THE ITALIAN RESEARCH & EDUCATION NETWORK | Consortium GARR

L'Attribute Authority come servizio centralizzato della Federazione IDEM

Identità digitale unica: Quinto Convegno della Federazione IDEM

Andrea Biancini @ Consortium GARR

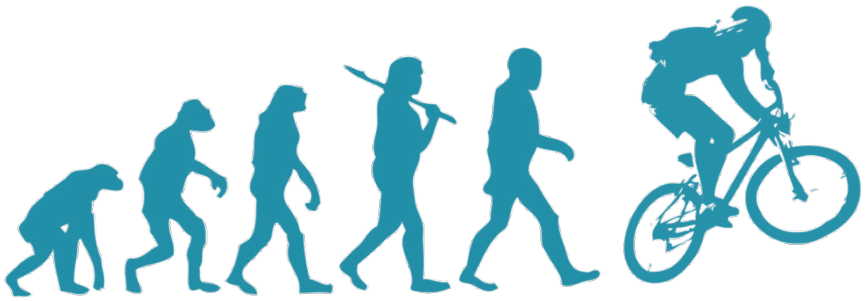
Quinto Convegno IDEM | Lecce, 14 maggio 2015

Le federazioni, oggi

Oggi, gli **obiettivi** di una **Federazione d'Identità** sono:

- **identificare gli utenti**, con meccanismi di delega delle responsabilità;
- **fornire un insieme di attributi** per gli utenti dopo l'autenticazione.

Il nostro obiettivo è stato quello di **estendere** le federazioni nell'**ambito dell'autorizzazione degli utenti**.



AuthN vs AuthZ

Autenticare significa verificare che un utente sia esattamente chi dichiara di essere.

Autorizzare significa specificare i diritti di accesso di un utente su un'applicazione o una risorsa.

- Gli attributi utente sono spesso utilizzati per permettere l'implementazione di regole di accesso (e quindi l'autorizzazione).

Separare AuthN e AuthZ

- Permettere agli IdP di delegare il rilascio di attributi per gli utenti ad altre entità presenti nella federazione:
  - in modo sicuro e fidato;
  - senza dover introdurre nuove tecnologie oltre a quelle già esistenti nelle federazioni odierne.

- Queste «nuove» entità sono chiamate **Attribute Authority**.

Il servizio di AA offerto da GARR

GARR fornisce la sua AA (https://grouper.idem.garr.it/idp/shibboleth) che usa **Grouper**.

Questa AA permette di gestire in un modo centralizzato:

- i **gruppi** di utenti;
- gli **attributi** per l'autorizzazione degli utenti.

Permettendo **meccanismi di delega** per l'amministrazione di queste informazioni.

Una AA cross/inter organizzazione

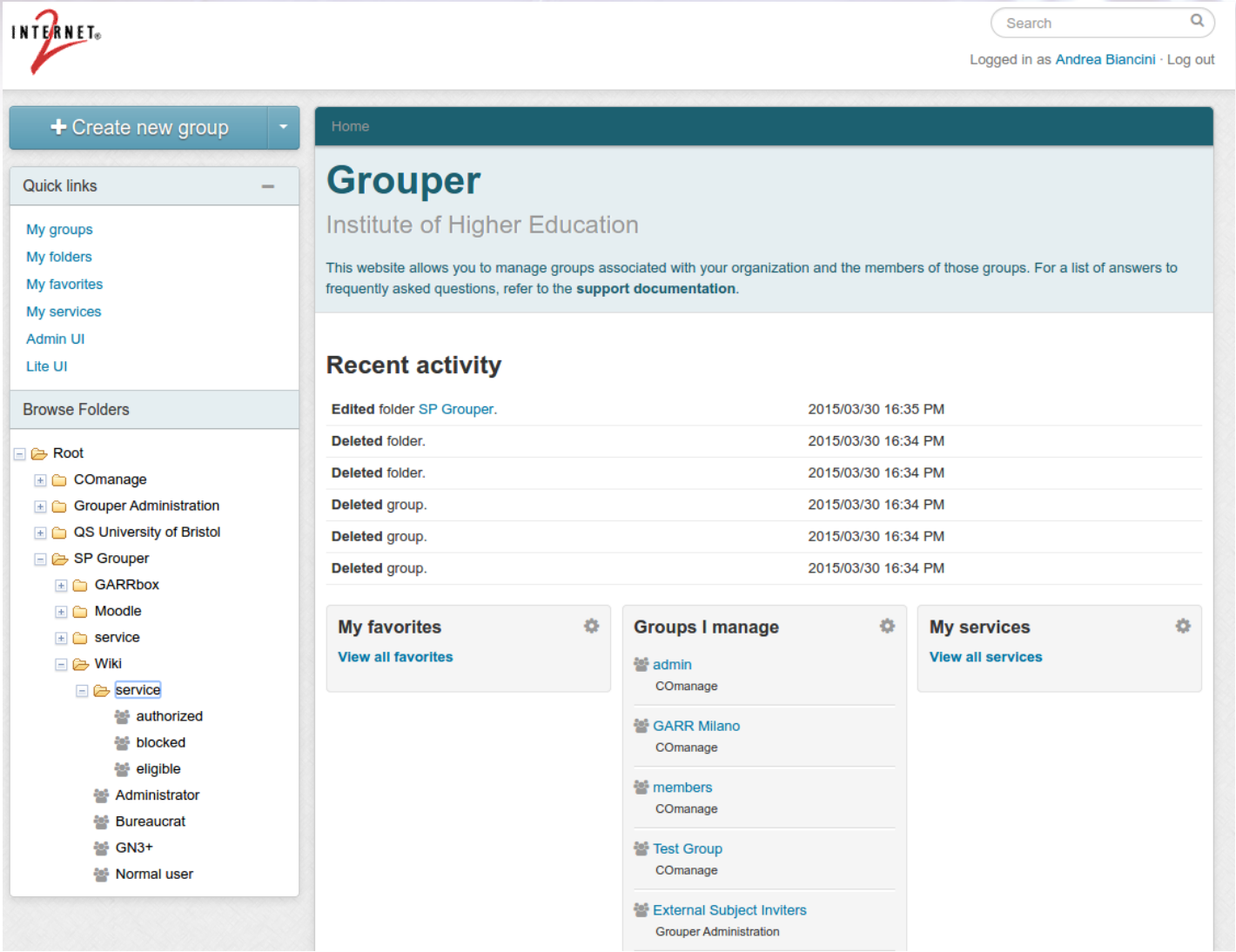
Una AA cross/inter organizzazione:

- definisce dei **gruppi di utenti** come elementi cui assegnare specifici **diritti di accesso**;
- ciascun **gruppo** può essere **composto da utenti di diverse organizzazioni**;
- la **gestione** di ciascun **gruppo** deve essere **delegata** a specifici amministratori di gruppo.

Gli amministratori dei diversi gruppi usano un'**interfaccia web** per gestirli.

I gruppi così definiti vengono letti dagli SP delle diverse applicazioni connessi all'**Attribute Authority**.

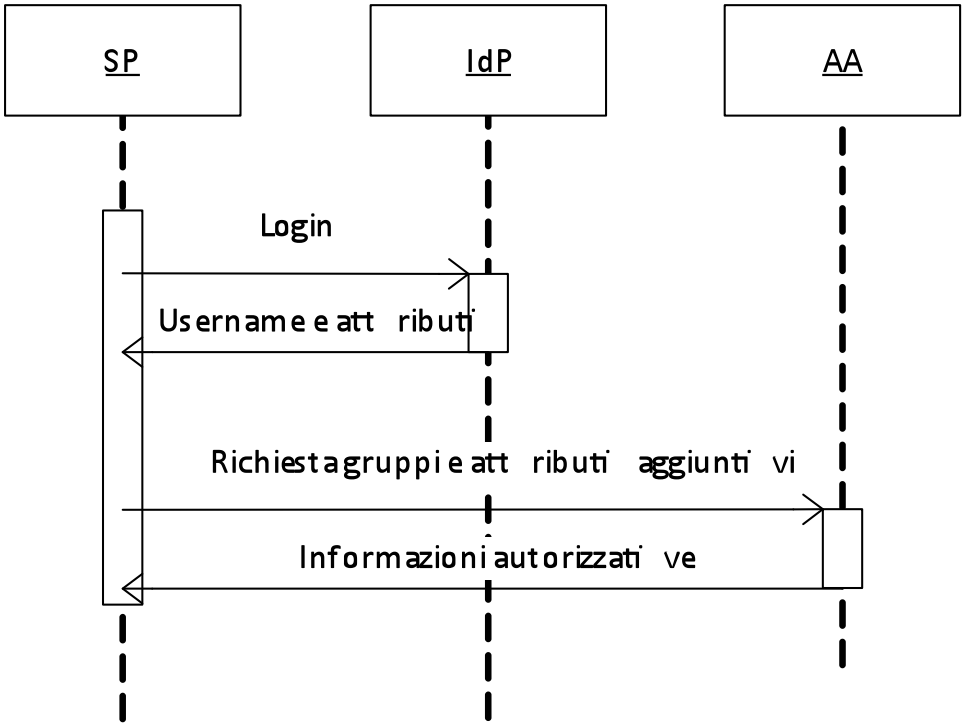
Grouper


INTERNET 2
Search
Logged in as Andrea Biancini · Log out
+ Create new group
Quick links
My groups
My folders
My favorites
My services
Admin UI
Lite UI
Browse Folders
Root
COmanage
Grouper Administration
QS University of Bristol
SP Grouper
GARRbox
Moodle
service
Wiki
service
authorized
blocked
eligible
Administrator
Bureaucrat
GN3+
Normal user
Home
Grouper
Institute of Higher Education
This website allows you to manage groups associated with your organization and the members of those groups. For a list of answers to frequently asked questions, refer to the support documentation.
Recent activity
Edited folder SP Grouper. 2015/03/30 16:35 PM
Deleted folder. 2015/03/30 16:34 PM
Deleted folder. 2015/03/30 16:34 PM
Deleted group. 2015/03/30 16:34 PM
Deleted group. 2015/03/30 16:34 PM
Deleted group. 2015/03/30 16:34 PM
My favorites
View all favorites
Groups I manage
admin
COmanage
GARR Milano
COmanage
members
COmanage
Test Group
COmanage
External Subject Inviters
Grouper Administration
My services
View all services

Come funziona una AA

Una AA viene **invocata dagli SP**, dopo il normale processo di autenticazione avvenuto su un IdP.

Essa rilascia degli **attributi SAML aggiuntivi** (tra cui i gruppi applicativi cui l'utente appartiene).



Cosa cambia nelle applicazioni

Per integrare una AA è necessario effettuare una **modifica di configurazione dell'SP**.

- In questo modo l'SP viene istruito per recuperare gli attributi aggiuntivi prodotti dalla AA.

Questi **attributi**, poi, devono essere correttamente **gestiti dall'applicazione** federata.

- L'applicazione, ad esempio, deve assegnare gli utenti ai gruppi corretti sulla base di quanto specificato dagli attributi di autorizzazione.

Un esempio pratico

GARR eroga alcuni **servizi** per la federazione IDEM, tra questi:

- il wiki della federazione IDEM;
- il registry, utilizzato per gestire le entità appartenenti alla federazione.

Gli utenti di questi servizi appartengono a diverse organizzazioni (quindi provengono da **diversi IdP**).

Con una **AA**, potremmo creare un **sistema centralizzato** in grado di gestire i **gruppi di accesso** dei vari utenti!

I gruppi applicativi del Wiki

Per implementare questo caso d'uso è necessario **definire dei gruppi di accesso** in MediaWiki.

MediaWiki definisce dei gruppi standard, sempre presenti:

- **Administrators**: amministratori del wiki
- **Bureaucrats**: personale tecnico del wiki
- **Users**: utenti registrati al wiki

È poi possibile creare gruppi nuovi, a proprio piacimento.

I gruppi applicativi del registry

Il registry, implementato in IDEM, utilizza il software Jagger, che definisce 3 ruoli utenti:

- **Administrator**: amministratori della federazione
- **Member**: responsabili di uno o più IdP o SP
- **Guest**: utenti con accesso limitato.

Integrazione nella AA

Definiamo quindi una **struttura gruppi coerente in Grouper** e assegniamo i diversi utenti (anche di diverse VO) ai gruppi così creati.

In questo modo l'appartenenza di un utente a determinati gruppi viene definita in Grouper e successivamente recuperata dal wiki e dal registry durante l'operazione di autenticazione degli utenti.

Un altro esempio, Moodle

Un altro caso d'uso, è l'integrazione di Moodle alla AA di GARR.

Questo caso d'uso necessita di recuperare gruppi e attributi per l'autorizzazione **durante la fase di login**.

È inoltre necessario avere delle interfacce che permettano l'**interrogazione "off-line" di Grouper**.

- ottiene la **lista dei corsi**;
- la lista dei **professori**; e
- la lista degli **studenti** per ogni corso.

L'integrazione di Moodle – 1/3

In Grouper creeremo **un gruppo per ogni corso** che deve essere attivato nella piattaforma Moodle.

I **membri** di questi gruppi potranno quindi essere di due tipi:

1. i membri **«admin»** saranno i **professori** del corso
2. gli **altri** membri saranno gli **studenti** del corso.

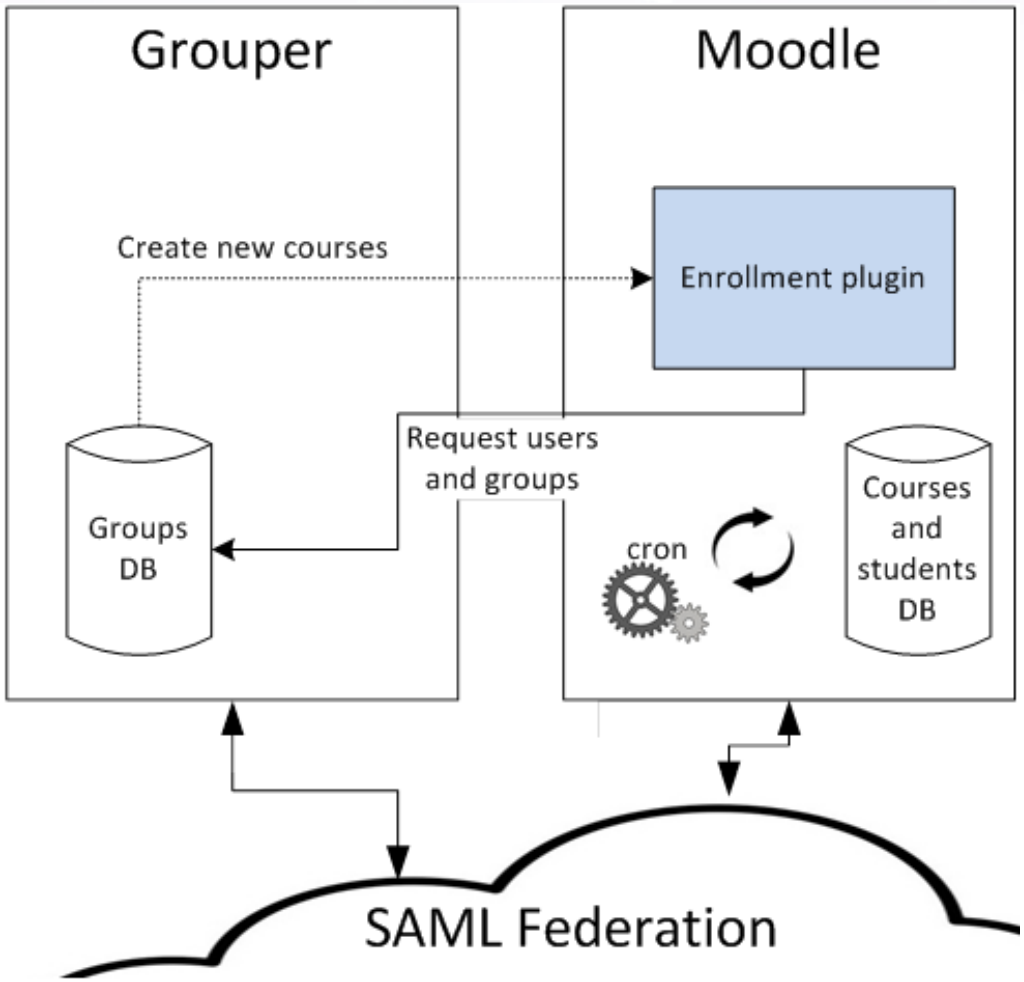
L’integrazione di Moodle – 2/3

Moodle utilizzerà quindi un **enrollment plugin** per recuperare le informazioni dei gruppi da Grouper.

È stato creato a questo scopo un enrollment plugin in grado di recuperare le informazioni da un **server VOOT**.

https://github.com/ConsortiumGARR/moodle-enrol_voot

L’integrazione di Moodle – 3/3



E ora?

La **GARR AA** è pronta per poter essere usata da servizi di produzione e già **supporta i servizi della federazione IDEM**.

Per chi fosse interessato, siamo disponibili a **integrare vostre applicazioni** (Wiki, Moodle) **alla nostra istanza di Grouper** per testare assieme casi d'uso reali!

Domande?

Grazie!

Andrea *Biancini* <***andrea.biancini@garr.it***>
Lalla *Mantovani* <***marialaura.mantovani@garr.it***>
Marco *Malavolti* <***marco.malavolti@garr.it***>

Cosa cambia nell'SP - Shibboleth

Per un SP shibboleth, in /etc/shibboleth/shibboleth.xml:

```
<AttributeResolver type="SimpleAggregation" attributeId="eppn">
        <Entity>https://grouper.idem.garr.it/idp/shibboleth</Entity>
</AttributeResolver>
```

Viene specificata:

- l'entityId della AA
- l'attributeId da utilizzare per identificare l'utente sulla AA

Cosa cambia nell'SP - SimpleSAML

Per un SP SimpleSamlPhp è necessario usare il modulo Attribute Aggregator. Quindi nel file config.php:

```
59 => array(
        'class' => 'attributeaggregator:attributeaggregator',
        'entityId' => 'https://grouper.idem.garr.it/idp/shibboleth',
        'attributeId' => 'urn:oid:1.3.6.1.4.1.5923.1.1.1.6',          //eppn
),
```

Viene specificata:

- l'entityId della AA
- l'OID dell'attributo da utilizzare per identificare l'utente sulla AA