(IDEntity Management federato per l'accesso ai servizi)

Maria Laura Mantovani
Università di Modena e Reggio Emilia
marialaura.mantovani@unimore.it

Agenda

- Identity and Access Management
- Shibboleth (overview generale)
- Il Progetto IDEM: verso la federazione italiana di AA degli atenei e degli enti di ricerca

Identity and Access Management (IAM)

Scopo:

all'interno di una organizzazione le persone giuste devono poter accedere ai servizi giusti

What is Identity Management?

- *"A set of processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities." (Burton Group)*
- **It is more than account creation, more than directories, authentication, access controls, etc.**
- **It includes policy, process, governance, trust, and new ways of thinking about I.T.**

Il passato visto dal fornitore di servizio:

- I dati delle identità venivano replicati per ogni servizio
- L'aggiunta di un nuovo servizio comportava l'aggiunta dell'intera infrastruttura di identificazione

Problemi di sicurezza:

- Replica dei dati delle identità su molti sistemi significa dover gestire la sicurezza su molti sistemi

Il passato visto dall'utente:

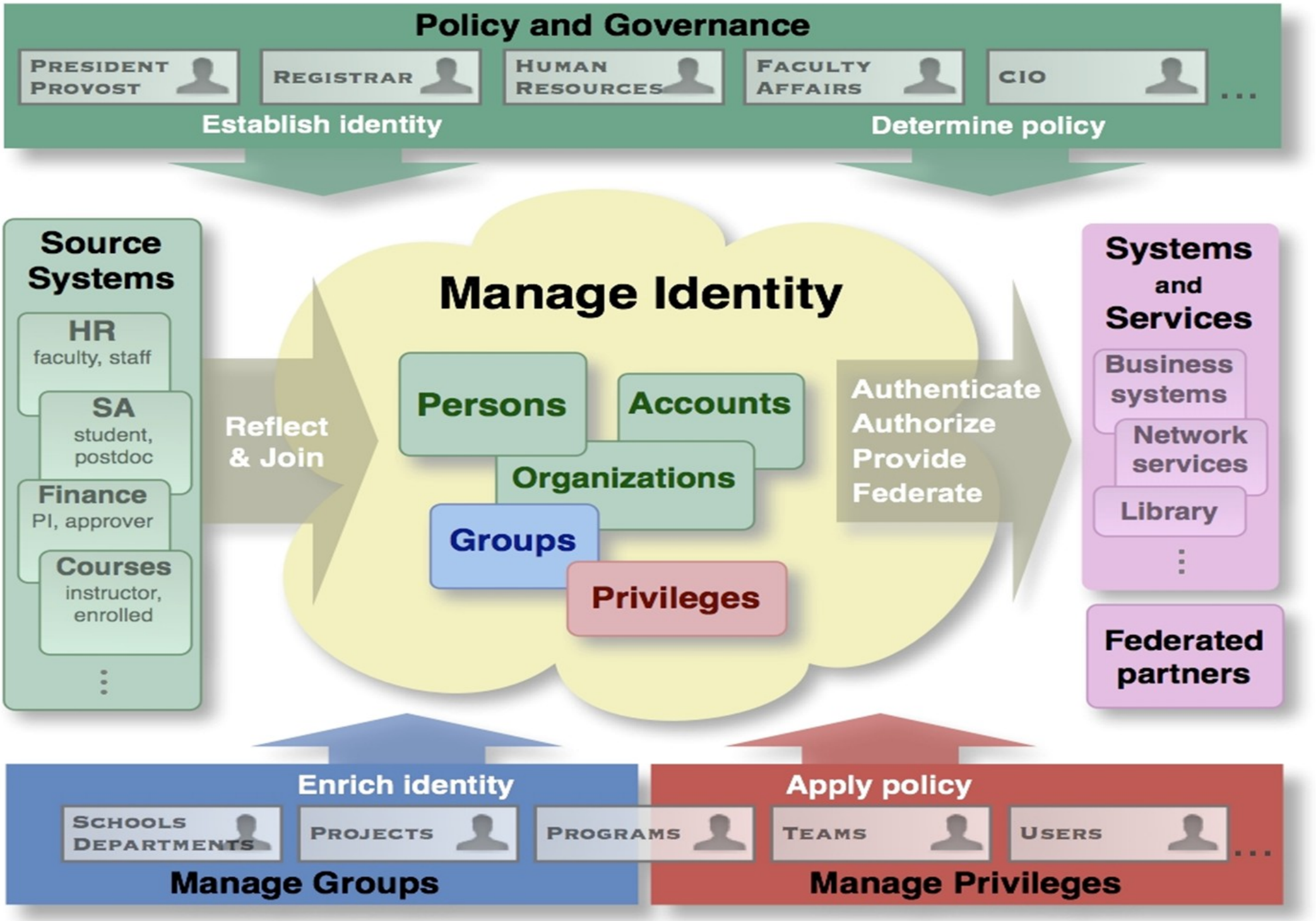
©Steve Devoti http://www.educause.edu/PeerDirectory/750?ID=141983

http://www.educause.edu/ir/library/pdf/CAMP08110A.pdf

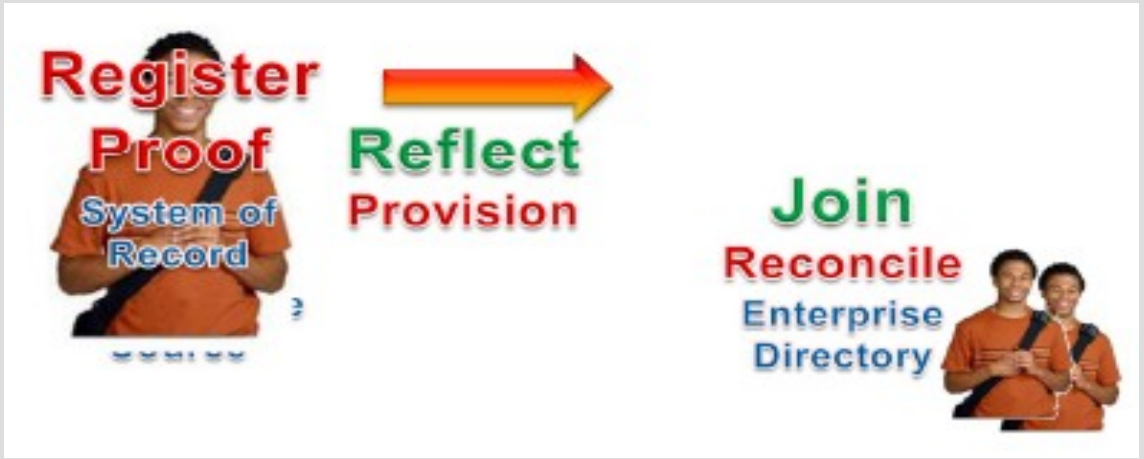
Soluzione:

- Usare lo stesso servizio di Identity and Access Management per tutte le applicazioni.
- Un solo posto da mettere in sicurezza
- Un solo posto dove applicare le procedure
- Un solo posto dove applicare le policy
- L'infrastruttura IAM viene riutilizzata ogni volta che si aggiunge un nuovo servizio

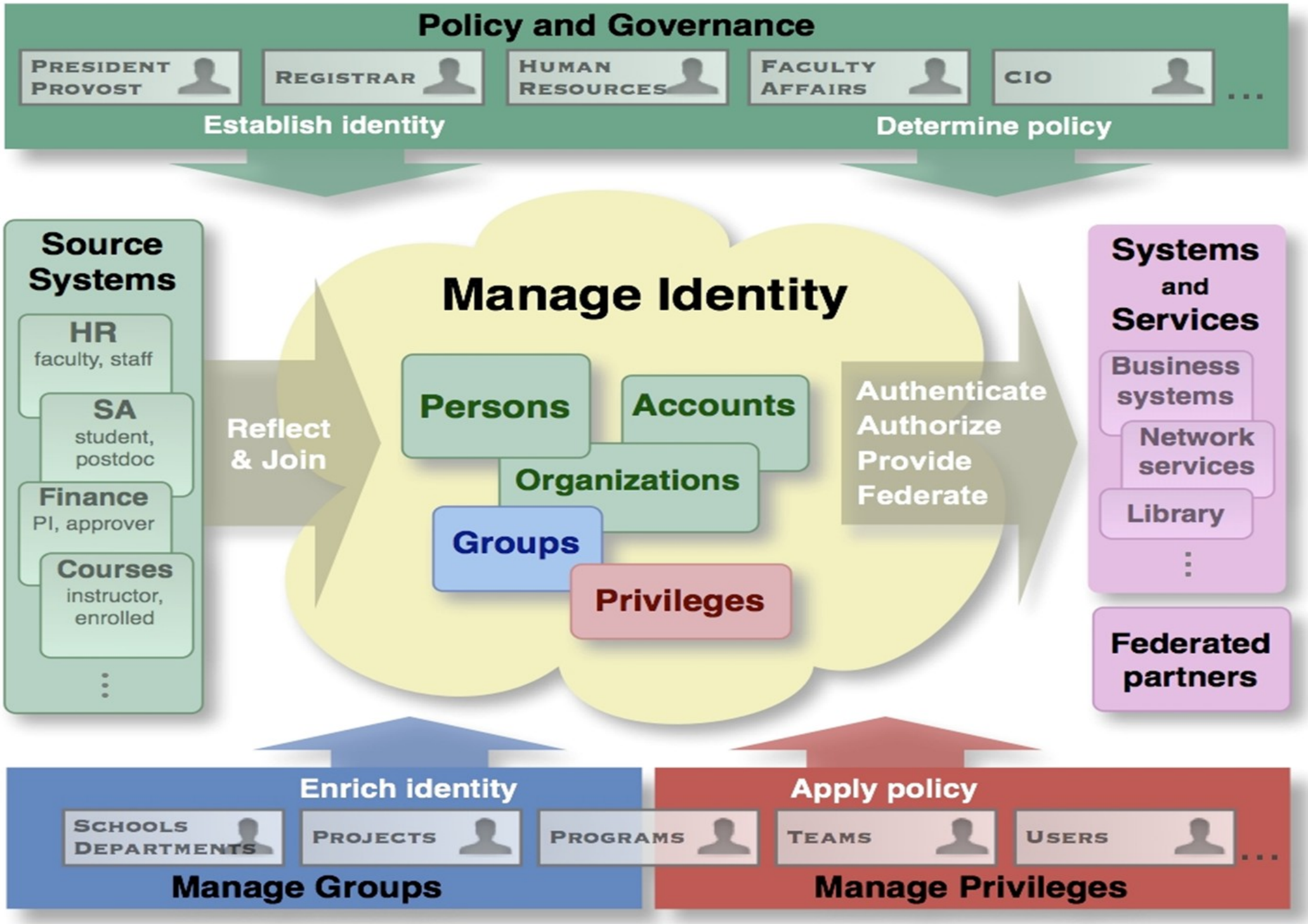
Risultato: semplificazione e sicurezza



La prima cosa da fare: prendere i dati personali dai DB esistenti e costruire le identità digitali nel sistema IAM



- Analizzare i DB esistenti, vedere quali sono autoritativi
- Decidere quali informazioni prendere e mantenere
- Consolidare (una persona può essere presente in più fonti)
- Tenere aggiornato automaticamente



Cosa si deve ottenere?

- Ogni persona identificata da una certa organizzazione è descritta da una entry (ad esempio in un directory)
- Ogni entry è costituita da **attributi**, ognuno di quali ha un nome e una certa molteplicità di valori

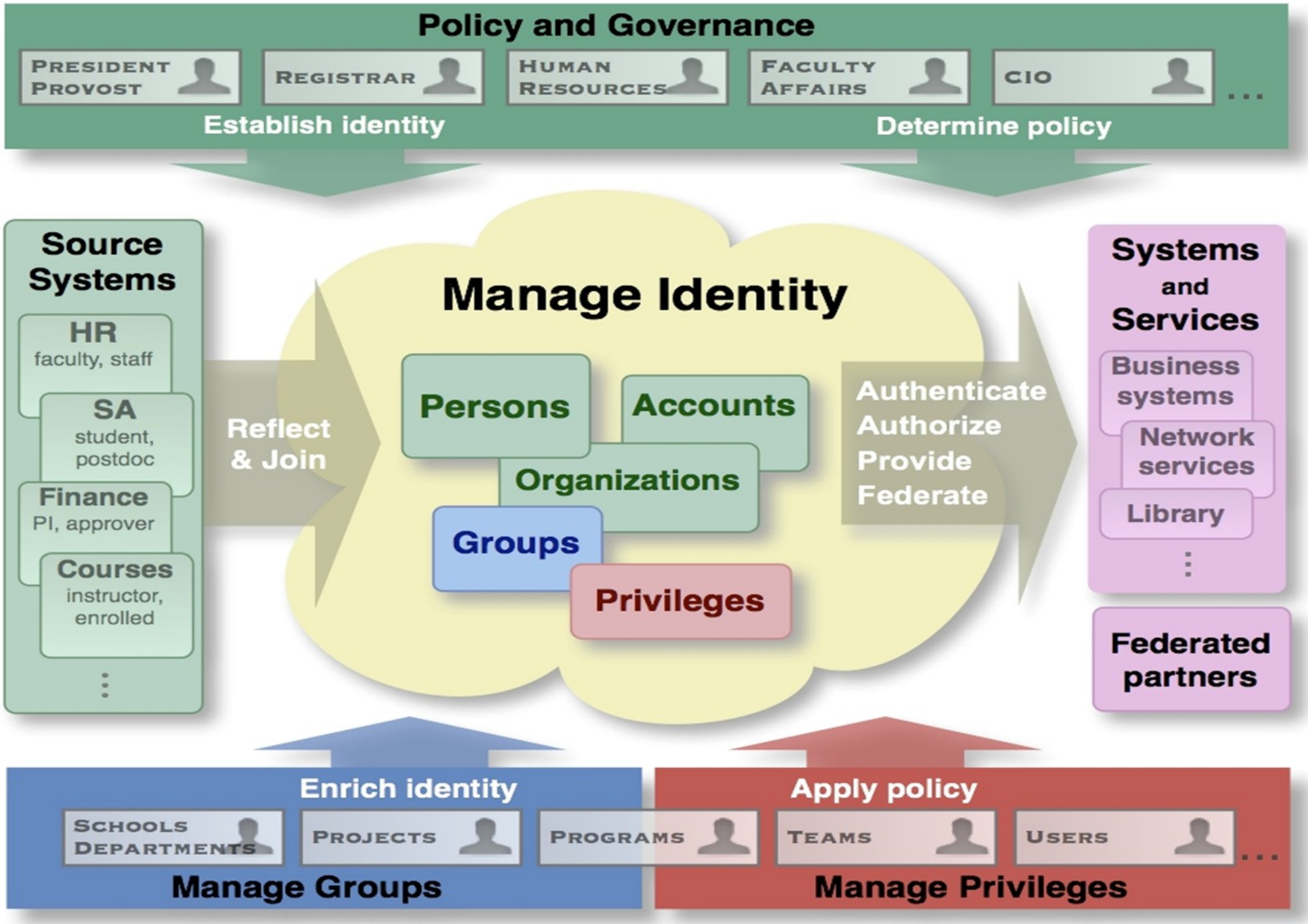
Ciclo di vita dell'identità

http://www.educause.edu/ir/library/pdf/CAMP08110A.pdf

In una seconda fase

- Enrich Identity
- Apply Policy

Esempio: un gruppo di ricerca può aver bisogno di un calendario condiviso, di una lista di distribuzione, di un wiki space. La definizione e la gestione di un unico gruppo permette l’accesso a più servizi, mediante un'unica modifica.



Benefici ottenuti dopo il consolidamento delle identità

- I decision makers possono attivare cambiamenti più velocemente (es: aggiungere un nuovo servizio; modificare i privilegi di accesso ad un gruppo di servizi)
- L'evoluzione dei requisiti si riflette nei cambiamenti che devono essere fatti solo in un posto: il sistema IAM
- Secondo EduCause (http://www.educause.edu) i costi di implementazione di nuovi servizi sono ridotti del 30%

Benefici ottenuti dopo il consolidamento delle identità

Trasparenza

- Le decisioni prese si applicano in un punto e si vedono i risultati e le conseguenze delle decisioni stesse
- Il logging è consolidato pertanto si possono applicare regole di privacy, di conservazione dei dati di auditing, si possono fare dei report, si monitora la sicurezza

Benefici ottenuti dopo il consolidamento delle identità

- Eliminato il problema del Deprovisioning relativo alla gestione delle identità in sistemi disgiunti.
- Ridotto il numero di credenziali da conoscere.
- Ridotto il carico dovuto alla disattivazione dei client che non hanno più diritto.
- L'organizzazione può modificare più velocemente i diritti di accesso basandosi sui ruoli.
- Nel processo di garantire che una persona è “quello che dice di essere” l'istituzione incrementa il suo livello di riservatezza.

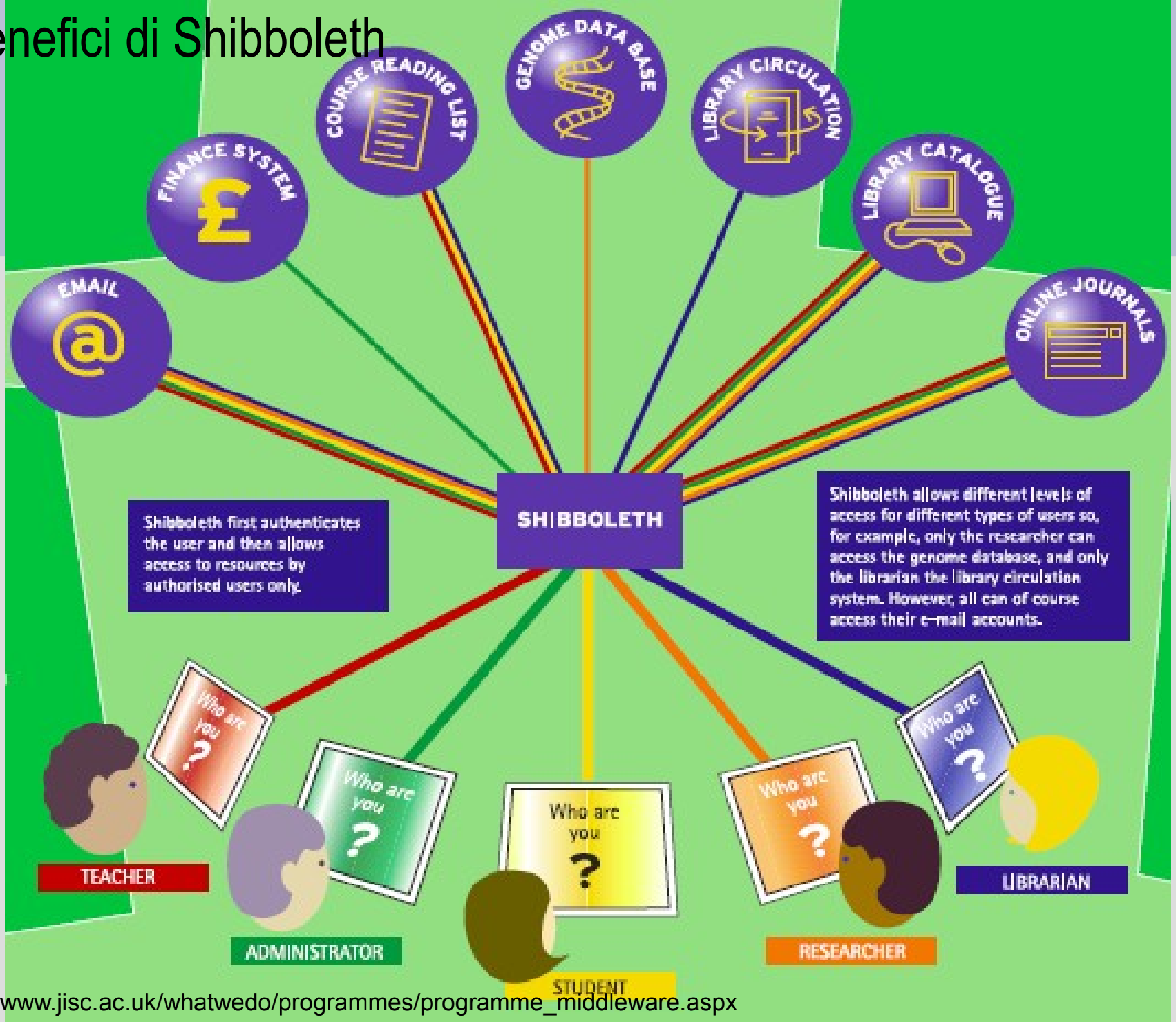
Domanda?

?

Il sistema IAM è un prerequisito per

- Un package openSource, basato su standard (SAML), di **SSO** e **autorizzazione** per il web.
- Fa leva sul sistema IAM locale per per permettere l'accesso alle applicazioni di Campus e a quelle Esterne (Costruisci e Gestisci Localmente, Accedi Globalmente)

I benefici di Shibboleth



©http://www.jisc.ac.uk/whatwedo/programmes/programme_middleware.aspx

Shibboleth.

Benefici

Per la Privacy

- Le persone possono accedere a risorse e servizi senza necessariamente fornire i propri dati personali.
- Le informazioni trasmesse sono quelle necessarie per stabilire il diritto all'accesso

Shibboleth.

Benefici

Per le istituzioni

- La persona, una volta registrata e dotata di credenziali, ha tutto quello che gli serve per accedere a tutte le risorse web alle quali è ammessa.
- L'accesso è ugualmente facile sia per le applicazioni interne al campus che per quelle esterne.
- Accesso facilitato significa migliore utilizzo delle risorse a pagamento (ad es. riviste elettroniche).

Shibboleth.

Benefici

Per i fornitori di servizi

- Garantisce l'accesso alla risorsa solo alle persone autorizzate
- Non devono preoccuparsi di mantenere le informazioni anagrafiche degli utenti
- Offrire un servizio diventa meno rischioso (non devono mantenere credenziali, né dati personali)
- I tempi di realizzazione del servizio diminuiscono
- I dati ricevuti sono sempre aggiornati

Shibboleth.

AUTENTICAZIONE

- La persona che si è presentata è quella che dice di essere?

AUTORIZZAZIONE

- OK, è lei! Ha diritto di entrare?

SINGLE SIGN-ON

- Si presenta ad un altro servizio: ha diritto di entrare? (NB: non chiedo più chi è)

Shibboleth.

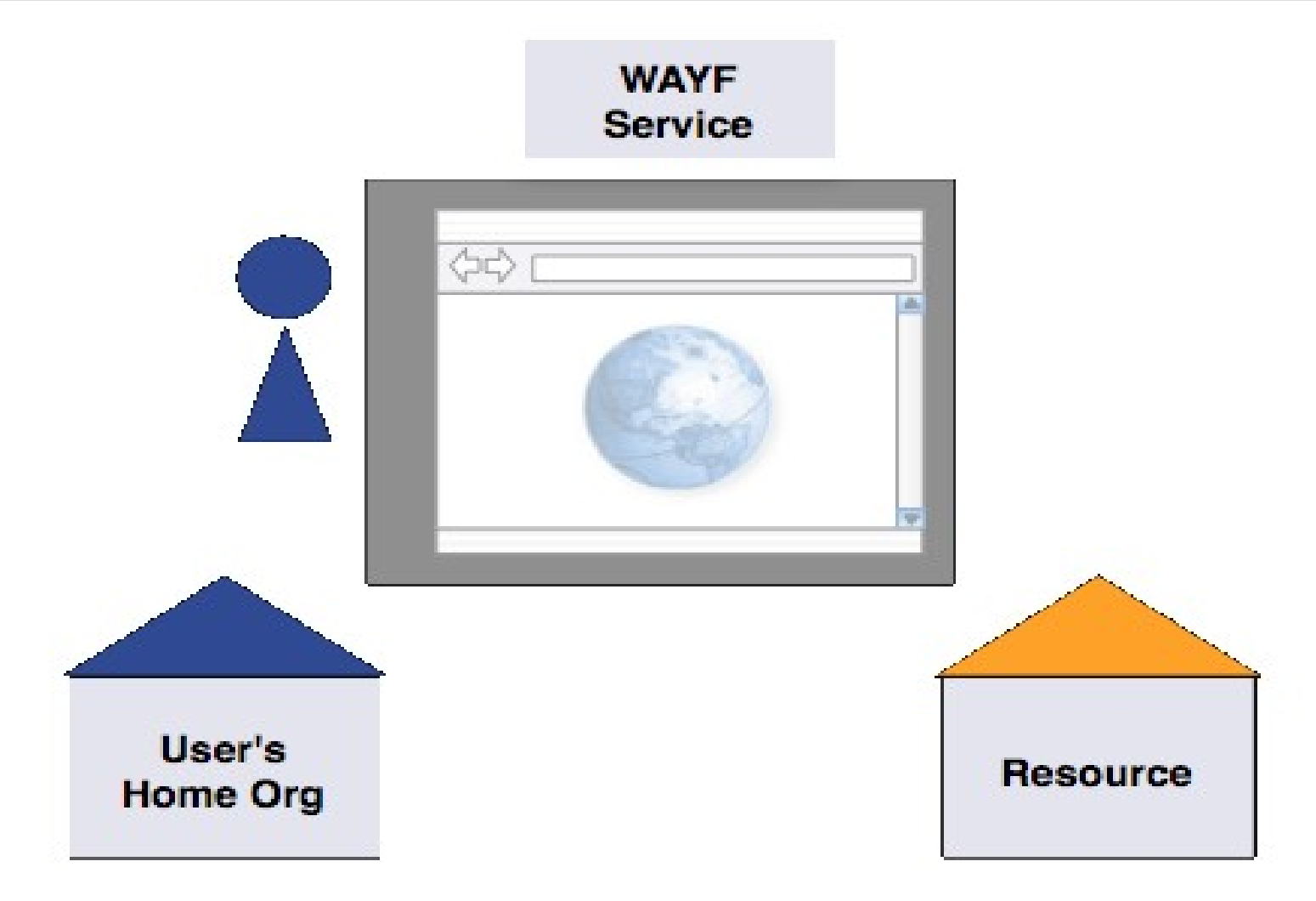
AUTENTICAZIONE

- Ho un metodo per verificare se è lei (credenziali, certificato, impronte digitali)

AUTORIZZAZIONE

- Alla persona è associata una entry con degli attributi, ogni attributo ha un nome e uno o più valori, l'autorizzazione viene concessa sulla base del valore di uno o più attributi.
- Shibboleth è un sistema per scambiare attributi in modo sicuro

Shibboleth : scenario

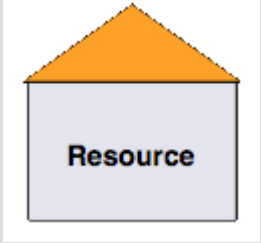


©http://www.switch.ch/aai/demo/medium.html

Shibboleth : gli attori

- l'Organizzazione di Appartenenza dell'Utente (End User Organization) che deve fornire il componente Shibboleth denominato Identity Provider (IdP)
- Dotata di un sistema IAM in cui ogni Persona è caratterizzata da ATTRIBUTI (eventualmente mappabili sugli schema Person (LDAP), eduPerson e SCHAC).
- Definisce una Attribute Release Policy (ARP), regole che permettono di decidere quali attributi e quali valori trasferire a ciascun servizio che ne fa richiesta.

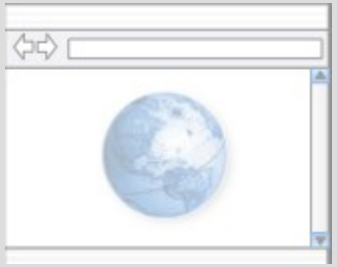
Shibboleth : gli attori



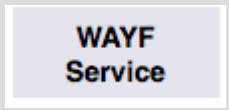
- il Fornitore di un certo servizio a cui l'utente vuole accedere il quale deve fornire il componente di Shibboleth denominato Service Provider (SP)
- Definice una Attribute Acceptance Policy (AAP), regole per decidere quali attributi ricevere (tra quelli rilasciati dall'IdP) e sulla base dei quali applicare la policy di autorizzazione.

Shibboleth : gli attori

- l’utente,

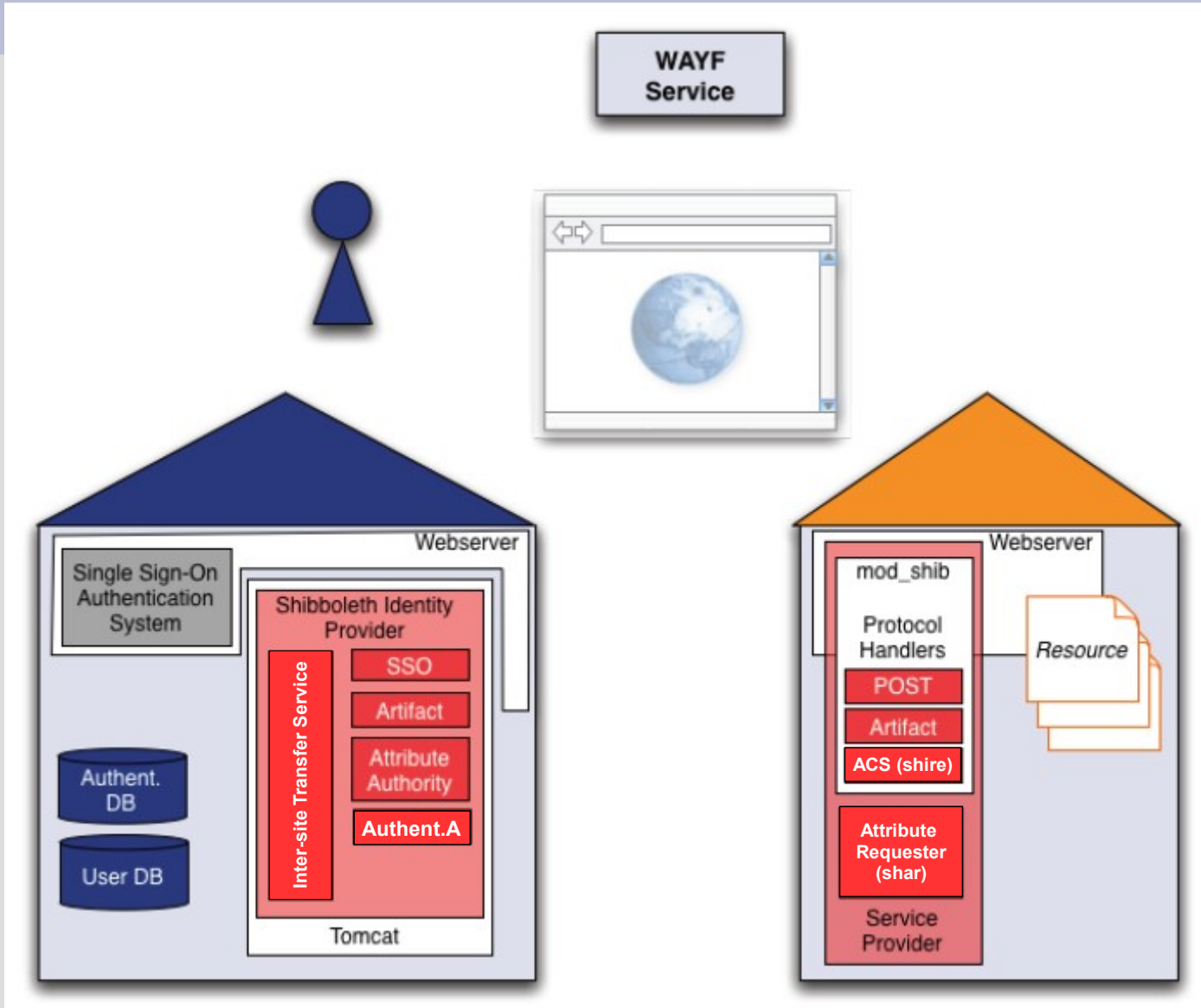


- il suo browser,

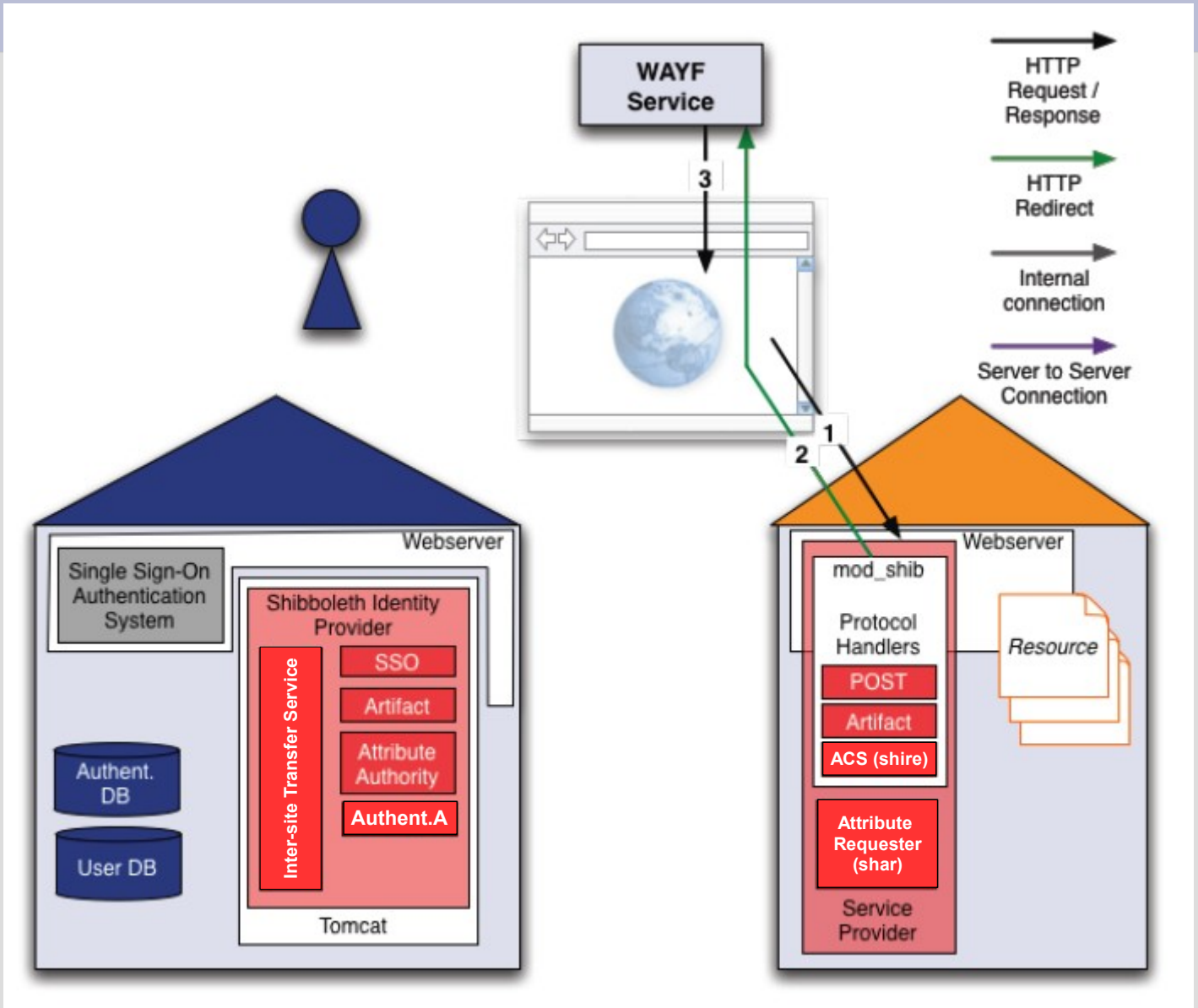


- un servizio WAYF (Where Are You From?) tipicamente offerto dalla Federazione a cui IdP e SP sono associati.

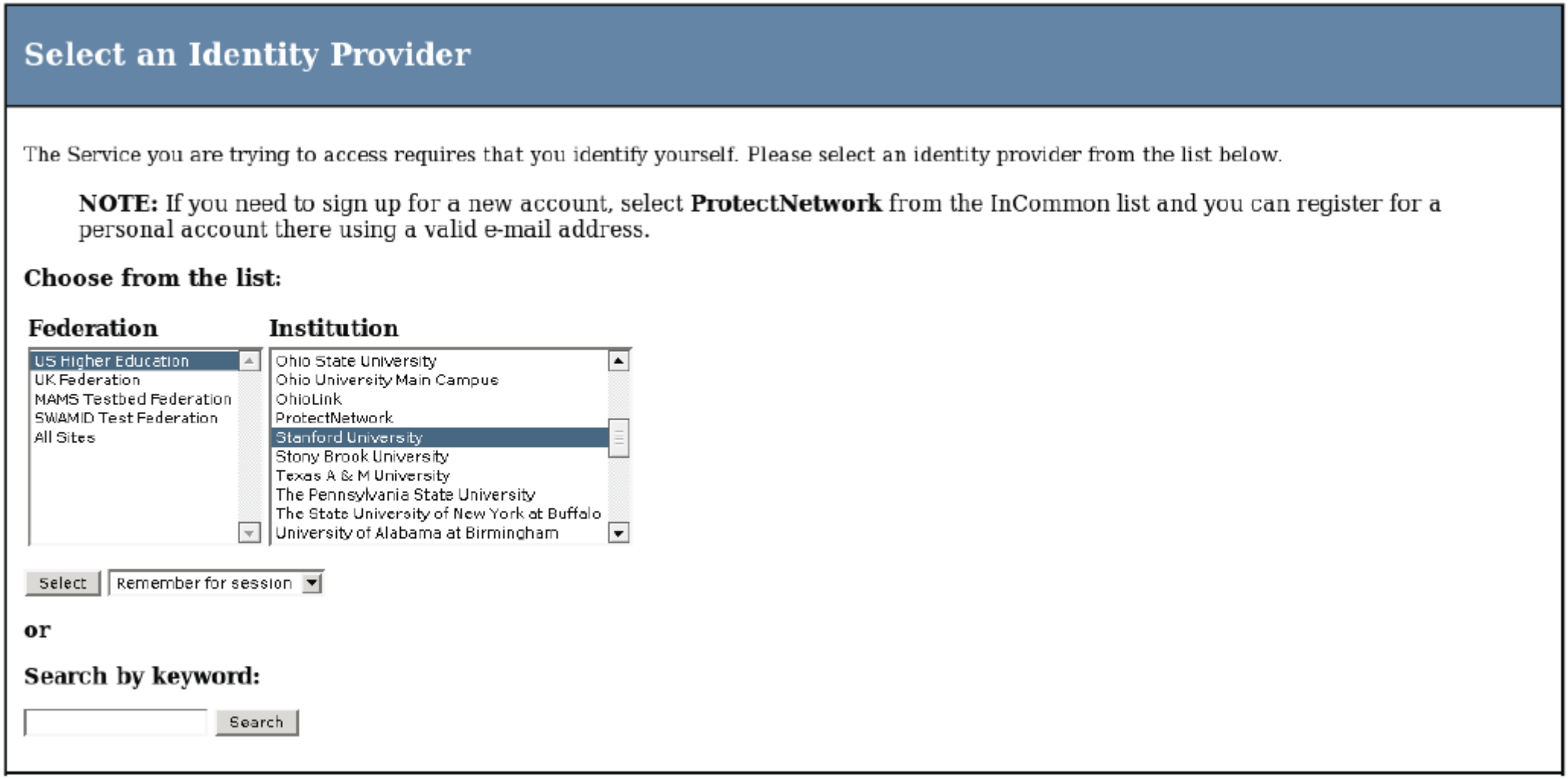
Shibboleth: scenario d'uso



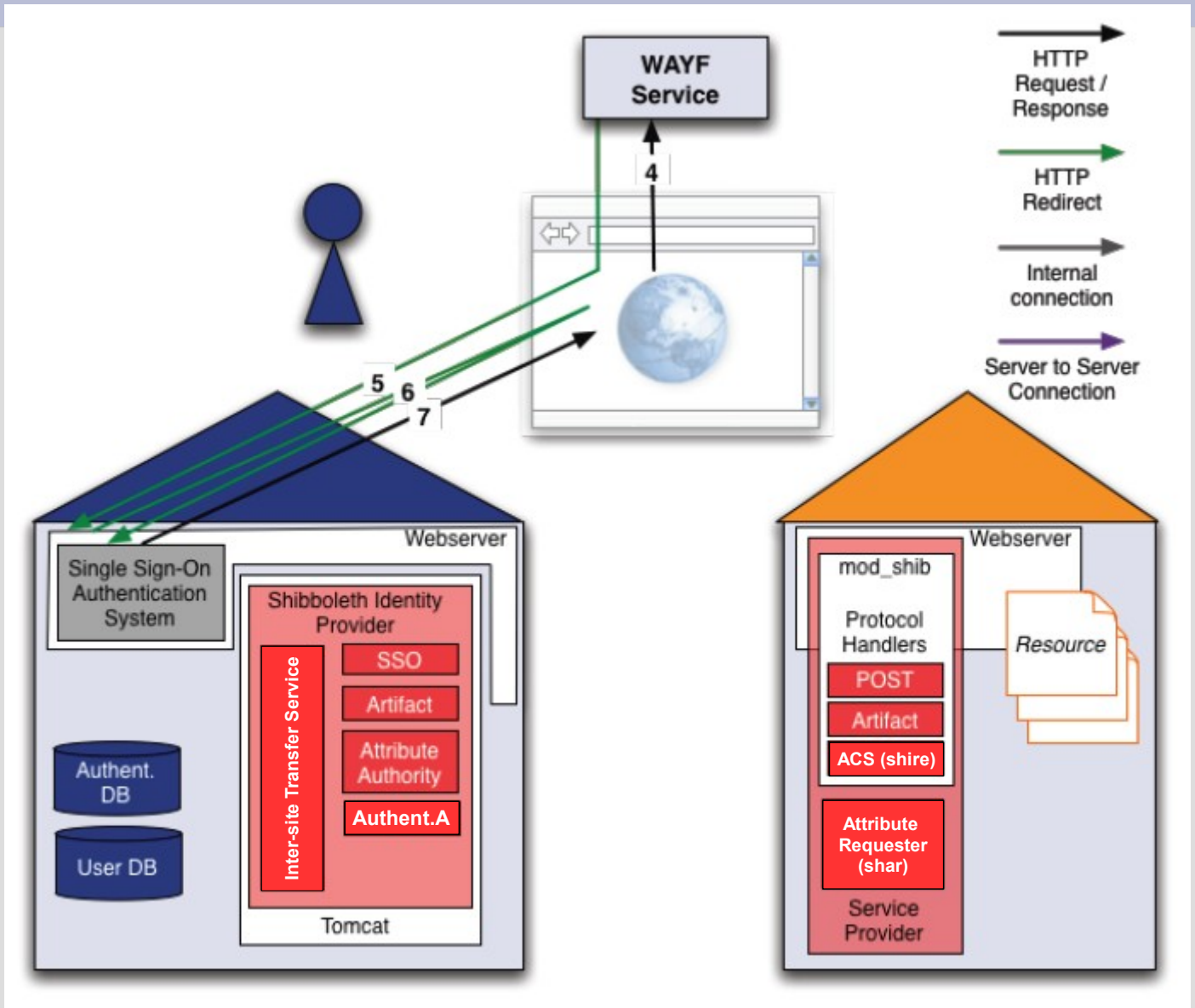
Shibboleth: richiesta risorsa

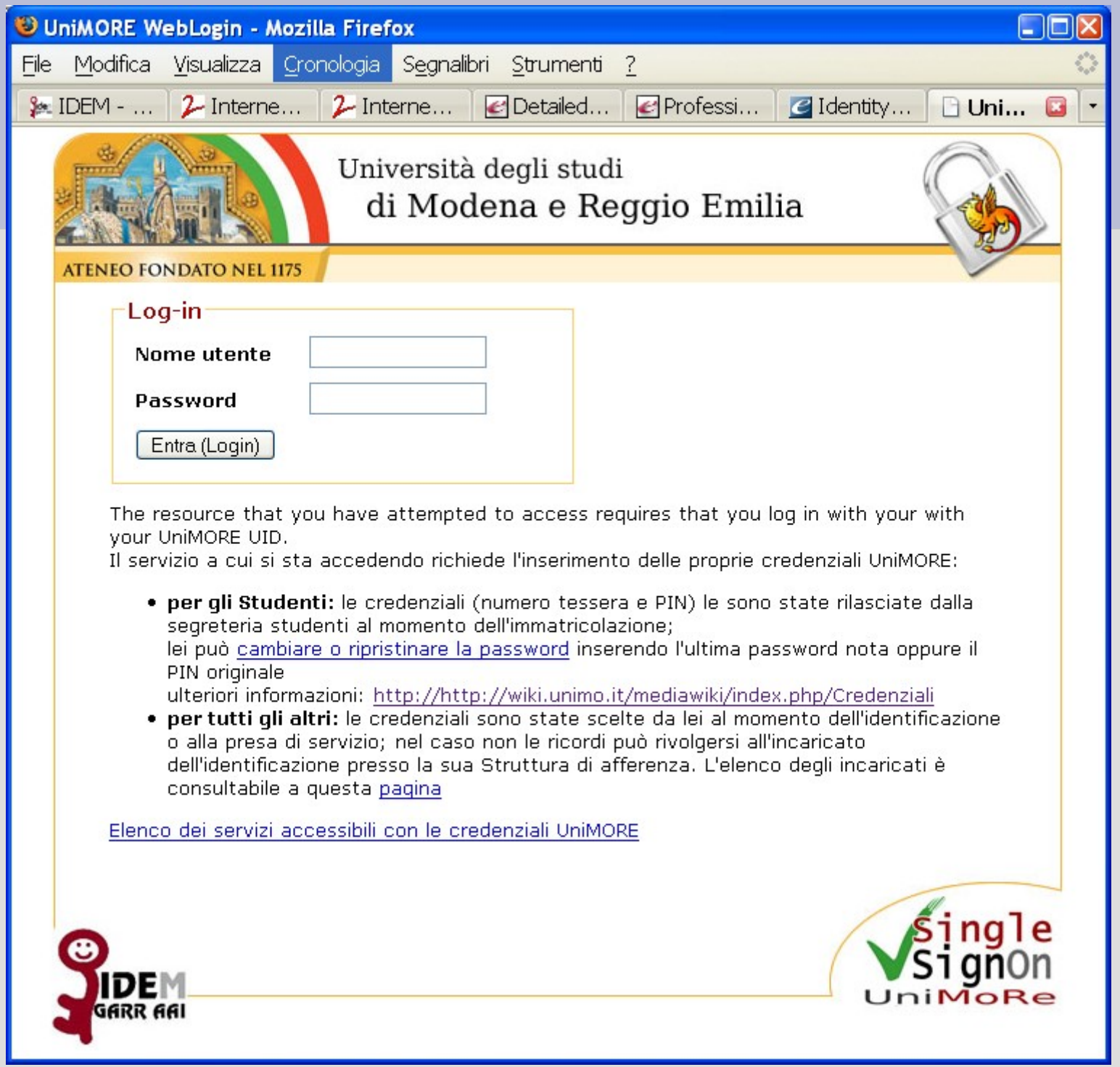


Shibboleth: WAYF Service

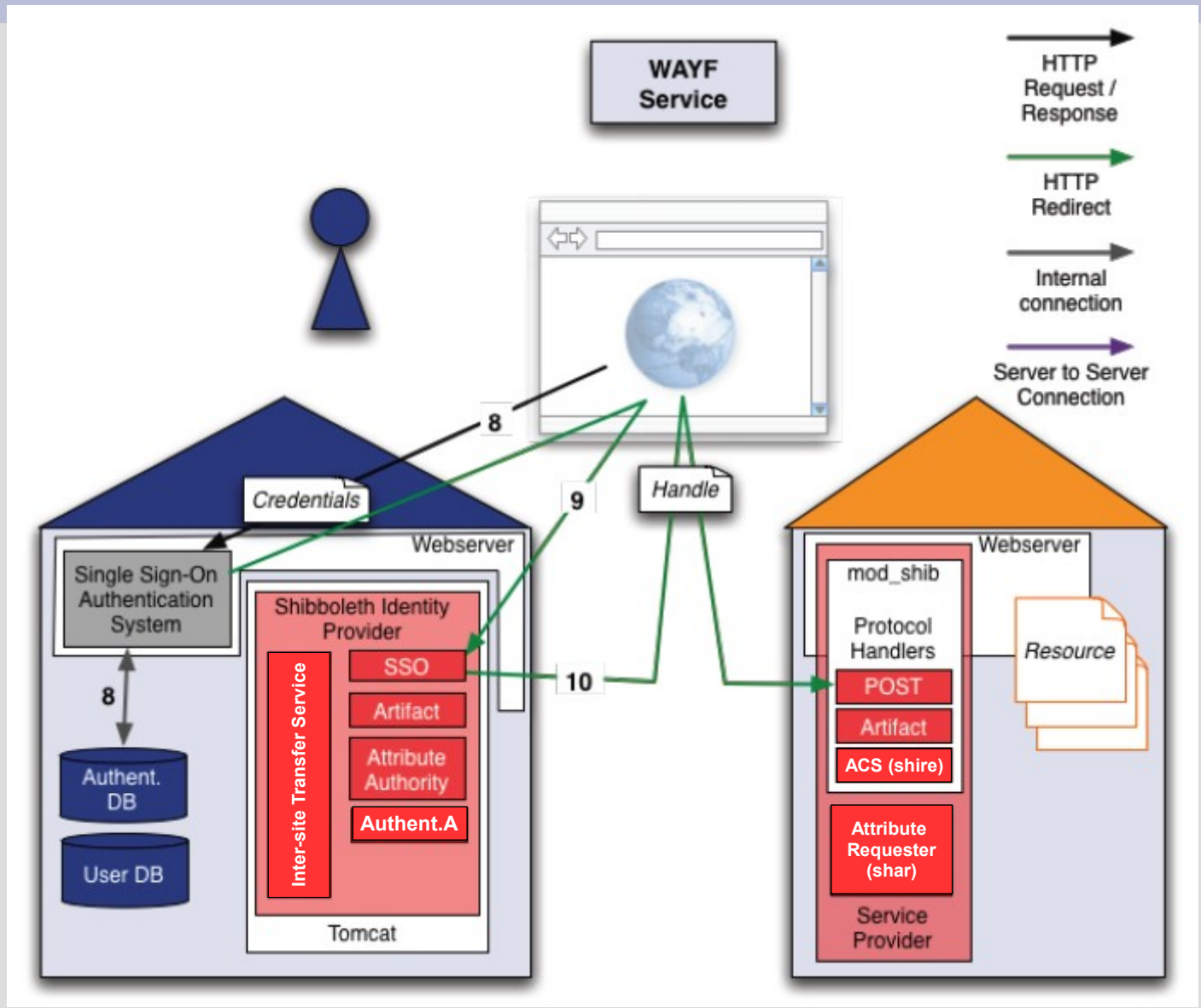


Shibboleth: autenticazione

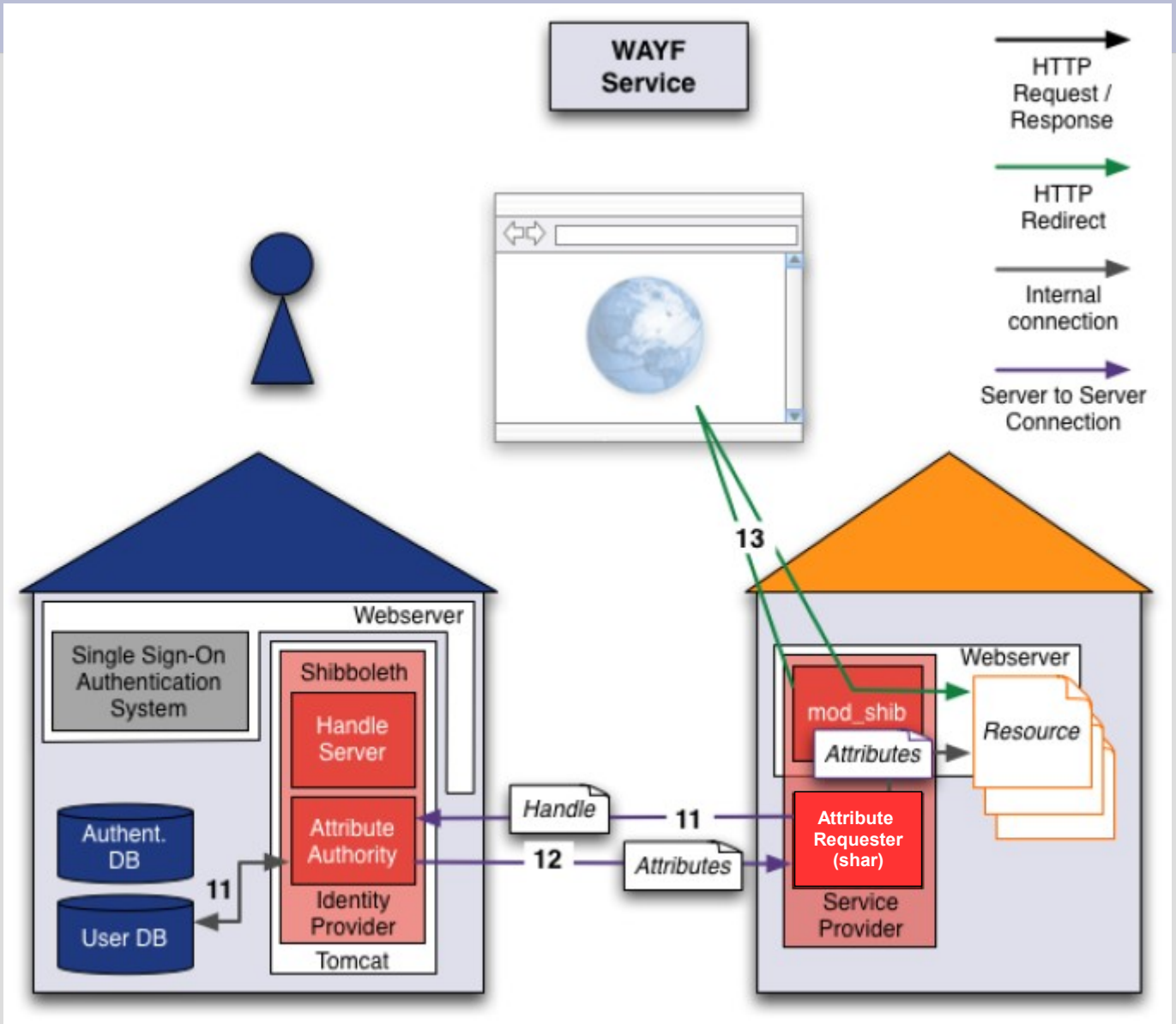



UniMORE WebLogin - Mozilla Firefox
File Modifica Visualizza Cronologia Segnalibri Strumenti ?
IDEM - ...
Interne...
Interne...
Detailed...
Professi...
Identity...
Uni...
Università degli studi
di Modena e Reggio Emilia
ATENEO FONDATO NEL 1175
Log-in
Nome utente
Password
Entra (Login)
The resource that you have attempted to access requires that you log in with your with your UniMORE UID.
Il servizio a cui si sta accedendo richiede l'inserimento delle proprie credenziali UniMORE:
per gli Studenti: le credenziali (numero tessera e PIN) le sono state rilasciate dalla segreteria studenti al momento dell'immatricolazione;
lei può cambiare o ripristinare la password inserendo l'ultima password nota oppure il PIN originale
ulteriori informazioni: http://http://wiki.unimo.it/mediawiki/index.php/Credenziali
per tutti gli altri: le credenziali sono state scelte da lei al momento dell'identificazione o alla presa di servizio; nel caso non le ricordi può rivolgersi all'incaricato dell'identificazione presso la sua Struttura di afferenza. L'elenco degli incaricati è consultabile a questa pagina
Elenco dei servizi accessibili con le credenziali UniMORE
IDEM GARR AAI
Single SignOn UniMoRe

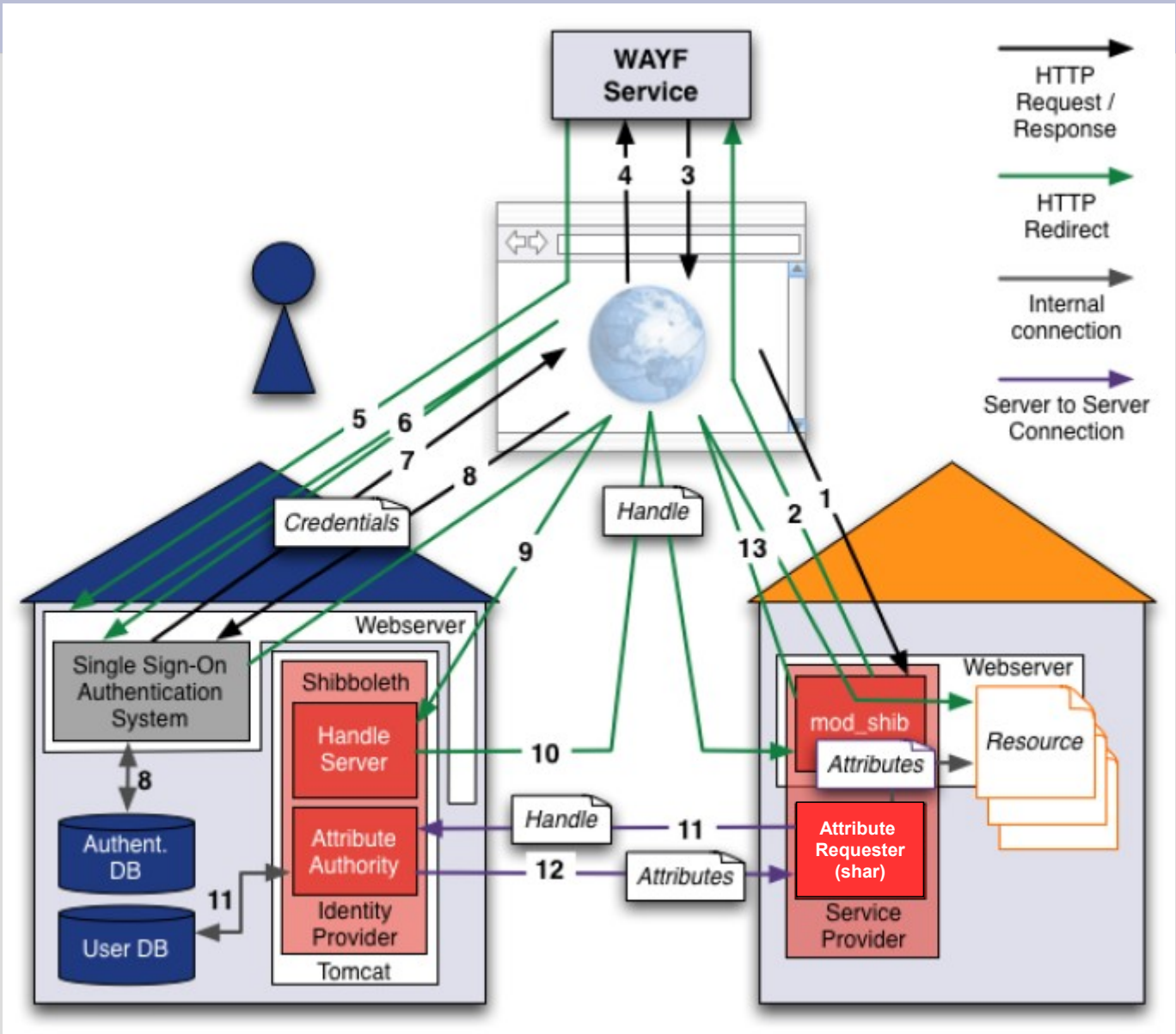
Shibboleth: accesso alla risorsa



Shibboleth: richiesta attributi



Shibboleth: riassunto



Sicurezza di Shibboleth

- mettere in sicurezza tutte le piattaforme
- usare SSL in tutte le comunicazioni per evitare attacchi man-in-the-middle
- assicurare che non vengano usati IdP, SP, WAYF fasulli – certificare i server mediante una CA accettata da tutti
- usare ntp su tutti i server

Domanda?

?

Deploying Shibboleth in 4 fasi

- Web-SSO intra-Campus
- Rilascio degli attributi intra-Campus
- Aderire ad una Federazione
- Aderire ad una inter-Federazione

Cosè una Federazione?

Una federazione è un gruppo di istituzioni e organizzazioni che aderiscono ad un insieme di politiche condivise riguardo gli utenti e le risorse per permettere l'accesso a risorse e servizi. La federazione congiunta ai sistemi di identity e access management delle istituzioni e delle organizzazioni permette la gestione federata dell'accesso.

Federazioni nazionali della ricerca e della formazione universitaria sparse nel mondo

- InCommon by Internet2 in the US
- SWITCHaai by Switch in Switzerland
- HAKA by CSC in Finland
- FEIDE by Uninett in Norway
- PAPI by Rediris in Spain
- SURFfederatie (A-Select) by Surfnet in the Netherlands
- UKfederation by Janet in UK
- MAMS in Australia
- CARSI in China
- CRU Federation in France
- DFN-AAI in Germany
- DK-AAI in Denmark
- K.U.Leuven in Belgium (university K.U.Leuven)
- AAI@EduHr in Croazia
- SWAMID in Sweden

Perché aderire ad una federazione?

- I membri convengono di rispettare determinate regole e modi di operare, quindi si forma un circolo di fiducia.
- Il circolo di fiducia permette di diminuire il carico amministrativo generato dagli accordi bilaterali che grava sugli IdP e sugli SP.
- E' più semplice rispettare la legislazione sulla Privacy.
- Si beneficia di economie di scala.
- La condivisione di contenuti e la collaborazione tra i membri viene facilitata.

Quando GARR ha iniziato a pensare alla Federazione si è posto il problema di quale standard adottare:
Shibboleth

Come fare?

- Seguire quello che si fa in USA
  - l'iniziativa Middleware di Internet2 (attiva dal 1998)
  - MACE-Dir (directories working group of the Middleware Architecture Committee for Education) -> eduPerson
  - NMI-EDIT (Enterprise and Desktop Integration Technologies (EDIT) Consortium, part of the NSF Middleware Initiative (NMI))
- Seguire quello che si fa in Europa
  - TERENA (Trans-European Research and Education Networking Association) in particolare TF-EMC2 (European Middleware Coordination and Collaboration) -> schac

Attività 2007

(IDEntity Management federato per l'accesso ai servizi)

Un gruppo di lavoro ha definito:

- Requisiti indispensabili per poter aderire
- Una base di specifiche (Attributi)
- Test

Attività 2008 – risultati attesi

- Un progetto pilota della durata di un anno durante il quale gli aderenti si impegnano a dimostrare la fattibilità operativa e l'utilità della Federazione
- Il rafforzamento dei sistemi IAM degli enti GARR
- La promozione presso i fornitori di servizi di criteri di riconoscimento utente basato su autenticazione personale
- La promozione del reciproco riconoscimento delle identità tra gli enti GARR
- Promozione della mobilità utente
- Confederazione con le altre federazioni europee

Attività 2008 – supporto GARR

- Catalogo e metadati dei servizi disponibili
- Server WAYF
- Servizio di supporto tecnico per l'implementazione di un IdP
- Servizio di certificazione SCS

Gruppo di lavoro “Attributi”

Ha lavorato alla definizione di un insieme minimale di attributi da usare tra i membri della federazione.

Sono stati scelti tra gli schemi standard LDAPv3, eduPerson e SCHAC – definizioni rigorose

Possono essere “Opzionali”, “Raccomandati” o “Obbligatori”

Salvaguardare al massimo la privacy e D. Lgs. 196/2003

Policy degli Attributi

In generale il Fornitore di Servizio non avrà necessità di ricevere dall'Organizzazione di Appartenenza di un Utente tutti gli Attributi che sono stati definiti; l'Organizzazione di Appartenenza dovrebbe trasferire solo quegli attributi che sono stati giudicati meritevoli di trasferimento (ARP) in conformità alla legislazione vigente, gli accordi tra i Membri, la volontà dell'Utente;

la risorsa che viene acceduta dovrebbe accettare soltanto gli attributi che le sono necessari per decidere riguardo l'autorizzazione all'accesso (AAP).

3 categorie

1. attributi riguardanti le caratteristiche personali del soggetto;
2. attributi riguardanti le modalità per contattare il soggetto;
3. attributi di ausilio alla fase di autorizzazione ed eventualmente di accounting;

Tutti gli attributi costituiscono dati personali ai sensi del D.Lgs. 196/2003 (ad eccezione degli attributi eduPersonScopedAffiliation e eduPersonTargetedID), pertanto il loro trattamento è soggetto alla normativa citata (non possono essere obbligatori).

Attributi (1)

Caratteristiche personali

Nome LDAP	Origine	Descrizione	Stato
sn	LDAPv3	Cognome	opzionale
givenName	LDAPv3	Nome	opzionale
cn	LDAPv3	Nome seguito da Cognome	raccomandato
preferredLanguage	inetOrg-Person	Lingua scritta o parlata preferita dal soggetto	raccomandato
schacMotherTongue	schac	Lingua madre del soggetto	opzionale
title	LDAPv3	Titolo nel contesto dell'organizzazione (es. "Direttore", "Responsabile Reparto X" ecc.)	opzionale
schacPersonalTitle	schac	Titolo usato per salutare il soggetto. Es: Sig., Sig.ra, Dott., Prof.	opzionale
schacPersonalPosition	schac	Il codice rappresentativo dell'inquadramento della persona all'interno dell'organizzazione	opzionale

Attributi (2)

Contatti

Nome LDAP	Origine	Descrizione	Stato
mail	Cosine	Indirizzo eMail	raccomandato
telephoneNumber	LDAPv3	Recapito telefonico ufficio	opzionale
mobile	Cosine	Recapito cellulare di servizio	opzionale
facsimileTelephoneNumber	LDAPv3	Recapito fax	opzionale
schacUserPresenceID	schac	Recapiti relativi a diversi protocolli di rete	opzionale
eduPersonOrgDN	eduPerson	Il Distinguished Name (DN) della entry che rappresenta l'organizzazione di appartenenza alla quale la persona è associata	opzionale
eduPersonOrgUnitDN	eduPerson	Il Distinguished Name (DN) della entry che rappresenta l'unità organizzativa di appartenenza alla quale la persona è associata (ad esempio Dipartimento)	opzionale

Attributi (3)

Autorizzazioni e accounting

Nome LDAP	Origine	Descrizione	Stato
eduPersonScopedAffiliation	eduPerson	Affiliazione secondo le convenzioni descritte nelle Appendici A e B	obbligatorio
eduPersonTargetedID	eduPerson	Identificativi anonimi persistenti per l'utente relativi ai diversi Servizi (vedi appendice C)	obbligatorio
eduPersonPrincipalName	eduPerson	Identificativo unico persistente dell'utente	raccomandato
eduPersonEntitlement	eduPerson	URI (URN o URL) che indica un diritto (standardizzato) di accesso ad una risorsa	raccomandato (se applicabile)

eduPersonScopedAffiliation

- Valore multiplo
- Composto da 2 parti: eduPersonAffiliation @ “dominio di affiliazione”
- Il “dominio di affiliazione” informa l'SP riguardo l'organizzazione di appartenenza dell'utente
- La prima parte può avere come valore uno o più dei seguenti: faculty, student, staff, alum, member, affiliate, employee, library-walk-in

eduPersonScopedAffiliation

Student = studenti regolarmente iscritti ad uno dei corsi dell'organizzazione di appartenenza.

Staff = tutto il personale (docenti, personale amministrativo, bibliotecario e tecnico di supporto) in servizio presso l'organizzazione di appartenenza con qualunque tipo di contratto, anche a tempo determinato, oppure rientrante nei contratti cosiddetti atipici (co.co.co, prestazioni professionali, interinali, ecc...).

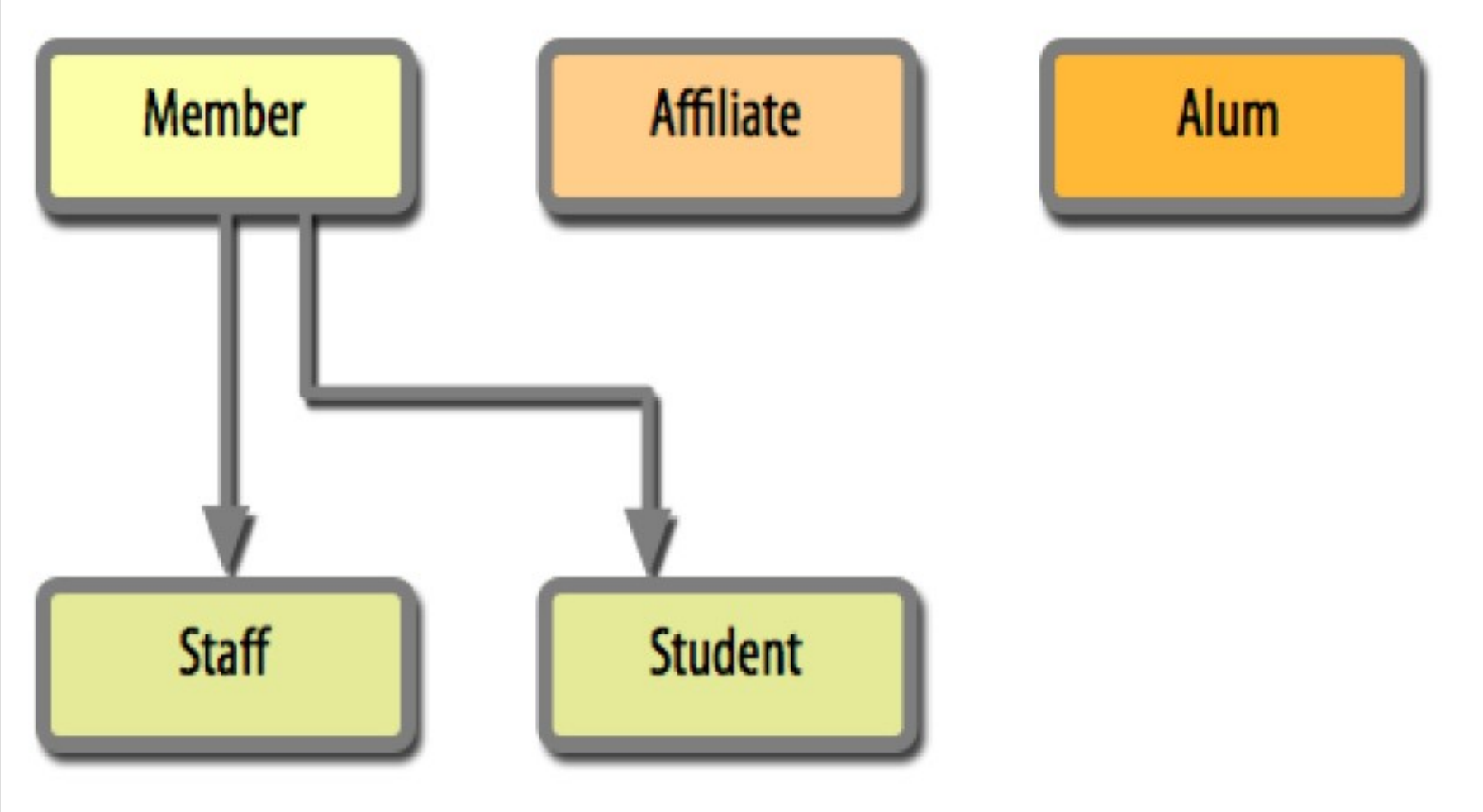
Alum = ex studenti dell'organizzazione di appartenenza

eduPersonScopedAffiliation

Member = tutte le persone che hanno un rapporto istituzionale con l'organizzazione di appartenenza e ai quali viene dato un insieme base di privilegi. Comprende gli student, gli staff, e tutti coloro che pur non rientrando nelle classi precedenti, hanno rapporti istituzionali con la comunità scientifica.

Affiliate = persone con le quali l'organizzazione di appartenenza ha una qualsiasi forma di rapporto ed alle quali è necessario attribuire una identità di utente, ma alle quali non vengono estesi i privilegi derivanti dall'essere membri dell'organizzazione stessa.

Classi di valori per eduPersonAffiliation



eduPersonTargetedId

- Identificativi anonimi persistenti per l'utente relativi ai diversi Servizi
- I valori di questo attributo non devono permettere al servizio di risalire direttamente all'identità dell'utente, ma solamente il suo riconoscimento univoco presso una istituzione (Privacy).
- Serve per riconoscere un utente che ha già visitato un certo servizio senza richiedere allo IdP nessun dato personale (Persistenza).

eduPersonTargetedId

Generazione/Memorizzazione dell'Attributo

- Algoritmica (ricalcolata al volo da valori di altri attributi; se cambia uno dei valori, cambia anche ePTID)
- Memorizzata (elevato numero di valori da memorizzare, ricerca del valore ad ogni richiesta da parte di un SP)

Shibboleth può calcolare ePTIP, secondo lo standard SAML, utilizzando 4 valori: **nameQualifier, SPNameQualifier, sourceName, salt**

eduPersonEntitlement

URI (URN o URL)

L'utente e` autorizzato ad accedere alla risorsa descritta dall'URI o dall'URL

A seguito di uno specifico accordo della federazione, l'IdP può asserire il valore stabilito per gli utenti che ne abbiano diritto. L'SP accetta quindi gli utenti dell'IdP che hanno il valore di eduPersonEntitlement concordato senza richiedere l'identità o ulteriori caratteristiche delle persone che hanno il valore stabilito.

eduPersonEntitlement

Valori URN corrispondono ad insiemi di diritti definiti all'interno della federazione. La federazione, avendo registrato il nome urn:mace:garr.it:idem, può definire autonomamente valori appropriati per specificare precisi diritti. Es: urn:mace:garr.it:idem:videoconferenza

Evita di mantenere la lista dei nomi utente per gli utenti autorizzati: un processo che risulta arduo da manutenere e anche rischioso per la privacy.

In generale eduPersonEntitlement non costituisce un dato personale, ma ci sono eccezioni.

IDEM


L'Infrastruttura di Autenticazione e Autorizzazione (AAI)
federata della rete GARR

Domande?

?

Grazie!


L'Infrastruttura di Autenticazione e Autorizzazione (AAI)
federata della rete GARR