AUTHENTICATION AND AUTHORIZATION PERSPECTIVES
INAF – Infrastructures

- INAF Astronomical Archives (IA2)
- LBT, TNG, Asiago Telescope, Medicina/Noto Radio telescopes
- VO (DAL protocol I/F-es)
- Workflow and Data sharing

- INAF Computing Center
- Cloud Infrastructure
- HPC
- Distributed storage (Lustre+Swift)
- VOSpace, Proc (UWS)
- Science Gateways and Workflows
National and International contest

- H2020 projects
  - Indigo
  - Asterics
  - EGI-Engage
- FP7 projects
  - VIALACTEA
  - Genius
  - Er-Flow
- European Open Science Cloud
- EGI.eu
- EuDat
- AARC
- EU-T0
- IVOA
- International collaborations:
  - Gaps
  - CADC
Authentication and Authorization

- International contest….AARC Project:

AAI: The e-Infrastructure view
What is happening on top of existing Federation infrastructures today

User Identity
- User may have different accounts in different IdPs and technologies

Attribute Enrollment
- LOA, EDOC and 3rd Party group management might be addressed through Attribute Authorities

Authentication
- AA: SAML, AA: EGDS, AA: VOMS

End-Service
- Three options to authenticate at a service: Directly, Via Proxy, Via Token Translation

Proxy
- Token Translation Service

Three options to authenticate at a service: Directly, Via Proxy, Via Token Translation

Site Token service

Identity
- GMS, Grouper, MariaDB table, LDAP, CAS...
EGI implementation of AARC
INDIGO implementation of AARC

INDIGO AAI architecture

- Home IDP
- AuthN Consent
- Login Service
- Group Membership Service
- AuthZ Service
- Provisioning Service
- Token Translation Service
- Non-INDIGO Service
- INDIGO Service
- AuthZ Service

INDIGO Identity and Access Management

- OIDC
- SAML/XACML
- SCIM

User/group provisioning

Local policies

Policy distribution

Identity information

Site boundary

AuthZ callout

Collaboration policies

Site Provisioning Service
Generic Use Case

Auth on Home Organization IdP

AuthZ as close as possible to your service

Service is aware of Authz policies

e-Infra? Also coarse grained Authz
Authentication

- **Status**: local in LDAP or Database (computing => X509)
- **Goal**: move towards IdP (complex for HPC computing clusters)
- **Protocols**: SAML (EDUGain), X509 or LDAP for HPC/HTC resources.
Authorization

- Authentication and authorization require different approaches.

- Authorization tools: Group Management Service, Grouper

- Authorization protocols:
  - OID connect, OAuth2.
  - exchange Authz token on distributed services.

- Local authorization and Global (if you use distributed infrastructures)
AuthZ Tools

- **Grouper**
  - Internet2
  - Groups and roles
  - In production
  - Manage only authz and require an ldap for users
  - No native OIDC or Oauth

- **GMS:**
  - CADC
  - In production
  - Groups and groups of groups
  - We have on installation
  - Manage both auth and authz
  - Based on LDAP backend
  - User x509certs

Authz properties containers (groups)
COMMUNITY SERVICES

- REST API
Grouper and GMS

OID-C / OAuth2

Grouper
- LDAP
  - User ID
- DB
  - Groups

GMS
- USER ID & Groups
Long Term Plan

ARCHIVES

Compute

Grouper

GMS

Loader

LDAP

Provision

OID-C / OAuth2

Authz Repo

GMS

Grouper
Local vs Global

- **Root**
- **e-Infrastructure**

Diagram showing the relationship between local and global infrastructure with Vo (Virtual Organizations) connected to the root.
AAI global view

Home IdP

Authz Service

Collaboration Policies

VOs

Policy distribution

GMS

Grouper

Local Policies

AuthZ Callout
QUESTIONS?