WLCG Authorisation; from X.509 to Tokens

Authored by the WLCG AuthZ Working Group

CHEP, Adelaide, November 5th 2019
Towards Tokens

X.509

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

2018
- February. Privacy Statement agreed and approved by CERN HR
- March. Identified technical solution (Indigo IAM)

2019
- April. Schema presented to OpenID Foundation
- September. WLCG Token Schema v1.0 Published
- November. Certificate Authority (RCAuth.eu)

Tokens

Towards Tokens
• **Evolving Identity Landscape**  
  – User-owned X.509 certificates -> federated identities (SAML & 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

• **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 token (OAuth2) based authorisation.

**Objective:** Understand & meet the requirements of a future-looking AuthZ service for WLCG experiments.
Representation from wide range of institutes and experiments. Development work of pilot projects supported by:

Work tracked in the [WLCG AuthZ WG wiki page](https://example.com)

**What are we improving?**

- **Usability**
  - Removing need for users to manage user-certificates
  - Ability to authenticate with home organisation credentials
- **Membership Management**
  - More flexibility on user authentication
- **Simplified integration**
  - Adopting widely accepted technologies (OAuth2 and OIDC)
  - Priority to stick to standards
What? Solution Design

CERN components are optional configuration – technical solution is widely relevant!

More details in Thursday’s talk
Draft usage flow
Token Schema
- Published on Zenodo, September 25th 2019
- Allows middleware developers to enable token based authorization to an agreed schema
- Tests to be run within WLCG DOMA WG
- Compliant Token issuer available for WLCG integration testing: https://wlcg.cloud.cnaf.infn.it
• Published on Zenodo, September 25th 2019
• Allows middleware developers to enable token based authorization to an agreed schema
• Tests to be run within WLCG DOMA WG
• Compliant Token issuer available for WLCG integration testing: https://wlcg.cloud.cnaf.infn.it

INDIGO IAM Test Client Application
You're now logged in as: Andrea Ceccanti
The authorization request included the following scopes:
- openId profile wlcg.groups
This application has received the following information:
- access_token (JWT):
  eyJraWQiOiI3yCZ2EiIiWixIiQiUUMYNTYiIIO.eyJ3bGNNlNzIiI6IkEwMCIsInNiI5IiI6InExYjkMzM1LTK

- access_token (decoded):
  
  ```json
  {
    "wlcg.ver": "1.0",
    "sub": "a1b98335-9649-4f80-861d-5a49ce188a49",
    "scope": "openid wlcg.groups profile",
    "iss": "https://cloud.cnaf.infn.it",
    "exp": 1572829780,
    "iat": 1572826188,
    "jti": "eb7b51b9-c24b-41b6-86b6-28084b9fe334",
    "wlcg.groups": ["wlcg"
  ]
  }
  ```

- OAuth token introspection endpoint response (invoked on access_token, authorized by client credentials):
  
  ```json
  {
    "active": true,
    "scope": "openid profile wlcg.groups",
    "expires_at": "2019-11-04T02:09:41+0100",
    "exp": 1572829781,
    "sub": "a1b98335-9649-4f80-861d-5a49ce188a49",
    "user_id": "andrea",
  }
  ```
# Token Claims

## Common Claims
- sub
- exp
- iss
- acr
- aud
- iat
- nbf
- jti
  - eduperson_assurance (REFEDS)
  - wlcg.ver (WLCG)
  - wlcg.groups (WLCG)

## ID Token Claims
- auth_time
- general OIDC Claims

## Access Token Claims
- scope (inspired by OAuth token exchange draft)

*Note: Where unspecified, the origin is RFC7519 or OpenID Connect core*
Tokens Assert **Group Membership**
- Similar to VOMS Groups
- VOMS Roles modeled as optional Groups

Token Asserts **Authorized Actions**
- Called “Capabilities/scopes”
- Specific ability to perform an action (optionally, at a specific path) e.g. `storage.create:/home/joe`

**A single schema to rule them all:**
*Scitokens library will soon have support for WLCG JWT profile*
Rucio AuthN/Z with Tokens
Rucio AuthN/Z with OAuth/OIDC and JWTs

- **Rucio user**
  - “account” (CERN LDAP username) + “identity” (auth_type + ID)
  - only carefully ‘pre-provisioned’ users
  - Rucio daemon syncs accounts & identities (using IAM* SCIM client)

- **Rucio development branch is currently supporting**
  - ”Authorization Code Flow” for basic user authentication
  - “Token Exchange” to propagate permissions to downstream services (e.g. FTS)
  - “Refresh Token” to act on behalf of a user (for configurable time)
  - Supporting multiple Identity Providers (Escape IAM, XDC IAM, …)
  - Rucio WebUI login
  - 3 CLI login strategies (automatic, browser redirect & browser redirect + auth server polling)

*More IAM details in Thursday’s talk*
Practical Tests

• XDC IAM response time
  – Rucio user authentication currently @ 2Hz
  – XDC IAM test cluster average response time ~ 0.5 s

• Initiate data transfer:
  – authenticated Rucio user requests Rucio to make a transfer
  – Rucio exchanges the token for a new one with ‘fts’ in audience claim
  – FTS receives JWT in the header and initiates the transfer on dCache storage

• Deploying testbed on Rucio Escape Instance:
  – development release is being deployed on Rucio Escape Instance

This works thanks to DOMA-TPC work with HTTP-TPC – also being presented at CHEP*!

Jaroslav Guenther

* https://indico.cern.ch/event/773049/contributions/3474402/
Conclusions

• Common JWT Profile has reached v1.0
  – stable reference for developers and integrators

• WLCG IAM instance available today to start the integration work
Questions?