WLCG AuthZ WG

WLCG Workshop, Naples

March 28th, 2018
Agenda

• WG background

• Activities
  – JWT Schema
  – AAI Pilot Projects

• Next steps
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 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
Timeline

- July 26 2017 [https://indico.cern.ch/event/656027/](https://indico.cern.ch/event/656027/)
  - Kickoff meeting
- September [https://indico.cern.ch/event/669715/](https://indico.cern.ch/event/669715/)
- October [https://indico.cern.ch/event/670330/](https://indico.cern.ch/event/670330/)
- November [https://indico.cern.ch/event/578976/](https://indico.cern.ch/event/578976/)
  - pre-GDB, Requirements Gathering
- December [https://indico.cern.ch/event/680452/](https://indico.cern.ch/event/680452/)
  - INDIGO IAM and EGI Check-in demos
- January [https://indico.cern.ch/event/696286/](https://indico.cern.ch/event/696286/)
  - Demo assessments
- February [https://indico.cern.ch/event/706302/](https://indico.cern.ch/event/706302/)
  - CRIC Authorization Workflow
  - AARC Pilots plan
- March 28 2018
  - WLCG Workshop
WLCG AuthZ Requirements

• **VO Membership Management**
  – Attributes? VO ID, ID of credential, Name, Email, Authorization
  – Support multiple federated credentials & their linkage
  – Active role selection
  – Token management achievable by the standard user

• **Service Requirements**
  – Attributes? Authorization plus traceability | | Groups/Roles
  – Ease of implementation
  – Use standard approaches
  – Token integrity and validity verifiable
    • Without connecting to the issuer
  – For non-web, users should not have to manage identities in addition to their login session

• **General**
  – Support for fine grained suspension
  – Smooth transition from current X509-based to token-based AAI

Splitting things more into “identity based” and “authorization based” approaches. Third-party services (e.g. storage) would primarily consume the latter.
WG Activities
Two separate activities were identified during the pre-GDB
- Design and testing of WLCG Membership Management and Token Translation services (AAI Pilot Projects)
- Definition of a JSON Web Token (JWT) profile for authentication and authorization for WLCG services and token issuers
  - See the SciTokens presentation for a pilot implementation
Computing services are increasingly turning to token based authentication & authorization (OIDC, OAuth2...)

Multiple infrastructure projects already using/supporting token based authorization but with diverging schemas or technologies

- INDIGO IAM
- EGI Check-in
- SciTokens
- dCache
- ALICE tokens

Is WLCG able to define a shared schema for participating infrastructures and services to agree?
• Initial analysis has concluded that two separate schemas are required
  – Identity Schema (who is this person?)
    • EGI Check-in, INDIGO IAM, dCache, ...
  – Capability Schema (what is the bearer of this token authorized to do?)
    • EGI Check-in, INDIGO IAM, dCache, SciTokens, ALICE...
  – Work is ongoing to draft schema definitions
AAl Pilot Projects

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

Future infrastructure should support a range of credential types for users and services and provide a user friendly experience.
AAI Pilot Projects

WLCG AuthZ WG
Central component to replace VOMS Admin & provide token translation

Possible feed of AuthZ back to e-groups (or replacement)

CERN HR DB for identity vetting

WLCG AAI and connected services must adopt JWT schema

VOMS provisioning and lookup for legacy services
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
  - AUP re-signing
• Aim: provide the WLCG MB with hands-on feedback on two possible solutions capable of taking the first step towards X509-free WLCG
  - Both approaches require additional developments
  - Both strategies will have to ensure sustainability of these developments in the forthcoming years

• Proposed timeline
  - Finalization of new required developments for EGI Check-in, COmanage and INDIGO IAM: March-July 2018
  - Deployment and pilot testing: August-September 2018
  - Reporting / Benchmarking: October-December 2018
  - Final dissemination on pilot: January-March 2019
Next Steps
AuthZ WG Objectives

- Objectives have become clear over past 6 months:
  - Gather requirements for a WLCG AAI to provide Membership Management & Token Translation services
    - To facilitate transition to token-based credentials
  - Guide the development of AAI Pilot Projects
    - INDIGO IAM (pilot supported e.g. by EOSC-Pilot & AARC)
    - EGI Check-in & COmanage (pilot supported e.g. by AARC)
  - Define a JSON Web Token (JWT) Schema for Authorization and agree to its use among WLCG Participants
  - Assess the AAI Pilot Projects against our requirements and move towards production deployment on a per-VO basis
Ongoing Tasks

- Continue JWT Schema Definition
- Guide development and testing of AAI Pilots
- Assess overlap of WLCG AAI and CERN SSO Infrastructure

Participation in the WG is welcome!
E-group: project-lcg-authz@cern.ch
Twiki: https://twiki.cern.ch/twiki/bin/view/LCG/WLCGAuthorizationWG
Questions?