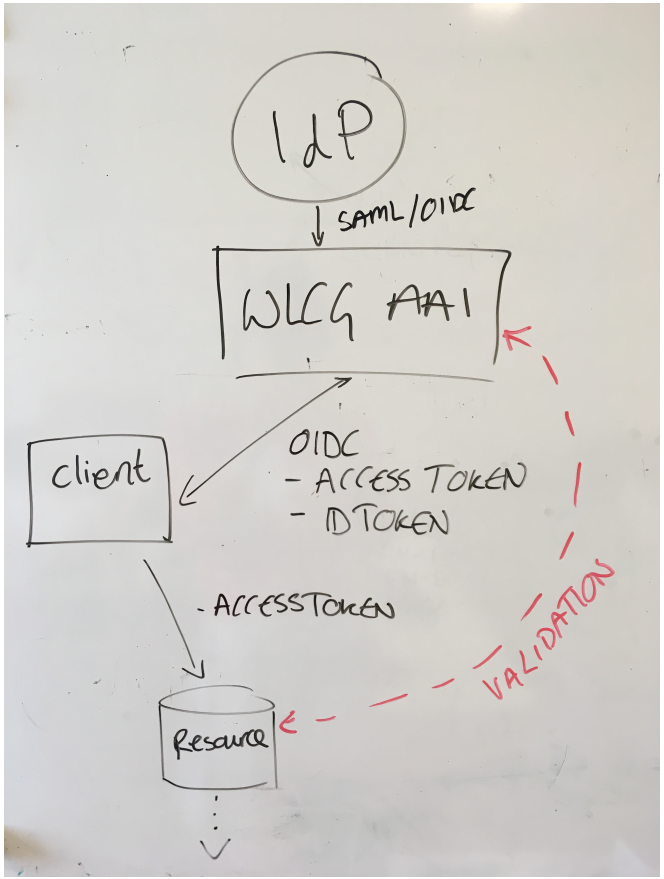
What? Solution Design

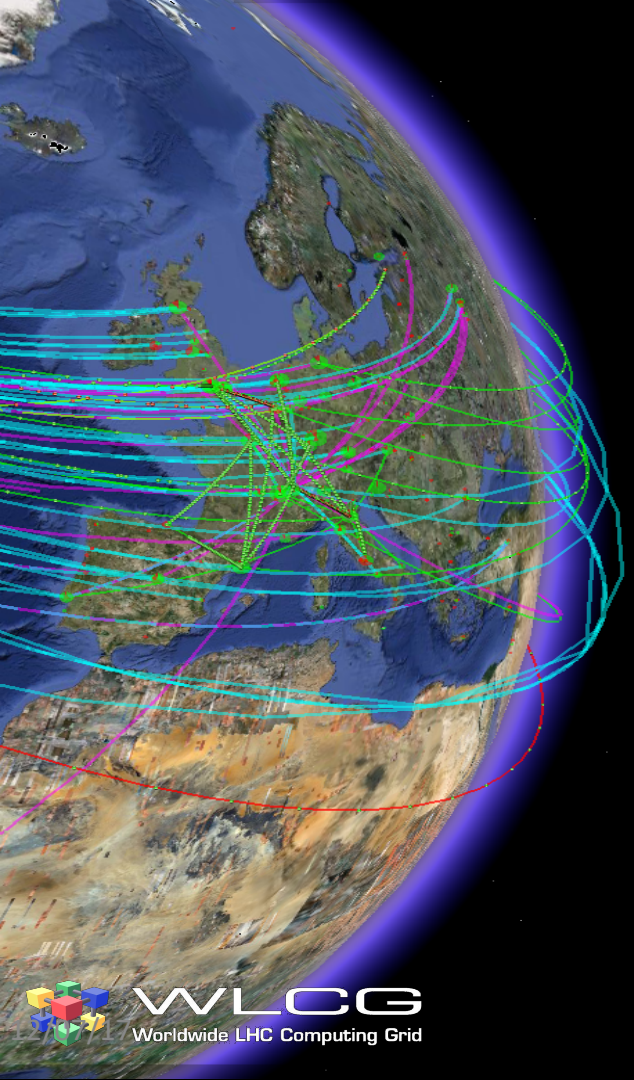
CERN components are optional configuration – technical solution is widely relevant!



More details in Thursday's talk

Draft usage flow



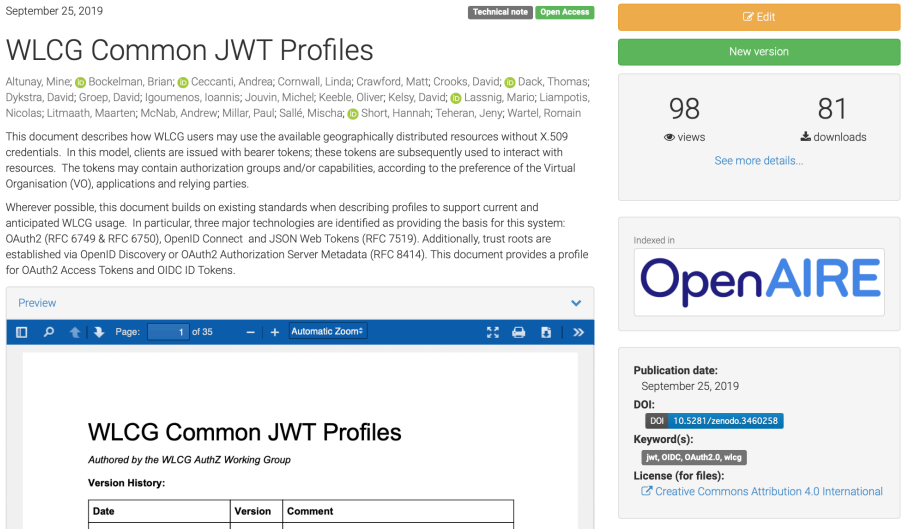


Token Schema

V1.0

- 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
- Compliant Token issuer available for WLCG integration testing:

https://wlcg.cloud.cnaf.infn.it

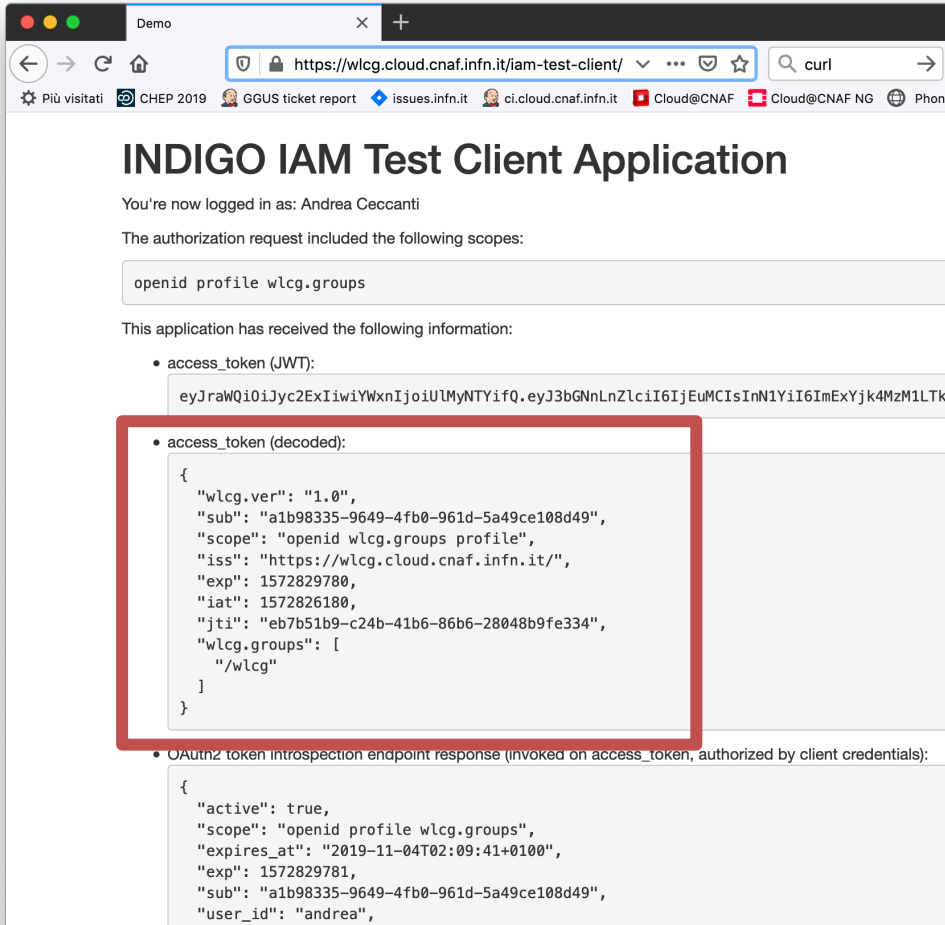


https://zenodo.org/record/3460258#.XacTNi2Q01I

V1.0

- 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
- Compliant Token issuer available for WLCG integration testing:

https://wlcg.cloud.cnaf.infn.it



Token Claims

Common Claims	ID Token Claims	Access Token Claims
• sub • exp • iss • acr • aud • iat • nbf • jti • eduperson_assurance (REFEDS) • wlcg.ver (WLCG) • wlcg.groups (WLCG)	• auth_time • general OIDC Claims	• scope (inspired by OAuth token exchange draft)

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

Two forms of Authorization

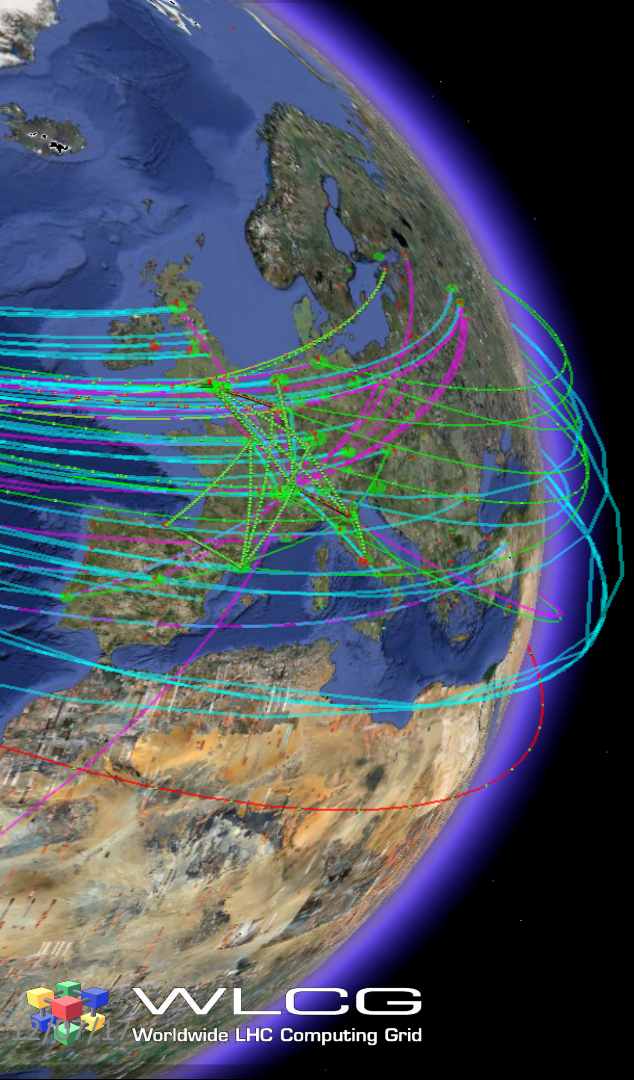
Tokens Assert **Group Membership**

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

Token Asserts **Authorized Actions**

- Called “Capabilities/scopes”
- Specific ability to perform an action (optionally, at a specific path) e.g. **storage.create:/home/joe**

A single schema to rule them all: Scitokens library will soon have support for WLCG JWT profile



Rucio AuthN/Z with Tokens

Rucio AuthN/Z with OAuth/OIDC and JWTs

Jaroslav Guenther

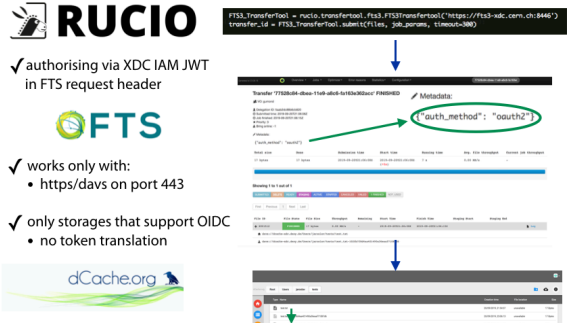
For more details see this talk

- **Rucio user**
  - "account" (CERN LDAP username) + "identity" (auth_type + ID)
  - only carefully 'pre-provisioned' users
  - Rucio daemon syncs accounts & identities (using IAM* SCIM client)
- **Rucio development branch is currently supporting**
  - "Authorization Code Flow" for basic user authentication
  - "Token Exchange" to propagate permissions to downstream services (e.g. FTS)
  - "Refresh Token" to act on behalf of a user (for configurable time)
  - Supporting multiple Identity Providers (Escape IAM, XDC IAM, …)
  - Rucio WebUI login
  - 3 CLI login strategies (automatic, browser redirect & browser redirect + auth server polling)

*More IAM details in Thursday's talk

Practical Tests

- XDC IAM response time
  - Rucio user authentication currently @ 2Hz
  - XDC IAM test cluster average response time ~ 0.5 s
- Initiate data transfer:
  - authenticated Rucio user requests Rucio to make a transfer
  - Rucio exchanges the token for a new one with ‘fts’ in audience claim
  - FTS receives JWT in the header and initiates the transfer on dCache storage



This works thanks to DOMA-TPC work with HTTP-TPC – also being presented at CHEP*!

- Deploying testbed on Rucio Escape Instance:
  - development release is being deployed on Rucio Escape Instance

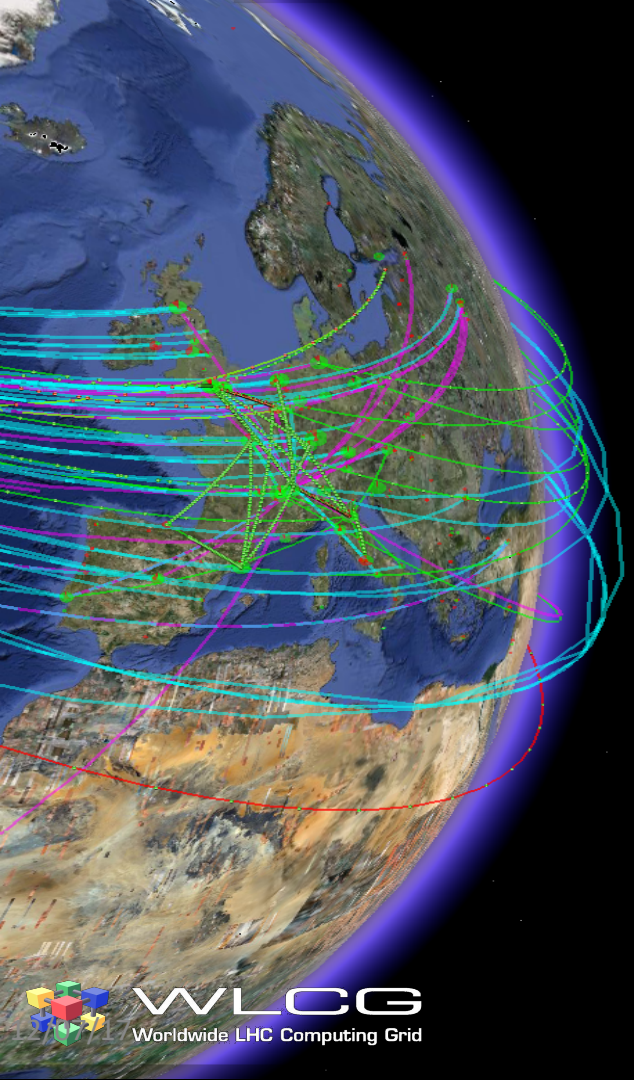
Jaroslav Guenther

* https://indico.cern.ch/event/773049/contributions/3474402/

Conclusions

- Common JWT Profile has reached v1.0
  - **stable reference** for developers and integrators

- WLCG IAM instance **available today** to start the integration work



Questions?