WLCG Authorization: from X.509 to Tokens

Authored by the WLCG AuthZ Working Group

PRACE-CERN-GÉANT-SKAO workshop on HPC, 29th September 2020
HEP Moving to Tokens

X.509 + VOMS

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

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

- 2019
  - April. Schema presented to OpenID Foundation
  - September. WLCG Token Schema v1.0 Published
  - November. CHEP Presentation

- Tokens

+ X.509 + VOMS for a while...
Why? Motivation

- **Evolving Identity Landscape**
  - User-owned X.509 certificates come with difficulties and significant support effort
  - Better alternatives now exist → JWT Tokens over OAuth2 and OpenID Connect

- **Technology Readiness**
  - 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

Much work is ongoing to enable token based authorization in HEP infrastructure, with WLCG leading the way.
What? Solution Design

WLCG AAI components

- eduGAIN
- Social Login
- x509
- CERN SSO IdP
- CERN e-groups/AuthSVC/DB
- VOMS Provisioning required for legacy services
- VOMS
- Token Translation
- Membership Management & Credential Store
- CERN HR DB

Integration with existing source of information (identity vetting)

HPC Centers

WLCG Legacy Service (X509)
WLCG Service (OIDC)

OpenID
eduGAIN

WLCG AuthZ WG
Token Schema

- Published on Zenodo, September 25th 2019
- Allows middleware developers to enable token-based authorization according to an agreed schema

https://zenodo.org/record/3460258
### Token Claims

<table>
<thead>
<tr>
<th>Common Claims</th>
<th>ID Token Claims</th>
<th>Access Token Claims</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sub</code></td>
<td><code>auth_time</code></td>
<td><code>scope</code> (inspired by OAuth token exchange draft)</td>
</tr>
<tr>
<td><code>exp</code></td>
<td><code>general OIDC Claims</code></td>
<td></td>
</tr>
<tr>
<td><code>iss</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>acr</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>aud</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>iat</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>nbf</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>jti</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>eduperson_assurance</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(REFEDS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>wlcg.ver</code> (WLCG)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>wlcg.groups</code> (WLCG)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Where unspecified, the origin is RFC7519 or OpenID Connect core
Two forms of Authorization

Tokens Assert **Group Membership**
- Similar to VOMS Groups
- VOMS Roles are modeled as optional Groups

Tokens Assert **Authorized Actions**
- Called “Capabilities/scopes”
- Specific ability to perform an action (optionally, at a specific path) e.g. `storage.create /dir-1/dir-2/my-file` (under the root directory of the given VO)

**Capabilities are used by SciTokens** *(a sub-schema of WLCG Schema)*
HPC Integration

• HPC centers would need to accept WLCG OAuth2 bearer tokens for authorization
  – Trust the few, closely guarded WLCG Token issuers
  – Support authorization mechanisms through groups and/or capabilities

• Possibly depending on the timescale, while not every supported VO has switched to tokens:
  support VOMS authorization as being used today
Questions?