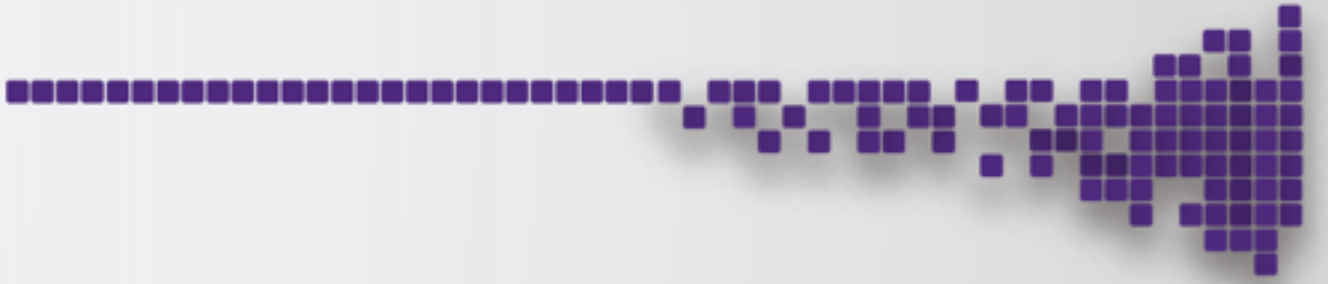
IAM and WLCG requirements

RIA-653549



Andrea Ceccanti (INFN)
andrea.ceccanti@cnaf.infn.it

WLCG AuthZ WG Meeting

Jan, 26th 2018

INDIGO-DataCloud is co-founded by the Horizon 2020Framework Programme

IAM and WLCG Requirements

INDIGO - DataCloud

- Authentication:
  - SAML (EduGAIN) ✓
  - X.509 certificates (IGTF) ✓
  - OpenID Connect (Google) ✓

- Above authN methods supported and demonstrated at the last meeting

IAM and WLCG Requirements

- Authentication (continued):
  - Combined assurance for identity and VO processes should meet equivalent assurance for X.509 IGTF
    - IDP meets security standard (SIRTFI), releases necessary attributes (R&S), etc.

- IAM can be configured to restrict AuthN only from IdPs that are SIRTFI and R&S compliant ✓

IAM and WLCG Requirements

- VO membership management:
  - VO has control on supported AuthN types ✓
  - VO knows the LoA of AuthN ✓
  - Users can link multiple accounts to VO account ✓
  - Periodic credential verification ?
  - Periodic AUP signing supported ✓
  - Integration with trusted identity vetting ✓
    - possible through provisioning APIs, or a registration plugin that implements dedicated changes for LHC VOs registration flow

IAM and WLCG Requirements

- Token provisioning workflow:
  - AuthZ attribute selection by the user must be possible
    - Possible via OAuth scopes ✓
  - Token renewal frequency and process should be manageable by the average user
    - Simple CLI and Web-based tools can be provided to simplify this
    - Ideally tokens could be completely hidden for the normal user

IAM and WLCG Requirements

- Service requirements:
  - Use existing standard approach
    - JWT, OAuth, OpenID connect ✓
  - Token requirements ✓
    - Should/must be possible to transparently provision user identity with the required token
    - Tokens must be supported on multiple platforms
    - Users must be able to allow services constrained delegation
    - Must be easily verifiable by the service (without returning to upstream provider)
    - Should include the minimal information to allow decentralized verification
    - Should be able to determine the token issuer

IAM and WLCG Requirements

- Required user attributes
  - Traceability information, i.e. Semi-Opaque ID that can be resolved to an identity for security purposes ✓
  - Authorisation attributes, i.e. Roles/Groups/Capabilities ✓
- Access right querying
  - AuthZ (groups and roles) attributes included in tokens/credentials where possible ✓
  - (provisioning) Protected API for queries ✓

IAM and WLCG Requirements

- Operational requirements
  - Suspension: must be able to do fine-grained emergency suspension
- IAM implements user suspension ✓
- IAM implements token revocation ✓
  - via REST APIs and IAM Web Dashboard
- Central banning list possible via Argus integration ✓
  - we developed an OIDC/OAuth plugin for Argus that allows to implement a site-central authorization service that understands OAuth/OIDC token claims
- Using short-lived tokens and OAuth token refresh support should make revocation and suspension a non-issue

Resources

- WLCG AuthZ WG reqs: https://docs.google.com/document/d/1hnsPWf9C7ODVXZ7JehsSEiEsQwf5UmqLfTwVDhuqHzk/edit
- IAM @ Github: https://github.com/indigo-iam/iam
- IAM docs @ Gitbook : https://iam-docs.gitbooks.io/iam-documentation/content/v/develop/
- INDIGO IAM test instance: https://iam-test.indigo-datacloud.eu

- Contacts:
  - andrea.ceccanti@cnaf.infn.it
  - indigo-aai.slack.com