AuthZ pre-GDB Requirements

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 VO
- VOs should be able to know the level of assurance of the VO identity (identity & authentication method)
- Users should be able to link multiple accounts, to cope with e.g. home organisation changes
- Periodic credential verification
- Periodic AUP Signing supported (including controlled delegation and consent) but not necessarily required
- For LHC VOs, we can leverage CERN infrastructure, such as
    - Integrated with trusted identity vetting process, e.g. CERN HR for WLCG
    - CERN SSO for a consistent identity mapping across Infrastructure

Required User Attributes (for the VO to operate)

- First Name & Last Name (or DisplayName)
- Email
- UniqueID of incoming credential (for each credential) (scope is global)
- 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/capabilities)

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

- Federated Credentials such as SAML/OIDC/OAuth/Certificates
- For LHC VOs, leverage CERN SSO
- *Doesn't matter what it is as long as it satisfies minimum LoA, VOs can choose*

Level of assurance for home organisations/credential authorities

(*See Policy on Acceptable Authentication Assurance https://documents.egi.eu/public/ShowDocument?docid=2930)*

- Combined assurance of identity and VO processes should 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 by the average user

Service Providers

Service Requirements Overview

- Aim at simplicity and ease of implementation
- Use existing, standard approaches
- Authorization schema should be consistent between VOs
- Tokens
    - Should/must be possible to transparently provision user 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 decentralised verification
    - Should be able to determine the token issuer
- *Long discussion whether services need to be able to authorise access based on LoA of identity - TBC*

Required User Attributes (for the services to operate)

- 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 (implemented by VO Management, consumed by services)

- (introspection) AuthZ (groups and roles) attributes included in tokens/credentials where possible
- (provisioning, out of scope for this group) Protected API for queries (debateable, preferably work with tokens directly)

Non-web

- Users should not have to request or manage x509 certificates or other identity tokens themselves in addition to their login session (required token should be provisioned transparently)
- AuthZ attributes should be consistent across all WLCG services (common to web and non-web services)

General

Operational Requirements

- Security must be able to do fine-grained emergency suspension
- VOs must be responsive enough to block users…
- Sites must be able to do/request emergency suspension
- Suspension

- Blocking of VO Users across all services/subset should be possible by a VO and the Infrastructure (i.e. security team) within an acceptable time frame
- Sites/Services must be able to block VO Users locally, in consultation with appropriate security and/or VO personnel
- Service token lifetime < operational response minimum time (e.g. if we want to block within an hour, they need to be less than that)
- Must support deprovisioning of long term tokens

Entity	**Supported Standard**
EGI	All authentication standards above. Much x509. Idea is to move to OIDC and OAuth2 (e.g. Fed cloud)
OSG	*unofficial* Trying to get out of end-user authentication business entirely (authn and VO membership mgmt left to VOs) Work is in authorization: Heading towards OAuth 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/OAuth. Group membership via eduTEAMS. Bridging via SATOSA

AARC document - 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