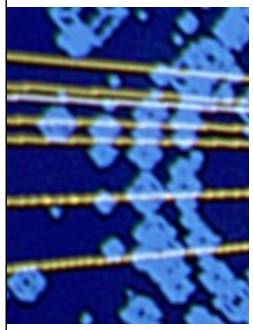
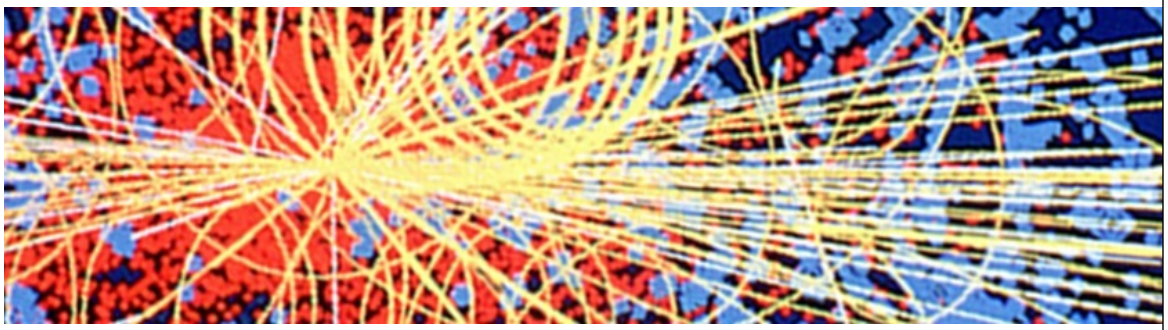
Workshop GARR
Calcolo e storage distribuito

Authentication a authorization federate nelle cloud

Estensioni a Shibbleth per l'applicazione in contesti di cloud computing



INFN
Istituto Nazionale
di Fisica Nucleare



Roma, 29.11.2012

Andrea Biancini (INFN Milano Bicocca)
Luca Prete, Simon Vocella (Consortium GARR)

Agenda

- Introduzione
- Sperimentazioni svolte
- Conclusioni

Shibboleth & IDEM

- «Federazione IDEM: una soluzione unica per accedere alle risorse online [web-based]».
- SSO attraverso username+password.
- Principi generali:
  - diffusione nella comunità (con diversi IdP e SP)
  - uniformità di tecnologie e schemi di utilizzo

Shibboleth nel contesto cloud

- Una soluzione cloud in ambito università e ricerca dovrebbe porsi l'obiettivo di proseguire ed estendere i modelli di federazione esistenti (facendo leva sulle federazioni d'identità).

- Vi sono alcune limitazioni generali, tuttavia:
  - Le cloud possono anche fornire risorse non fruibili via browser. In questo caso il meccanismo standard di Shibboleth (che è basato sul web) non offre soluzioni adatte a tale esigenza.
  - In ambito cloud sono emersi protocolli standard che disciplinano anche gli aspetti di autenticazione e autorizzazione. Shibboleth deve essere in grado di offrire interfacce compatibili a questi standard.

Estensioni realizzate

① Estensione di IDEM ad applicazioni non web-based che quindi non si utilizzano un browser web (API per Java e Phyton).

② Estensione di IDEM per l'autenticazione di utenti su sistemi Linux (tramite PAM e NSS).

③ Estensione per supportare differenti schemi di autenticazione (non basati su username+password).

① Scopo e benefici

- **Benefici**: grazie a queste estensioni la federazione IDEM è in grado di integrare nativamente l'autenticazione Shibboleth in famiglie di applicazioni attualmente "escluse".

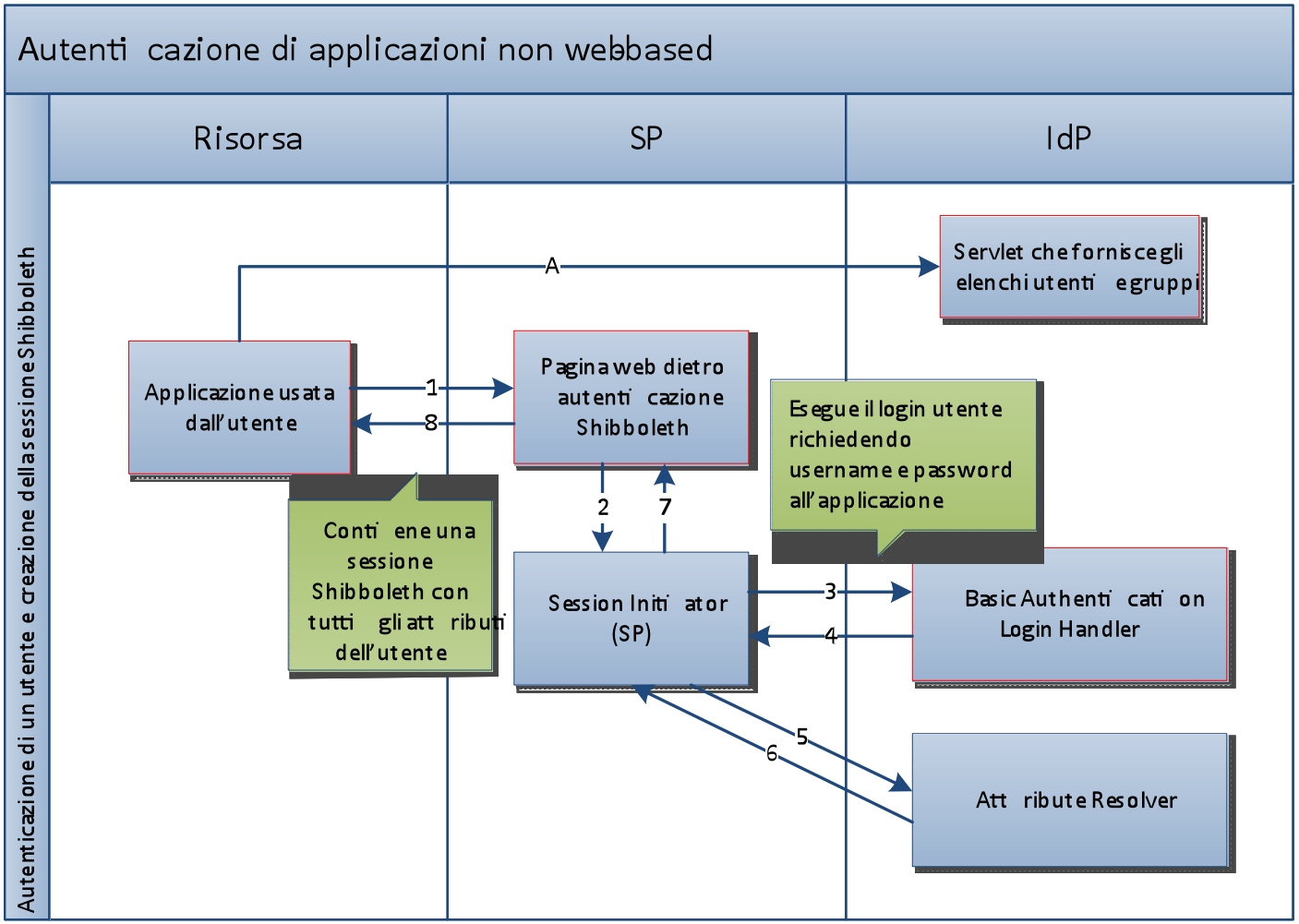
- **Esempio**: attraverso le API realizzate è possibile avere applicazioni client scritta in Java o in Python che effettuano un'autenticazione nativa tramite Shibboleth (con una gestione completa degli attributi della sessione utente).

② Scopo e benefici

- **Benefici**: grazie a queste estensioni la federazione IDEM è in grado di essere usata come strumento di autenticazione per macchine Linux (login come utente del sistema).

- **Esempio**: il problema ci si è presentato quando per il progetto GarrBox abbiamo pensato come includere in Shibboleth interfacce a blocchi per i filesystem (CIFS e NFS), le quali non transitano da browser web ma necessitano di appoggiarsi all'autenticazione del sistema operativo linux.

① e ② Architettura ad alto livello



(con bordo rosso le componenti sviluppate o configurate ad-hoc)

① e ② Modifiche apportate

- **IdP**: deploy di una servlet per fornire gli elenchi di utenti e gruppi da LDAP e attivazione (tramite configurazione) del Basic Authentication Login Handler.

- **SP**: deploy di librerie per PAM (moduli di autorizzazione dei sistemi Linux) e configurazione di Shibboleth SP.

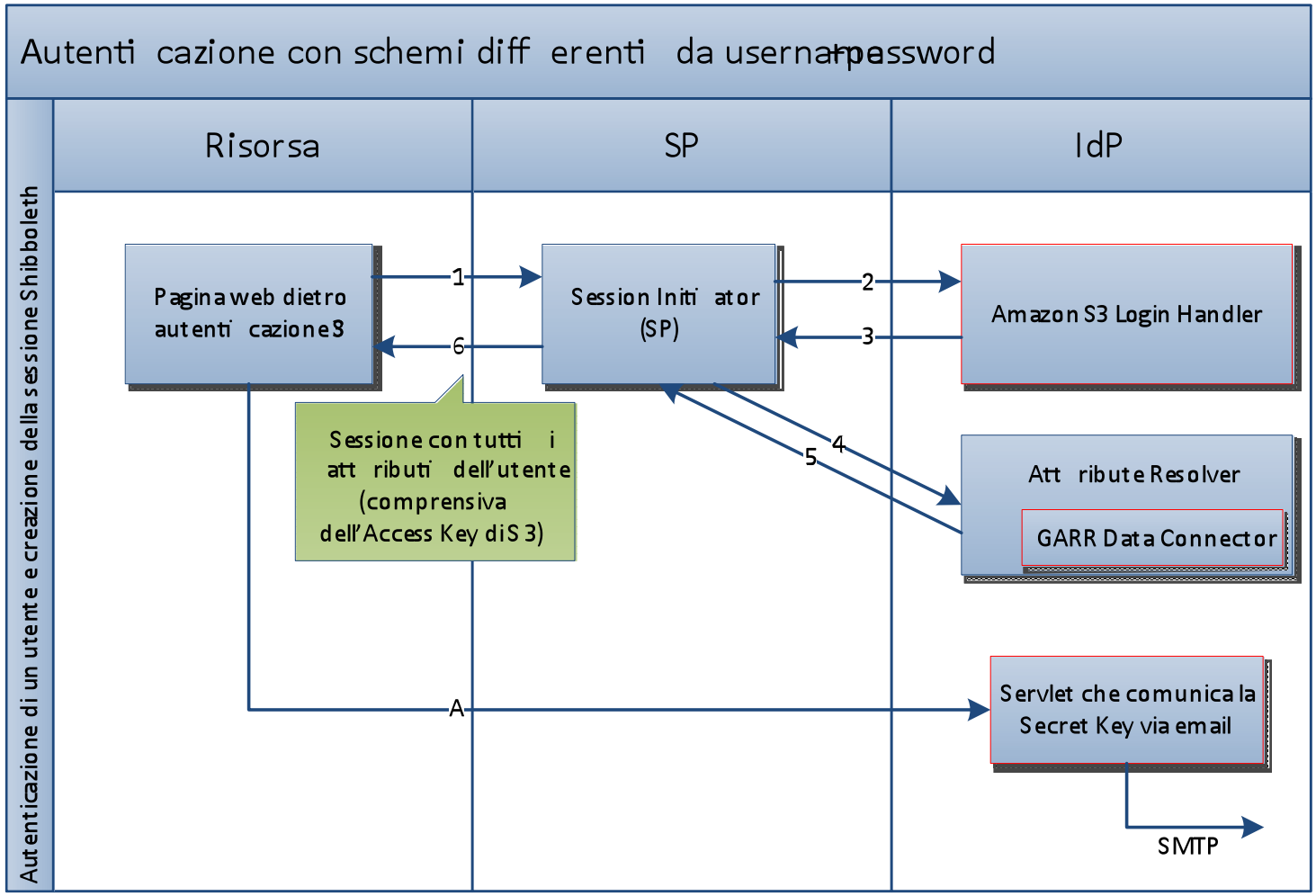
- **Applicazione**: inclusione delle librerie con le API per integrare l'autenticazione Shibboleth; per il login di macchine linux vengono forniti un modulo PAM e NSS da installare e configurare sulla macchina client.

③ Scopo e benefici

- **Benefici**: grazie a queste estensione la federazione IDEM può estendersi a includere applicazioni che usano protocolli di autenticazione sofisticati.

- **Esempio**: il problema ci si è presentato nel momento in cui per GarrBox abbiamo dovuto integrare l'interfaccia Amazon S3, che ha un suo schema autorizzativo non basato su username +password.

③ Architettura ad alto livello



(con bordo rosso le componenti sviluppate o configurate ad-hoc)

③ Modifiche apportate

- **IdP**: deploy di un LoginHandler e di un DataConnector e loro attivazione (tramite configurazione); deploy di una servlet per l'invio via posta elettronica della Secret Key all'utente.

- **SP**: modifiche solo a livello dei file di configurazione dell'SP Shibboleth.

① + ② + ③ Problemi aperti

- Attualmente le estensioni ①, ② e ③ non supportano il discovery dell'IdP tramite WAYF (possibile dopo uno sviluppo lato DS).

- Le estensioni ①, ② e ③ necessitano di un deploy (comunque abbastanza semplice) sugli IdP della federazione (peraltro il codice realizzato funziona solo sugli IdP che utilizzano il software Shibboleth sviluppato da Internet2).

- Il lavoro si è concentrato sugli aspetti di AuthN e AuthZ, non ha preso in considerazione aspetti di accounting, che invece rappresentano un elemento distintivo per le soluzioni cloud.

Conclusioni

- Una cloud per il mondo università ricerca potrebbe voler estendere schemi di federazione già realizzati negli stessi ambienti, in particolare le federazioni di identità.
- IDEM, federazione di identità GARR, per trovare applicazione in ambienti cloud deve risolvere alcuni problemi.
- Le sperimentazioni descritte in questo intervento rappresentano un tentativo, da raffinare, di superare alcune limitazioni attuali (più tecnologiche che di modello).

Fine presentazione.

GRAZIE PER L'ATTENZIONE!

① + ② + ③ Benefici per IDEM

- Le estensioni ① + ② permettono ad IDEM di allargarsi includendo nuove applicazioni.

- Le estensioni non alterano i concetti comunitari di IDEM:
  - uniformità d'accesso e di gestione degli attributi utente
  - gestione federata e distribuita dell'AAI

① Esempi di utilizzo delle API

Login da un programma Java

```
try {
    LoginContext lc = new LoginContext(
            "Shibboleth",
            new MyCallbackHandler());

    lc.login();
    System.out.println("User logged in successfully.");
}
catch (LoginException e) {          System.err.println
("Error logging in user.");
    e.printStackTrace();
}
```

Login da un programma Python

```
import shibauth

if __name__ == "__main__":
    username = raw_input('Enter username: ')
    password = getpass.getpass('Enter password: ')
    try:
        loggeduser, session =     shibauth.login(username,
password)
        print "User logged in successfully."
    except Exception, e:
        print "Error logging in user: %s" % e
```

② Esempio login da Linux

```
login as: andrea
andrea@212.189.204.232's password:
Last login: Mon Jun 11 16:20:38 2012 from omero.mib.infn.it

[andrea@cloud-mi-03 ~]$ env | grep Shib
Shib_Session_ID=_da1c55cd894a17514551fb6b3ba68c36
Shib_Authentication_Method=urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport:BasicAuthn
Shib_Application_ID=default
Shib_Session_Unique=64656661756c7468747470733a2f2f636c6f75642d6d692d30332e6d69622e696e666e2e6974
Shib_AuthnContext_Class=urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport:BasicAuthn
Shib_Session_Index=13a7536381ecfb87dfff48c8e8ed48e84ec902d76d67de6c842fc2fae36d6a30
Shib_Authentication_Instant=2012-07-16T06:07:27.534Z
Shib_Identity_Provider=http://idp-test1.mib.infn.it/idp/shibboleth

[andrea@cloud-mi-03 ~]$ echo $eduPersonScopedAffiliation
member@garr.it;student@garr.it

[andrea@cloud-mi-03 ~]$
```

③ Esempio di configurazione DragonDisk