ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

CESIA | CENTRO SERVIZI INFORMATICI DI ATENEO

Autorizzazione basata sugli attributi dentro le organizzazioni e oltre

Giacomo Farneti

Workshop congiunto INFN CCR - GARR 2012

16 Maggio 2012

Sommario

- ✓ L'Università di Bologna
  - ✓ Chi siamo
  - ✓ I nostri servizi web
- ✓ Migrazione da altri sistemi (WS)
  - ✓ Autorizzazione tramite WS
  - ✓ Autorizzazione tramite Single Sign-On
  - ✓ Autorizzazione in federazione IDEM
  - ✓ Mappatura degli attributi autorizzativi
- ✓ Ciclo di vita delle utenze

L'Università di Bologna: chi siamo

IdM: Directory Service basato su Active Directory

316.395	Studenti
14.653	Dipendenti (Docenti + Personale TA)
8.264	Dottorandi
6.200	Esterni
1.719	Unità organizzative
12.111	Gruppi di sicurezza per la profilazione

IdP: Active Directory Federation Services 2.0

Nella federazione GARR da Agosto 2010

L'Università di Bologna: i nostri servizi web

- ✓ Portale web (www.unibo.it) per studenti, docenti e personale
- ✓ Applicazioni web per servizi agli studenti (e-mail, iscrizioni ad esami, pagamento tasse, ...) e personale (stipendi, presenze, portale intranet, ...)
- ✓ Applicazioni di dipartimenti e facoltà, che hanno un buon livello di indipendenza dall'amministrazione centrale
- ✓ Applicazioni sviluppate da strutture esterne all'Ateneo
- ✓ Migrazione di autenticazione e autorizzazione da WS a SSO

Autorizzazione tramite WS

Approccio tramite WS:

- ✓ Le applicazioni accedono a tutti gli attributi dell'utente messi a disposizione dal WS
- ✓ Accesso superfluo a dati riservati
- ✓ Autorizzazione basata sull'analisi dei gruppi di appartenenza dell'utente
- ✓ Lo sviluppatore spesso interpreta i dati, potenzialmente anche in modo sbagliato (ad es. alcune applicazioni utilizzano la posizione dell'utente nella Directory per la profilazione)

Rilasciati 125 account applicativi per utilizzo WS di autenticazione (2005-2011)

Autorizzazione tramite SSO

Approccio tramite SSO:

- ✓ L'applicazione riceve solo informazioni qualificanti sull'utente
- ✓ L'applicazione riceve solo i dati strettamente necessari ai fini dell'identificazione e della profilazione dell'utente
- ✓ L'autorizzazione è basata su attributi che identificano il ruolo (o i ruoli) dell'utente
- ✓ Le regole di autorizzazione sono trasparenti al servizio web
- ✓ In caso di modifica di un gruppo (spostamento, cambio nome, applicazione di nuove policy) è sufficiente aggiornare le regole dell'IdP senza l'intervento del programmatore

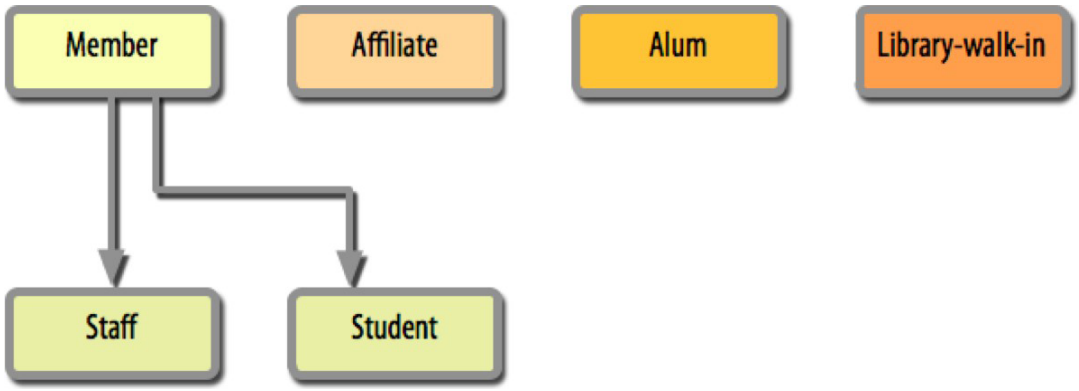
Attualmente 52 applicazioni già integrate in SSO:

UNIBO 32

Federazione IDEM 20

Autorizzazione in federazione IDEM

In federazione il principale metodo di autorizzazione è l'analisi dell'attributo **eduPersconScopedAffiliation** per la determinazione del tipo utente:



Ogni organizzazione può seguire le specifiche tecniche per la determinazione di questo attributo fornite dal GARR, che contengono le corrispondenze tra le categorie note e le relative affiliazioni.

Mappatura degli attributi autorizzativi

	Staff	Student	Alumn	Affiliate	Member
Personale docente	X				X
RAM e PAM	X				X
Docenti a contratto	X				X
Personale tecnico-amministrativo	X				X
RUP e RAO					–
Personale TA ab. PEC					–
Contrattisti/assegnisti	X				X
Accreditati interni	X				X
Docenti cessati				X	X
Altri dipendenti cessati (transitorio)				X	X
Altri dipendenti cessati (evoluzione)					–
Dottorandi	X	X			X
Studenti incoming		X			X
Specializzandi		X			X
Laureati frequentatori		X			X
Studenti attivi		X			X
Studenti cessati con titolo			X		X
Studenti preiscritti					–

Ciclo di vita delle utenze

L'Università di Bologna gestisce il provisioning/deprovisioning degli utenti e dei relativi attributi in base al **Decreto Rettorale 271/2009 (Testo Unico sulla Privacy e sull'Utilizzo dei Sistemi Informatici)**.

Il ciclo di vita degli utenti prevede gli stati:

- ✓ *preiscrizione* (solo per gli studenti)
- ✓ *attivazione* dell'utenza (provisioning)
- ✓ *deprovisioning* (costituito da: *cessazione* immediata, *disabilitazione* dell'account dopo 1 mese, *cancellazione* della mailbox dopo 6 mesi)

Come gestire le autorizzazioni degli utenti in fase di passaggio da uno stato all'altro? Attraverso un attributo dell'utente che viene restituito da SSO per la determinazione dello stato attuale.

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Domande?

CeSIA – Centro per lo Sviluppo e Gestione Servizi Informatici d'Ateneo

Mailing List di supporto al Single Sign-On

cesia-sso-support@unibo.it

www.unibo.it