

Group Membership Service 1.0

Request for Comments

Brian Major et al.
IVOA Virtual Interop, November 2021



Agenda

1. Overview of Group Membership Service 1.0
2. Go through open RFC issues

GMS Overview

GMS = **G**roup **M**embership **S**ervice

What it does: An API that answers questions about your group memberships.

Current state: First version (1.0) in RFC: <https://ivoa.net/documents/GMS/index.html>

RFC Page: <https://wiki.ivoa.net/twiki/bin/view/IVOA/GMSRFC>

Issues or Pull Requests here: <https://github.com/ivoa-std/GMS>

GMS Overview: API

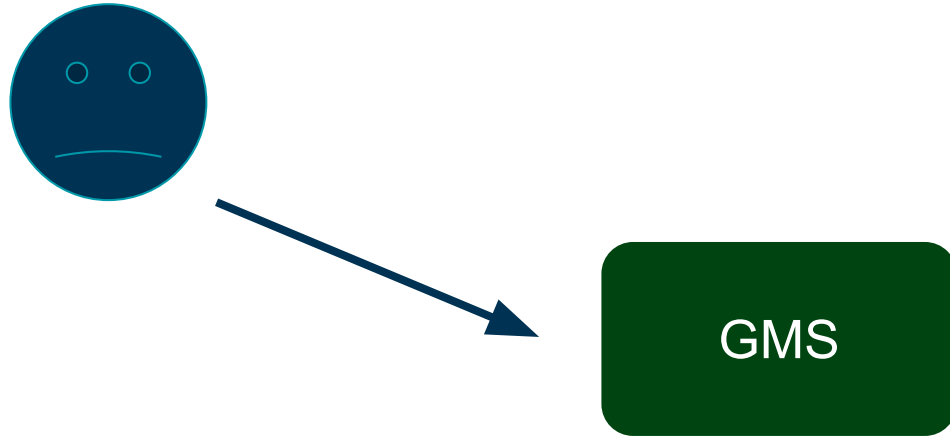
What it does: An **API** that answers questions about ***your*** group memberships.

1. Am I a member of group A?
2. Am I a member of group A or group B (or both)?
3. In what groups am I a member?

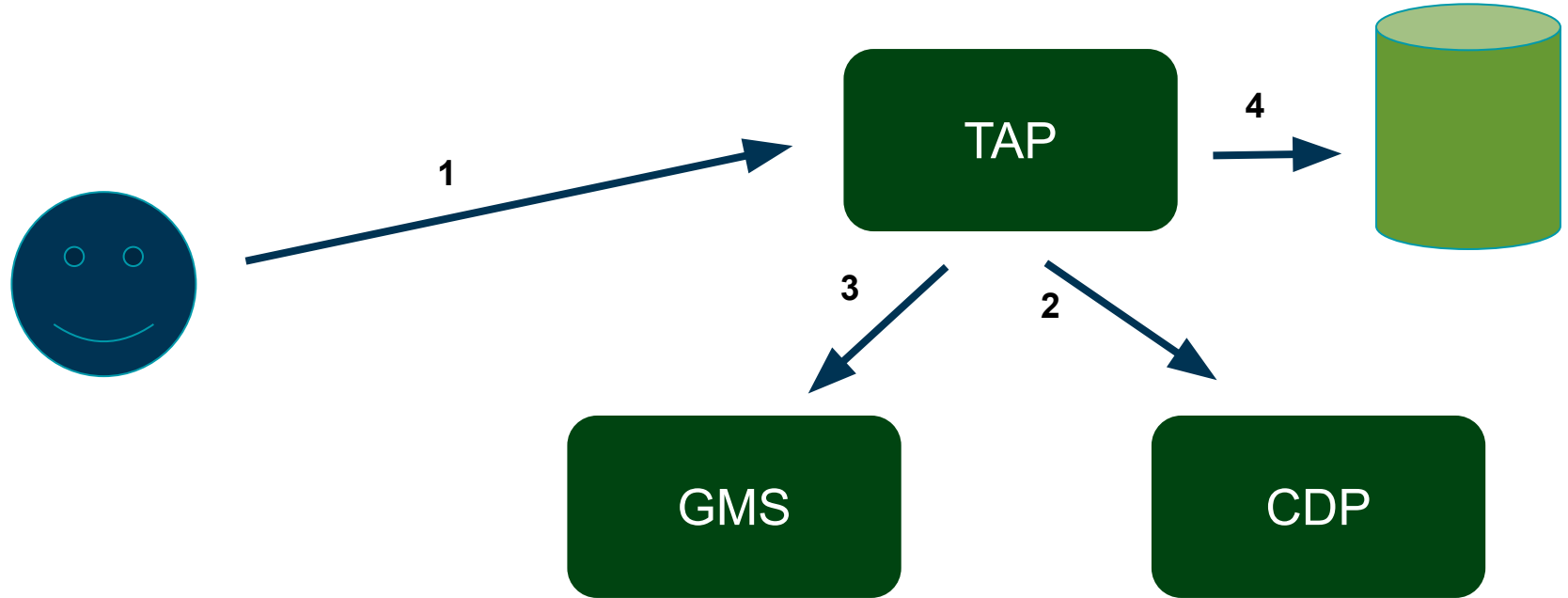
No anonymous access (all calls must be authenticated)

Information Privacy: Only you should see your group memberships

GMS Supports Authorization in Other Services



GMS Supports Authorization in Other Services



Example: TAP Query

TAP Query to table with readGroup column.

Only members of the groups in that column can read the rows.

When a user makes a query to the table via TAP:

1. TAP calls GMS to get **all** the calling user's groups
2. GMS returns:
 - a. `ivo://cadc.nrc.ca/gms#groupA`
 - b. `ivo://cadc.nrc.ca/gms#groupB`
3. TAP appends to the query:

Observation readGroup

```
WHERE metaReadGroup IN ('ivo://cadc.nrc.ca/gms#groupA', 'ivo://cadc.nrc.ca/gms#groupA')
```

Group Identifier gives Interoperability

Groups authorized to use the Science Platform:

`ivo://oats.inaf.it/gms#platform-users-italy`

`ivo://cadc.nrc.ca/gms#platform-users-canada`



Other uses

- Offering OpenID Connect and/or GMS as a service to external partners is powerful
- Same group can be set on multiple services, thus enabling a project or collaboration
 - Membership changes reflected immediately across services
 - Example: PI data in archive + VOSpace + Science Platform
- GMS use not restricted to IVOA ecosystem
 - Can be used in custom services or pipelines
- Extend GMS API with User-controlled group management
 - Users create their own groups, become group owner
 - Owners add group administrators
 - Owners and administrators manage group membership

Registry Entry (snippets)

```
<header>
  <identifier>ivo://cadc.nrc.ca/gms</identifier>
</header>

<capability standardID="ivo://ivoa.net/std/GMS#search-1.0">
  <interface xsi:type="vs:ParamHTTP" role="std" version="1.0">
    <accessURL use="base">https://ws-cadc.canfar.net/ac/search</accessURL>
    <securityMethod standardID="ivo://ivoa.net/sso# cookie" />
    <securityMethod standardID="ivo://ivoa.net/sso# tls-with-certificate" />
    <securityMethod standardID="ivo://ivoa.net/sso# token" />
  </interface>
</capability>
```

RFC - Outstanding Issues

<https://wiki.ivoa.net/twiki/bin/view/IVOA/GMSRFC>

<https://github.com/ivoa-std/GMS>

- ◉ Add text about GMS services may require high availability**
#13 opened 41 minutes ago by brianmajor
- ◉ Group Identifier Reuse**
#12 opened 44 minutes ago by brianmajor
- ◉ Group name character restrictions**
#11 opened 1 hour ago by brianmajor
- ◉ Register INAF GMS service**
#10 opened 1 hour ago by brianmajor
- ◉ Add comparisons section to other related initiatives**
#8 opened 11 days ago by brianmajor
- ◉ Versioning**
#6 opened on Sep 15 by msdemlei

THANK YOU

Brian Major • CADC • brian.major@nrc-cnrc.gc.ca

