INAF
ISTITUTO NAZIONALE
DI ASTROFISICA
OSSERVATORIO ASTRONOMICO
DI TRIESTE

IVOA Interoperability meeting

Group membership based authorization and group management standardization

S.Bertocco, G. Taffoni, M.Molinaro, F. Pasian

26 May – 1 Jun 2018, Victoria Canada

Why this talk?

“ For context, using groups for authorization has been raised (yes, by me :) and discussed at a number of recent interops:

Shanghai:http://wiki.ivoa.net/internal/IVOA/InterOpMay2017-GWS/GMS-Specification.pdf

Trieste:http://wiki.ivoa.net/internal/IVOA/InteropOct2016GWS/Group_Management_Service.pdf

Sydney:http://wiki.ivoa.net/internal/IVOA/InteropOct2015GWS/InteroperableAA.pdf ”

Brian

Group Membership Service
http://wiki.ivoa.net/internal/IVOA/IvoaGridAndWebServices/GMS.pdf

INAF
ISTITUTO NAZIONALE
DI ASTROFISICA
OSSERVATORIO ASTRONOMICO
DI TRIESTE

OATs Data Center

Cloud site:

- 200 physical cores
- OpenStack (Mikata) based
- Storage: 10T for Cinder, the virtual machine storage service
  50TB for the object storage Swift

IA2 Archives:

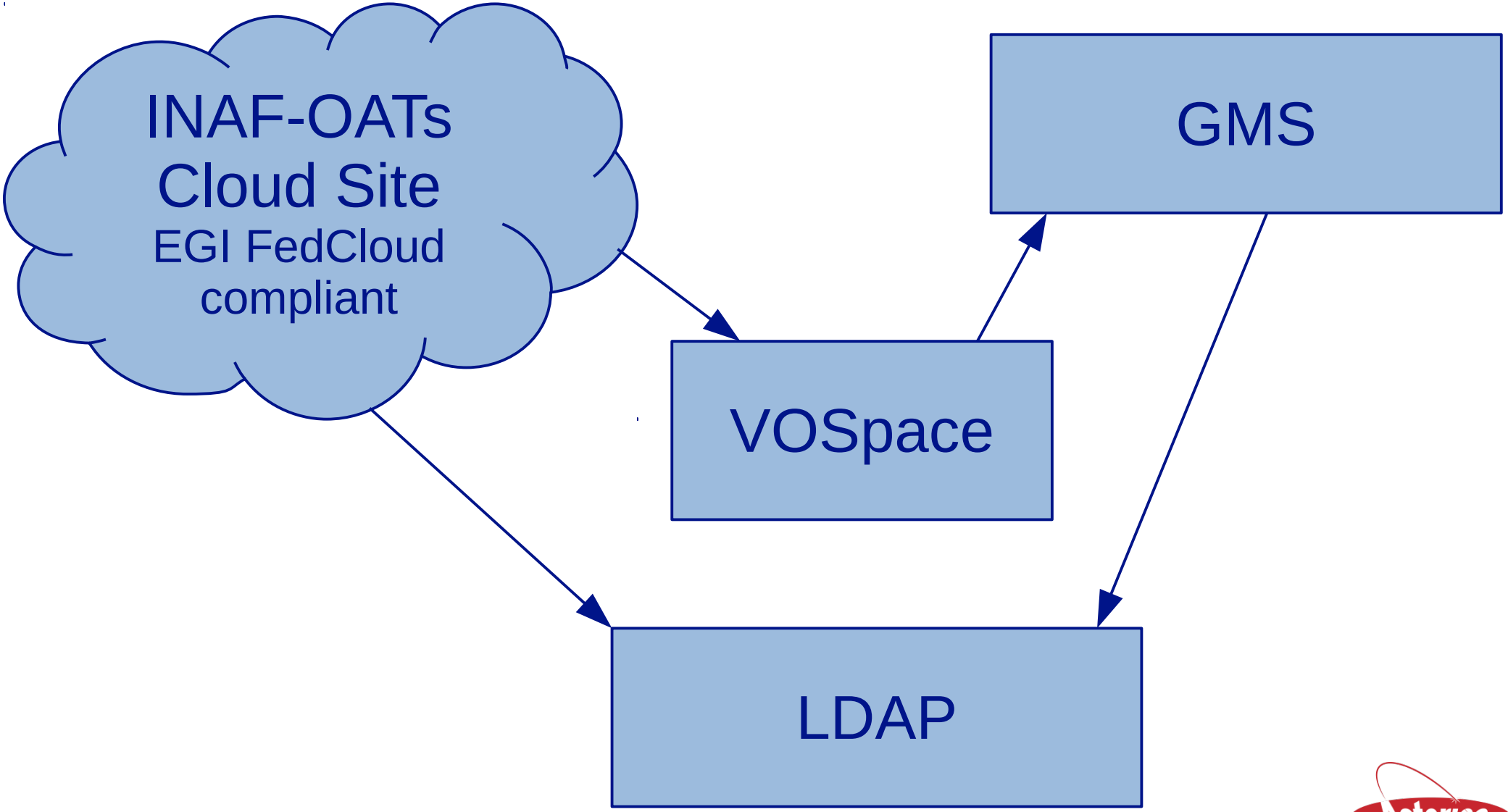
- on line :
  - 500 TB (500 TB used)
  - backup : 100 TB
- off line : 200 TB with expansion to 2 PB
- Bandwidth: : 10Gb/s GARR

HPC cluster (HOTCAT):

- physical cores: 20 computation nodes and one login node;
- Storage: 24TB reliable, based on RAID6, but slow acess,
  270TB (1P soon) parallel file system BeeGFS
  (fast but less reliable -if crash not data recovery granted)

Asterics
Astronomy ESFRI & Research Infrastructure Cluster

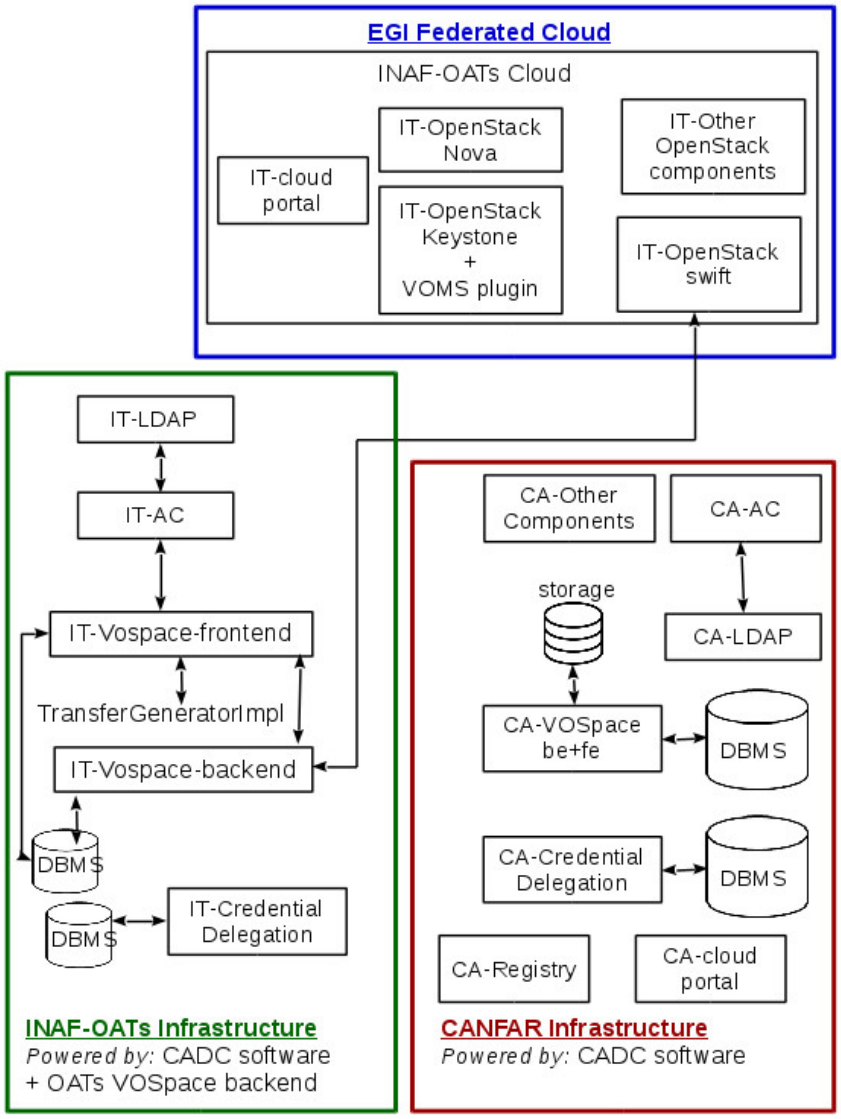
Use case: OATs cloud site & VOSpace(s)

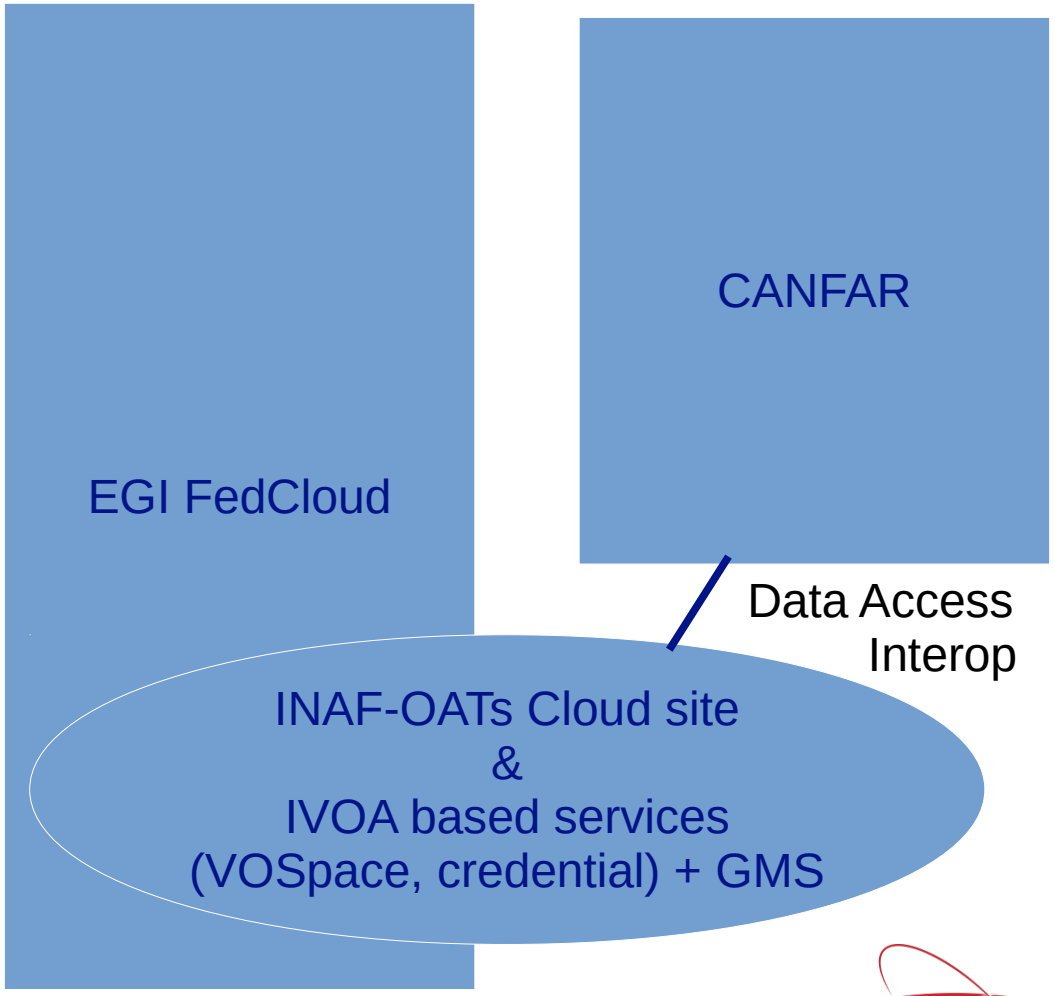


Cloud site Authn & Authz

- Users and groups are stored in LDAP
- Authentication: X.509 certificates
- VOSpace authorization is performed through group membership verification querying GMS
- Cloud site authentication Openstack-Keystone, query LDAP
- Cloud site authorization keystone-voms module, verifies Virtual Organization membership
- Cloud resources access rights based on Virtual Organization membership
- Fine grained data access rights based on groups stored in GMS (subset of Virtual Organization)

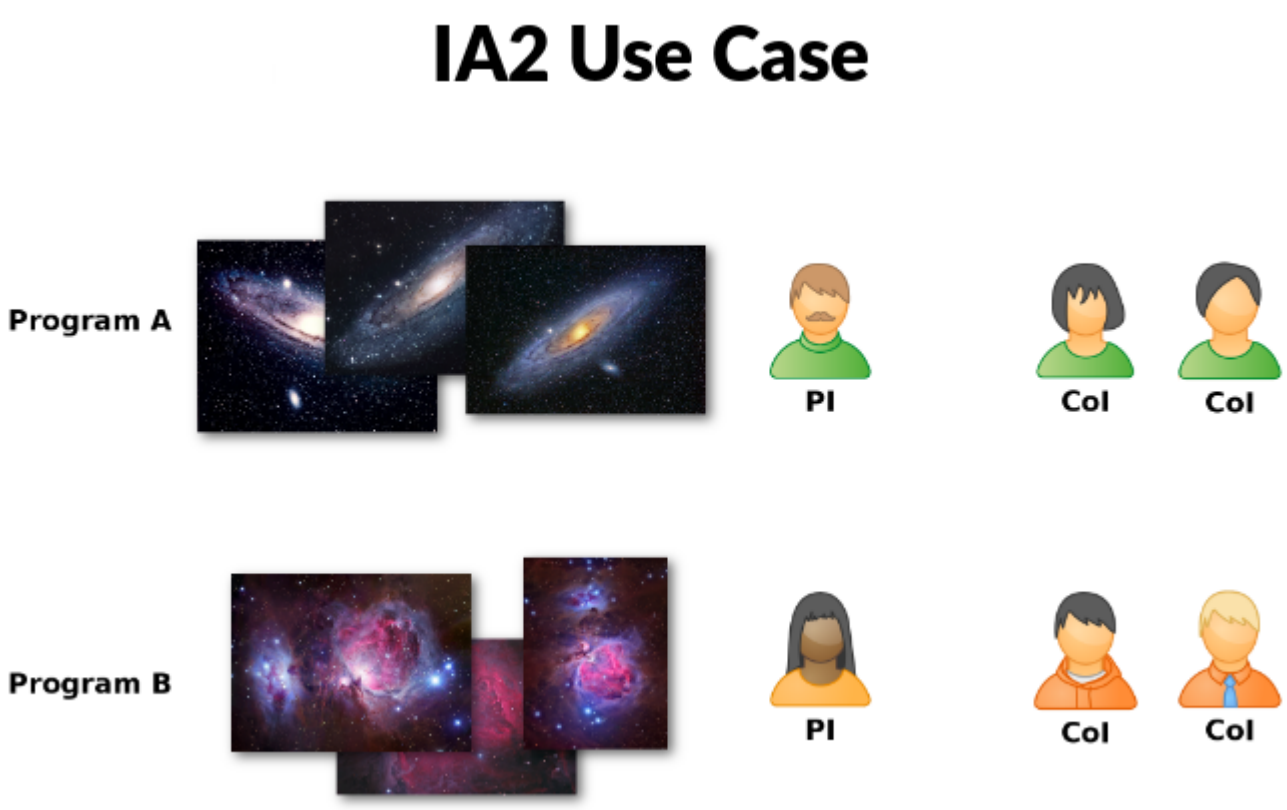
Infrastructures Interoperability





"Cloud access to interoperable IVOA-compliant VOSpace storage", A&C paper

Use case: iA2 archives

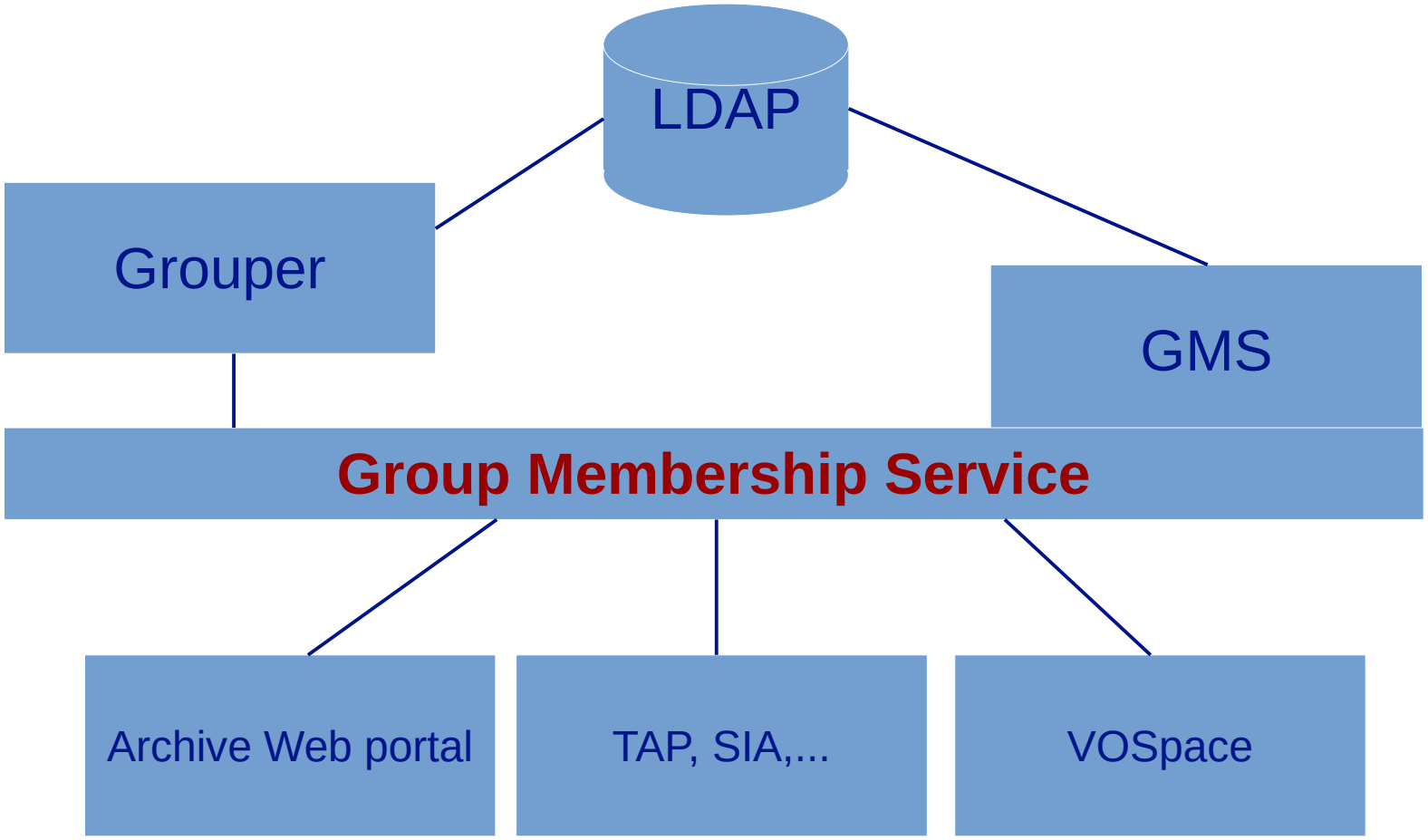


Courtesy by Sonia Zorba, INAF - OATs

iA2 archives Authn & Authz

- Users are stored in LDAP
- Program Name = Group Name
- PI can manage collaborators group memberships using Grouper UI
- Authorization is performed through group membership verification querying Grouper
- Authentication performed through the archive web page
- Users authentication performed with a SSO service: RAP (Remote Authentication Portal)
- Multiple authentication methods are supported (SAML 2.0, OAuth2, X.509)
- Account linking mechanism is provided

IA2 archives & VOSpace uniform authorization requiremens



Open Issue

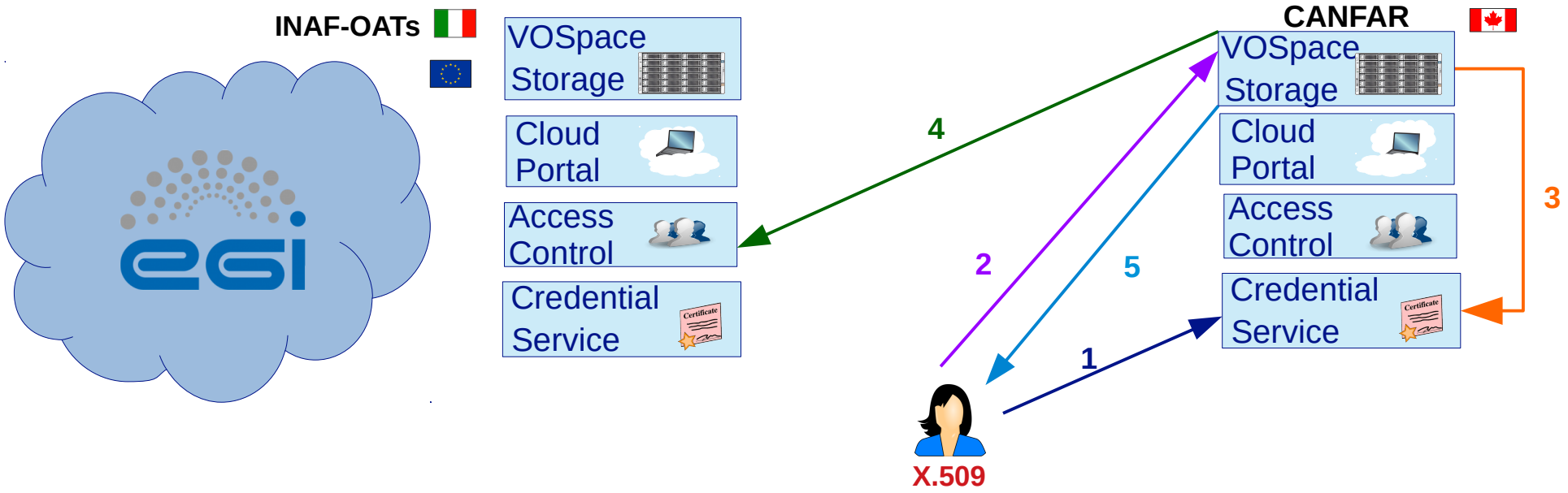
- How to manage user authentication?
  - IVOA has SSO recommendation
  - A lot of tools:
    - RAP
    - EGI check-in
    - IAM (InDiGo Data Cloud)
  - CADC GMS manages also users authentication and different identities

Questions

?

Backup slides

Infrastructures interoperability



1) INAF-OATs user Bertocco delegates her x509 credentials to CANFAR Credential Service

2) user Bertocco asks for data of her INAF-OATs group to CANFAR storage service

3) CANFAR storage service gets the user's delegated credentials from the CANFAR Credential Delegation Service to be able to make calls to each other service on behalf of the initial user

4) CANFAR storage service checks the group affiliation of the user in the INAF-OATs group management service

5) CANFAR storage service returns data to the INAF-OATs user Bertocco