cta cherenkov telescope array

Federated access for the Cherenkov Telescope Array in INAF European Projects

Fabio Vitello, Alessandro Costa, Eva Sciacca, Ugo Becciani
INAF - OACT

Outline

- **CTA**
  - **Use Case** collection
  - **User Requirement** elicitation
  - **A&A Overview**
  - **INAF Prototype**
- **ASTERICS**
- **AARC2**

Use Case Collection

The project team identifies the Use Case Collection as:

- **Constraints** on a system solution.
- Representative set of activities corresponding to constraints and **Scenarios**.

Use cases are are used to analyse the operation of the system in its intended environment in order to identify requirements that may not have been yet formally specified.

Use Case Collection

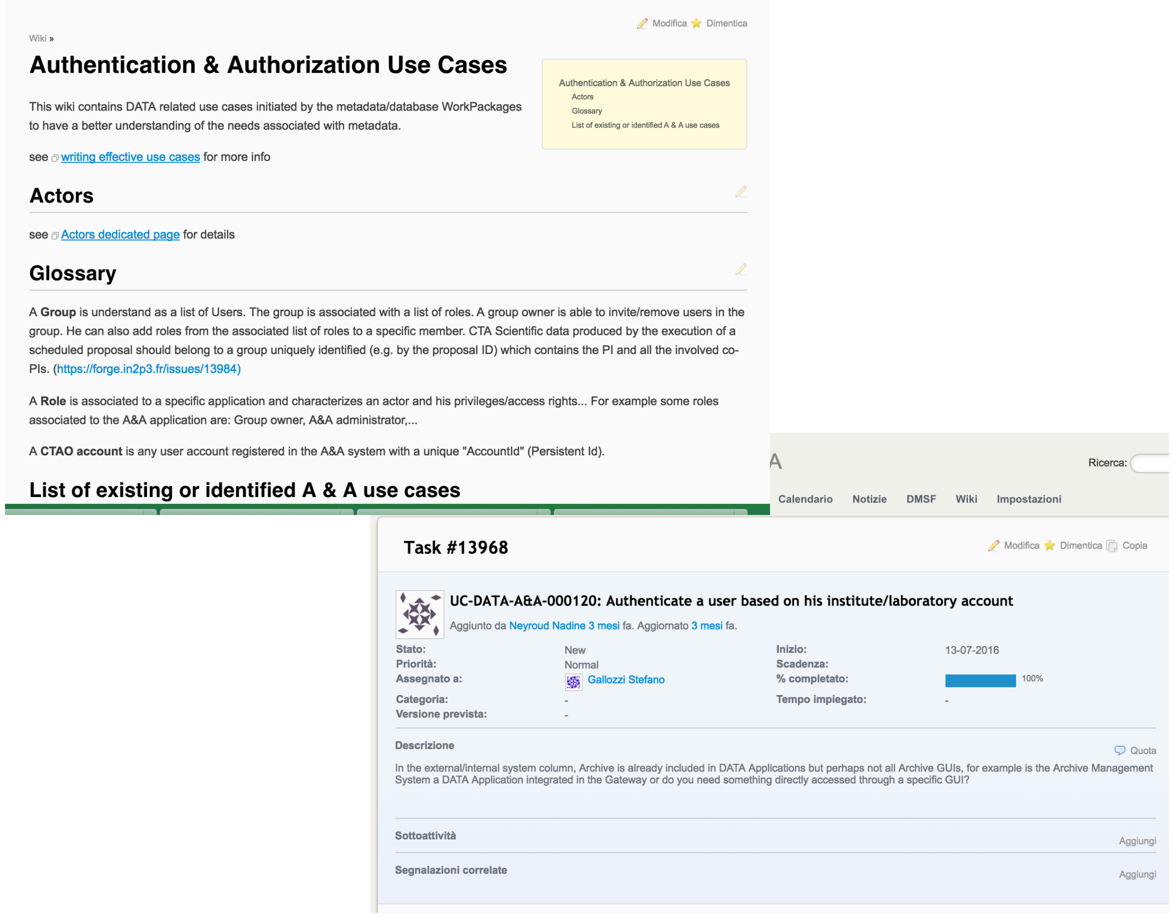
ACTOR Definition

- Human
  - name, role, description
- System
  - name, description, Sub-System

USE CASES Definition

- name, description, ID

redmine issue tracking



Authentication & Authorization Use Cases

This wiki contains DATA related use cases initiated by the metadata/database WorkPackages to have a better understanding of the needs associated with metadata.

see writing effective use cases for more info

Actors

see Actors dedicated page for details

Glossary

A **Group** is understand as a list of Users. The group is associated with a list of roles. A group owner is able to invite/remove users in the group. He can also add roles from the associated list of roles to a specific member. CTA Scientific data produced by the execution of a scheduled proposal should belong to a group uniquely identified (e.g. by the proposal ID) which contains the PI and all the involved co-PIs. (https://forge.in2p3.fr/issues/13984)

A **Role** is associated to a specific application and characterizes an actor and his privileges/access rights... For example some roles associated to the A&A application are: Group owner, A&A administrator,...

A **CTAO account** is any user account registered in the A&A system with a unique "AccountId" (Persistent Id).

List of existing or identified A & A use cases

Task #13968

UC-DATA-A&A-000120: Authenticate a user based on his institute/laboratory account

Aggiunto da Neyroud Nadine 3 mesi fa. Aggiornato 3 mesi fa.

Stato:	New	**Inizio:**	13-07-2016
Priorità:	Normal	**Scadenza:**	
Assegnato a:	Gallozzi Stefano	**% completato:**	100%
Categoria:	-	**Tempo impiegato:**	-
Versione prevista:	-		

Descrizione

In the external/internal system column, Archive is already included in DATA Applications but perhaps not all Archive GUIs, for example is the Archive Management System a DATA Application integrated in the Gateway or do you need something directly accessed through a specific GUI?

Sottoattività

Segnalazioni correlate

A&A Use Case Collection

Some of the defined Use Cases:

- Authenticate an already registered CTA Consortium user
- Authenticate a user based on his institute/laboratory account
- Lost password management
  - User with a local A&A login/password must be able to ask for a new password in case of lost password
- Group creation
  - A&A Administrator or DATA Applications must be able to create a group, associate roles and define group owner(s)
- Group management
  - A group owner is able to manage his group from a central A&A management system or from specific DATA applications integrated or not in the Gateway: **invite users, remove users, account expiration dates**,...

User Requirement Elicitation

User Requirement are grouped in the following Classes:

- Authentication capabilities
- Authorization capabilities
- Account Management capabilities
- Group Management by users/group owner
- Interfaces
- Availability
- Performance
- Security
- Portability

User Requirement: Authentication Capabilities

- **UR-A&A-0010** A Guest Observer that cannot be identified by a scientific community must be able to be identified by a local account protected by login/password.
- **UR-A&A-0030** A CTA consortium user could be identified using his CTA login/password.
- **UR-A&A-0035** User wants to log in once on the CTA applications from the gateway and gains access to his authorized applications and datasets without being prompted to log in again at each of them, so that user needs to authenticate himself only once per session.

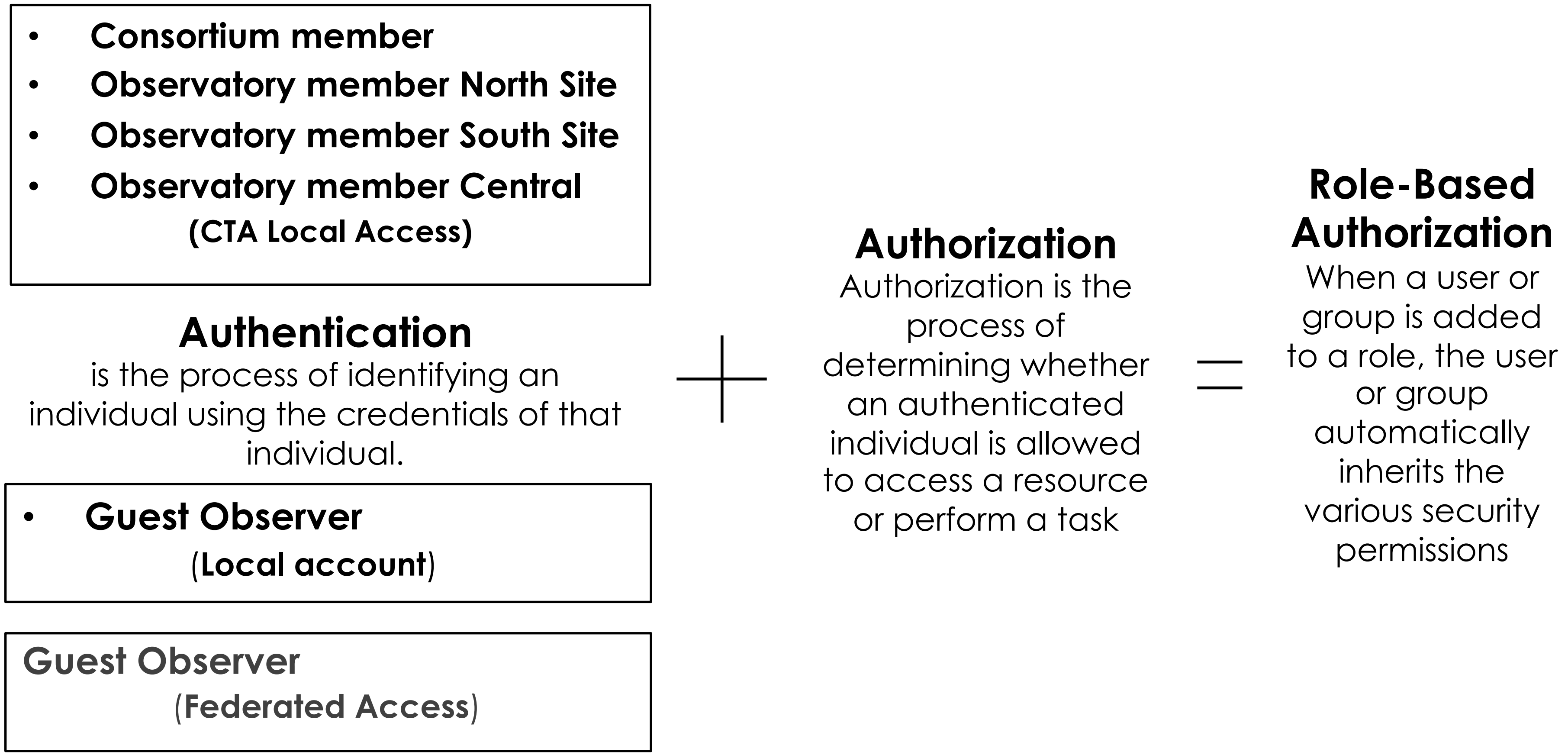
User Requirement: Authorization Capabilities

- **UR-A&A-0100** The A&A system administrator or an authorized application should be able to create a group.
- **UR-A&A-0105** The A&A system administrator should be able to manage the list of roles associated to a group.
- **UR-A&A-0110** Authorization should be granted to users, groups of users.
- **UR-A&A-0130** The A&A system administrator has a tool to add privilege to any user.

Outline

- CTA
  - **Use Case** collection
  - **User Requirement** elicitation
  - **A&A Overview**
  - **INAF Prototype**
- **ASTERICS**
- **AARC2**

A&A Architecture



- **Consortium member**
- **Observatory member North Site**
- **Observatory member South Site**
- **Observatory member Central**

(CTA Local Access)

Authentication
is the process of identifying an individual using the credentials of that individual.

- **Guest Observer**

(**Local account**)

Guest Observer

(**Federated Access**)

+

Authorization
Authorization is the process of determining whether an authenticated individual is allowed to access a resource or perform a task

=

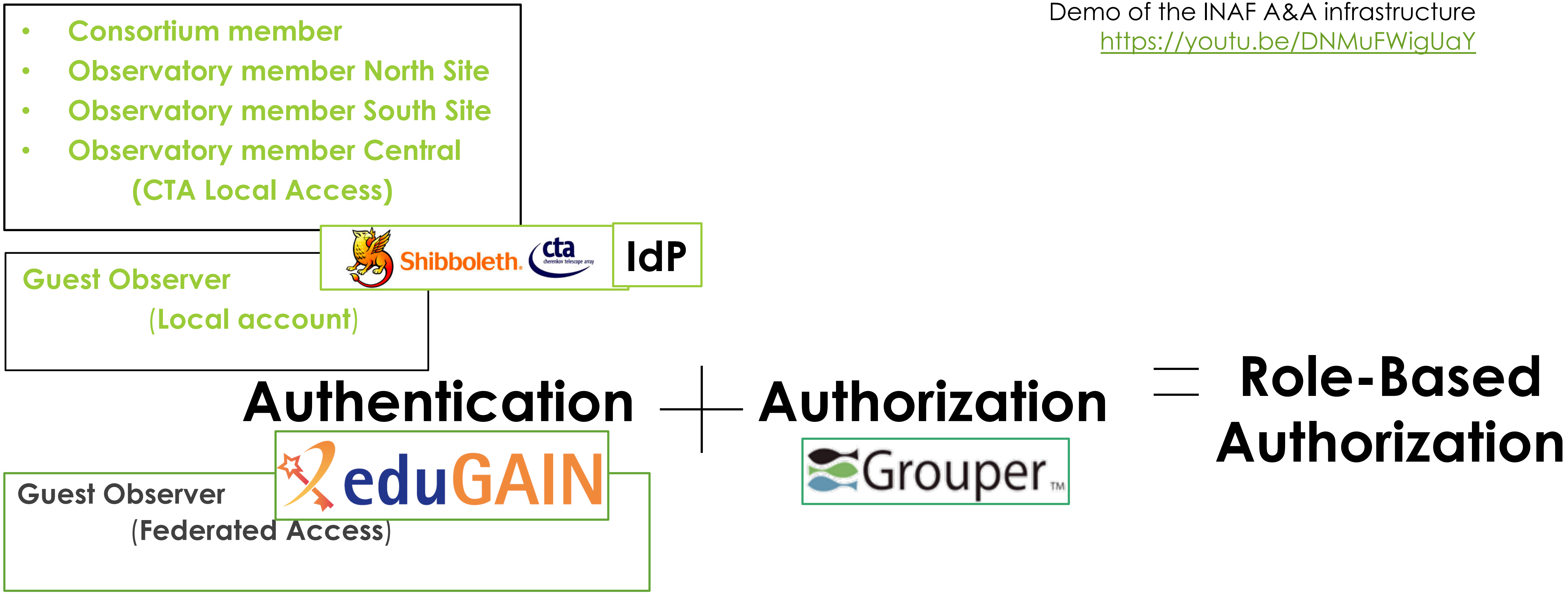
Role-Based Authorization
When a user or group is added to a role, the user or group automatically inherits the various security permissions

Outline

- CTA
  - **Use Case** collection
  - **User Requirement** elicitation
  - **A&A Overview**
  - **INAF Prototype**
- **ASTERICS**
- **AARC2**

A&A “INAF Prototype” Architecture

Demo of the INAF A&A infrastructure
https://youtu.be/DNMuFWigUaY



- Consortium member
- Observatory member North Site
- Observatory member South Site
- Observatory member Central

(CTA Local Access)

Shibboleth. cta cherenkov telescope array IdP

Guest Observer

(Local account)

Authentication + Authorization = Role-Based Authorization

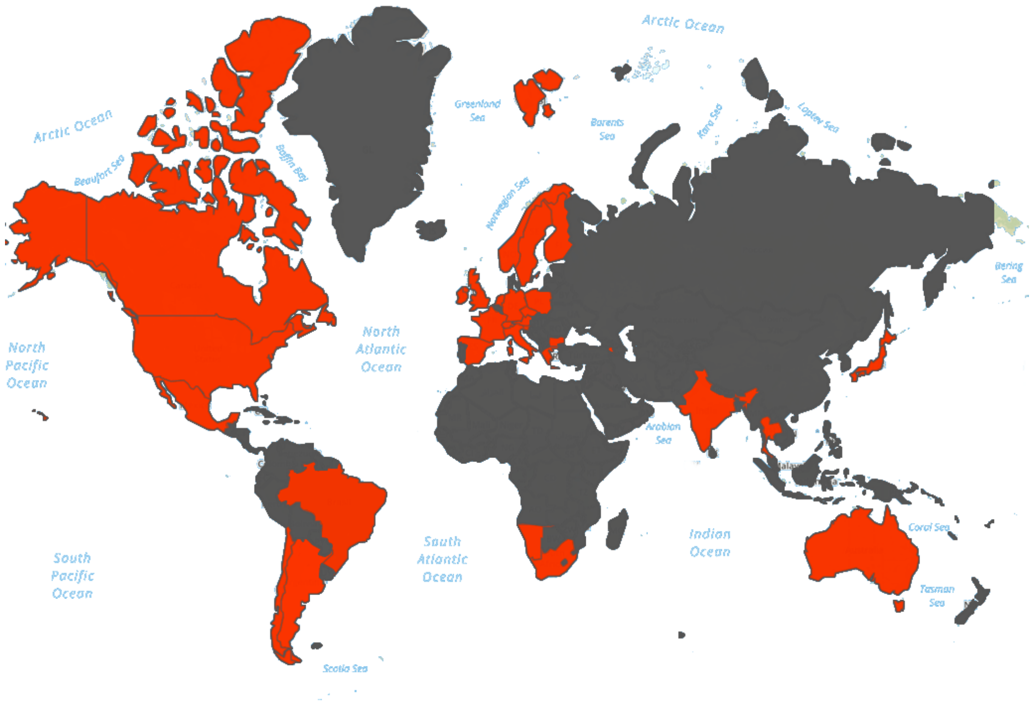
eduGAIN

Grouper™

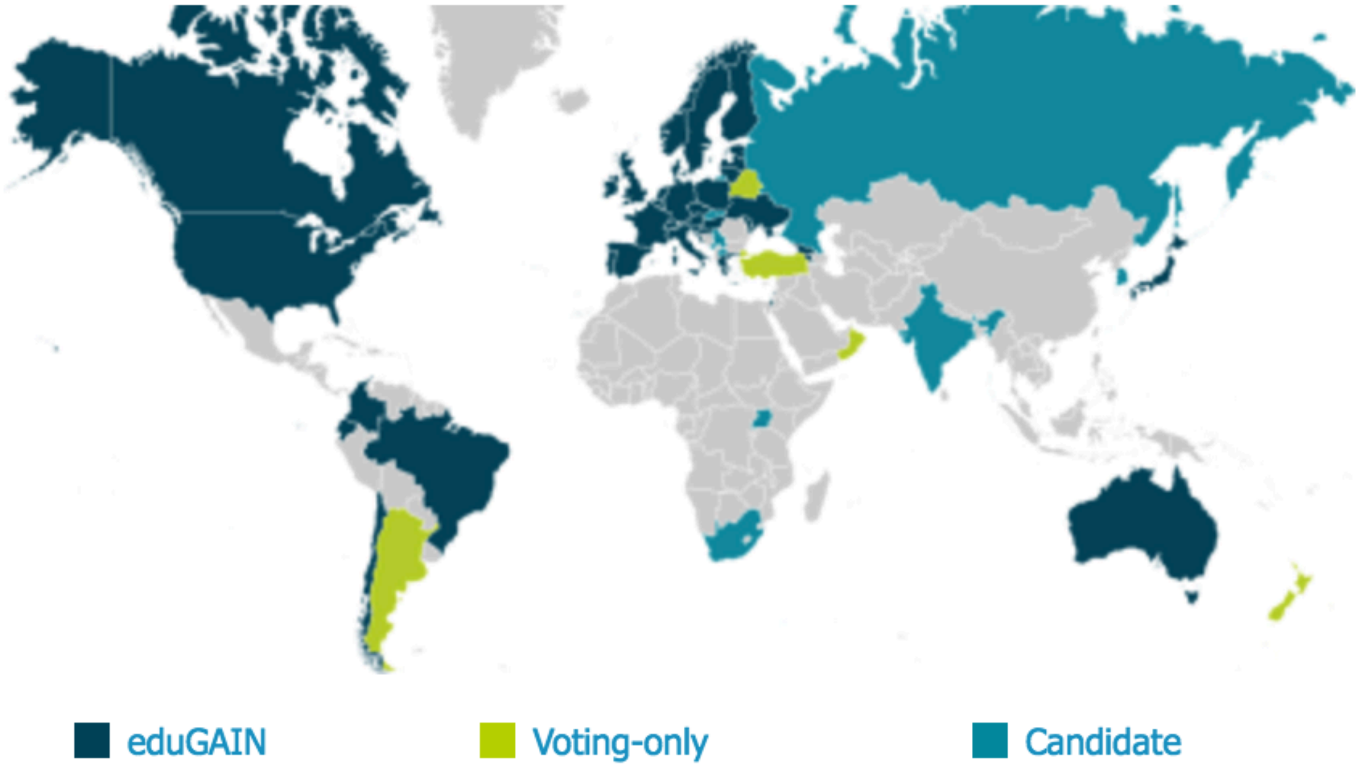
Guest Observer

(Federated Access)

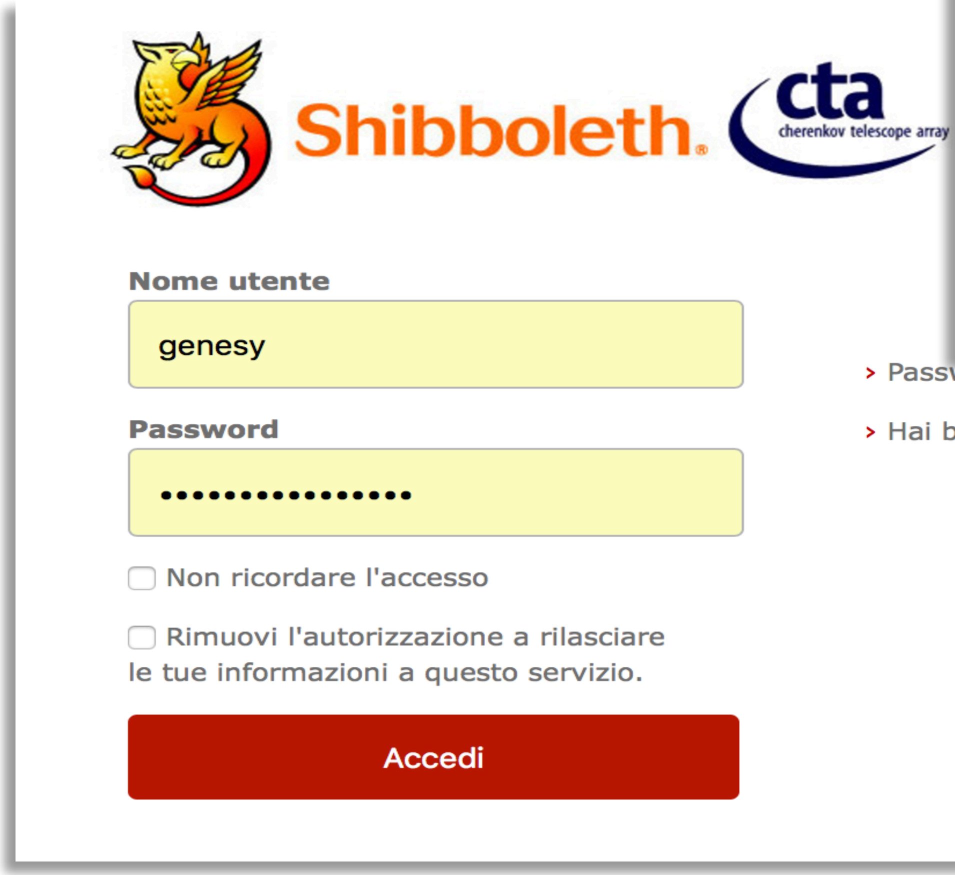
A&A “INAF Prototype” Authentication



Geographical distribution of CTA consortium members



A&A “INAF Prototype” Authentication



Nome utente

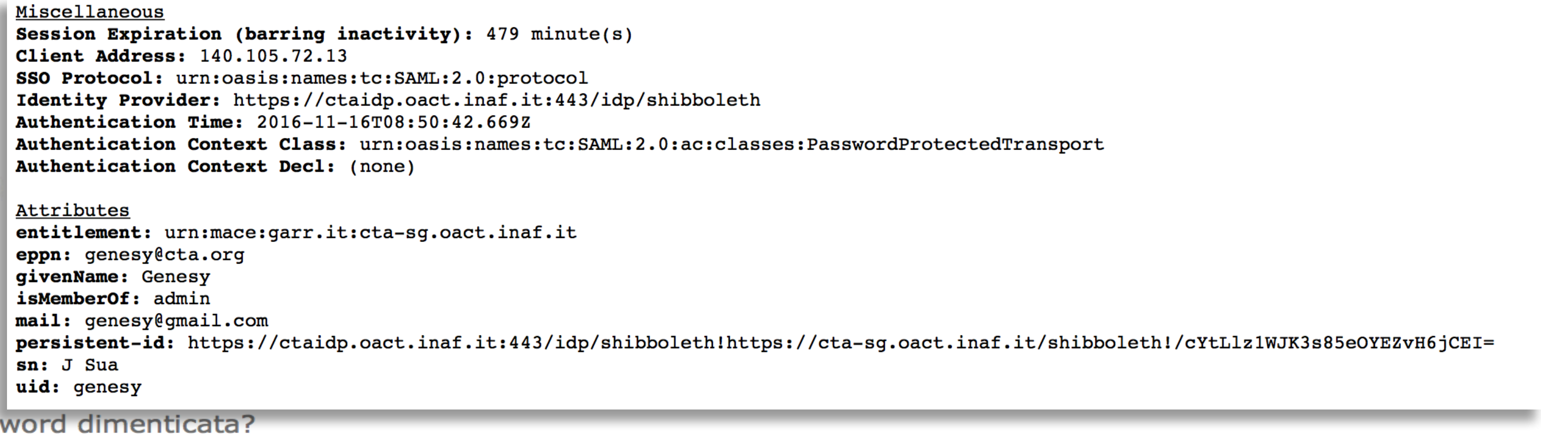
genesy

Password

••••••••••••••••

□ Non ricordare l'accesso

□ Rimuovi l'autorizzazione a rilasciare le tue informazioni a questo servizio.



```
Miscellaneous
Session Expiration (barring inactivity): 479 minute(s)
Client Address: 140.105.72.13
SSO Protocol: urn:oasis:names:tc:SAML:2.0:protocol
Identity Provider: https://ctaidp.oact.inaf.it:443/idp/shibboleth
Authentication Time: 2016-11-16T08:50:42.669Z
Authentication Context Class: urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Authentication Context Decl: (none)

Attributes
entitlement: urn:mace:garr.it:cta-sg.oact.inaf.it
eppn: genesy@cta.org
givenName: Genesy
isMemberOf: admin
mail: genesy@gmail.com
persistent-id: https://ctaidp.oact.inaf.it:443/idp/shibboleth!https://cta-sg.oact.inaf.it/shibboleth!/cYtLlz1WJK3s85eOYEZvH6jCEI=
sn: J Sua
uid: genesy
```

CTA IdP released attributes:

- eppn
- givenName
- mail
- persistent-id
- sn
- uid
- isMemberOf (Grouper)

“INAF Prototype” Authorization

Widely used for research and education (LIGO, LHC…)

Grouper™

https://grouper.oact.inaf.it/grouper

Grouper allows to create and manage institutional **groups**.

- Define resources a group can access
- Manages group membership

Grouper:

- defines groups once allowing to use that group across multiple applications.
- creates a single point of management for the groups.
  - If groups are managed separately in each application keeping the membership list consistent is difficult.
  - Once a person is added or removed from a group, the group-related privileges are automatically updated in all of your collaborative applications.

Management of groups is separated from the technical system, a change in technology has no effect on group management

“INAF Prototype” Authorization Sustainability

Grouper is open-source software.

- **Apache** 2.0 **license**

Supported with funding from

- Internet2 (US research and education network)
- National Science Foundation (NSF)
  - Grant No. OCI-0330626,
  - OCI-0721896,
  - OCI-1032468
- Joint Information Systems Committee (JISC) (UK)
- University of Chicago, University of Pennsylvania, Duke University, University of Washington, University of Memphis, University of Bristol (UK)

Outline

- CTA
  - **Use Case** collection
  - **User Requirement** elicitation
  - **A&A Overview**
  - **INAF Prototype**
- **ASTERICS**
- **AARC2**

ASTERICS: The Astronomy **ESFRI** and Research Infrastructure Cluster

€15 million Research Infrastructure EU Funded

Aims to address cross-cutting synergies and common challenges shared by Astronomy ESFRI facilities

- (SKA, CTA, KM3NeT & E-ELT)

Support and **Accelerate** the implementation of the ESFRI telescopes

ASTERICS: Work Packages

- **AMST**: ASTERICS Management Support Team
- **CLEOPATRA:** Connecting Locations of ESFRI Observatories and Partners in Astronomy for Timing and Real-time Alerts
- **DADI:** Data Access, Discovery & Interoperability
- **DECS:** Dissemination, Engagement and Citizen Science
- **OBELICS:** Observatory E-environments Linked by common ChallengeS

OBELICS - D-ANA: Data ANAlysis / interpretation

The ASTERICS/OBELICS/D-ANA task is developing software libraries for statistically robust analysis of PetaByte-scale datasets in astronomy.

The data analysis software developments target three main aspects:

- Scientific software methods for information extraction;
- Data reduction technique and software for big-data sets management;
- Orchestration of services for data and metadata sets for effective extraction of archived information.

A&A support and accelerate the implementation beyond the current state-of-the-art of technological solutions

OBELICS - D-ANA: A&A Software Survey

- List of standards and protocols
- List of **Authentication** tools and standard implementations
- List of **Authorization** tools and standard implementations
- List of A&A ecosystems
- **Workflows Management Systems**

Outline

- **CTA**
  - **Use Case** collection
  - **User Requirement** elicitation
  - **A&A Overview**
  - **INAF Prototype**
- **ASTERICS**
- **AARC2**

AARC2

AARC Authentication and Authorisation for Research and Collaboration

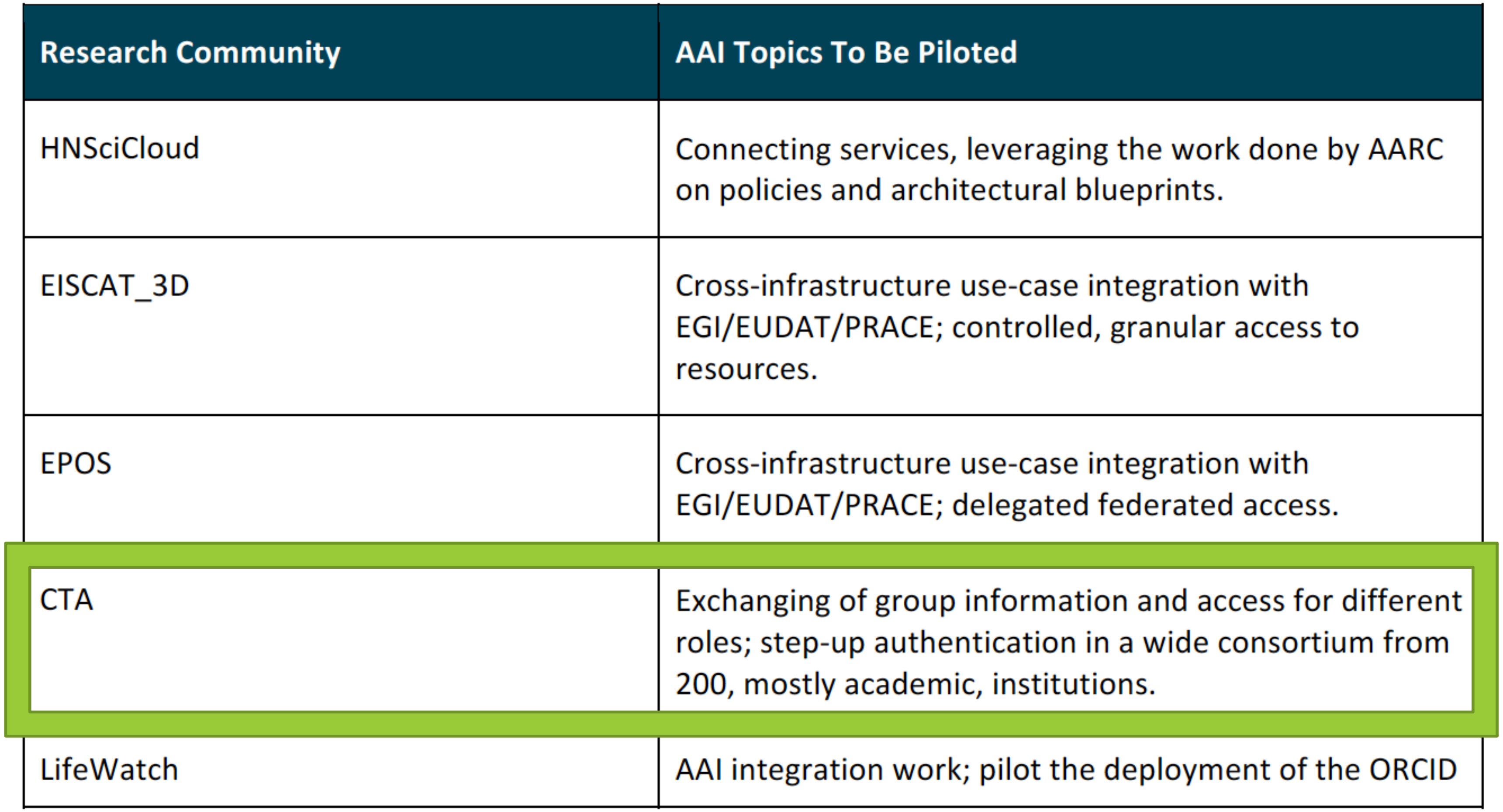
- Duration: 24 MM starting in 2017
- Project coordinator – GÉANT
- Partners – 26 which cover e-Infrastructures, research infrastructures, libraries, NRENs and SMEs.

- RI: **ELIXIR, BBMRI-ERIC, DARIAH**….
- e-infra: **GEANT, EGI, PRACE and EUDAT**
- **User Driven approach**

AARC2: Vision

- A unified, inter-operable AAI for R&E
  - collaboration
  - support data intensive research
  - reduce the overall cost delivery for all participants.
- SSO across e-infrastructures
- AARC2 will move towards the implementation of its vision by working with different research communities.
  - supporting them to deploy federated access
  - map their requirements to existing (AAI) services and policy frameworks

AARC2



Research Community	AAI Topics To Be Piloted
HNSciCloud	Connecting services, leveraging the work done by AARC on policies and architectural blueprints.
EISCAT_3D	Cross-infrastructure use-case integration with EGI/EUDAT/PRACE; controlled, granular access to resources.
EPOS	Cross-infrastructure use-case integration with EGI/EUDAT/PRACE; delegated federated access.
CTA	Exchanging of group information and access for different roles; step-up authentication in a wide consortium from 200, mostly academic, institutions.
LifeWatch	AAI integration work; pilot the deployment of the ORCID