Tokens in WLCG - Introduction

WoTBAn&Az

October 18th 2021
Overview

- WLCG (Worldwide LHC Computing Grid) used for high energy physics data analysis
- Since 2000s has relied on X.509 certificates for client and user authentication, and VOMS for authorization
- Since 2017 have been looking to move to JWT tokens over OAuth2.0
  - WLCG Authorization Working Group meets every 2 weeks
Towards Tokens

X.509

2017
- July. WLCG AuthZ WG Formed
- November. Identified Pilot Software Options

2018
- February. Privacy Statement agreed and approved by CERN HR
- July. Identified Certificate Authority (RCAuth.eu)

2019
- March. Identified technical solution (Indigo IAM)
- Sep. WLCG Token Schema v1.0 Published

2020
- WLCG IAM deployed for CMS and ATLAS
- Hackathons demonstrated full token workflow
- WLCG IAM deployed for ALICE and LHCb

2021
- Command line flows and tools clarified

Tokens
Published on Zenodo, September 25th 2019

Allows middleware developers to enable token based authorization to an agreed schema

AAI Design

CERN SSO configured as sole Identity Provider, enables identity verification via HR DB (match CERN PersonID)

INDIGO IAM chosen as WLCG AAI software

Follows the AARC Blueprint https://aarc-community.org/architecture/
Anticipated Token Flows

Small number of registered clients, large number of unregistered resources

Usability of command line flows proving more complex than anticipated! Discussions ongoing in the WLCG Authorization Working Group
## Certificate fadeout

- X.509 will continue to play a vital role in our infrastructure as host certificates, but users will no longer need to manage the certificate lifecycle themselves.
- It is likely that power users, e.g. admins, may need to manage certificates for much longer.
- This is a very early plan and significant changes are expected.

<table>
<thead>
<tr>
<th>Activity</th>
<th>2019</th>
<th>2020</th>
<th>2021</th>
<th>2022</th>
<th>2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrate RCAuth.eu for on-demand IOTA X.509</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Migrate VOs to IAM, retire VOMS Admin</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add Token support to Middleware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dual mode (IAM issues X.509/VOMS and Tokens)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privilege Tokens, analyse remaining X.509 use</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Begin removing X.509 User Certificate Support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Today’s Talks

<table>
<thead>
<tr>
<th>Time</th>
<th>Item</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td>5m</td>
<td>Introduction</td>
<td>Hannah Short (CERN)</td>
</tr>
<tr>
<td>20m</td>
<td>Lightning talk: Fermilab</td>
<td>Mine Altunay, Dave Dykstra (Fermilab)</td>
</tr>
<tr>
<td></td>
<td>Lightning talk: CERN - WLCG IAM deployment</td>
<td>Hannah Short (CERN)</td>
</tr>
<tr>
<td></td>
<td>Lightning talk: CiLogon and WLCG</td>
<td>Jim Basney (Uni Illinois)</td>
</tr>
<tr>
<td></td>
<td>Lightning Talk: Condor with Vault</td>
<td>Dave Dykstra (Fermilab)</td>
</tr>
<tr>
<td>10m</td>
<td>IAM Development Roadmap</td>
<td>Andrea Ceccanti (INFN)</td>
</tr>
</tbody>
</table>
Questions?