Group Membership Service Updates

IVOA Interop -- Paris 2019

Brian Major

NRC·CNRC

Overview

A web service with a RESTful API that allows for the determination of whether a user is a member of a group.

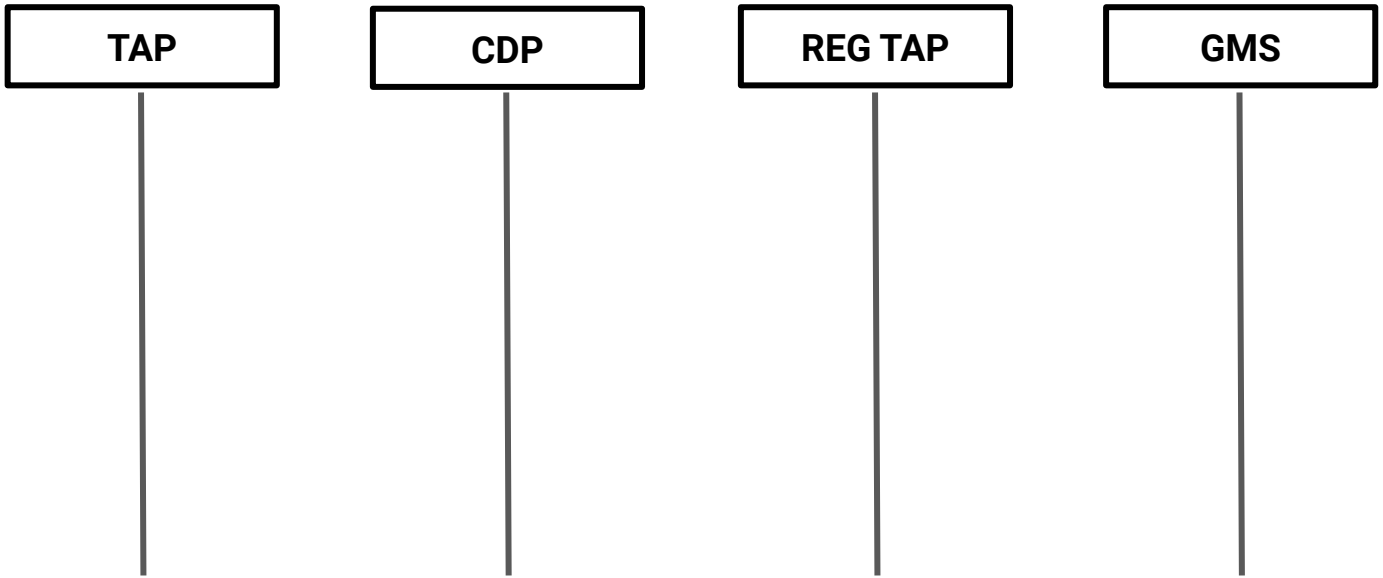
The answer to this ‘isMember’ question can be use to allow (or deny) the user access to a resource.

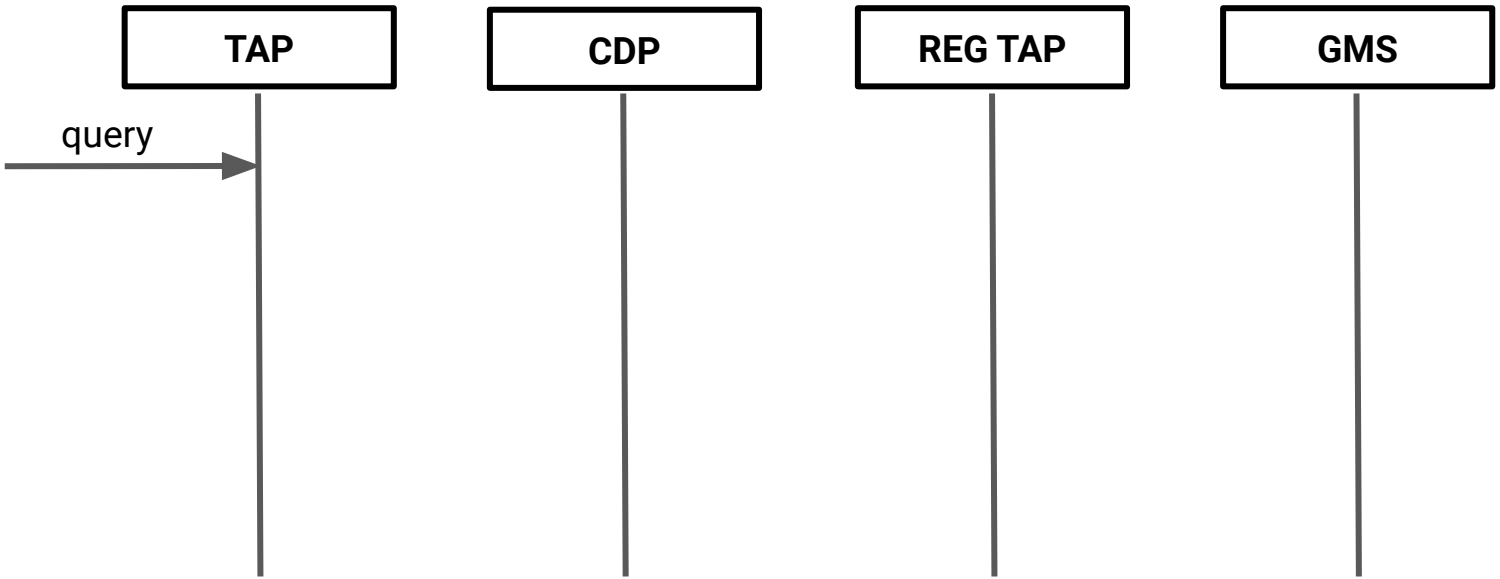
This is the authorization decision.

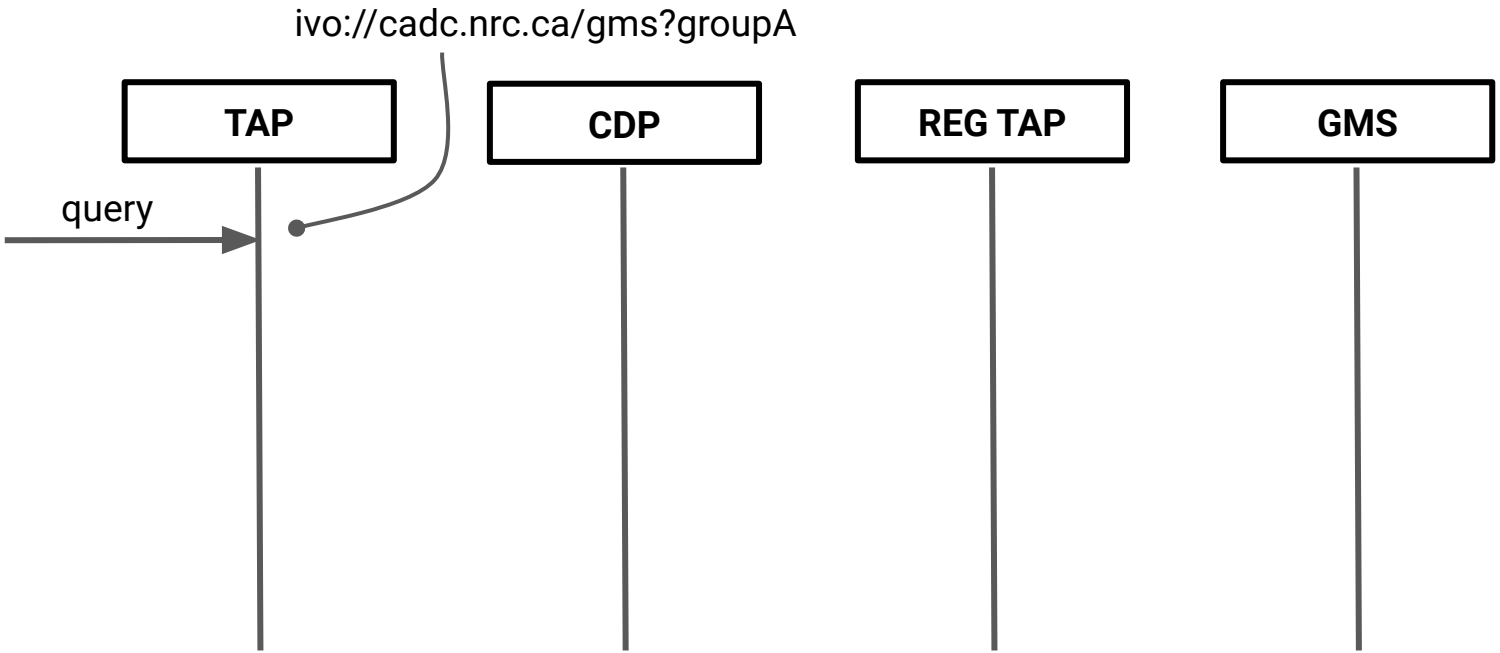
The owner(s) of the resource may, at any time, change the group(s) and/or the group memberships of the groups that is protecting the resource.

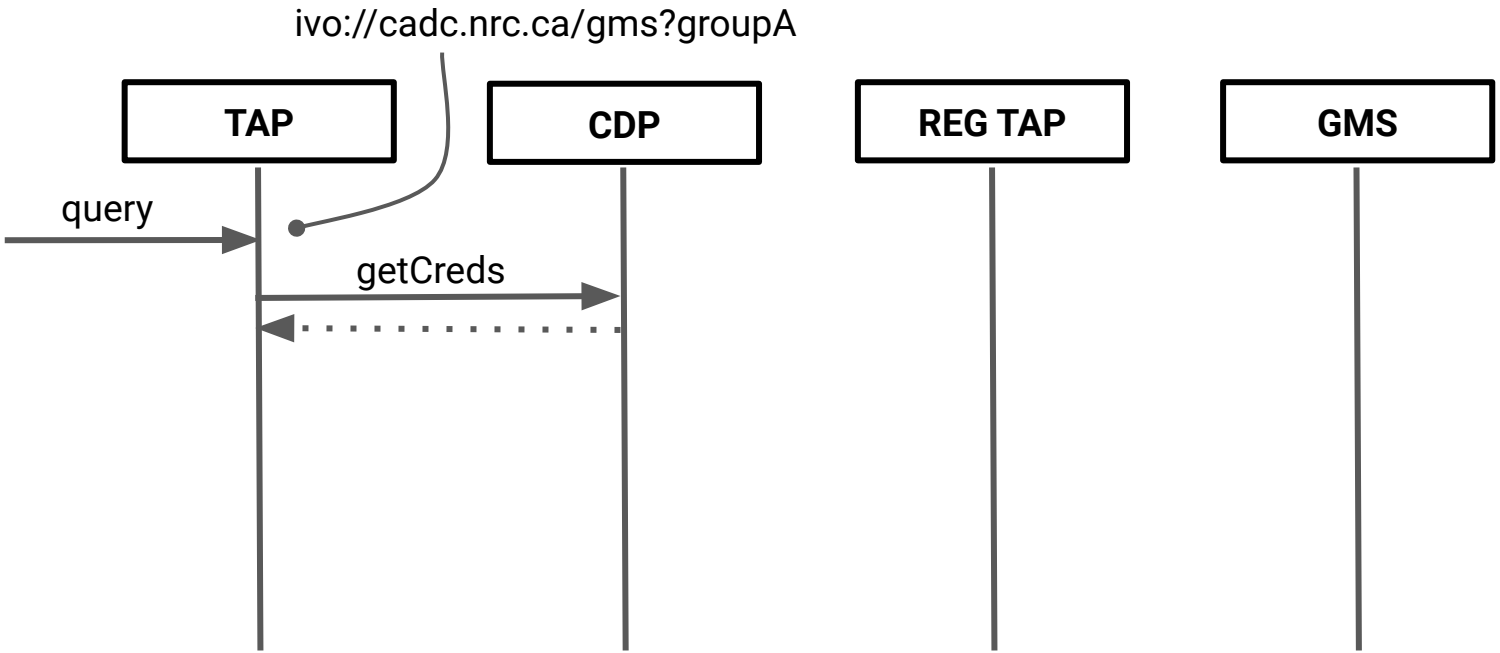
This is the granting and revoking of access.

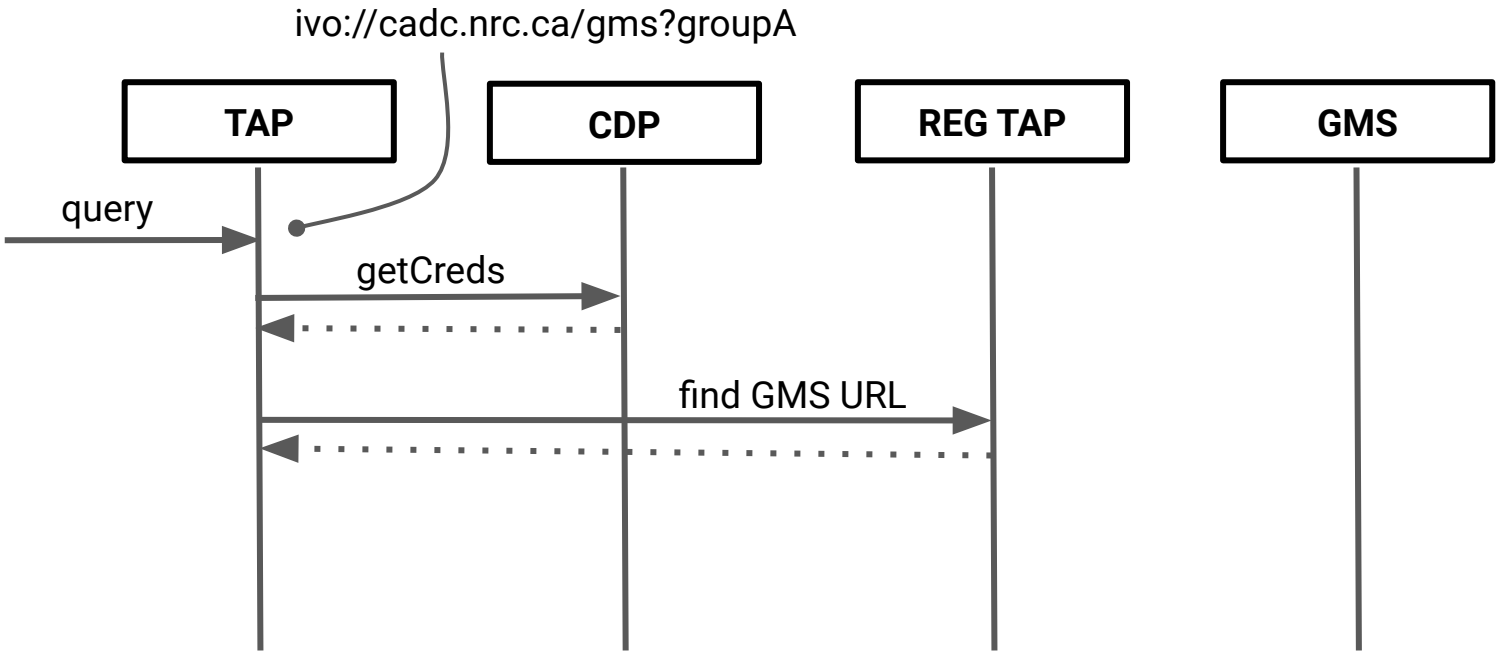
NRC·CNRC

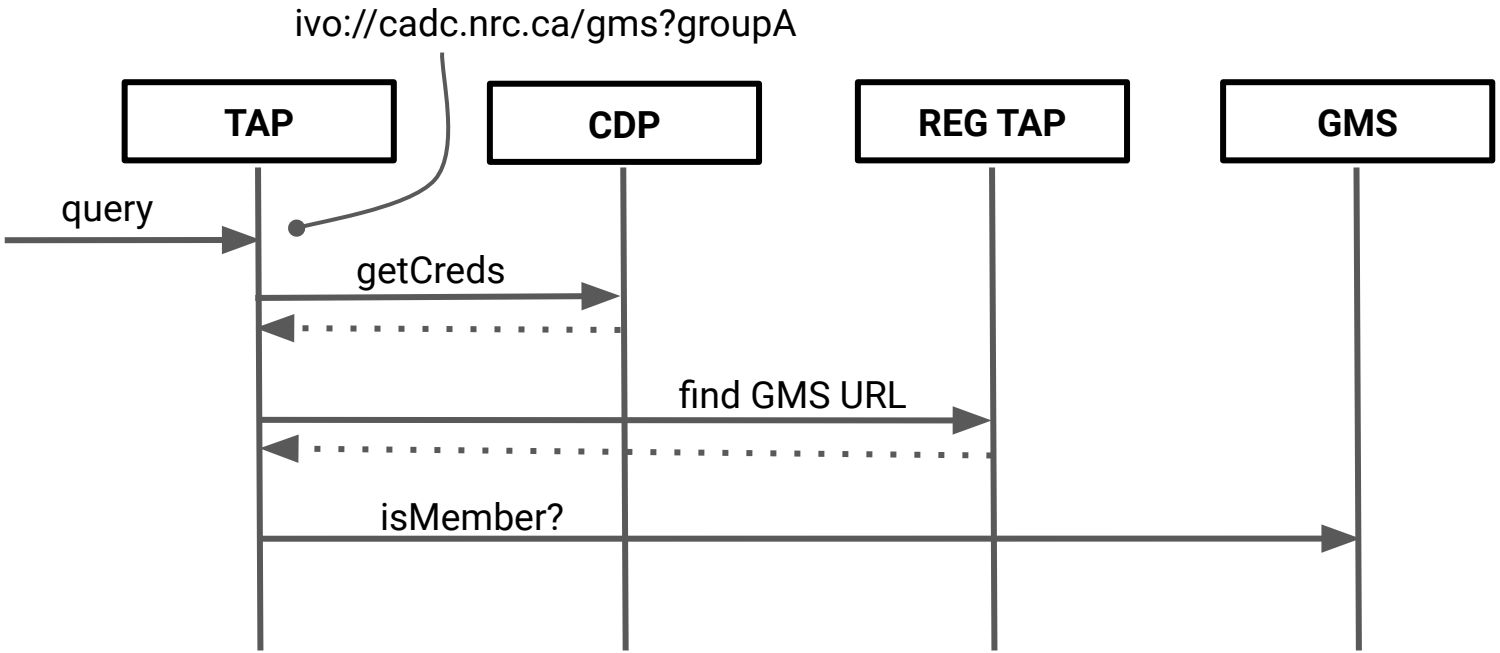

TAP
CDP
REG TAP
GMS

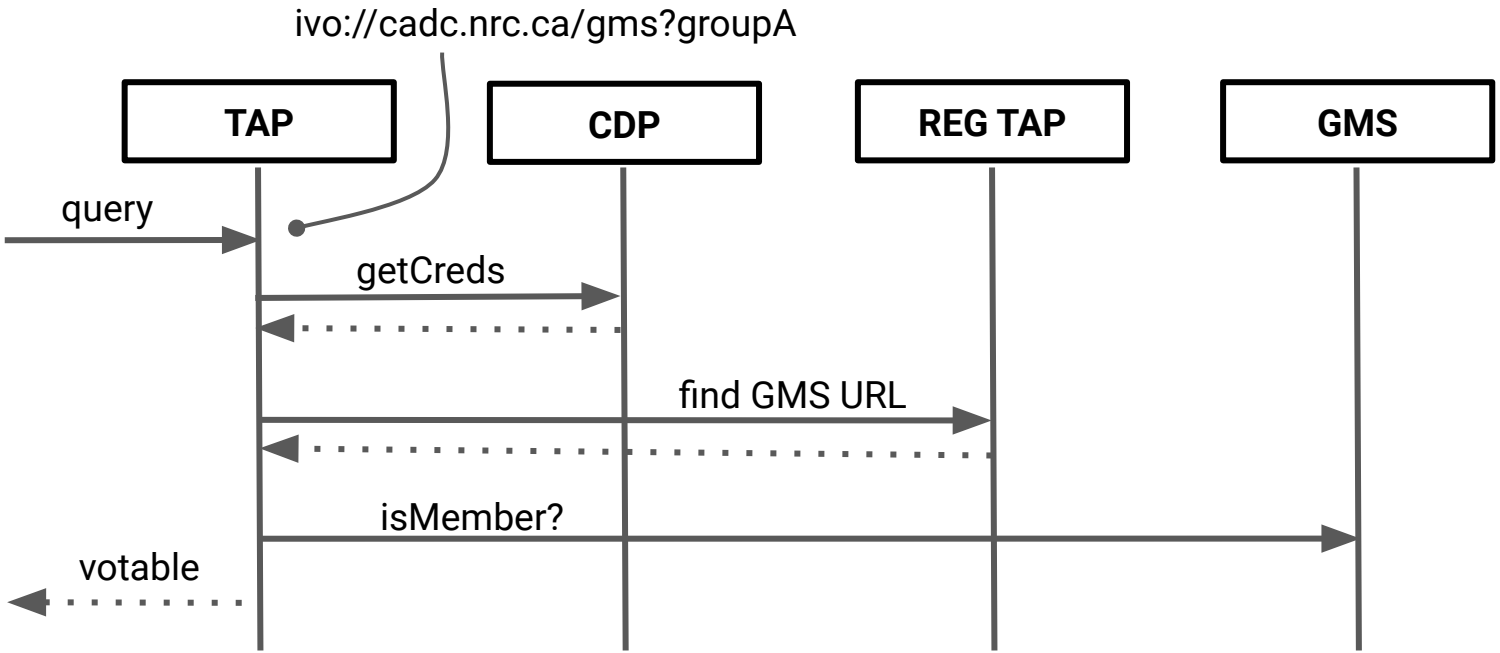

TAP
CDP
REG TAP
GMS
query

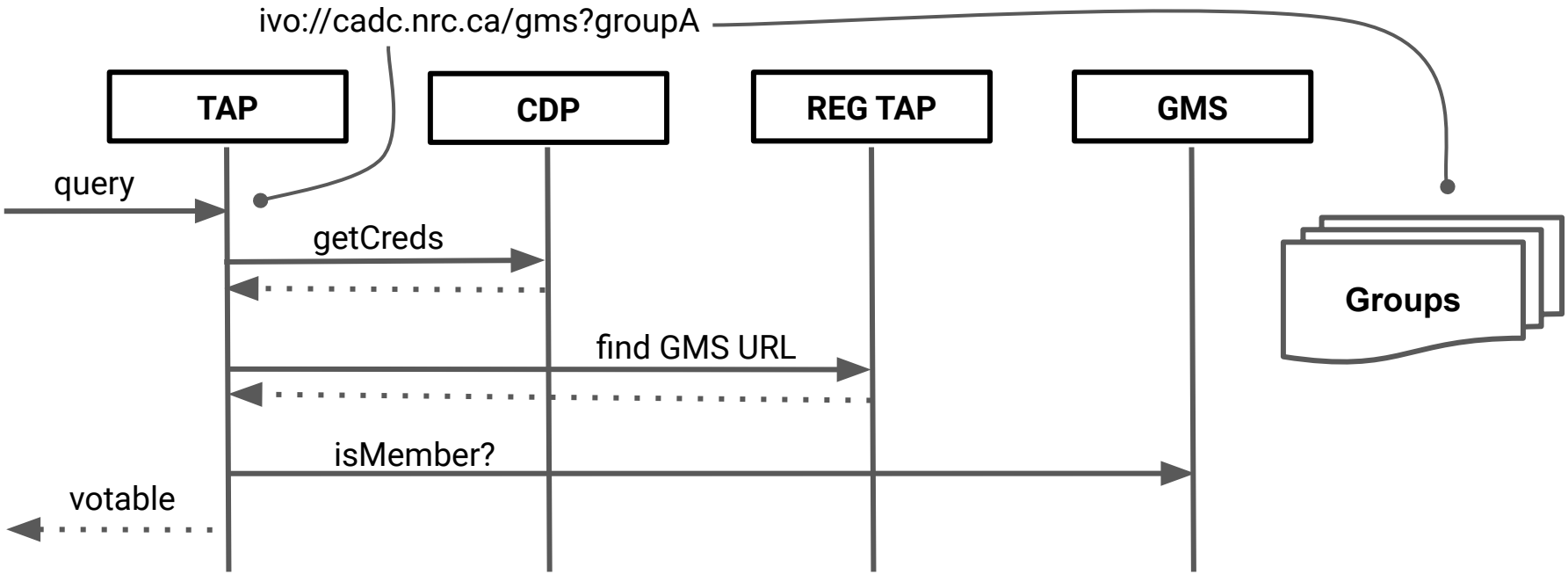

ivo://cadc.nrc.ca/gms?groupA
TAP
CDP
REG TAP
GMS
query

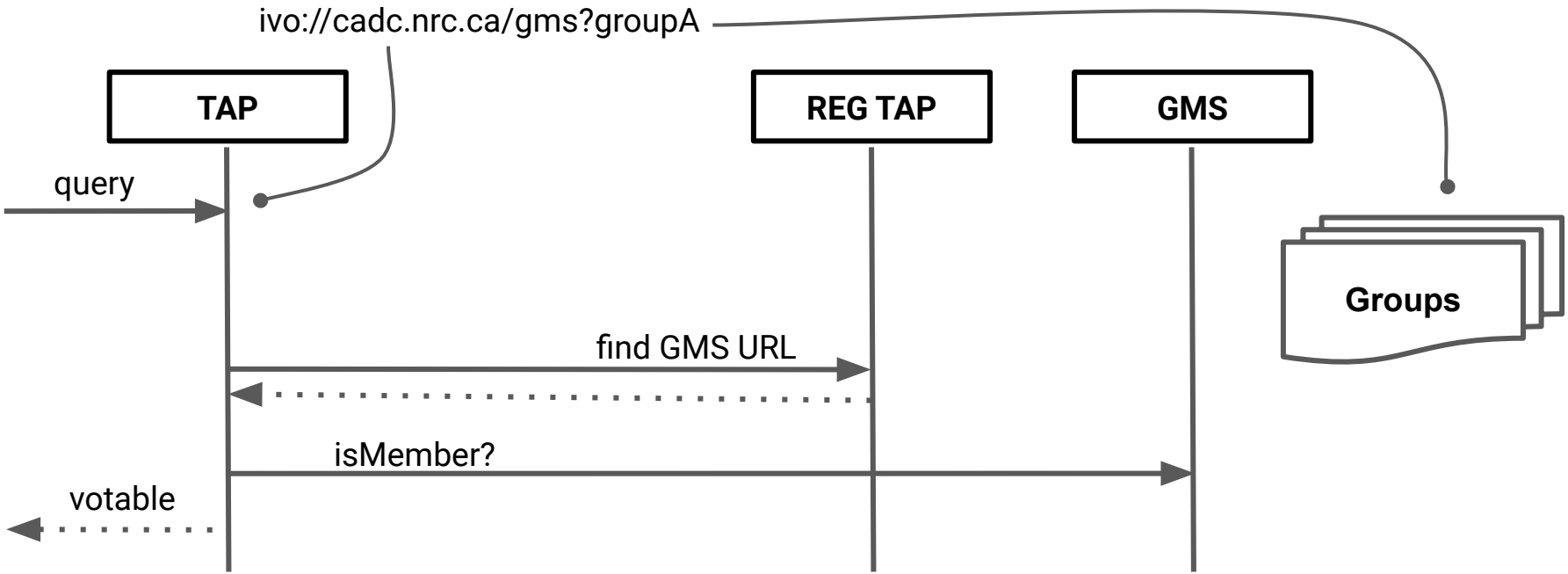

ivo://cadc.nrc.ca/gms?groupA
TAP
CDP
REG TAP
GMS
query
getCreds

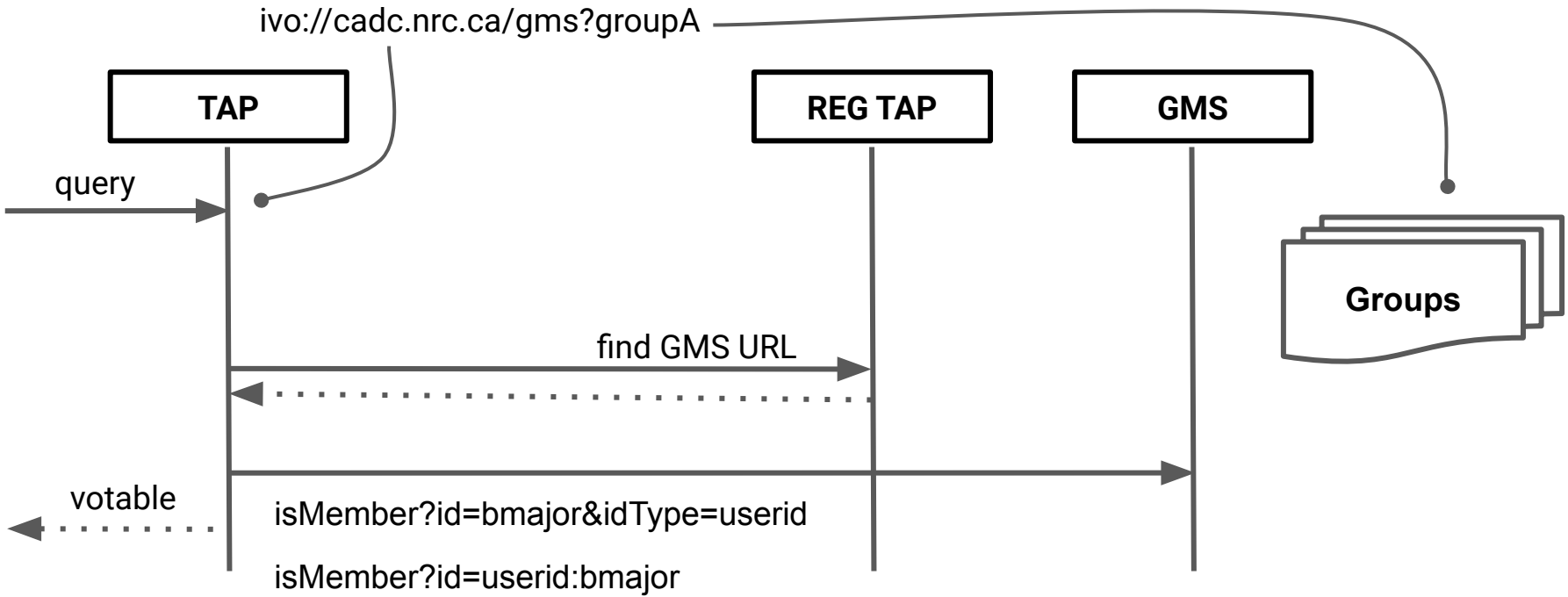

ivo://cadc.nrc.ca/gms?groupA
TAP
CDP
REG TAP
GMS
query
getCreds
find GMS URL

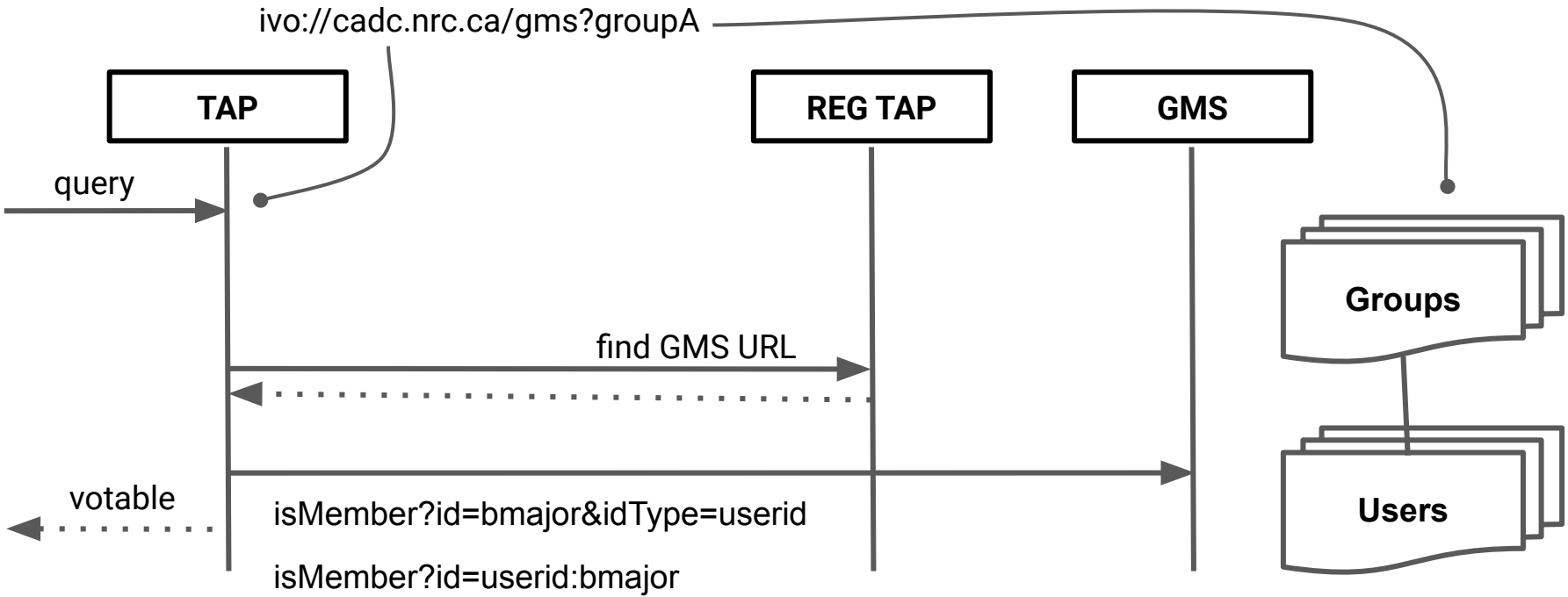

ivo://cadc.nrc.ca/gms?groupA
TAP
CDP
REG TAP
GMS
query
getCreds
find GMS URL
isMember?


ivo://cadc.nrc.ca/gms?groupA
TAP
CDP
REG TAP
GMS
query
getCreds
find GMS URL
isMember?
votable

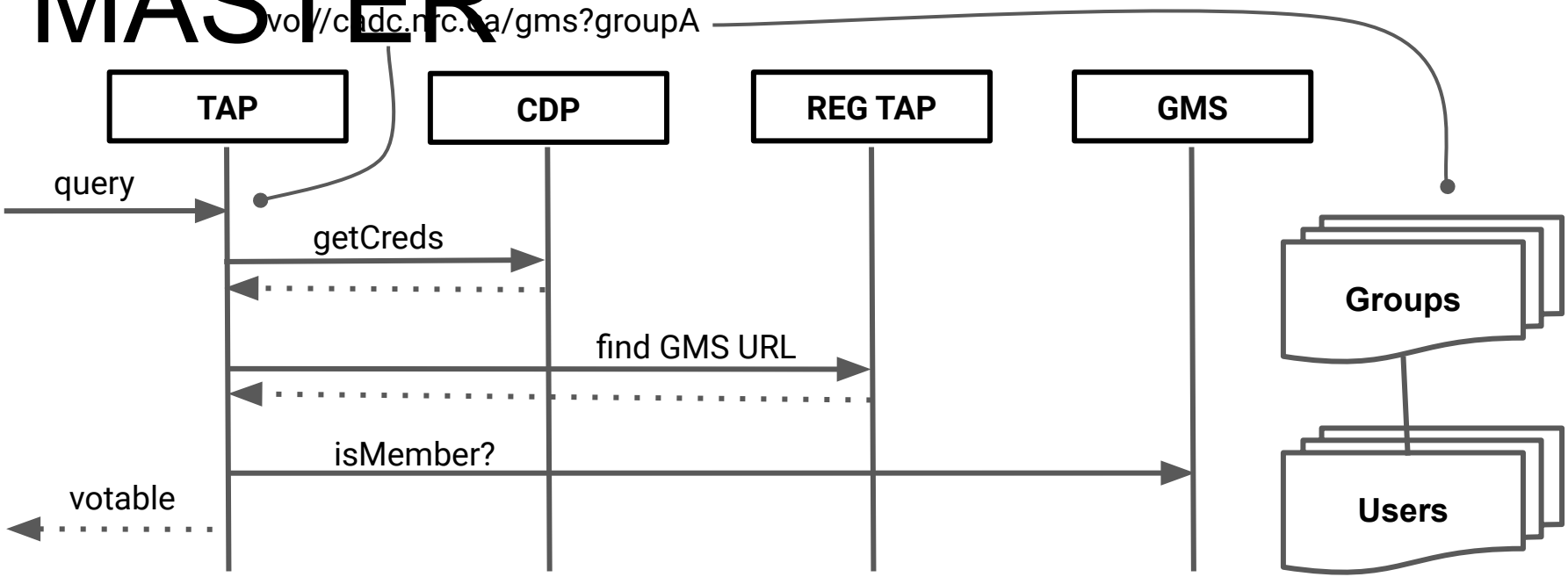

ivo://cadc.nrc.ca/gms?groupA
TAP
CDP
REG TAP
GMS
query
getCreds
find GMS URL
isMember?
votable
Groups


ivo://cadc.nrc.ca/gms?groupA
TAP
REG TAP
GMS
query
Groups
find GMS URL
isMember?
votable


ivo://cadc.nrc.ca/gms?groupA
TAP
REG TAP
GMS
query
Groups
find GMS URL
votable
isMember?id=bmajor&idType=userid
isMember?id=userid:bmajor


ivo://cadc.nrc.ca/gms?groupA
TAP
REG TAP
GMS
query
find GMS URL
votable
isMember?id=bmajor&idType=userid
isMember?id=userid:bmajor
Groups
Users

MASTER



isMember?id=bmajor&idType=userid

isMember?id=userid:bmajor

User identities

```
idType=userid&id=majorb
idType=x509&id=c=ca,o=grid,ou=nrc-cnrc.gc.ca,cn=brian major
idType=oauth2&id=9J0AOIJFA79HP4H89HJLKAAP8H4

id=userid:majorb
id=x509:d=c=ca,o=grid,ou=nrc-cnrc.gc.ca,cn=brian major
id=oauth2:9J0AOIJFA79HP4H89HJLKAAP8H4

id=ivo:userid:majorb
id=ivo:x509:d=c=ca,o=grid,ou=nrc-cnrc.gc.ca,cn=brian major
id=ivo:oauth2:9J0AOIJFA79HP4H89HJLKAAP8H4
```

userid : derived from cookie, basic auth, or token
x509 : derived from x509 client certificate
oauth2 : derived from identity provider

User Identification and Scope

1. How should users be identified in the GMS REST API? Should they relate to the auth methods described in SSO?

2. What is the extent or realm of a user identifier?

    a. With the existence of identity providers, is it enough to keep their scope local to the group membership service?

    b. Can groups reference remote users?

    c. What if the internal representation of groups referenced remote groups? (transitive memberships)