Moving to Tokens: IRIS and WLCG

Migrating to Token-Based AuthN and AuthZ
Internet2 TechEx 2022
Tom Dack
IRIS

• eInfrastructure for Research and Innovation for STFC
• A coordinating body for the provision of STFC eInfrastructure
• Common elements are required for IRIS resources to function as a coherent infrastructure
  • Policy and Trust Framework
  • Identity Management
  • Resource Accounting
  • Monitoring

WLCG

• Worldwide LHC Computing Grid
• Replacing existing X509 + VOMS system with token flows
• Working towards token support across the full WLCG stack
Motivations for Migration

- There is a landscape shift away from X.509 user certificates
  - Not user friendly
  - Mobility issues – moving certificates around
  - Interoperability issues with the broader federated infrastructure landscape

- Shift towards OAuth2 and OpenID Connect (Tokens)
  - Tokens widely accepted
  - Easy to implement – used by major industry players
  - Links directly to home institutions
An authentication and authorization application that
- supports **multiple authentication mechanisms**
- provides users with a **persistent, organization scoped** identifier
- exposes **identity information, attributes and capabilities** to services via **JSON Web Tokens** and standard **OAuth & OpenID Connect** protocols
- can integrate existing **VOMS-aware services**
- supports **Web and non-Web access, delegation and token renewal**
INDIGO IAM and the AARC Blueprint Architecture for Infrastructures

Authentication and Authorisation for Research and Collaboration (AARC)
## WLCG Token Schema

<table>
<thead>
<tr>
<th>Common Claims</th>
<th>ID Tokens</th>
<th>Access Tokens</th>
</tr>
</thead>
<tbody>
<tr>
<td>• sub</td>
<td>• auth_time</td>
<td>• scope (RFC8693)</td>
</tr>
<tr>
<td>• exp</td>
<td>• general OIDC Claims</td>
<td></td>
</tr>
<tr>
<td>• iss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• acr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• aud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• iat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• nbf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• jti</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• eduperson_assurance (REFEDS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• wlcg.ver (WLCG)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• wlcg.groups (WLCG)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

- **iss+sub** used to uniquely identify a user, e.g. for blocking
- **wlcg** prefix added to avoid collisions with other schemas

Access tokens should include at least scope (capabilities) or group for authorization
**Token Status:**

**IRIS**

- Multi-tenancy Identity Management Platform, serving multiple IRIS communities
- IRIS IAM is a production service, providing AuthN/Z to IRIS and STFC communities
- Primary authentication to IRIS services, including Accounting Portals, IRIS DynaFed (Storage), MISP Security Portal and OpenStack Clouds

**WLCG**

- IAM is in production for the four LHC experiments
  - Contents are automatically replicated from VOMS-Admin
- IAM VOMS endpoints can be used alongside the legacy VOMS services
  - In production for ATLAS and CMS
  - TBD for ALICE and LHCb
- ATLAS, CMS and SAM ETF can use tokens to submit jobs to HTCondor CEs
  - CEs on OSG, which only support tokens since May
  - Those jobs still use X509 VOMS proxies for data management etc.
The Big Challenges

- **Token Lifetimes**
  - *Token lifetime is typically short for security reasons – what happens with a job longer than the token*
  - *Current WLCG Pilot job submission token lifetimes are a few days*
    - *Allows times to resolve service incidents transparently*
    - *Only used in security handshakes with Ces*
  - *Refresh Tokens – potential security concerns*
- **High Availability Operations**
- **Interoperability**
  - *Following AARC guidelines where possible*
Challenges - IRIS

• How to provide access to services which operate only over command line
  • OAuth Device Code PAM with Group Authorization
  • https://github.com/stfc/pam_oauth2_device

• Assurance for users who do not have an eduGAIN IdP
  • Using the AAI platform as an Identity-Provider-of-last-resort
  • ”Community” IAM instances with local credentials acting as IdPs
Challenges - WLCG

• Support Level
  • *Staff availability and service reliability has caused issues here*

• Phasing out VOMS-Admin
  • *User, group, and role management needs to migrate to IAM*
  • *Transition phase will require supporting both in tandem*
Questions?
Thank you