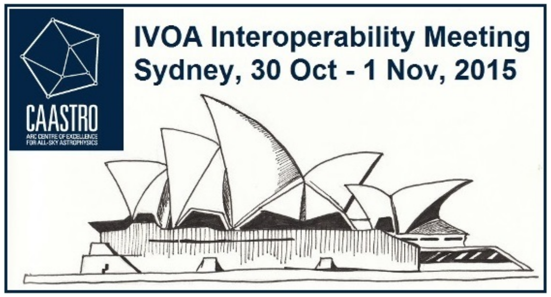

IVOA Interoperability Meeting
Sydney, 30 Oct - 1 Nov, 2015
CAASTRO
ARC CENTRE OF EXCELLENCE FOR ALL-SKY ASTROPHYSICS

Interoperable Authorization: A Real Life Use Case

IVOA Interop, Sydney AU

Brian Major

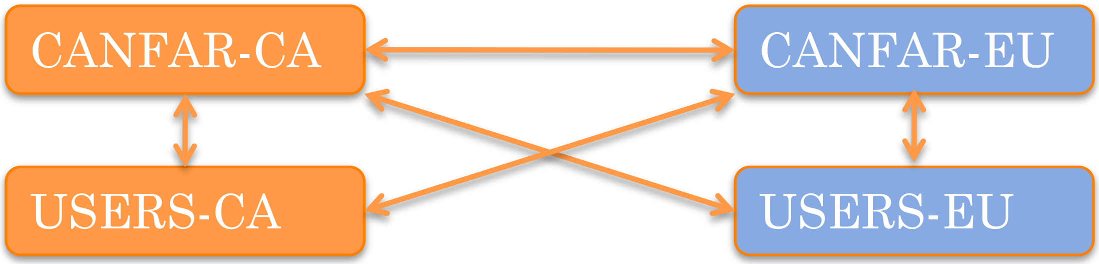
October 2015

The use case

CANFAR: Canadian Advanced Network for Astronomical Research.

- storage (through VOSpace)
- batch processing services (through OpenStack)
- authorization (through group membership)

Canada and Europe working to have collaborating CANFAR instances, one in each location.



CANFAR-CA

CANFAR-EU

USERS-CA

USERS-EU

Baby Steps: Phase I

Phase I Goal: Users from one CANFAR instance can access ***proprietary*** VOSpace data in the other instance.

Key requirement: Users need not create a remote account to use a remote VOSpace.

The approach is described in the remainder of these slides. Does it have a place in the IVOA?

AUTHENTICATION

For proprietary access to data, an authentication mechanism is assumed to be in place.

In this example, x509 client certificates are used for authentication, but other methods can be used.

- IVOA Sesto 2015: *Shibboleth and OpenID at VOPDC*, Mathieu Servillat and Pierre Le Sidaner
- IVOA SSO Document – Lists supported authentication mechanisms.
- EduLink – Will likely be the system used to initially authenticate the user in this collaboration project.

(Note: The above statement is not entirely true because the IVOA CDP protocol is built on x509, something to look at…)

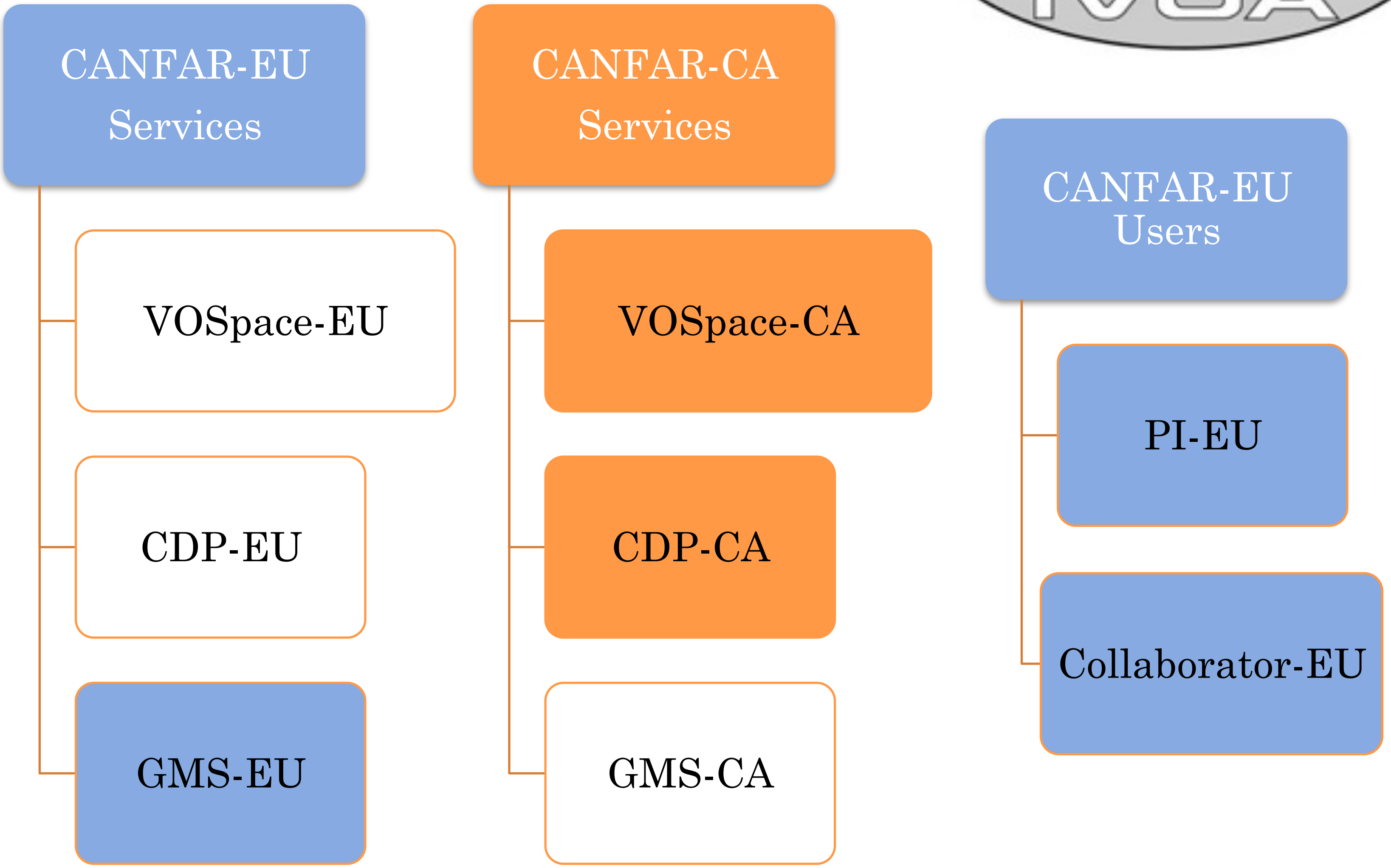
Group Management

Authorization checks are calls to a Group Management REST Service (GMS)

The authorization question: Is this user a member of this group?

This isMember() call to GMS is done by services on behalf of the user by using the proxy certificate obtained through the Credential Delegation Protocol (CDP)

The Players



CANFAR-EU Services

VOSpace-EU

CDP-EU

GMS-EU

CANFAR-CA Services

VOSpace-CA

CDP-CA

GMS-CA

CANFAR-EU Users

PI-EU

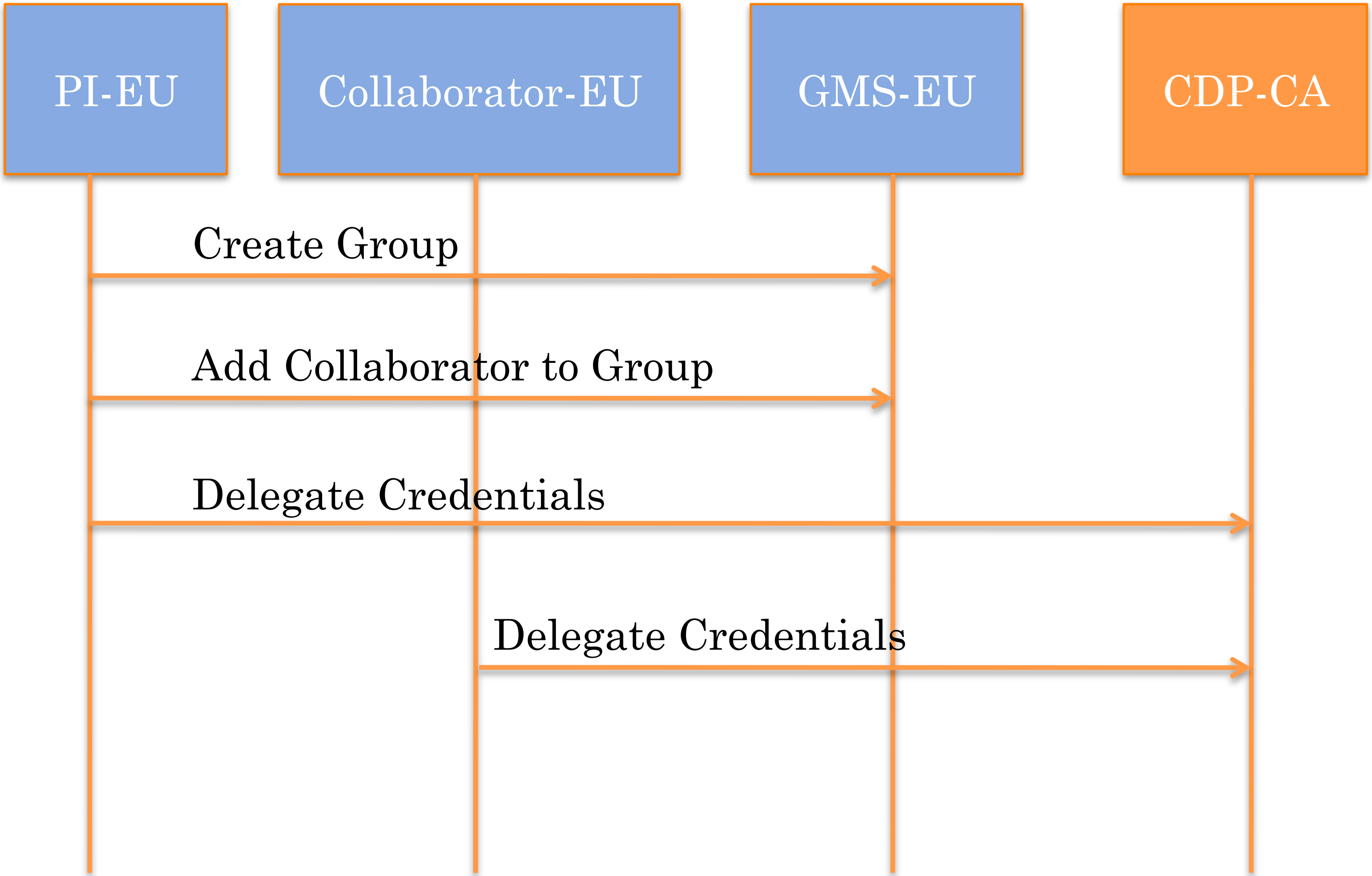
Collaborator-EU

PROJECT SETUP

1. PI-EU creates access group in GMS-EU
2. PI-EU adds Collaborator identity to the access group using GMS-EU
3. PI-EU and Collaborator delegate their credentials to CANFAR-CA using CDP-CA

   (This allows CANFAR-CA to make GMS-EU calls on behalf of PI-EU and Collaborator-EU. The frequency in which the certificate must be delegated is flexible.)

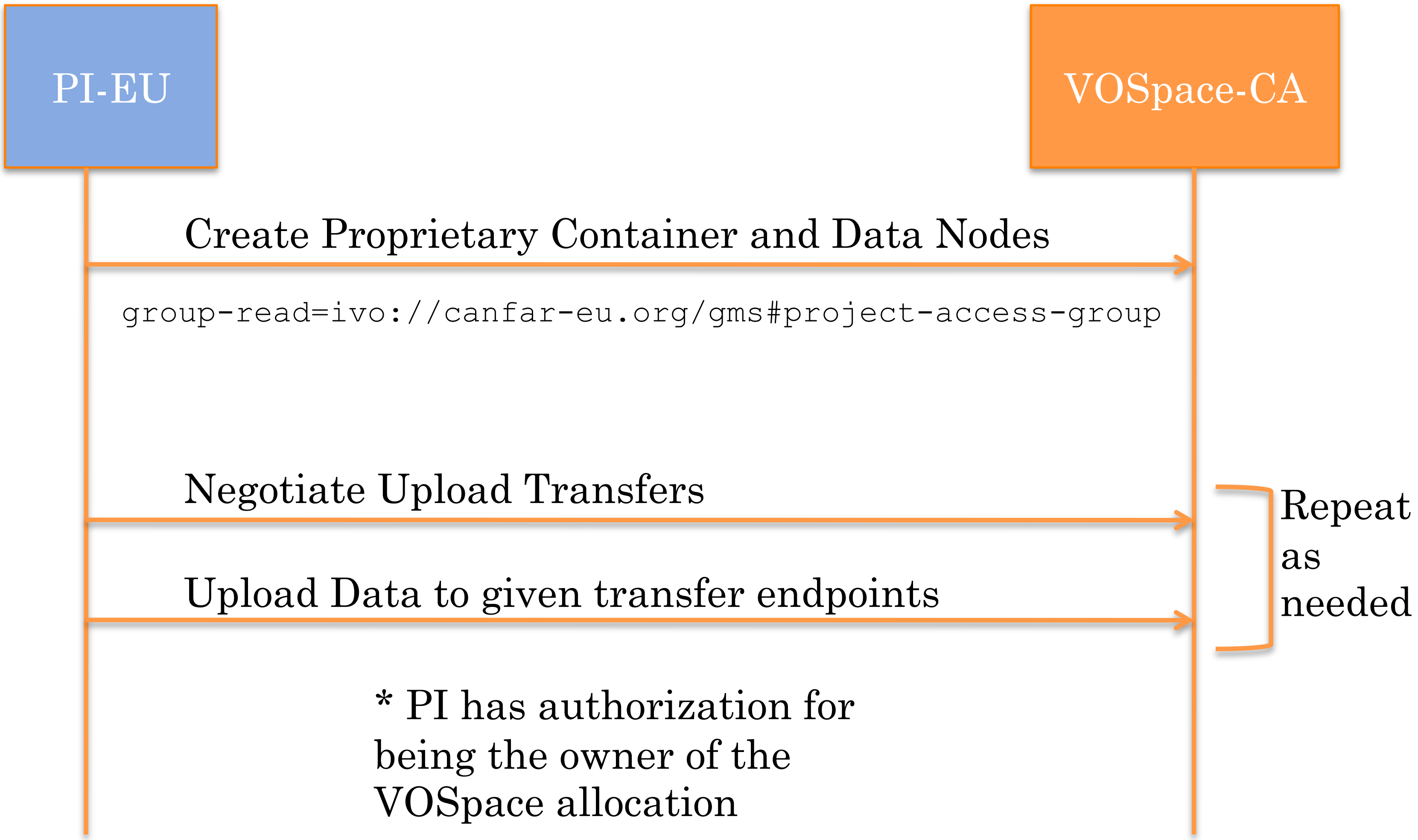
Project setup



STORE PROJECT DATA

1. PI-EU creates a container node in VOSpace-CA with a 'group-read' property that is a uniquely resolvable identifier of the group that can access this data. For example:
   `ivo://canfar-eu.org/gms#project-access-group`
2. PI-EU creates data nodes in VOSpace-CA
3. PI-EU does upload transfer negotiations to VOSpace-CA data nodes
4. PI-EU uploads the data to one of the negotiated endpoints of the transfer

STORE PROJECT DATA



PI-EU

VOSpace-CA

Create Proprietary Container and Data Nodes

```
group-read=ivo://canfar-eu.org/gms#project-access-group
```

Negotiate Upload Transfers

Upload Data to given transfer endpoints

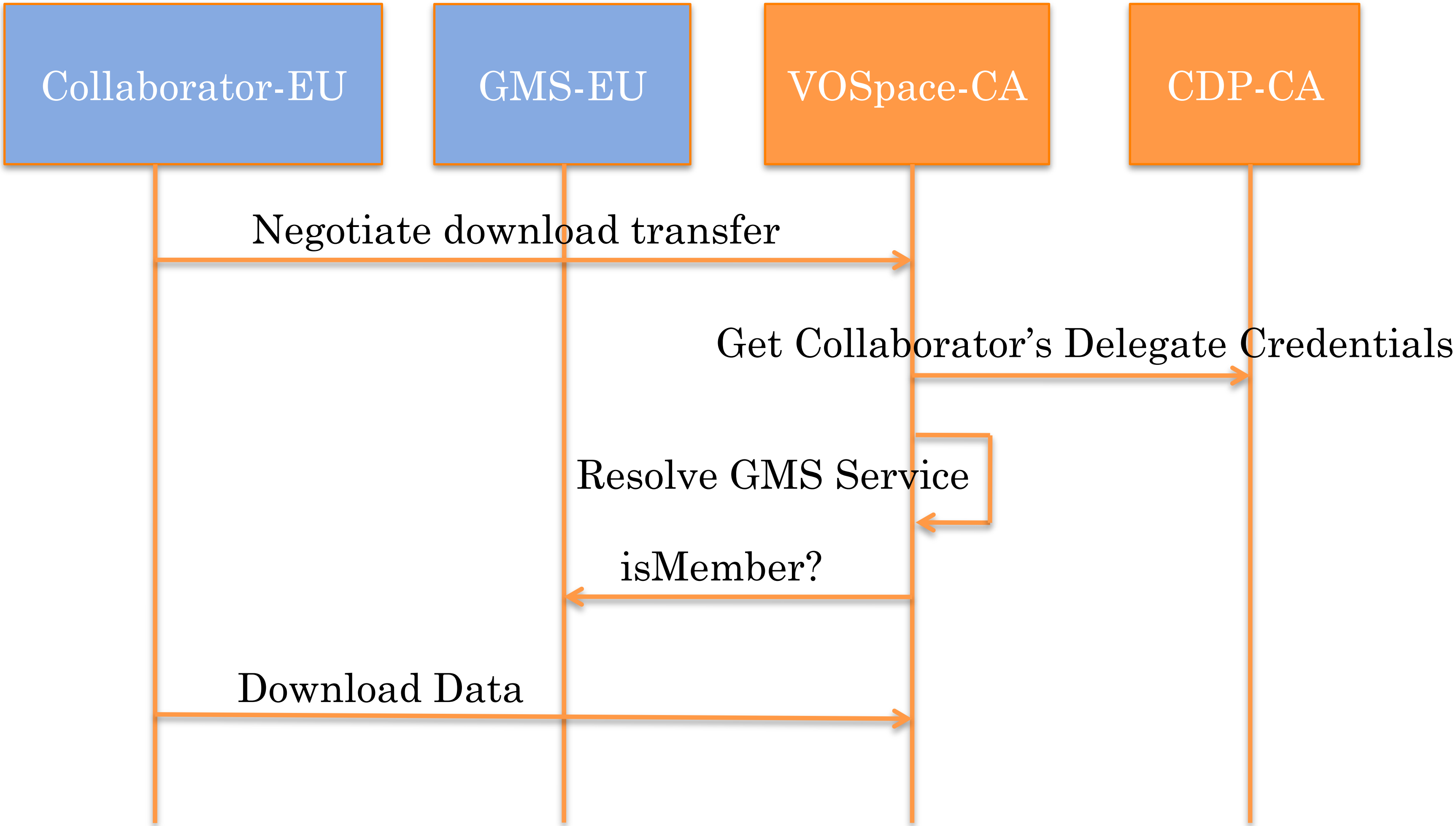
Repeat
as
needed

* PI has authorization for
being the owner of the
VOSpace allocation

Access Project data

1. Collaborator-EU does a download transfer negotiation to VOSpace-CA using their x509 certificate
2. VOSpace-CA sees that the node is protected with the ‘group-read’ property
3. VOSpace-CA does a local CDP call to obtain the Collaborator-EU’s delegated certificate
4. VOSpace-CA resolves the GMS-EU service URL from the group-read URI
5. VOSpace-CA calls GMS-EU and asks if Collaborator-EU is a member of the group in the group-read URI

Access Project Data



Collaborator-EU

GMS-EU

VOSpace-CA

CDP-CA

Negotiate download transfer

Get Collaborator’s Delegate Credentials

Resolve GMS Service

isMember?

Download Data

QUESTIONS

Reality: Authentication & Authorization the most difficult part of interoperability.

Is GMS a good protocol for the IVOA?

Should CDP be more general so as to support something like EduLink?

(CANFAR currently creates x509 certificates for users internally to save them from the headaches…)