Group Membership Based Authorization to CADC Resources

Adrian Damian, Patrick Dowler, Séverin Gaudet, and Norman Hill
Herzberg Institute of Astrophysics, Victoria, British Columbia, Canada

Adrian.Damian@nrc-cnrc.gc.ca

ABSTRACT

The Group Membership Service (GMS), implemented at the Canadian Astronomy Data Centre (CADC), is a prototype of what could eventually be an IVOA standard for a distributed and interoperable group membership protocol. Group membership is the core authorization concept that enables teamwork and collaboration amongst astronomers accessing distributed resources and services. The service integrates and complements other access control related IVOA standards such as single-sign-on (SSO) using X.509 proxy certificates and the Credential Delegation Protocol (CDP).

– Groups are identified with unique URIs
  Ex: `ivo://cadc.nrc.ca/GEMINI-PI-GS-2011-Q-11`

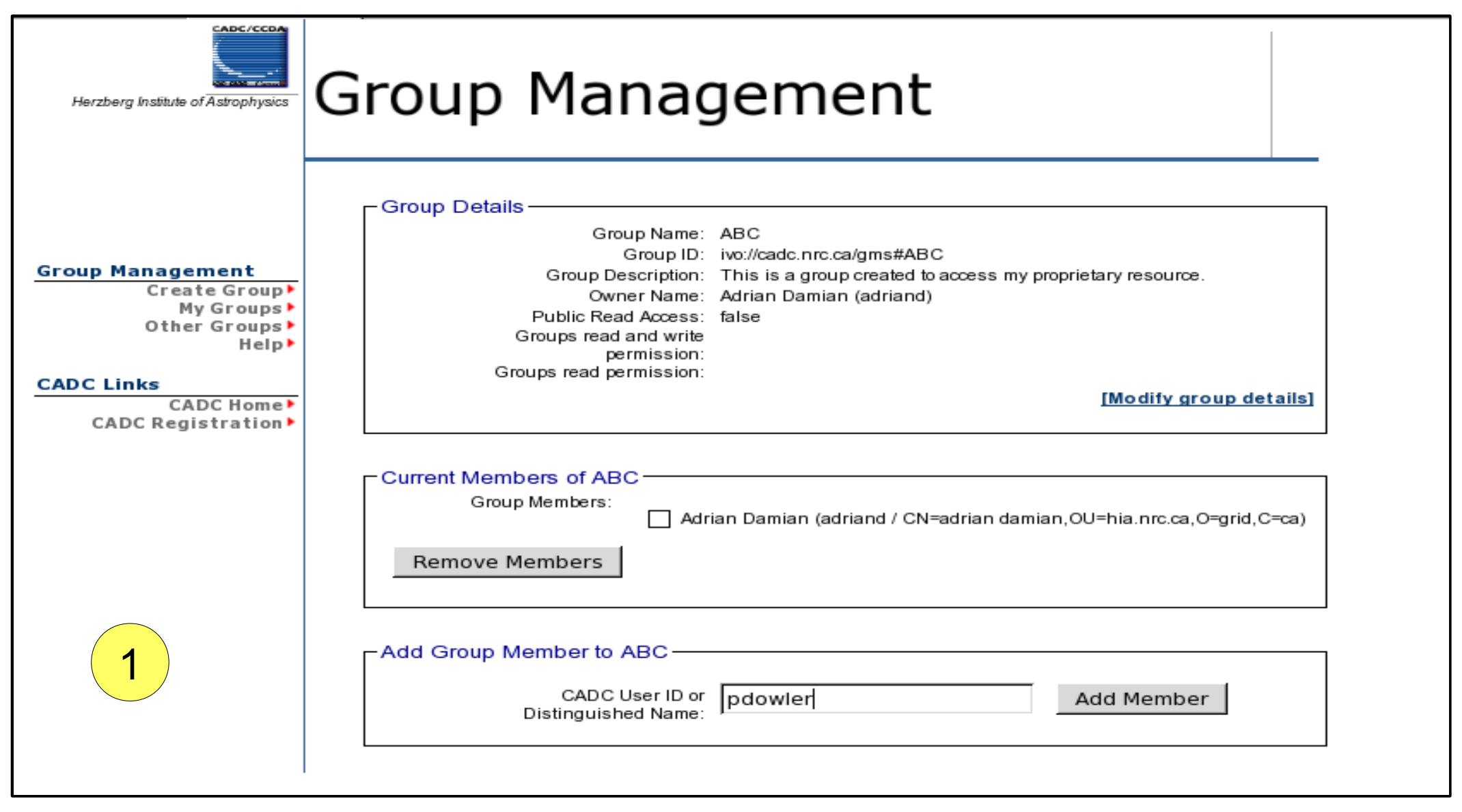
– Group Members identified with their X.509 Distinguished Name
  Ex: `CN=Adrian Damian,OU=hia.nrc.ca,O=Grid,C=CA`

GMS hosts are interoperable and independent of each other. Each service maintains its own group membership list.

GMS at the CADC

At the CADC, there are currently 15,000 groups with more than 17,000 members. Resources that use GMS for authorizing:

- **Proprietary archives.** PI and Program Access groups for Gemini Science Archive (GSA), Canada-France-Hawaii Telescope (CFHT), James Clerk Maxwell Telescope (JCMT) and Dominion Astrophysical Observatory Science Archive (DAOSA),
- **VOSpace.** User control access to their directories and files,
- **CAOM TAP Service.** Access to metadata in the Common Archive Observation Model TAP Service,
- **Restricted access Web sites.** Restricted areas include logging pages, telescope data specialists pages, GSA librarian pages, etc.,
- **Annotations Web Service.** Service that allows users to annotate resources.
- **GMS.** Authorization for accessing and/or updating group information uses GMS.



Herzberg Institute of Astrophysics

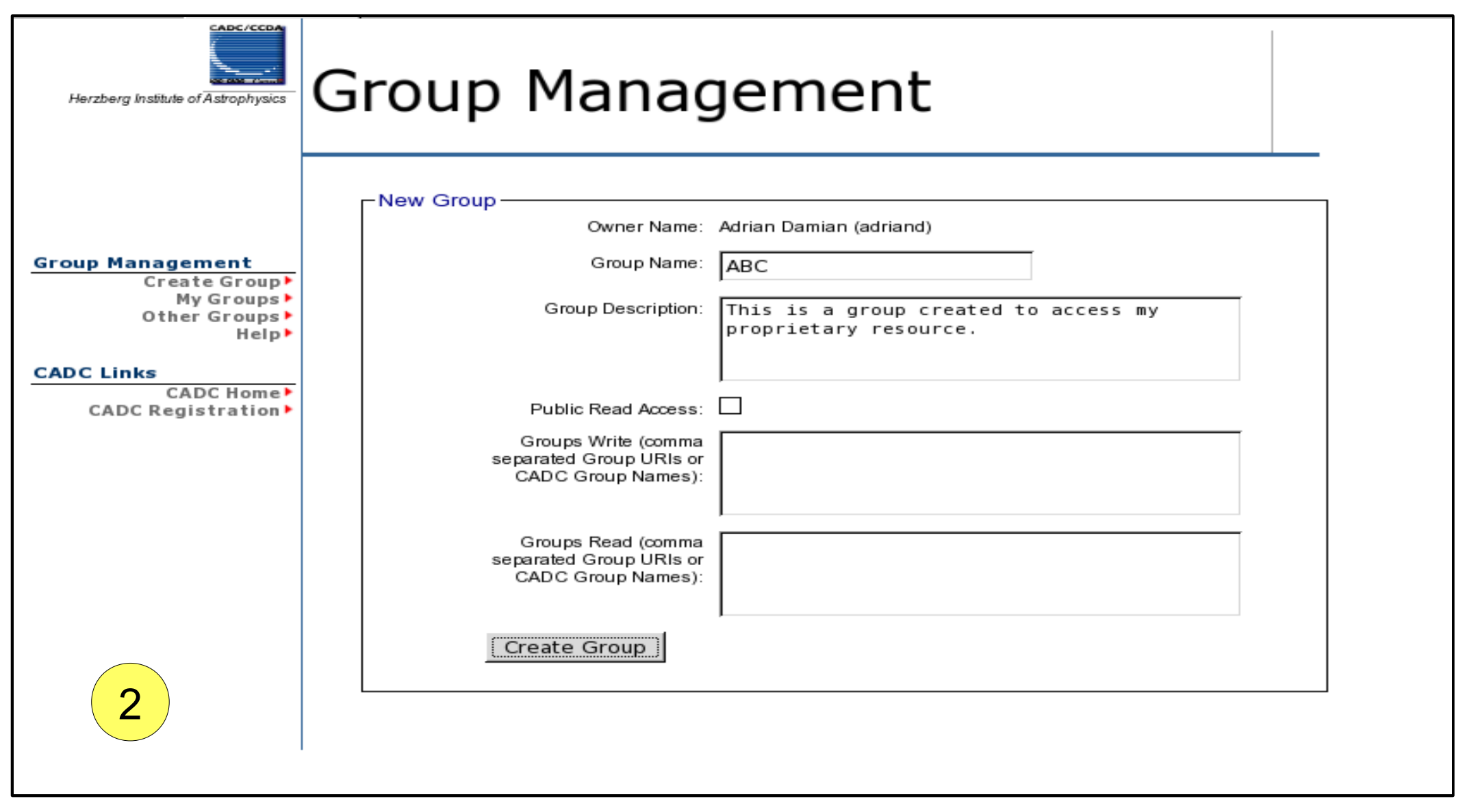
Group Management

Group Details
Group Name: ABC
Group ID: ivo://cadc.nrc.ca/gms#ABC
Group Description: This is a group created to access my proprietary resource.
Owner Name: Adrian Damian (adriand)
Public Read Access: false
Groups read and write permission:
Groups read permission:
[Modify group details]

Current Members of ABC
Group Members: □ Adrian Damian (adriand / CN=adrian damian,OU=hia.nrc.ca,O=grid,C=ca)
Remove Members

Add Group Member to ABC
CADC User ID or Distinguished Name: pdowler
Add Member

1

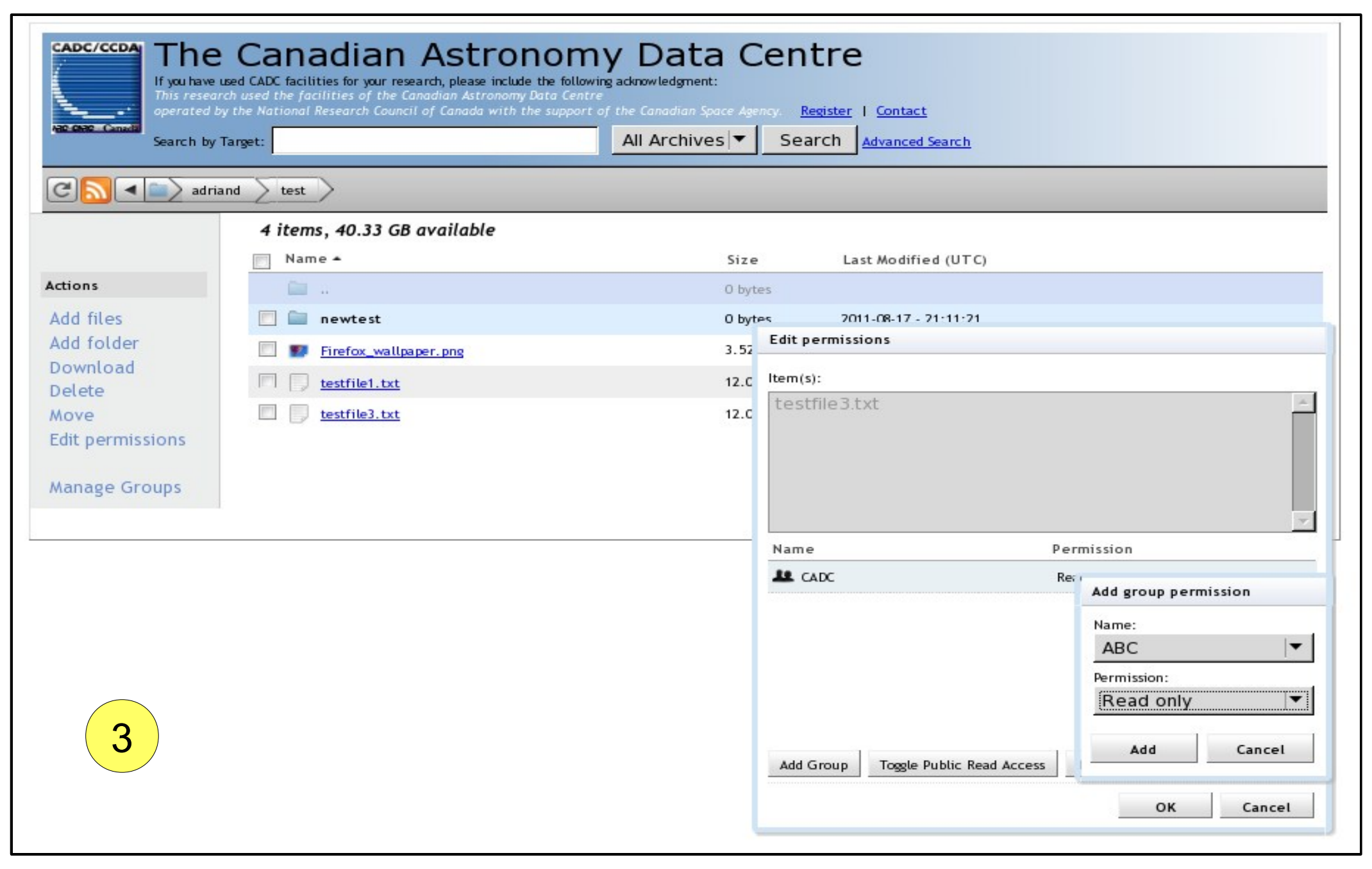


Herzberg Institute of Astrophysics

Group Management

New Group
Owner Name: Adrian Damian (adriand)
Group Name: ABC
Group Description: This is a group created to access my proprietary resource.
Public Read Access: □
Groups Write (comma separated Group URIs or CADC Group Names):
Groups Read (comma separated Group URIs or CADC Group Names):
Create Group

2



The Canadian Astronomy Data Centre

If you have used CADC facilities for your research, please include the following acknowledgment:
This research used the facilities of the Canadian Astronomy Data Centre operated by the National Research Council of Canada with the support of the Canadian Space Agency. Register | Contact

Search by Target: All Archives Search Advanced Search

adriand test

4 items, 40.33 GB available

Name	Size	Last Modified (UTC)
..	0 bytes	
newtest	0 bytes	2011-08-17 - 21:11:21
Firefox_wallpaper.png	3.52	
testfile1.txt	12.0	
testfile3.txt	12.0	

Edit permissions
Item(s): testfile3.txt

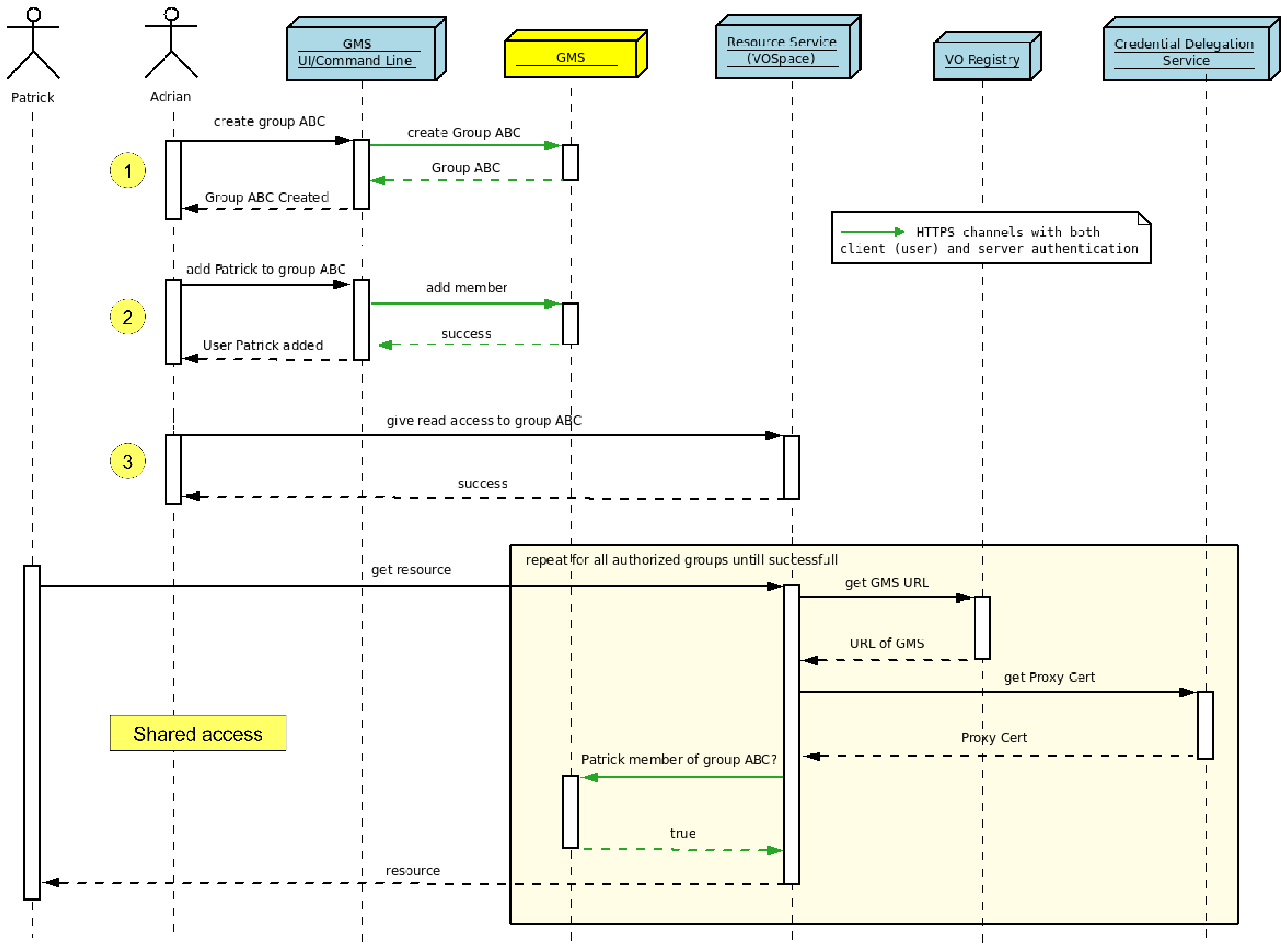
Name	Permission
CADC	Re

Add Group | Toggle Public Read Access
OK | Cancel

Add group permission
Name: ABC
Permission: Read only
Add | Cancel

3

1 2 3 Steps to Share Private Distributed Resources Using GMS



Advantages

- **Simplicity.** GMS is a simple service that captures group membership information only. This allows resource services to independently define their own authorization schemes.
- **Decentralized approach.** Clients will use IVO Registries to dynamically discover available GMS hosts.
- **Interoperability.** Users will be able to create groups in any registered IVOA GMS provider and use them in the authorization systems of any other resource providers.
- **Scalability.** Because of its simplicity, the implementation will scale well with the number of groups and users.
- **Group properties.** This feature that allows clients to described categories of groups and search for groups with certain properties.

Challenges and Future Work

- **Trust.** Because the GMS is part of their authentication mechanism, resource owners need to trust in the GMS hosts. Good security measures at the GMS host, such as communication over HTTPS channels and proper user authorization, are essential.
- **Availability.** Without access to the GMS, resource authorization will fail. Consider running mirror GMS for backup.
- **Deleted Groups.** Deleting groups might leave resources inaccessible (authorization fails). To assist resource services with the clean-up process, GMS hosts could return the status of a group ID, for example: not in use, in use or deleted.
- **openID support.** Use openID as an alternative to X.509 DN for identifying the user globally.

http://www.cadc-ccda.hia-iha.nrc-cnrc.gc.ca/gms/

National Research Council Canada
Conseil national de recherches Canada