Università di Padova

Rinnovare l'Identity Management con Shibboleth e Esse3

Stefano Zanmarchi
stefano.zanmarchi@unipd.it

Carlo Manfredi
carlo.manfredi@unipd.it

Secondo Convegno IDEM, Politecnico di Bari 10/03/10

Vincoli di progetto: l'autenticazione

- Esse3 ha due modalità di autenticazione:
  - locale: utenze e password interne a Esse3
  - esterna: Shibboleth (scelta di Unipd)
- Sono modalità esclusive:
  - non è implementata la *Shibboleth lazy session*

Esse 3 *non* consente di autenticare alcuni utenti localmente ed altri mediante SSO.

Vincoli di progetto: l'autorizzazione

La home page di Esse3 presenta due pulsanti:

- "Accedi": per utenti già in anagrafe di Esse3
- "Registrati": per utenti non in anagrafe

Esse3 *non* autorizza ad utenti non registrati l'accesso alle proprie funzionalità :

- Accesso alla carriera
- Domanda di preimmatricolazione
- Domanda di esame di stato
- …

Utenti di Esse3

Devono quindi autenticarsi sull'Identity Provider:

- studenti, ex-studenti, docenti
  - Iscrizione/registrazione esami, visualizzazione carriera

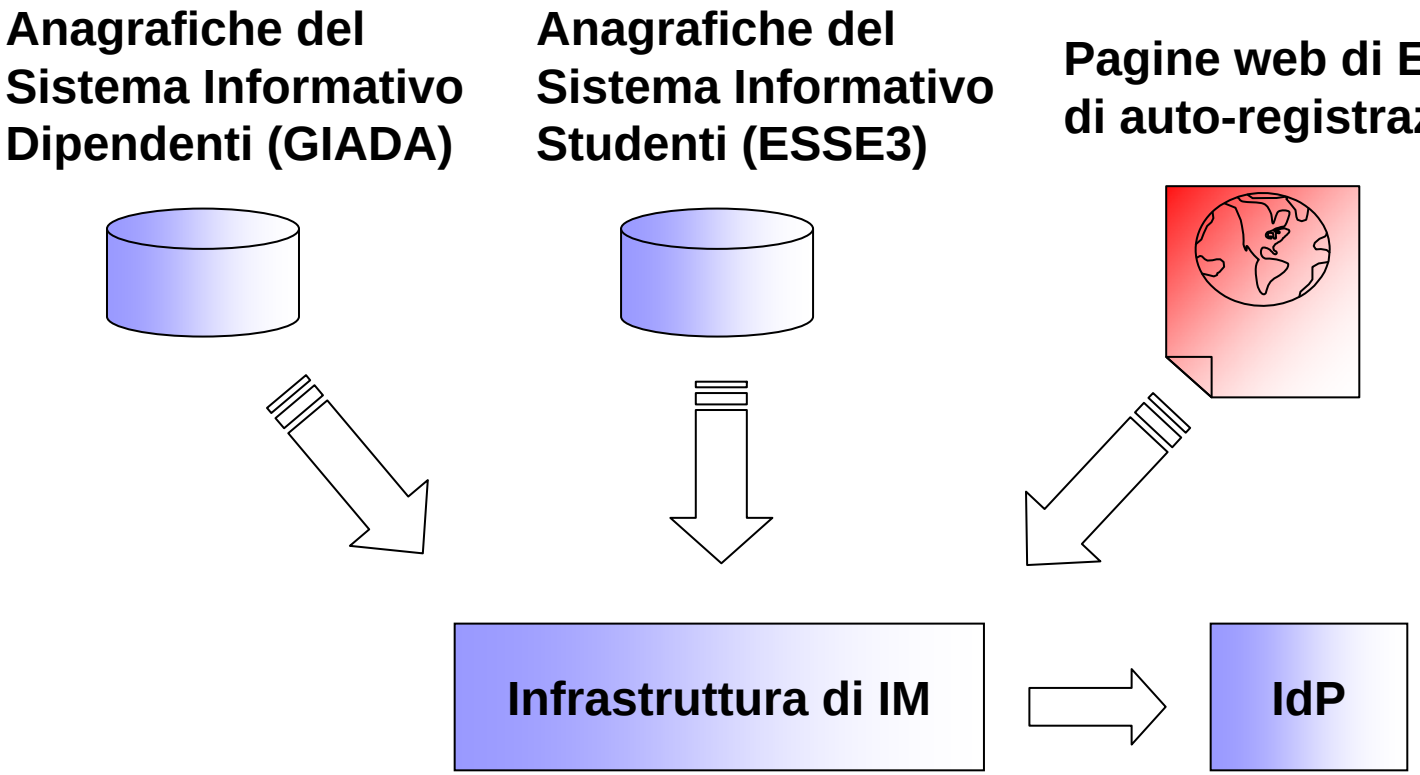
Cioè utenti già incardinati in Ateneo.

Ma anche:

- utenti sconosciuti:
  - preimmatricolazioni, responsabili di tirocinio,…

Fonti dati anagrafici

L'infrastruttura di Identity Management sottostante l'Identity Provider viene alimentata da:



Credenziali di accesso 1

L'Università di Padova ha scelto come credenziali:

- *Username* ◄ mail istituzionale, due domini:
  - @unipd.it per docenti (e dipendenti)
  - @studenti.unipd.it per studenti
- *Password* ◄ password della mail istituzionale

Lo username viene mantenuto anche quando l'utente perde la casella di posta:

- Attuali studenti quando chiuderanno la carriera
- Ex-studenti

Credenziali di accesso 2

Per chi non ha (avuto) diritto a una casella:

- Username= numero@unipd.it

  (es 12345678@unipd.it)

Assegnato a:

- registrati in Esse3
  - ricevono un codice attivazione pwd alla registrazione
- studenti carriera chiusa pre-mail
  - il codice attivazione pwd è il CF

Interfacce di Esse3

Esse3 espone due interfacce:

- Web (studenti, dipendenti e semplici registrati)
  - domande (immatricolazione, esami stato,…)
  - iscrizione esami
  - registrazione esami

è il SP shibbolettato (apache + mod_shib)

- Client (segreterie)
  - accettazione domande (immatricolazione, esami stato,…)
  - accesso alle carriere

L’external_id

- L’external_id è l’identificativo utente condiviso da Esse3 e dall’IdP. È quindi contenuto:
  - in anagrafica di Esse3
    (può essere associato a più carriere)
  - in una tabella attributi dell’IdP
    (può essere associato a più username)
- Generato da Unipd (unico per ogni utente)
- Passato dall’IdP come attributo al SP Esse3 quando l’utente s’è autenticato

L’accesso all’interfaccia web via SSO

1. L’utente clicca su “ACCEDI”
2. Viene diretto all’IdP
3. Si autentica con lo/gli username a disposizione:
   - Mail istituzionale (anche più d’una) e/o
   - Id numerico (es. 12345678@unipd.it)
4. L’IdP passa al SP Esse3 l’external_id
5. Esse3 lo fa accedere alla/e carriere associate

IdP:		ESSE3:
mario.rossi@unipd.it		carriera A
m.rossi@studenti.unipd.it	external_id	carriera B
12345678@unipd.it	(es: 25417411)	carriera C

Generazione dell'external_id

L'external_id è generato di Unipd ed è già in anagrafe di Esse3 prima dell'accesso utente.

Ma allora:

quando è stato inserito in anagrafe di Esse3?

- alla registrazione (web) dell'utente in Esse3
- generato da interfaccia pl/sql (il "**bocchettone-generazione**")

Il bocchettone-generazione

Alla registrazione (web) in Esse3:

- L'utente riempie una form coi propri dati
- Esse3 consulta il bocchettone-generazione:
  - Input: CF
  - Output:
    - external_id (es: 25417411)
    - Username (numerico: **12345678@unipd.it**)
    - codice attivazione password
- Esse3 salva in anagrafe l'*ext_id* e passa *username* e *codice attivazione password* all'utente
- L'utente attiva la password (procedura web) e può accedere a Esse3

Il bocchettone-generazione

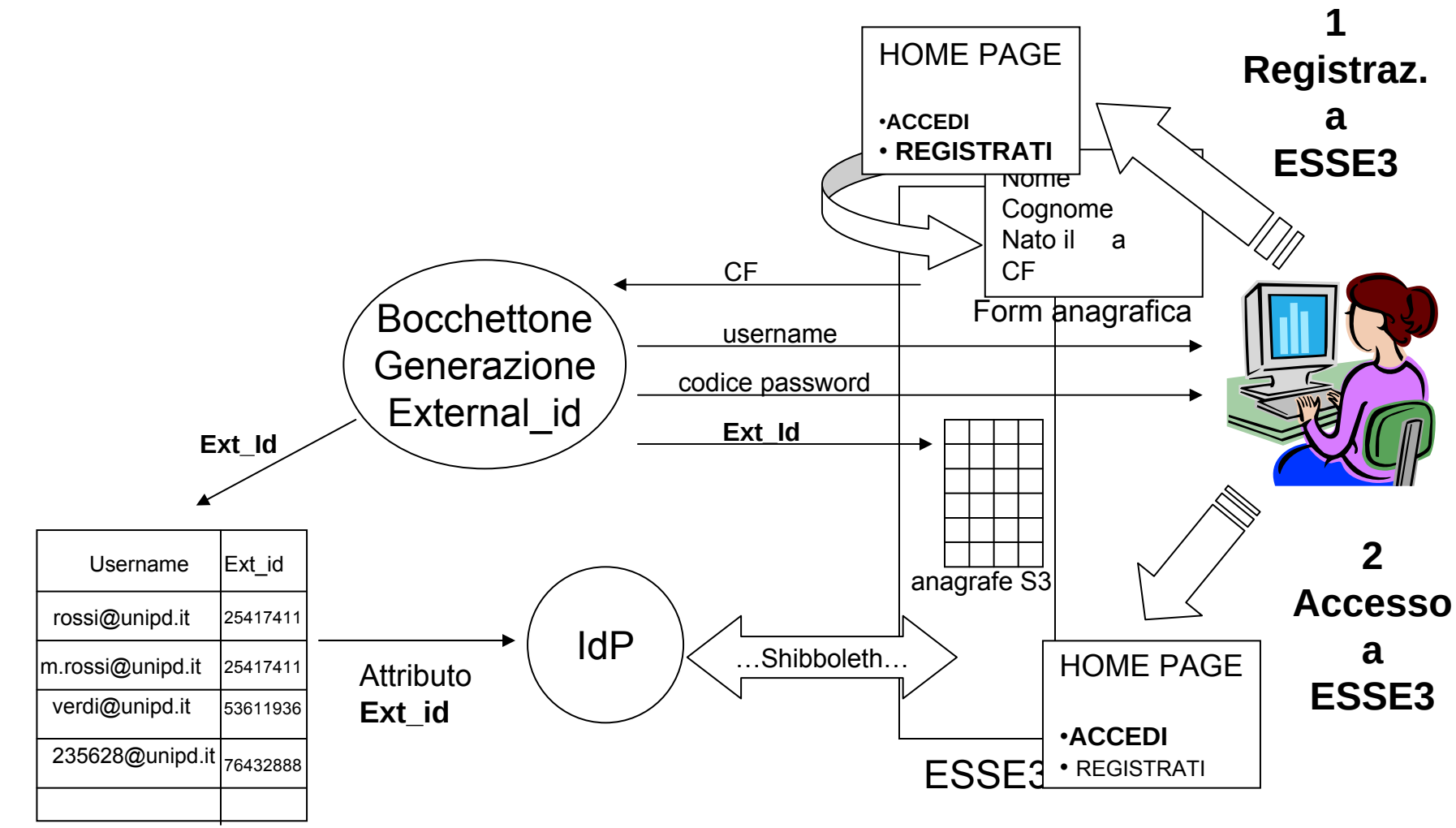


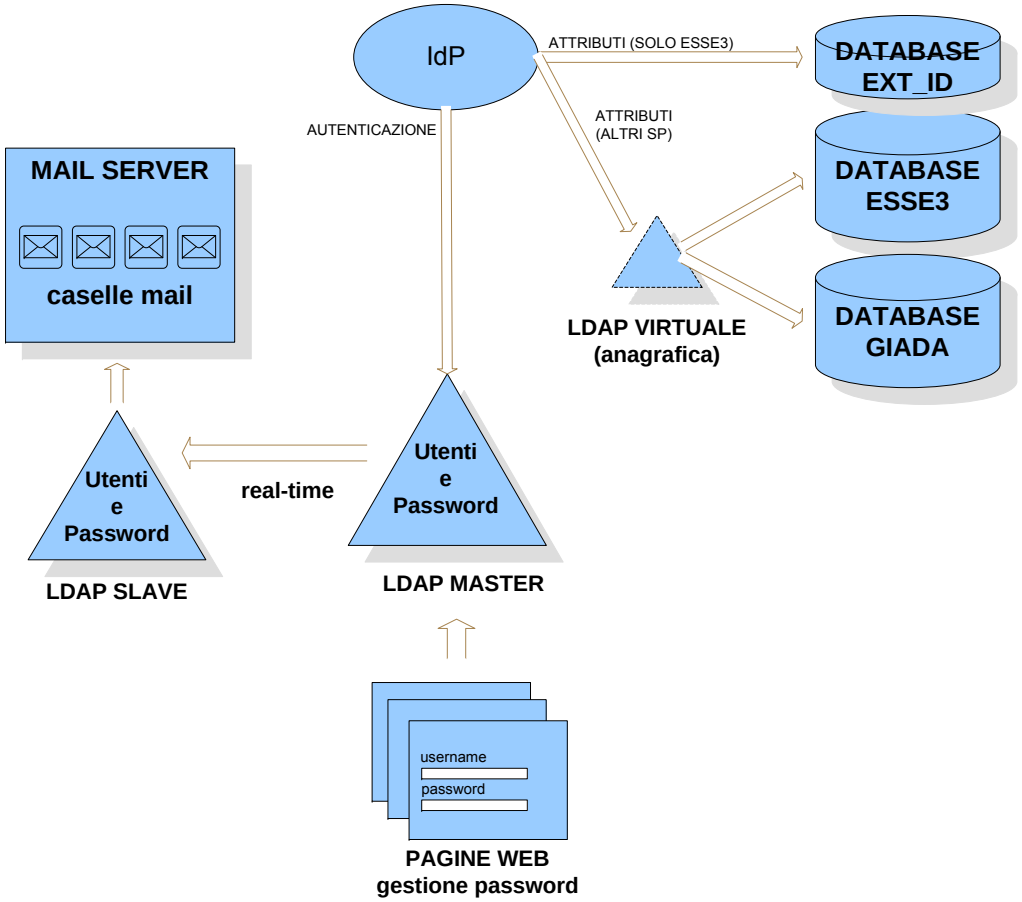
Tabella associativa

Il bocchettone-incardinamento

- All'immatricolazione (via client):
  - l'utente riceve la mail che sostituisce l'Id numerico
  - l'external_id resta invariato.

  Come?
- Esse3 invoca il **bocchettone-incardinamento**:
  - *Input*: external_id, nome, cognome, CF
  - *Output*: la mail (m.rossi @studenti.unipd.it)
  - *Azione*: update in tabella associativa da numerico a mail
- Per Esse3 è solo un maquillage dello username

Schema complessivo AuthN & AuthZ



Componenti infrastrutturali

- Infrastruttura SP Esse3
  - reverse proxy
  - apache_mod_shib
  - Esse3:
    - Tomcat
    - Jboss
  - RDBMS: Oracle
  - LDAP: Openldap
  - Virtual directory: Penrose:
    - eliminati i problemi di provisioning e di sincronizzazione dei dati
    - massima flessibilità: mapping attributi, utenti di test, ospiti non in anagrafica,…

Domande???