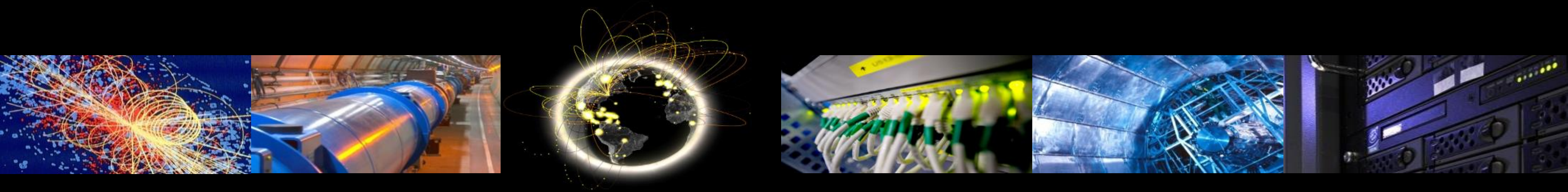
Presented by Hannah Short

WLCG Token Schema

WLCG Management Board

September 17th 2019



WLCG
Worldwide LHC Computing Grid

CERN

WLCG AuthZ WG

- Includes current major users of tokens in HEP
  - INDIGO IAM
  - EGI Check-in
  - SciTokens
  - dCache
  - ALICE
- Development work of pilot projects supported by:

  AARC EOSC-hub EOSCpilot The European Open Science Cloud for Research Pilot Project
- Priority to stick to industry and R&E standards wherever possible
- Started July 2017
- Planning to **publish WLCG Token Schema version 1.0**

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

Status

Step	Result	Status	Due/Completed
Create group	WLCG AuthZ WG	Done	July 2017
Collect Requirements	Document completed and revised	Done	July 2018
Identify Pilot Options	EGI Check-in (EOSC-hub/AARC), INDIGO-IAM (EOSC)	Done	November 2017
Identify Certificate Authority	RCAuth.eu	Done	July 2018
CERN HR Identity Vetting integration	Privacy Statement approved, DB connected via API	Done	February 2019
Enhance Pilot	Pilots presented on March 5th	Done	March 2019
Interview experiments	Questionnaire sent and completed	Done	December 2018
Pilot progress review	Pre-GDB held. Pilots assessed their current state	Done	December 2018
Provide Recommendation to WLCG MB		Done	April 2019
Define JWT Schema for Tokens	**Completed at September pre-GDB**	Done	September 2019
Publish Schema v 1.0		Pending	September 2019
Define Trust Distribution	Collaborate with IGTF	Pending	
Provide guidelines on Token Flows		Pending	

Draft

- Attached to Agenda https://indico.cern.ch/event/769180/
- Presented to the Open ID R&E Working Group (and many participants involved in both groups)
- Discussion for > 1 year during recurring WG meetings
- Input sought from VOs and Software Experts

Token Claims

Common Claims

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

ID Tokens

- auth_time
- general OIDC Claims

Access Tokens

- scope (inspired by OAuth token exchange draft)

Token should include at least scope or group to convey authorisation

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

Two forms of Authorization

- Groups
  - Similar to VOMS Groups
  - VOMS Roles modeled as optional Groups
- Capabilities/scopes
  - Specific ability to perform an action (optionally, at a specific path) e.g. `storage.create /home/joe`
- Both can be requested via scopes
- Capabilities are **interoperable** with SciTokens*

* https://indico.cern.ch/event/739896/#10-scitokens-and-iam-interoper

Assurance

- We adopt the **eduperson_assurance** multi-valued claim proposed by RAF to convey the assurance component values and profile.
- The **acr** claim is included in addition to the **eduperson_assurance** claim to specifically convey the authentication assurance.

Distribution of Trust

- Small number of registered clients (e.g. HTCondor submit nodes, token provisioning scripts)
  - Clients authenticate with Client Secret
- Large number of unregistered Resource Servers (e.g. storage node)
  - Validate tokens using issuer’s public key for signing*
- **Standard** OIDC discovery (well-known configuration)
- TLS connection to issuer must be validated and verified*
  - Trust roots needed by a wide range of agents/clients

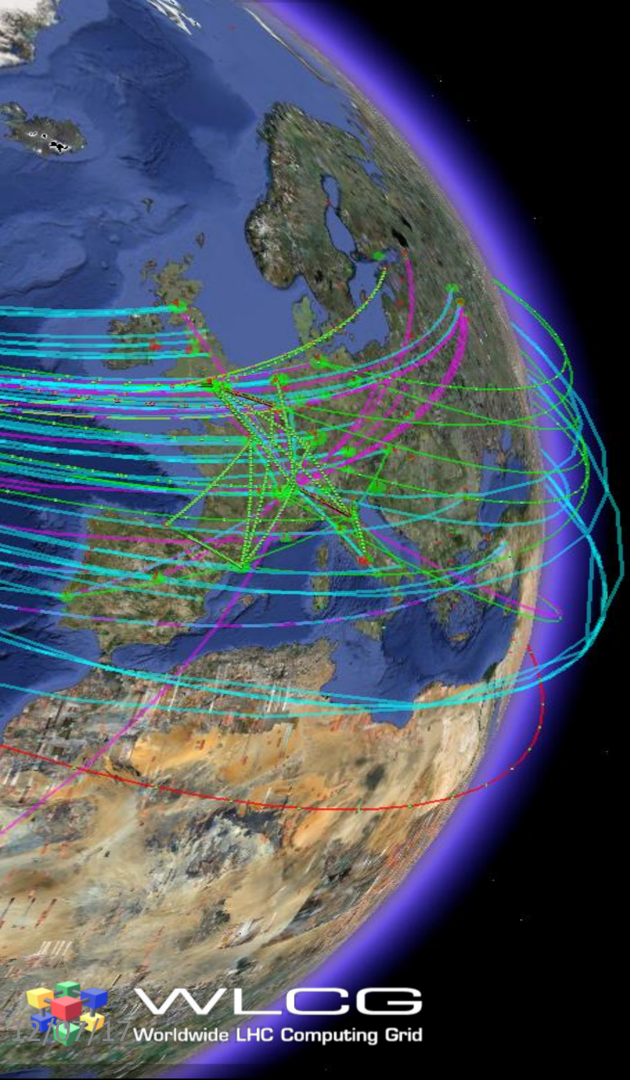
* Signing and transport keys may support different trust models, discussion pending

Lifetimes

Token Type	Recommended Lifetime	Minimum Lifetime	Maximum Lifetime	Justification
Access Token & ID Token	20 minutes	5 minutes	6 hours	Access token lifetime should be short as there is no revocation mechanism. The granted lifetime has implications for the maximum allowable downtime of the Access Token server.
Refresh Token	10 days	1 day	30 days	Refresh token lifetimes should be kept bounded, but can be longer-lived as they are revocable. Meant to be long-lived enough to be on a “human timescale”.
Issuer Public Key Cache	6 hours	1 hour	1 day	The public key cache lifetime defines the minimum revocation time of the public key. The actual lifetime is the maximum allowable downtime of the public key server
Issuer Public Key	6 months	2 days	12 months	JWT has built-in mechanisms for key rotation; these do not need to live as long as CAs. This may evolve following operational experience, provision should be made for flexible lifetimes.

Next Steps

- Middleware developers would like published Schema to guide work towards token based authorisation => publish version WLCG:1.0
  - Asked for comments by Friday 20th
  - Publish to Zenodo
- Provide stable testing environment to issue tokens based on WLCG v1.0



Questions?