WLCG Authentication and Authorisation Infrastructure (AAI) Update

HOW2019, JLab

March 19th 2019
Motivation

- **Evolving Identity Landscape**
  - User-owned X.509 certificates -> federated identities (SAML & OpenID Connect)
  - 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 federated identities or token based authorisation.

**Objective:** Understand & meet the requirements of a future-looking AuthZ service for WLCG experiments
• Includes current major users of tokens in HEP
  – INDIGO IAM
  – EGI Check-in
  – SciTokens
  – dCache
  – ALICE

• Development work of pilot projects supported by:

• Priority to stick to industry and R&E standards wherever possible

• Bi-monthly calls & 3 pre-GDBs since July 2017
WLCG AuthZ WG

• Twiki:
https://twiki.cern.ch/twiki/bin/view/LCG/WLCG AuthorizationWG
What are we doing?

- Removing the need for researchers to manage x509 certificates
- Enabling token based authorisation (linked to DOMA work)
- Replacing VOMS-Admin
Solution Design

WLCG AAI components

- Token Translation
- Membership Management & Credential Store

Integration with existing source of information (identity vetting)

CERN HR DB

VOMS Provisioning required for legacy services

VOMS

WLCG Web Service

WLCG Grid Service

eduGAIN

Social Login

x509

CERN SSO IdP

CERN AuthSVC/DB
<table>
<thead>
<tr>
<th>Step</th>
<th>Result</th>
<th>Status</th>
<th>Due/Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create group of relevant people able to influence WLCG and make changes</td>
<td>WLCG AuthZ WG</td>
<td>Done</td>
<td>July 2017</td>
</tr>
<tr>
<td>Collect Requirements</td>
<td>Document completed and revised</td>
<td>Done</td>
<td>July 2018</td>
</tr>
<tr>
<td>Identify Pilot Options</td>
<td>EGI Check-in + COManage (EOSC-hub/AARC), INDIGO-IAM (EOSC)</td>
<td>Done</td>
<td>November 2017</td>
</tr>
<tr>
<td>Identify Certificate Authority for token translation</td>
<td>RCAuth.eu</td>
<td>Done</td>
<td>July 2018</td>
</tr>
<tr>
<td>CERN HR Identity Vetting integration</td>
<td>Must be on site, Privacy Statement approved, DB connected. API layer developed by Andrea</td>
<td>Done</td>
<td>February 2019</td>
</tr>
<tr>
<td>Define JWT Schema for tokens (capability based &amp; group based)</td>
<td>Converging and ironing out details</td>
<td>In Progress</td>
<td>April 2019</td>
</tr>
<tr>
<td>Enhance Pilot Options to match requirements</td>
<td>Pilots presented on March 5&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Done</td>
<td>March 2019</td>
</tr>
<tr>
<td>Interview experiments to match proposal to workflows</td>
<td>Questionnaire sent and completed for 3 LHC VOs (1 in progress)</td>
<td>Done</td>
<td>December 2018</td>
</tr>
<tr>
<td>Pilot progress review</td>
<td>Pre-GDB held. Pilots assessed their current state</td>
<td>Done</td>
<td>December 2018</td>
</tr>
<tr>
<td>Provide Recommendation to WLCG Management Board</td>
<td></td>
<td>Not Started</td>
<td>April 2019</td>
</tr>
</tbody>
</table>
Summary

• Two services being enhanced to meet WLCG Requirements [1]
  – EGI-Check-in (Nicolas Liampotis, Ioannis Igoumenos - GRNET)
  – IAM (Andrea Ceccanti - INFN)

[1] https://twiki.cern.ch/twiki/bin/viewauth/LCG/WLCGAuthorizationWG
Both solutions

- Are backwards compatible (i.e. VOMS provisioning)
- Fulfill 90% of the requirements [1] (exception being 2FA that can be handled at the CERN SSO layer for LHC VOs)
- Integrate IOTA Certificates from RCAuth.eu
- Can verify membership against the CERN HR DB (thanks to Andrea Ceccanti from IAM for creating and sharing an API)
- Provided sustainability statements

[1] https://twiki.cern.ch/twiki/bin/viewauth/LCG/WLCGAuthorizationWG
EGI-Check-in

Advantages
• Components in common usage (COManage, SimpleSamlPhP)
• Powerful configuration options

Disadvantages
• User friendliness
• Complexity
• Many components, deployment considerations
INDIGO IAM

Advantages
• User friendliness, particularly RCAuth integration and command line flow
• Ease of deployment

Disadvantages
• Fewer users
• HR DB periodic synch not yet implemented (implementation path well understood, HR identity vetting already integrated at registration time)
Two user-friendly methods identified:

- **SSH Key Upload workflow**
  - User uploads an SSH key and can retrieve a proxy on the command line
- **Device Code Flow (see video on next slide)**

Both pilots enable command line access:

- IAM supports Device Code Flow
- EGI-Check-in supports SSH Key Upload and Device Code Flow (for access tokens, not proxies)

Both methods could be integrated in both solutions
Video lasts 3.34 minutes, also available at https://videos.cern.ch/record/2667022

**Note:** This is an example from IAM. The script can be extended to generate VOMS proxies, rather than generic proxies, and can be simplified to eliminate the need to copy-and-paste the code.
Key decisions include defining the token content and manner in which they are requested

Progress

- Document has been significantly restructured to a clearer format
- Many of the trust and security aspects are now well understood
- Convergence that tokens should be provisioned over OIDC

Work required to finalise token content

- Bi-weekly calls scheduled
Next Steps

• Complete JWT Document
• Provide feedback to WLCG Management Board
• Deployment considerations
  – Assurance profiles for LHC VOs
  – Policies regarding deployment and operations

All information at https://twiki.cern.ch/twiki/bin/view/LCG/WLCGAutorizationWG
Questions?