# Specifiche tecniche per la compilazione e l'uso degli attributi

## Incontro con il CdG IDEM

*13 Ottobre 2008*

Raffaele Conte

*Istituto di Fisiologia Clinica*

*Comitato di Gestione - Federazione IDEM*

# Scopo del documento

- Standardizzare gli attributi scambiati fra i partecipanti alla Federazione. In particolare:
  - denominazione
  - sintassi
  - semantica
- Limitare l'uso degli attributi ai soli effettivamente necessari per l'erogazione del servizio

# Denominazione e sintassi

- Sono state utilizzate denominazioni e sintassi degli schemi LDAP
  - LDAPv3 (RFC 4519)
  - Cosine
  - inetOrgPerson
  - eduPerson
  - SCHAC

# L'insieme degli attributi

- Gli attributi sono suddivisi in:
  - **caratteristiche personali**: sn, givenName, cn, preferredLanguage ecc.
  - **contatti**: mail, telephoneNumber, mobile ecc.
  - **autorizzazione e accounting**: eduPersonScopedAffiliation, eduPersonTargetedID, eduPersonPrincipalName, eduPersonEntitlement

# Notazione e metadati

- Necessari per comprendere le modalità di utilizzo dell'attributo
- La prossima versione del documento indicherà l'identificativo dell'attributo, tramite urn, come indicato da SAML1 e SAML2
- es.

  (SAML 1) urn:mace:dir:attribute-def:sn

  (SAML 2) urn:oid:2.5.4.4

# Notazione: classificazione

- Gli attributi sono classificati come:
  - **obbligatori**: un IdP deve fornire questi attributi per poter fare parte della federazione
  - **raccomandati**: è fortemente raccomandato che un IdP fornisca questi attributi
  - **opzionali**: alcuni SP potrebbero richiedere questi attributi

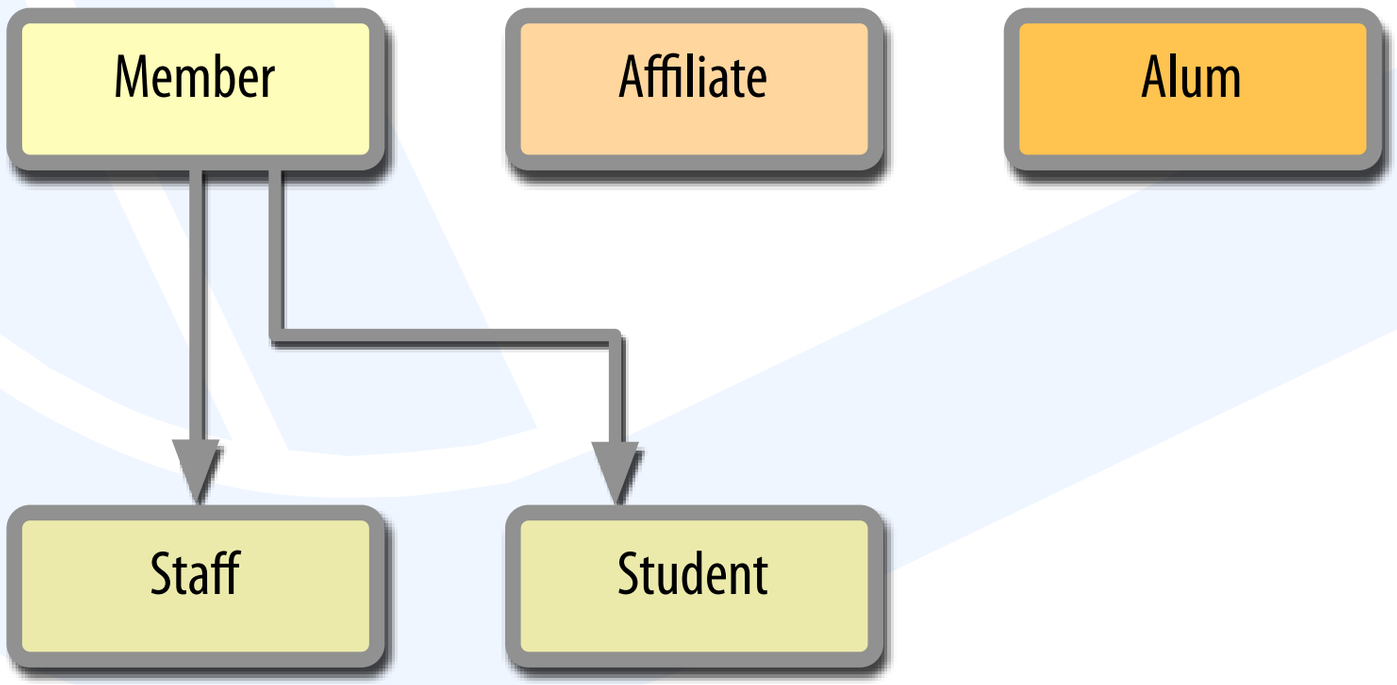
# Configurazione per IdP

## Quasi tutti gli attributi possono essere definiti in Shibboleth 2 con il tipo *simple*

```
<resolver:AttributeDefinition id="cn" xsi:type="Simple"
    xmlns="urn:mace:shibboleth:2.0:resolver:ad"
    sourceAttributeID="cn">

  <resolver:Dependency ref="myLDAP" />

  <resolver:AttributeEncoder xsi:type="SAML1String"
      xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
      name="urn:mace:dir:attribute-def:cn" />

  <resolver:AttributeEncoder xsi:type="SAML2String"
      xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
      name="urn:oid:2.5.4.3" friendlyName="cn" />

</resolver:AttributeDefinition>
```

# eduPersonScopedAffiliation

- Definisce la relazione fra utente ed Organizzazione nel formato *affiliation@organisation*
- Organizzazione nel formato DNS
- L'affiliazione prevede (al momento) come valori possibili:



# eduPersonScopedAffiliation

- Configurazione:
  - *scoped attribute*
  - potrebbe utilizzare eduPersonAffiliation definito come *mapped attribute*

```
<resolver:AttributeDefinition
    id="eduPersonScopedAffiliation"
    xsi:type="Scoped"
    xmlns="urn:mace:shibboleth:2.0:resolver:ad"
    scope="ifc.cnr.it">

  <resolver:Dependency ref="eduPersonAffiliation" />

        [...]
</resolver:AttributeDefinition>
```

# eduPersonScopedAffiliation

## eduPersonAffiliation

### *mapped attribute*

```
[...]
     <DefaultValue>affiliate</DefaultValue>

  [...]

     <ValueMap>
          <ReturnValue>staff</ReturnValue>
          <SourceValue>dirigente tecnologo</SourceValue>
          <SourceValue>dirigente di ricerca</SourceValue>
          <SourceValue>primo tecnologo</SourceValue>
          <SourceValue>primo ricercatore</SourceValue>
          <SourceValue>tecnologo</SourceValue>
          <SourceValue>ricercatore</SourceValue>
          <SourceValue>personale tecnico-amministrativo</SourceValue>
          <SourceValue>specializzando</SourceValue>
     </ValueMap>
[...]
```

# eduPersonTargetedID

- implementa il *persistent identifier* di SAML 2
- permette la gestione di sessioni in forma anonima
- in IDEM si utilizza la versione 2006 (conforme a SAML 2)
- prevede *n* valori per *n* servizi
- valori nel formato:

```
nameQualifier!SPNameQualifier!stringa_opaca
```

# eduPersonTargetedID

- Gestione:
  - algoritmica
    - gestione più semplice
      - variando l'attributo sorgente variano tutti i valori con conseguente perdita personalizzazioni
    - deprecato in Shibboleth 2.x
  - per memorizzazione
    - richiede tabella in DB
    - consente la revoca e rigenerazione
    - può essere usato come identificativo

# eduPersonTargetedID

## Configurazione lato IdP (attribute-resolver):

```
<resolver:AttributeDefinition
    id="eduPersonTargetedID"
    xsi:type="SAML2NameID"
    xmlns="urn:mace:shibboleth:2.0:resolver:ad"
    nameIdFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
    sourceAttributeID="computedID">

    <resolver:Dependency ref="computedID" />

    <resolver:AttributeEncoder
        xsi:type="SAML2XMLObject"
        xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
        name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10"
        friendlyName="eduPersonTargetedID" />

</resolver:AttributeDefinition>

<resolver:DataConnector
    xsi:type="ComputedId"
    xmlns="urn:mace:shibboleth:2.0:resolver:dc"
    id="computedID"
    generatedAttributeID="computedID"
    sourceAttributeID="uid"
    salt="<stringa casuale>">

    <resolver:Dependency ref="myLDAP" />
</resolver:DataConnector>
```

# eduPersonTargetedID

## Configurazione lato SP (attribute-map):

```
<!-- First, the deprecated version: -->
<Attribute name="urn:mace:dir:attribute-def:eduPersonTargetedID"
    id="targeted-id">

    <AttributeDecoder xsi:type="ScopedAttributeDecoder"/>
</Attribute>

<!-- Second, the new version (note the OID-style name): -->
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" id="persistent-id">

<AttributeDecoder xsi:type="NameIDAttributeDecoder"
    formatter="$NameQualifier!$SPNameQualifier!$Name"/>
</Attribute>

<!-- Third, the SAML 2.0 NameID Format: -->
<Attribute name="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
    id="persistent-id">

<AttributeDecoder xsi:type="NameIDAttributeDecoder"
    formatter="$NameQualifier!$SPNameQualifier!$Name"/>
</Attribute>
```

# eduPersonEntitlement

- metodo di autorizzazione "*esplicita*"
  - hanno diritto di accedere alla risorsa x solo gli utenti per cui l'attributo contiene la uri di x
  - es.:

    http://nilde.bo.cnr.it

    urn:mace:internet2:terena.nl:garr:service
- in questo modo è l'IdP che autorizza l'accesso a determinate risorse

# Domande?