# Table of Contents

**WLCG Authorization WG**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Contact</td>
<td>1</td>
</tr>
<tr>
<td>Development tips</td>
<td>1</td>
</tr>
<tr>
<td>CE token configuration</td>
<td>1</td>
</tr>
<tr>
<td>Current Work</td>
<td>1</td>
</tr>
<tr>
<td>Token based bulk data transfer workflows</td>
<td>1</td>
</tr>
<tr>
<td>Design and test command line workflow tools</td>
<td>2</td>
</tr>
<tr>
<td>Update the WLCG Profile</td>
<td>2</td>
</tr>
<tr>
<td>Analyse the impact of Tokens on the WLCG Security Model</td>
<td>2</td>
</tr>
<tr>
<td>Traceability &amp; Suspension</td>
<td>2</td>
</tr>
<tr>
<td>Provide backwards compatibility tools</td>
<td>3</td>
</tr>
<tr>
<td>Guidance on capability vs group usage</td>
<td>3</td>
</tr>
<tr>
<td>Recommendations on client registration</td>
<td>3</td>
</tr>
<tr>
<td>Workplan</td>
<td>3</td>
</tr>
<tr>
<td>Face-to-Face Meetings</td>
<td>3</td>
</tr>
<tr>
<td>Video-Conference Meetings</td>
<td>4</td>
</tr>
<tr>
<td>Public Facing Documents</td>
<td>4</td>
</tr>
<tr>
<td>WG Documents</td>
<td>4</td>
</tr>
<tr>
<td>Internal / Draft documents</td>
<td>5</td>
</tr>
<tr>
<td>Related Presentations</td>
<td>5</td>
</tr>
<tr>
<td>Reference Documents</td>
<td>5</td>
</tr>
</tbody>
</table>
WLCG Authorization WG

Introduction

The shift towards federated identities and the adoption of new authorization standards by industry is a strong signal for WLCG to adapt its authorization infrastructure. It is necessary to continue to connect with users globally as well as peer organisation, infrastructures and cloud services.

Although it is clear that WLCG has to evolve away from X.509 at least for end users, there has been no community wide strategy. Several independent efforts to provide an authorization infrastructure supporting federated identity and authorization without certificates have been started and it is essential that a common vision be agreed upon. Different solutions are being implemented in the Research & Education sector and a number of translation services will be required to allow interoperable services.

The objective of this working group is to understand & meet the requirements of an AuthZ service for WLCG experiments focused on serving the 99% of our researchers.

There are several main activities

1. Design and testing of a WLCG Membership Management and Token Translation service, facilitated by pilot projects with the support of AARC (AAI Pilot Projects)
2. Definition of a token based authorization schema for downstream WLCG services and token issuers (JWT)
3. Definition of token based workflows

Contact

e-group and mailing list, project-lcg-authz@cernNOSPAMPLEASE.ch

Development tips

• Token support development tips
• WLCG VO token usage examples
• HTCondor CE client configuration tips
• HTCondor CE test service on a single host

CE token configuration

• HTCondor CE token configuration tips
• ARC-CE token configuration tips

Current Work

Token based bulk data transfer workflows

Many workflows for WLCG rely on one service calling another, for example Rucio & FTS. Each service in these workflows may expect different tokens with specific groups/capabilities for authorization. The
mechanisms to provision the correct tokens to the correct services must be defined, taking into account operational impact. Please see the Slides for an overview.

**Leader:** Andrea/Francesco  
**Output:** Specification/Documentation

## Design and test command line workflow tools

Physics workflows typically start on the command line. The WLCG community will need a user friendly mechanism to provision tokens locally, and that these tokens be correctly scoped for the workflow in question. There are several options under consideration such as OIDC-agent, myToken and htgettoken with Vault. Requirements include:

- Users should not need to manage additional passwords  
- Browser interaction should be limited (i.e. once per 10 days)  
- Users should not need to manage client credentials  
- The use of public clients (i.e. clients that do not require a client secret) should be well controlled

A next step is to install htgettoken with Vault for the WLCG IAMs to allow for user feedback.

**Leader:**  
**Output:** Report with recommendations following user feedback

## Update the WLCG Profile

The WLCG JWT Profile was published in September 2019 on Zenodo. Since then practical experience and feedback has been gathered. The Profile will be updated to incorporate points such as:

- Leverage RFC 9068 wherever possible  
- Make the profile more inclusive and open for use by other communities, i.e. not call it "WLCG"  
- Specify fine grained compute scopes

**Leader:** Brian B  
**Output:** New version of the JWT Profile

## Analyse the impact of Tokens on the WLCG Security Model

A thorough study of the security impact of Tokens and their use in WLCG will be made. This may be via direct comparison with the risks of X.509.

**Leader:**  
**Output:** Report with recommendations

## Traceability & Suspension

Work is needed to ensure traceability requirements (from the traceability working group) are respected. Additionally, mechanisms to suspend users and revoke tokens must be defined and tested.

**Leader:** David C
**Output:** Report with recommendations

**Provide backwards compatibility tools**

Certain tools, e.g. grid mapfile generation, must be replicated for the new infrastructure.

**Leader:** Maarten L

**Output:** Tools

**Guidance on capability vs group usage**

Guidance is needed to help services understand whether groups or capabilities are more suitable for their use case, and to clarify some aspects of when groups and capabilities may be used in parallel.

**Leader:**

**Output:** Documentation

**Recommendations on client registration**

The topic of usability of client registration has been raised several times. Registering clients is a manual process and requires generating a clientID and secret from a WLCG IAM instance - this is significantly different from the previous certificate based authorisation model. Discussion is needed to understand what is acceptable for our community and provide recommendations.

**Leader:**

**Output:** Report with recommendations

**Workplan**

This is a rough timeline of priorities for the coming months

<table>
<thead>
<tr>
<th>Work item</th>
<th>Oct 21</th>
<th>Nov 21</th>
<th>Dec 21</th>
<th>Jan 22</th>
<th>Feb 22</th>
<th>Mar 22</th>
<th>Apr 22</th>
<th>May 22</th>
<th>Jun 22</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token based bulk data transfer</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Command Line Tools</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Update WLCG Profile</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Security Analysis</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Suspension mechanisms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backwards Compatibility Tools</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capability vs group usage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Registration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Face-to-Face Meetings**

- July 26 2017 https://indico.cern.ch/event/656027/ Kickoff meeting, GDB
- November 2017 https://indico.cern.ch/event/578976/ pre-GDB, Requirements Gathering
- March 28 2018 WLCG Workshop https://indico.cern.ch/event/658060/
- July 17 2018 pre-GDB https://indico.cern.ch/event/651343/
- July 18 2018 Summary in GDB https://indico.cern.ch/event/651355/
- December 11 2018 pre-GDB https://indico.cern.ch/event/651348/
• March 13 2019 Summary in GDB https://indico.cern.ch/event/739876/
• March 19 2019 HOW Workshop Session https://indico.cern.ch/event/759388/contributions/3324311/
• September 10th 2019 pre-GDB at Fermilab https://indico.cern.ch/event/739896/
• January 16-17 2020 Token Hackathon https://indico.cern.ch/event/870616/

Video-Conference Meetings

See the Indico Category https://indico.cern.ch/category/68/

Particular meetings to note:

• December 14th 2017 AAI Pilot Projects https://indico.cern.ch/event/680452/ Indigo IAM and EGI Checkin demos
• January 26th 2018 AAI Pilot Projects https://indico.cern.ch/event/696286/ Demo assessments
• February 21st 2018 AAI Pilot Projects https://indico.cern.ch/event/706302/ CRIC Authorization Workflow & AARC Pilots plan
• May 28th 2018 AAI Pilot Projects https://indico.cern.ch/event/731164/ SciTokens and Condor
• September 20th 2018 VO Interviews https://indico.cern.ch/event/752370/
• December 13th 2018 https://indico.cern.ch/event/779671/ (VO Meetings, ALICE and LHCb)
• February 1st 2019 https://indico.cern.ch/event/792989/ (VO Meetings, CMS and ATLAS)
• March 5th 2019 https://indico.cern.ch/event/791175/ DEMOS
• April 8th 2019 https://indico.cern.ch/event/812344/ (with OpenID Foundation R&E Working Group)
• April 11th 2019 https://indico.cern.ch/event/804340/ (with ARC expert)
• January 28th 2020 https://indico.cern.ch/event/881002/ (Fermilab Questions)
• November 2021 pre-GDB https://indico.cern.ch/event/876810/

Presentations have been recorded where possible and are available at https://videos.cern.ch/deposit/project/aefb5d6eab4747008b54f305a9d721c5

Public Facing Documents

• WLCG JWT Schema v1.0 on Zenodo
• Software supporting the WLCG JWT Schema on Github
• CHEP2019 Proceedings on EPJ Web of Conferences
• Bearer Token Discovery specification on Zenodo

WG Documents

• (PUBLISHED) WLCG Authorisation Requirements Version 1.0, September 2018, Version 0.1, Working Doc
• (PUBLISHED) Catalogue of JWT usage in Infrastructures Version 1.0, November 2018, Google Doc
• (FINAL) VO Interview Qs Google Doc
• (FINAL) Supporting Information for VOs Hackmd page
• VO Interviews
  ♦ LHCb
  ♦ ATLAS
  ♦ ALICE
  ♦ CMS
Internal / Draft documents

- WLCG Token Transition Timeline
- Client Tools Google Doc
- Timeline
- Github Repository
- Token Issuer Deployment

Related Presentations

- Federated Identity Management for Research https://indico.cern.ch/event/587955/contributions/2936916/
- EOSC-hub AAI: A federated authentication and authorisation infrastructure for international scientific collaboration at scale https://indico.cern.ch/event/587955/contributions/2936245/
- Capability-Based Authorization for HEP (SciTokens) https://indico.cern.ch/event/587955/contributions/2936866/
- WLCG Authorisation; from X.509 to Tokens, CHEP 2019 https://indico.cern.ch/event/773049/contributions/3473383/
- Beyond X.509: token-based authentication and authorization in practice, CHEP 2019 https://indico.cern.ch/event/773049/contributions/3473393/

Reference Documents

- VOMS Admin key features from Maria Dimou
- CERN Authorisation Service Plan from Paolo Tedesco
- Requirements matching to solutions exercise Google Doc
- AARC Pilot Intake Form
- The Road to the New CERN Authentication System, IT CDA
- lifetime of grid jobs from CERN Batch (2 week sample) PRELIMINARY DATA:

![Histogram of Distribution of jobs]

This topic: LCG > WLCGAuthorizationWG
Topic revision: r53 - 2022-05-30 - MaartenLitmaath