GARR

The Italian Academic & Research Network

www.garr.it

Federated Authorization

Implementing Grouper to federate user authorization

Andrea Biancini, (Maarten Kremers, Lalla Mantovani and Marco Malavolti)

Indianapolis, IN, USA, 10.29.2014

Consortium GARR

Agenda

- **Introduction**: *authentication* and *authorization*
- The **experimentations** using Grouper
- **Use cases** implemented
    - MediaWiki
    - Moodle
    - Custom application
- **Advantages** from different points of view:
    - **SP** point of view
    - **IdP** point fo view
    - **Federation** point of view
- **Conclusions** and future works

Federations today

- Currently, the **goals** of an **Identity Federation** are:
  - give a delegated mechanism to **manage user identification** among different entities and within different subjects;
  - **provide a set of attributes** to an authenticated users to be used by the final application.

- We decided to **extend** the success of current identity federation **to the field of user authorization**.
  - This research has been supported by the European Commission. Within the FP7 programme the **GN3+ project** supported these activities with the specific **Joint Research Activity 3, Task 1**.

AuthN vs AuthZ

- **Authentication** is the act of confirming the truth of an attribute of a single piece of data or entity (the user of an application, for instance).

- **Authorization** is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular.
  - More formally, ”to authorize” is to define an access policy.

How to reach that goal?

- Traditionally, identity federations have solved the authorization problems with two opposite approaches:
  - **SP managed authorization**
  - **IdP managed authorization**

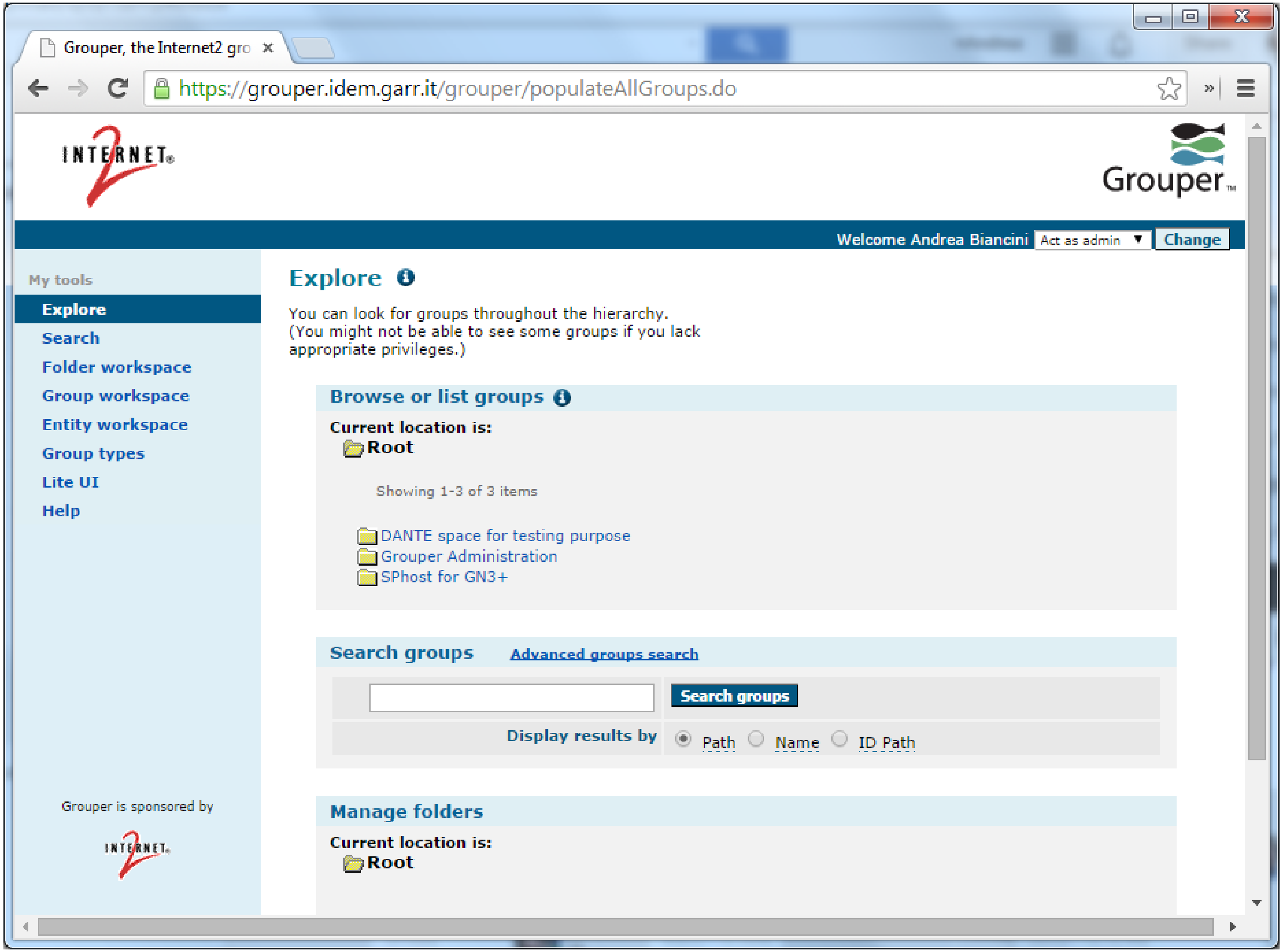
- A different approach may be followed (leveraging Attributes Authorities and implementing tools like Grouper) where **authorization is delegated to a specific system** designed for that purpose.

Tools

- We want to evaluate the **introduction of Grouper** for a **cross/inter organizational** use.

- Grouper will be used to manage in a centralized way (yet eventually permitting delegation):
  - **Groups** of users
  - Authorization **attributes** for users.

Grouper



Explore

You can look for groups throughout the hierarchy. (You might not be able to see some groups if you lack appropriate privileges.)

Browse or list groups

Current location is:
Root

Showing 1-3 of 3 items

- DANTE space for testing purpose
- Grouper Administration
- SPhost for GN3+

Search groups

Advanced groups search

Display results by ● Path ○ Name ○ ID Path

Manage folders

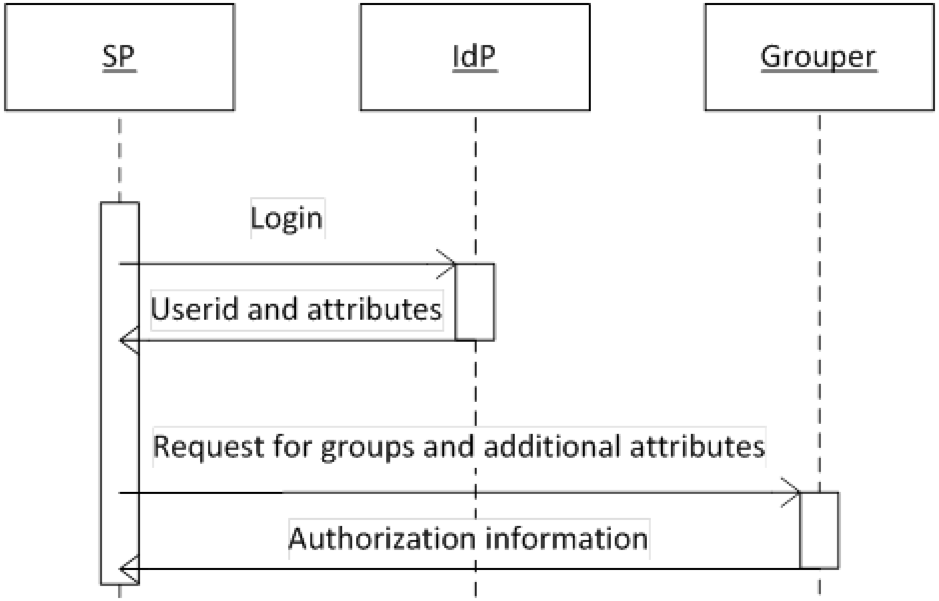
Current location is:
Root

Proof of Concept

- To prove real use cases, **three SPs** will be integrated with Grouper in a Proof of Concept:
  - A **MediaWiki application**: Grouper will manage user groups for read/write access;
  - A **Moodle application**: Grouper will provide course list and manage students/teachers enrolment to courses;
  - A **custom application**: Grouper will provide user groups and other authorization attributes specific to the service.

MediaWiki

- This use case will require user groups and attributes to be retrieved **during the login phase**.
  - To give the user the correct access rights.
  - Using the **Attribute Authority** to add SAML attributes.


SP
IdP
Grouper
Login
Userid and attributes
Request for groups and additional attributes
Authorization information

Moodle

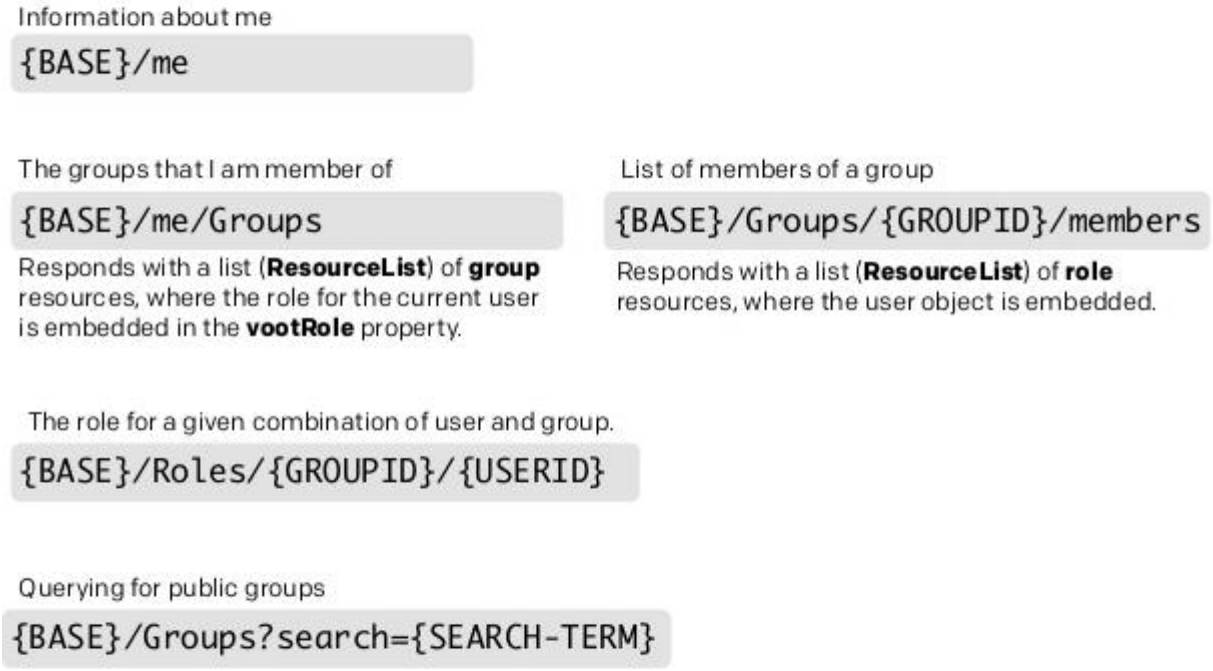
- This use case will require groups and attributes to be retrieved **during the login phase**.

- It will also require to have an **"off-line" query from Moodle to Grouper**.
  - to obtain the **list of courses** (defined as groups in Grouper), the list of **teachers** and the list of **students** for every course.
  - implemented in **VOOT** with a specific connector for Grouper.

VOOT Protocol

- VOOT is a protocol for **exchanging group information** externally to applications.

- Very simple API:



Information about me

```
{BASE}/me
```

The groups that I am member of

```
{BASE}/me/Groups
```

Responds with a list (**ResourceList**) of **group** resources, where the role for the current user is embedded in the **vootRole** property.

List of members of a group

```
{BASE}/Groups/{GROUPID}/members
```

Responds with a list (**ResourceList**) of **role** resources, where the user object is embedded.

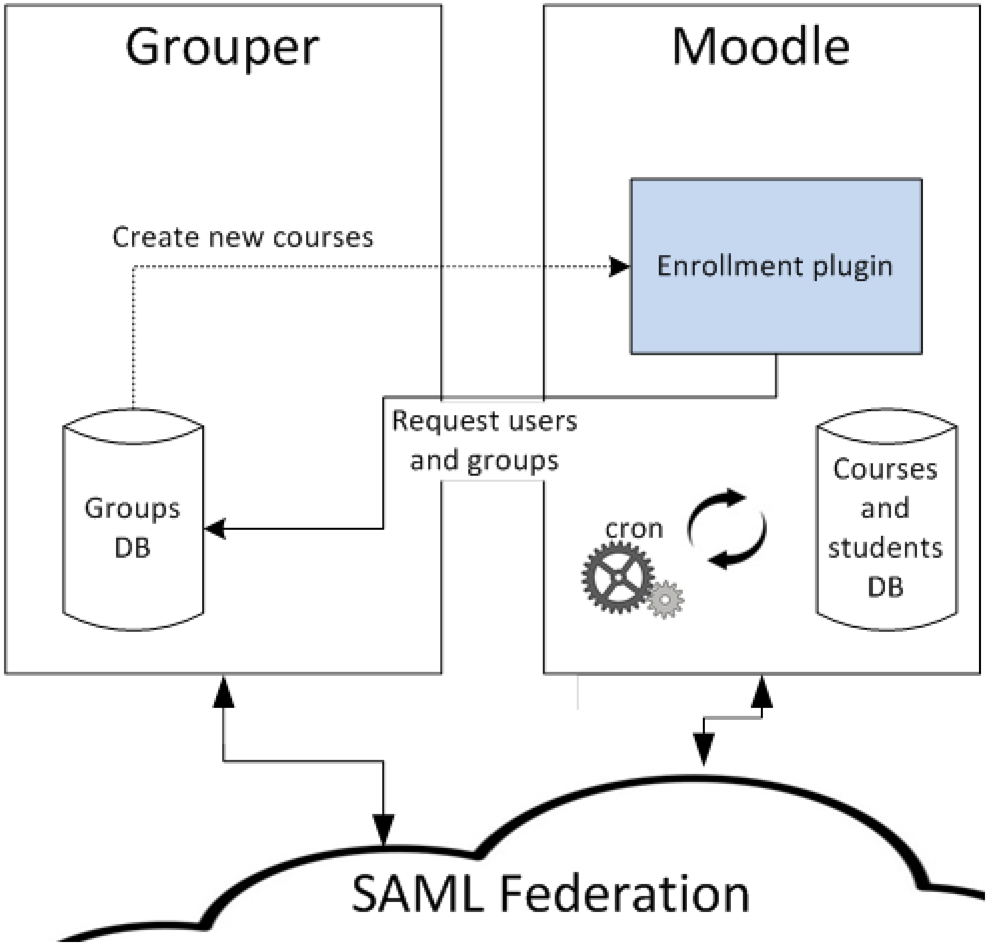
The role for a given combination of user and group.

```
{BASE}/Roles/{GROUPID}/{USERID}
```

Querying for public groups

```
{BASE}/Groups?search={SEARCH-TERM}
```

Moodle integration Architecture



Custom application

- The integration of a custom application permits:
  - on one hand, to **understand how** emerging **applications can be designed and modelled** to be fully compliant with the delegated authorization process introduced;
  - on the other hand, we can study **how to manage** directly **additional authorization attributes** for the users (and not only groups).

Advantages: externalizing from SP

- The process of managing authorization is **split into two main tasks**:
    - Authentication **attributes representation** and assignment to users: this task is completely externalized by the SP to Grouper;
    - Implementation of **allow or deny grants to functionalities** or resources: this task remains in the SP (or, better, in the application itself). The SP will leverage relevant authorization information retrieved from Grouper.

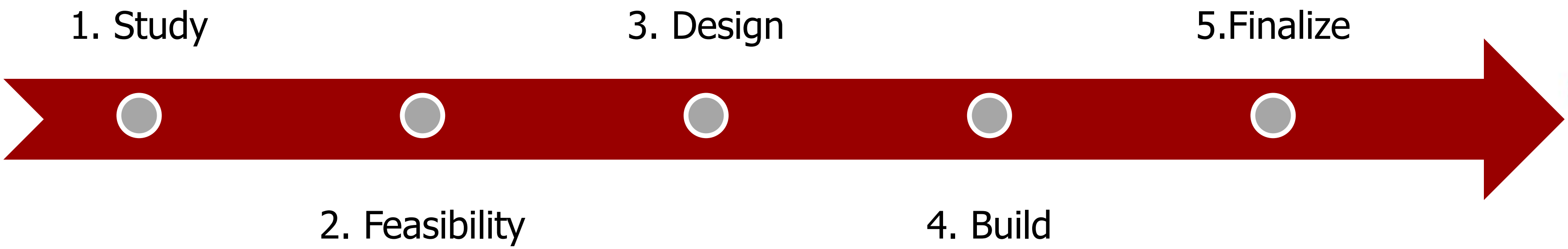
Advantages: no burden to IdPs

- The **authorization attributes** will be **managed** inside Grouper and thus **in a single point**.
- Inside Grouper the proper **delegation mechanism** can be implemented to permit each organization’s administrator to **deal only with the attributes of** his **interest**.
- This approach will **simplify** authorization management but at the same time will permit to **maintain full control** and **accountability** on user attributes.

Advantages: clear accountability

- The **delegation** will happen **in a clear and secure way** so that responsibilities are very clearly defined and attributed.
- The different subjects interacting in the authorization definition process must **rely on a reciprocal trust**, which is usually built at a federation level.
- The technical representation and exploitation of **authorization attributes** is **coherent with** the already defined **authentication process** *(to simplify technical adoption of such a solution by all the participants to the federation)*.

GN3+ JRA3 T1 milestones



1. Study

2. Feasibility

3. Design

4. Build

5.Finalize

1. **Study** *(started 03/2014):*
   - gaining knowledge on the tools and processes
2. **Feasibility** *(end 05/2014):*
   - introduction the context of authorization processes
3. **Design** *(end 09/2014):*
   - architectural design and description the technical choices
4. **Build** *(end 12/2014):*
   - realization of the PoC with the integration of the three SPs

Conclusion

- The **approach** described **proved to be effective** and paves the way to have it implemented as a real functionality into existing Identity Federations.
- This PoC permitted to **identify the key problems** and main aspects of realizing a central system for authorization.
- Future developments could be to **move** from the laboratory **to real production environments** in order to test on the field the robustness of the choices made.

Q&A

www.garr.it