IDEM day
24-25 Novembre 2009
Roma, Sede centrale ENEA

Progettare Identità Digitali interoperabili negli Enti e nelle Federazioni

Maria Laura Mantovani

(GARR e Università degli Studi di Modena e Reggio Emilia)

Consortium GARR

Agenda

- Che cos'è un Identity Management System (IMS)
- Sviluppare un sistema di gestione delle identità e degli accessi (IAM)
- Identità nell'Istituzione Accademica. La persona è descritta da un insieme standardizzato di attributi
- Pronti per l'accesso ad applicazioni esterne attraverso la Federazione IDEM

marialaura.mantovani@garr.it

Le 7 leggi dell'identità

Per l'IMS di successo

1. Controllo da parte dell'utente e consenso
2. Rivelazione minima e per uso prestabilito
3. L'utente comprende la ragionevolezza del trasferimento
4. L'utente può usare uno pseudonimo
5. Il sistema deve essere pluralista rispetto ad operatori e tecnologie
6. Azione umana integrata nel sistema
7. Semplicità e usabilità delle molte identità digitali parziali

marialaura.mantovani@garr.it

Identity Management

- Un insieme di processi (decisionali, organizzativi, procedurali, informatizzati) e una infrastruttura di supporto (per memorizzare/conservare, trasmettere, proteggere) che permette di:
  - CREARE
  - GESTIRE/MODIFICARE
  - USARE
  - ELIMINARE

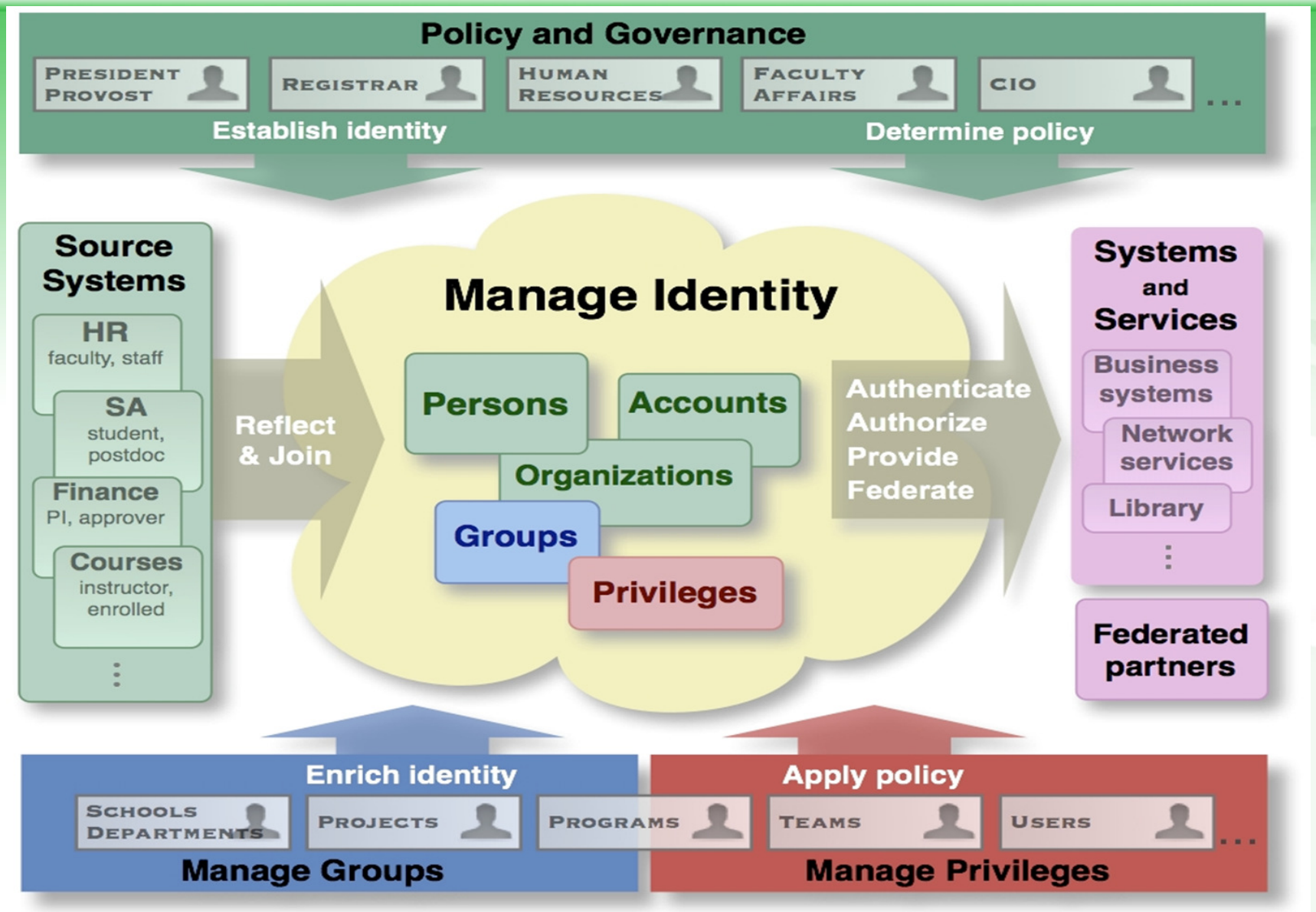
  le identità digitali parziali
  [relativamente al contesto (education&research)]
  rispettando la legge (cioè i diritti delle persone, in particolare il diritto alla privacy e il diritto all'onore).

marialaura.mantovani@garr.it

Identity & Access Management per...

- Permettere alle organizzazioni di:
  - Dare ai propri utenti l'accesso alle risorse migliorando la loro padronanza e usabilità (user experience)
  - Controllare l'accesso degli utenti alle risorse e alle applicazioni on-line
- Con le seguenti condizioni:
  - Proteggere i dati personali dell'utilizzo non autorizzato
  - Proteggere le informazioni riservate dall'accesso da parte di utenti non autorizzati
- Si esplicita in un complesso di applicazioni e sistemi che vengono utilizzati per gestire l'autenticazione degli utenti, l'accesso (o la restrizione dell'accesso) alle risorse, i profili, le password, e altri attributi che aiutano a definire ruoli e profili degli utenti.

marialaura.mantovani@garr.it



Developed by Ann West, of Internet2, Lynn McRae, of Stanford, Tom Barton, of the University of Chicago, and Steven Carmody, of Brown University, and used with permission from Internet2.

marialaura.mantovani@garr.it

Policy and Governance

PRESIDENT PROVOST | REGISTRAR | HUMAN RESOURCES | FACULTY AFFAIRS | CIO | ...

Establish identity — Determine policy

SEGRETERIE STUDENTI

RISORSE UMANE

IDENTIFICATORI in BIBLIOTECHE DIPARTIMENTI FACOLTA'

SELF-SERVICE

STUDENTI

DIPENDENTI

ESTERNI

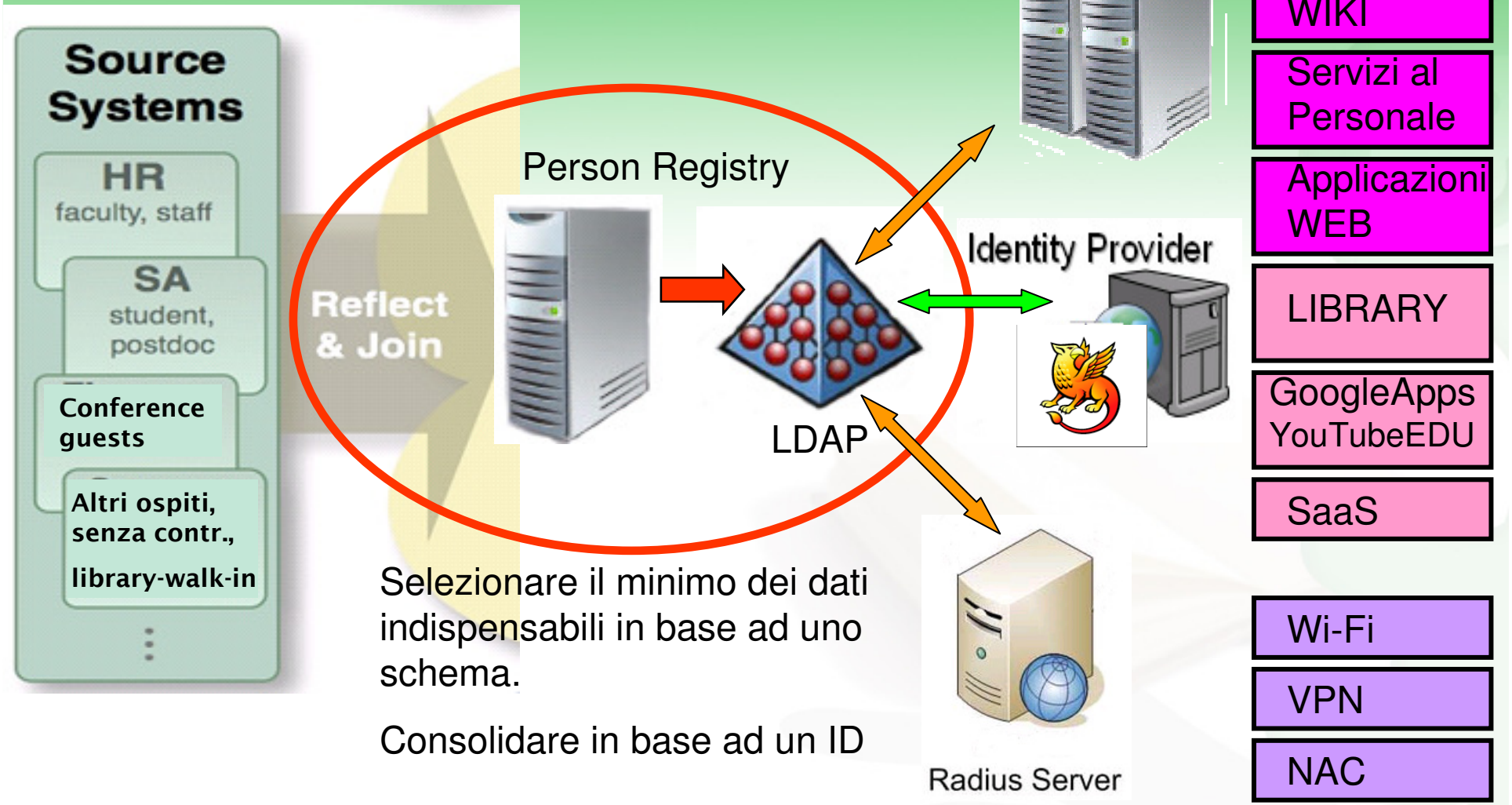
ALTRI DATI

marialaura.mantovani@garr.it

Il ciclo di vita dell'identità

marialaura.mantovani@garr.it

Sincronizzazione / Backend



Selezionare il minimo dei dati indispensabili in base ad uno schema.

Consolidare in base ad un ID

marialaura.mantovani@garr.it

Core.schema

objectclass (2.5.6.6 NAME **'person**'
DESC 'RFC2256: a person'
SUP top
STRUCTURAL
MUST (
sn $
cn)
MAY (userPassword $
telephoneNumber
$ seeAlso $ description))

cognome

nome cognome

Gli Attributi si devono valorizzare secondo il significato definito negli RFC

Gli Attributi possono essere non valorizzati

marialaura.mantovani@garr.it

Core.schema

objectclass (2.5.6.7 NAME **'organizationalPerson**'

DESC 'RFC2256: an organizational person'
SUP person
STRUCTURAL
MAY (

title

Examples: "Vice President", "Software Engineer", and "CEO"

$ x121Address $ registeredAddress $ destinationIndicator $ preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $

telephoneNumber

$ internationaliSDNNumber $

facsimileTelephoneNumber

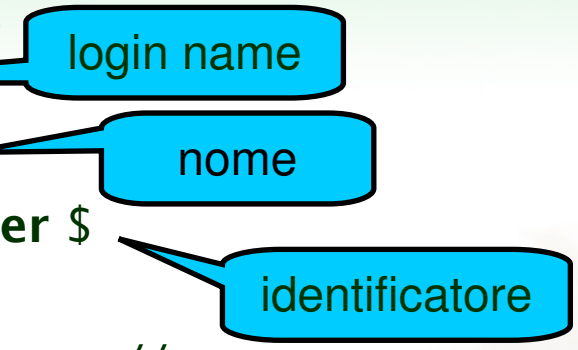
$ street $ postOfficeBox $ postalCode $ postalAddress $ physicalDeliveryOfficeName $ ou $ st $ l))

marialaura.mantovani@garr.it

inetorgperson.schema

NAME **'inetOrgPerson'**

SUP organizationalPerson
STRUCTURAL
MAY (audio $ businessCategory $ carLicense $ departmentNumber $ displayName $
uid $
givenName $
employeeNumber $
mail $
employeeType $ //type of employment for a person
mobile $
homePhone $ homePostalAddress $ initials $ jpegPhoto $ labeledURI $ manager $ o $ pager $ photo $ roomNumber $ secretary $ userCertificate $ x500uniqueIdentifier $ preferredLanguage $ userSMIMECertificate $ userPKCS12))



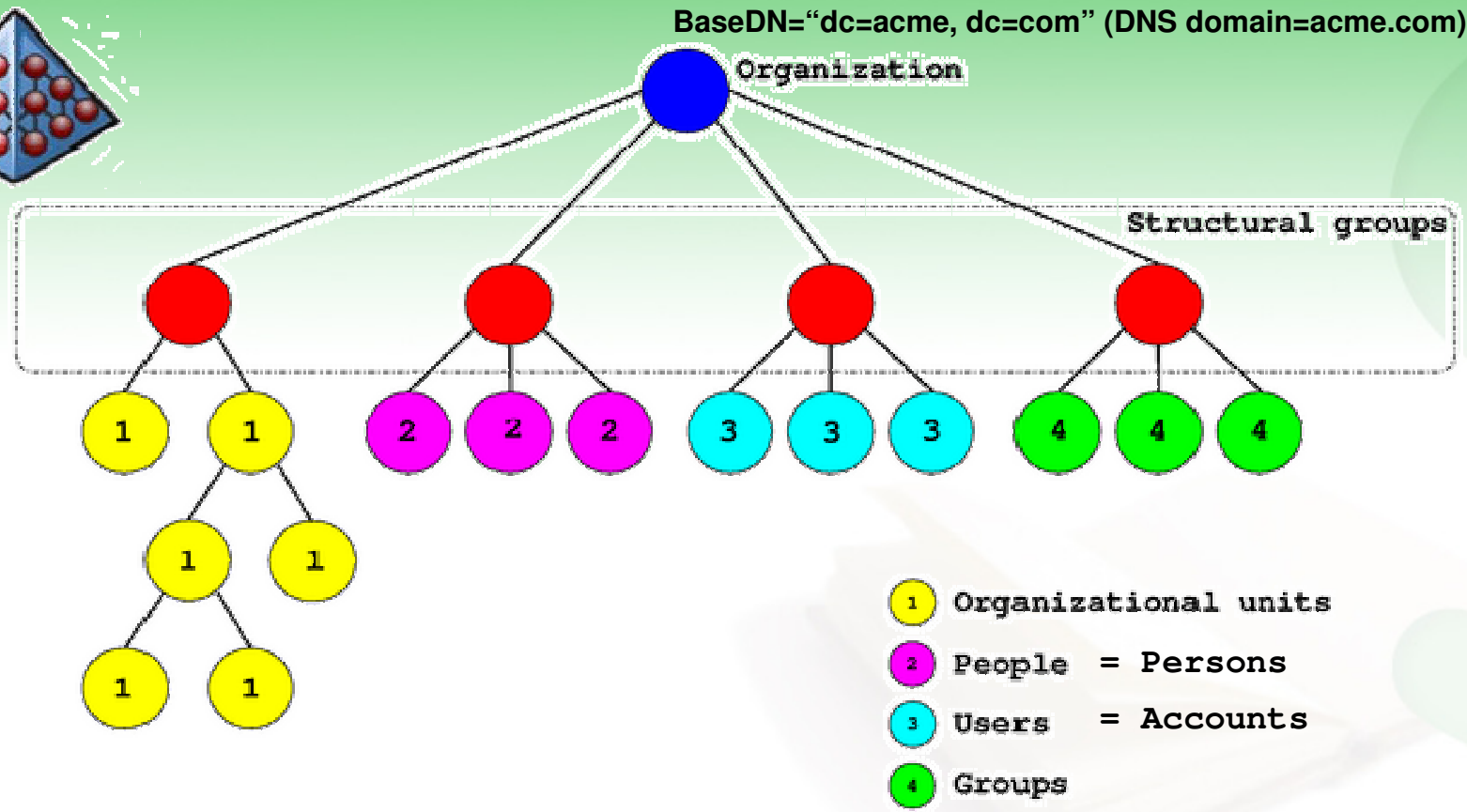
marialaura.mantovani@garr.it

eduPerson

```
# The eduPerson objectclass is used to represent people who are
# associated with a university/school in some way.  It is derived
# from the inetOrgPerson objectclass.
objectclass ( 1.3.6.1.4.1.5923.1.1.2
        NAME 'eduPerson'
        AUXILIARY
        MAY ( eduPersonAffiliation $
            eduPersonNickname $eduPersonOrgDN $
            eduPersonOrgUnitDN $eduPersonPrimaryAffiliation $
             eduPersonPrincipalName $
             eduPersonEntitlement
            $ eduPersonPrimaryOrgUnitDN $
             eduPersonScopedAffiliation $
            eduPersonTargetedID
           )
        )
```


marialaura.mantovani@garr.it

LDAP DIT (Directory Information Tree)



Dn="cn=John Smith, dc=acme, dc=com"
Dn="uid=JSmith, dc=acme, dc=com"
Dn="uid=John.Smith@acme.com, dc=acme, dc=com"

RFC 2377 "Naming Plan for Internet Directory-Enabled Applications" September 1998

marialaura.mantovani@garr.it

Arricchimento People

Unifica accesso UNIX

```
<nis.schema>
loginShell:
uidNumber:
gidNumber:
homeDirectory:
gecos:
shadowExpire:
shadowInactive:
shadowLastChange:
```

```
<samba.schema>
sambaNTPassword:
sambaPwdMustChange:
sambaPrimaryGroupSID:
sambaPwdLastSet:
sambaSID:
sambaHomeDrive:
```

Unifica accesso Windows

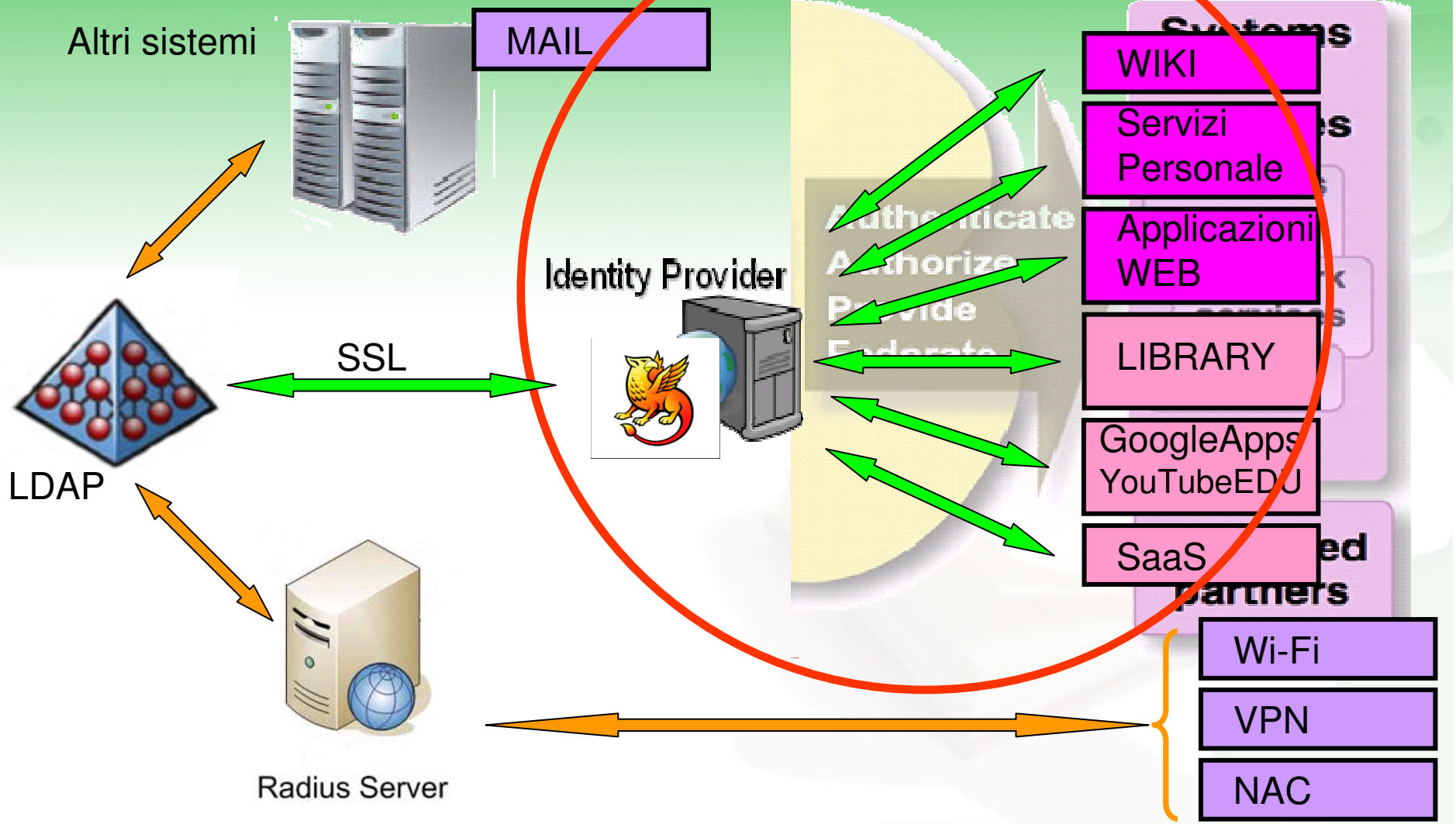
Attributi utili per autorizzare applicazioni istituzionali

```
<myorg.schema>
unimorecodicefiscale:
unimorestudnumerotessera:
unimorestuddescrcorso:
unimorestudmatricola:
unimorestudduratacorso:
unimorecorscodicetipocorso:
unimorecorsdescrizionecorso:
unimorecorsdurataanni:
unimorestudultimoannoaccademico:
unimorestuddatarilasciotessera:
```

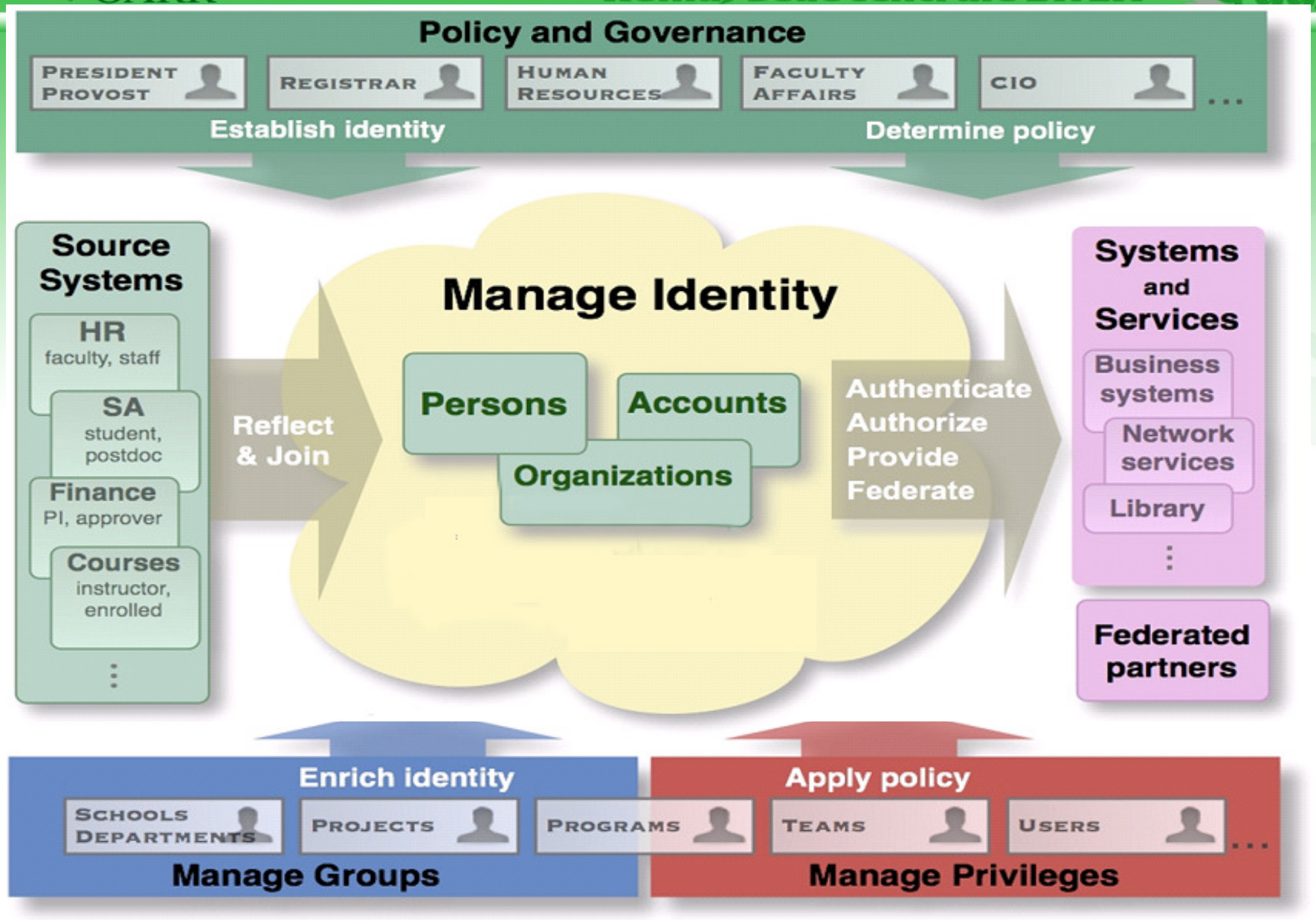
Per federarsi

```
<eduPerson.schema>
<schac.schema>
```

SSO interno ed esterno/SinglePassword



marialaura.mantovani@garr.it



marialaura.mantovani@garr.it

Le basi della fiducia reciproca

Per entrare in idem garr aai

- Persone Reali
- Account Tracciabili
- Profilatura condivisa

marialaura.mantovani@garr.it

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

marialaura.mantovani@garr.it

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).

marialaura.mantovani@garr.it

3 categorie di attributi

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 di eduPersonScopedAffiliation), pertanto il loro trattamento è soggetto alla normativa citata.

marialaura.mantovani@garr.it

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

marialaura.mantovani@garr.it

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

marialaura.mantovani@garr.it

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)

marialaura.mantovani@garr.it

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

marialaura.mantovani@garr.it

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

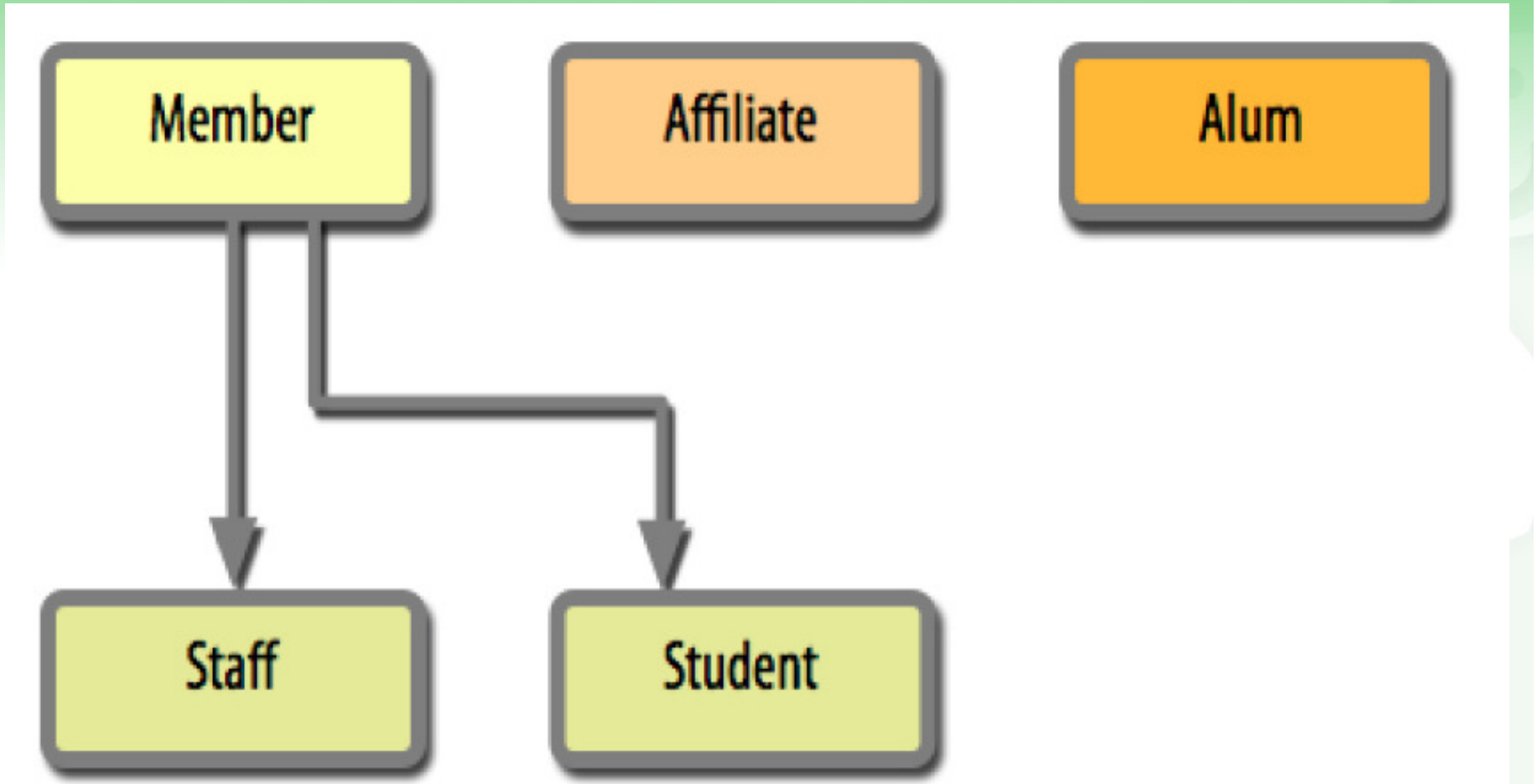
marialaura.mantovani@garr.it

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 digitale, ma alle quali non vengono estesi i privilegi derivanti dall'essere membri dell'organizzazione stessa. Ha diritto a servizi locali. Non ha diritto a servizi federati.

marialaura.mantovani@garr.it

Classi di valori per eduPersonAffiliation



marialaura.mantovani@garr.it

Corrispondenza tra i ruoli dell'organizzazione di appartenenza e le possibili affiliazioni

Ruolo	eduPersonAffiliation
assistente universitario	staff, member
cessato	affiliate
collaboratore coordinato continuativo	staff, member
collaboratore linguistico	staff, member
consorziato (membro del consorzio a cui l'ente appartiene)	member
convenzionato (cliente delle convenzioni)	affiliate
cultore della materia	staff, member
dipendente altra università	member
dipendente altro ente di ricerca	member

N.B. Le affiliazioni **alum** e **library-walk-in** possono essere aggiunte a tutti i ruoli, ove risultasse applicabile.

marialaura.mantovani@garr.it

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 (Privacy).
- Serve al Servizio per riconoscere un utente che ritorna, senza richiedere allo IdP nessun dato personale (Persistenza).

marialaura.mantovani@garr.it

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**

marialaura.mantovani@garr.it

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.

marialaura.mantovani@garr.it

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 all'SP 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

marialaura.mantovani@garr.it

Un caso reale: Elsevier (ScienceDirect e Scopus)

- Gli utenti hanno diritto di entrare se

  eduPersonEntitlement = urn:mace:dir:entitlement:common-lib-terms

marialaura.mantovani@garr.it

Benefici per l'organizzazione se c'è IAM

- Capacità di gestire rapidi cambiamenti
  - es. utenti per uno o pochi giorni
  - es. attivazione di molti nuovi servizi anche federati o in cloud
- Governance più efficace
  - perché è finalmente possibile applicare le policy (non solo enunciarle)
- Aiuta a rispettare le leggi
  - es. diritti privacy
- Soddisfazione dell'utenza
  - grazie all'accesso facile e sicuro a numerose risorse

marialaura.mantovani@garr.it

Riferimenti

- Kim Cameron, Le leggi dell'identità http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf
- Jack Suess and Kevin Morooney, Identity Management and Trust Services: Foundations for Cloud Computing http://doiop.com/idmforcloud http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume44/IdentityManagementandTrustServ/178410
- Internet2 Middleware Background http://www.internet2.edu/middleware/background.html
- RFC 2247 "Using Domains in LDAP/X.500 Distinguished Names" January 1998
- RFC 2377 "Naming Plan for Internet Directory-Enabled Applications" September 1998
- RFC 2798 "Definition of the inetOrgPerson LDAP Object Class", April 2000
- RFC 4519 "LDAP: Schema for User Applications" June 2006
- RFC 4524 "COSINE LDAP/X.500 Schema" June 2006
- eduPerson Object Class http://middleware.internet2.edu/eduperson/
- SCHAC, SCHema for ACademia http://www.terena.org/activities/tf-emc2/schac.html
- Federazione IDEM, Specifiche tecniche per la compilazione e l'uso degli attributi (ST-A) http://doiop.com/ST-A http://www.servizi.garr.it/index.php/it/documenti/doc_download/26-specifiche-tecniche-per-la-compilazione-e-luso-degli-attributi-

marialaura.mantovani@garr.it