WLCG Authorisation Requirements

This document includes requirements for authorisation for WLCG as agreed within the WLCG AuthZ Working Group. It aims to record specific needs in the context of token based authorisation. An initial set of Requirements was gathered in November 2017 and updated in July 2018.

Contributors (including vocal participation at pre-GDB): H. Short, A. Ceccanti, M. Sallé, N. Liampotis, B. Bockelman, R. Wartel, V. Brillault, M. Litmaath, D. Crooks, D. Kelsey, P. Millar, L. Cornwall

VO Membership Management

VO Membership Management Overview

- Membership requests must be possible with different user owned credential types (e.g. SAML, certificate, OIDC/OAuth2) as defined by the VO
- VOs should be able to know the level of assurance of the VO identity (identity & authentication method)
- Users must be able to link multiple accounts, to cope with e.g. home organisation changes
- Periodic membership renewal should be supported, as defined by policy
- Periodic credential verification should be supported, as defined by policy
- Periodic AUP Signing should be supported, as defined by policy, including:
    - user suspension upon failure to sign
    - controlled delegation and consent
- Integration of additional trusted data sources must be supported (e.g. Institute Affiliation Expiry from CERN HR DB)
- VO managers must be able to overwrite the information from integrated data sources
- For LHC VOs, the option to leverage CERN Infrastructure must be supported, such as
    - Integrated with trusted identity vetting process, e.g. CERN HR for WLCG
    - Membership expiration based on home institute affiliation
    - CERN SSO as a trusted IdP
- VO management should provide a process that, given a token or identifier, can resolve user attributes. This should be restricted to VO and Infrastructure level use.
- Hierarchical groups should be supported.

Required User Attributes (for the VO to operate)

- First Name & Last Name (or DisplayName)
- Email
- UniqueID of incoming credential (for each credential) (combination of Identity Provider and credential ID must be unique)
- Unique VO User ID (e.g. for LHC VOs: CERN ID for link to HR db) (scope is VO)
- VO name
- Authorization attributes (groups/roles/generics)

User Credential types (i.e. Authentication, not server-server auth tokens)

- Federated Credentials such as SAML/OIDC/OAuth2.0/Certificates
- Flexibility to enable a trusted IdP where appropriate, e.g. CERN SSO
- All credentials must be able to satisfy minimum requirements for Assurance, VOs should be able to select which specific Identity Providers they enable

Assurance profiles for home organisations/credential authorities

(*See WLCG Policy on Acceptable Authentication Assurance[1] and AARC Guidelines[2]*)

- Combined assurance of identity and VO processes must meet equivalent assurance for x509 IGTF
    - IdP meets security standards (e.g. via Sirtfi)
    - IdP releases necessary attributes (eg. R&S)
    - REFEDS assurance framework
- Step-up for critical services e.g. 2FA

Token provisioning workflow

- AuthZ attribute selection by the user must be possible (i.e. active role selection)
- Token renewal frequency and process should be manageable without additional training

Usability

- Documentation should be provided and maintained
- Bulk actions for VO Managers and Users should be enabled where appropriate

Service Providers[3]

Service Requirements Overview

- Aim at simplicity and ease of implementation
- Use existing, standard approaches
- Authorization schemas should be consistent between VOs
- All Tokens
    - Tokens must be supported on web and non-web
    - Must be able to determine the token issuer
- Identity/Access Tokens
    - Must be short lived
    - Should be possible to transparently provision the user with the required token
    - Users must be able to allow services constrained delegation
    - Should include sufficient information to allow decentralised verification
- Refresh Tokens
    - Must be revocable

---

[1] *https://documents.egi.eu/public/ShowDocument?docid=2930*

[2] AARC Guideline on expression of Assurance https://wiki.geant.org/download/attachments/92573909/AARC-G021-Exchange-of-specific-assurance-information-between-Infrastructures.pdf

[3] Otherwise known as Resource Providers or Clients

Required User Attributes (for the services to operate)

- Traceability information, i.e. potentially Semi-Opaque IDs that can be resolved to an identity for security purposes
- At least one of
    - Authorisation attributes, i.e. Roles/Groups
    - Capabilities
- Additional identity information should be supported, as required by policy

Non-web

- Users should not have to manage x509 certificates or other identity tokens themselves in addition to their login session
- AuthZ attributes should be consistent across WLCG web and non-web services

General

Operational Requirements

- Access token lifetime < operational response minimum time, as defined by policy and in line with standard recommendations
- Must support revocation of long lived tokens
- Suspension
    - Blocking of individual VO Users across all services/subset must be possible by a VO and/or the Infrastructure (i.e. Security Team) within a timeframe defined by policy
    - Sites/Services must be able to block (potentially opaque) VO Users locally, and inform relevant parties (e.g. Infrastructure security or VO management) as defined by policy

Change Management

- A smooth transition path should be defined, including backwards compatibility for a necessary timeframe

References:

[1] AARC Milestone MJRA1.1: Existing AAI and available technologies for federated access: https://aarc-project.eu/wp-content/uploads/2016/01/MJRA1.1-Existing-AAI-and-available-technologies.pdf

Appendix

Cataloguing Existing Support

The following entities support the following standards, as of mid 2018.

Entity	**Supported Standard**
EGI	All authentication standards above. Much x509. Idea is to move to OIDC and OAuth2 (e.g. Fed cloud)
OSG	OSG no longer performs end-user authentication (authn and VO membership mgmt left to VOs). We utilize federated IdPs where possible. Active work is in authorization: Heading towards OAuth2 based bearer tokens, JWT
IGTF	Mostly technology agnostic but supporting X509 and looking into federation for OIDC RPs and any OP-RP bridges
INDIGO	All authentication standards above:X.509, SAML, OIDC OAuth2 for authorization @ services
EUDAT	All authentication standards above. x509/SAML/OIDC, a mix. Like EGI
GEANT (eduTEAMS)	SAML & OIDC/OAuth2. Group membership via eduTEAMS. Bridging via SATOSA