NRC·CNRC

Current Status of the Group Membership Service (GMS) Working Draft

Brian Major

October 2019

IVOA Groningen, NL

National Research Council Canada

Conseil national de recherches Canada

Canada

Overview of the GMS API

GMS API:

1. isMember? (return yes/no)
2. getMemberships (return set of 0-n groups)

RESTful:

1. GET /gms/search/{groupName}
2. GET /gms/search

Information privacy

Users' group membership information is likely considered private so this cannot be a publicly accessible API…

The membership information must be only seen by those allowed to see it:

- The actual user
- Possibly administrators of the group
- Possibly a privileged account, so long as it is not stored, interpreted, or used in a way that is outside the scope of use of the services which rely on it (and so on)

Who can call GMS? (1)

1. The actual user via delegated credentials

- Callers are identified (authenticated) by rules of SSO 2.0
- Users can find out their own memberships (not useful)
- Users can delegate credentials so that services can can determine group membership for authorization checks (very useful)

For this scenario, GMS relies on working CDP implementations

Credential Delegation Protocol (CDP) version 1.0:

- X.509 certificates

Who can call GMS? (2)

2. A privileged account?
   - SSO 2.0 can be used to identify the calling (privileged) user, but...
   - The subject of the membership check must be identified by another means, for example, an optional parameter, relaying:

```
x509:c=ca,o=grid,ou=nrc-cnrc.gc.ca,cn=brian major

userid:bmajor
```

   - This would likely require a new user identification standard
   - Perhaps needed in other contexts:
     - CDP doesn't explain how to get a user's delegated credentials
     - The idea of an 'owner' of resources is common (eg UWS)
     - Authentication support: a 'whoami' service

GMS: The way forward

If we decide we need privileged account access to GMS, then we need:

- **A user (and group?) data model**
- **Serialized format of a user**

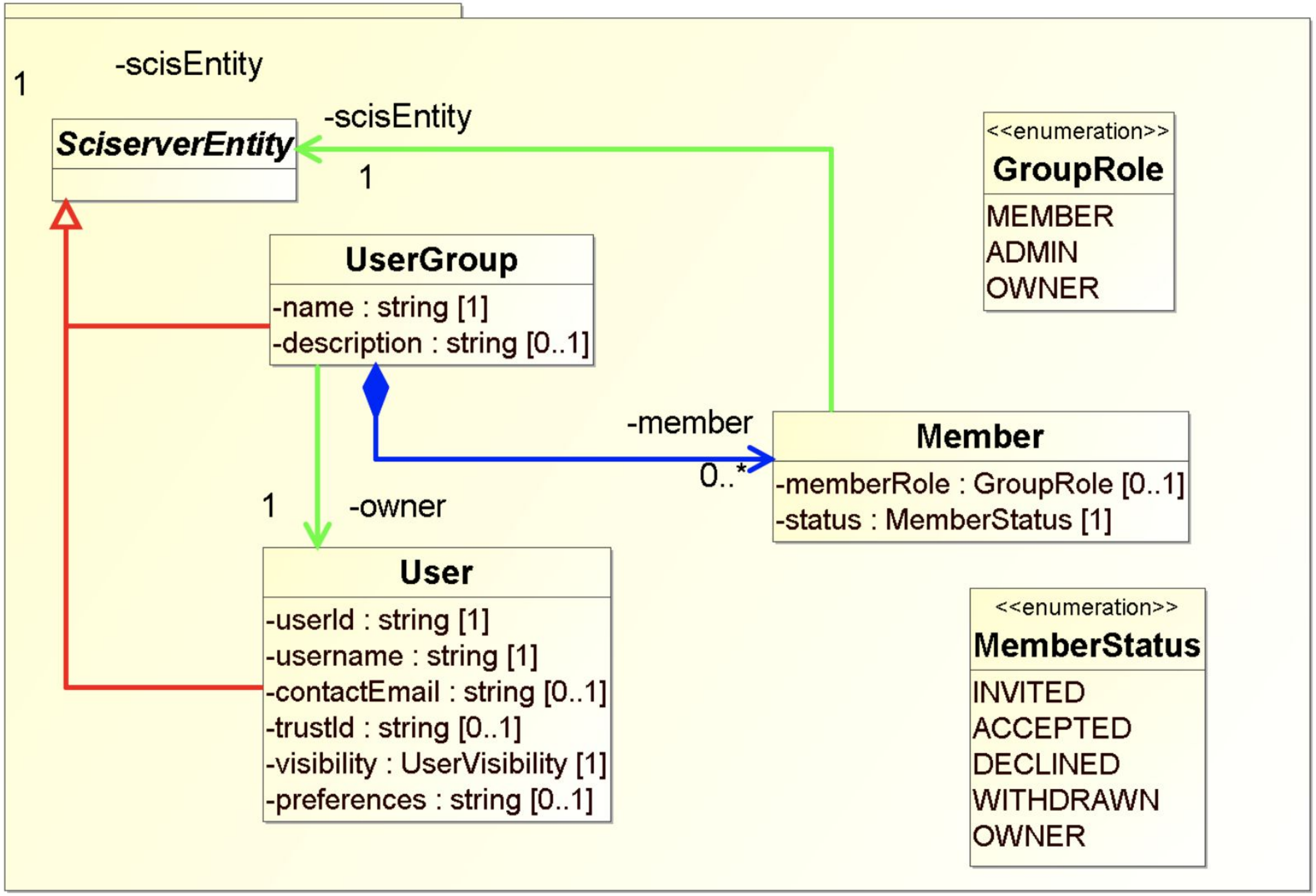
Non privileged GMS access (recommended) is based on CDP. CDP only supports X.509 right now.

- **Add OAuth2 to CDP standard?**

Related items from other auth contexts:

- If we need a **login/token/whoami service**, it needs a the user (and group?) model

User and Group data model?



SciServer Sharing Model
Gerard Lemson, Victoria Interop 2018