



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

**v. 3.0**

## 6 giugno 2016

# Revisioni

| Versione | Data | Descrizione | Note |
|---|---|---|---|
| 1.0 | 24/10/2008 | Versione iniziale | Raffaele Conte[1]<br>Maria Laura Mantovani[2]<br><br>contributi di:<br>Roberto Gaffuri[3]<br>Francesco Malvezzi[4]<br>Giacomo Tenaglia[5] |
| 2.0 | 26/01/2010 | Revisione generale del testo.<br>Adeguamento della terminologia in funzione di Shibboleth 2.0.<br>Inserimento identificativi (urn) in "Attributi: definizione dei metadati e notazione".<br>Modifica paragrafo "Confidenzialità/Visibilità".<br>Riorganizzazione delle Appendici A e B con indicazioni su configurazione di Shibboleth adeguate alla versione 2.x ed esempi.<br>Correzioni minori. | Ra. C. |
| 2.1 | 07/05/2011 | Piccole modifiche capitolo 2 "Panoramica sugli attributi" (secondo e terzo capoverso).<br>Modificata descrizione di eduPersonEntitlement in tabella al paragrafo 2.3.<br>Modificata descrizione di attributo raccomandato e opzionale (capitolo 3).<br>Modificata organizzazione capitolo "Attributi".<br>Modificati "Riferimenti" obsoleti per 4.1.4 preferredLanguage, 4.1.5 schacMotherTongue e 4.1.7 schacPersonalTitle<br>Aggiunto riferimento a [SCHAC] su definizione di 4.1.5 schacMotherTongue, 4.2.5 schacUserPresenceID<br>Modificati "Semantica", "Riferimenti" e "Valori permessi" per 4.1.8 schacPersonalPosition | Ra. C.<br>M.L.M. |

[1] Istituto di Fisiologia Clinica, CNR, Pisa <raffaele.conte@cnr.it>

[2] GARR e Università di Modena e Reggio Emilia <marialaura.mantovani@garr.it>

[3] Politecnico di Milano <roberto.gaffuri@ceda.polimi.it>

[4] Università di Modena e Reggio Emilia <francesco.malvezzi@unimore.it>

[5] CNR, Biblioteca Area della Ricerca di Bologna <giacomo.tenaglia@area.bo.cnr.it>

| | | | |
|---|---|---|---|
| | | Modificata descrizione, semantica e riferimenti di 4.2.6 eduPersonOrgDN e 4.2.7 EduPersonOrgUnitDN.<br>Modificati "Riferimenti" e "Valori permessi" per 4.3.1 eduPersonScopedAffiliation.<br>Modificate "Note" per 4.3.2 eduPersonTargetedID .<br>Corretto "Identificativo" per 4.3.3 eduPersoPrincipalName e aggiunto valore in "Riferimenti" per 4.3.4 eduPersonEntitlement.<br>Spostata Bibliografia in fondo al documento.<br><br>Piccole correzioni Appendice B e nuovi valori di corrispondenza nelle affiliazioni.<br>Aggiunto riferimento a [RFC5646] e aggiornati i link [NO1], [NO2], [EDUPER] e [SCHAC] in Bibliografia.<br>Aggiunta bibliografia relativa a Shibboleth. | |
| 2.2 | 19/06/12 | Traduzione inglese<br>Revisioni minori | Alessandra De Nicola<br>M.L.M. |
| 3.0 | 06/06/16 | Revisione generale del testo alla luce dell'adozione di SAML 2, Entity Category, Resource Registry e Shibboleth 3.<br>Riscrittura dell'introduzione con aggiornamento sui concetti di privacy e data protection europei e definizione ulteriore degli ambiti di competenza.<br>Approfondimento sul filtraggio degli attributi.<br>Aggiunta di un paragrafo sul consenso informato dell'utente al rilascio degli attributi.<br>Eliminazione di facsimileTelephoneNumber.<br>Elenco sintetico degli attributi ripulito, rivisto e ordinato con un criterio misto di importanza ed effettivo utilizzo degli attributi in federazione.<br>Aggiunti gli attributi eduPersonOrcid e DisplayName.<br>Deprecato il rilascio di eduPersonTargetedID in favore dell'uso di SAML 2.0 NameID nel subject dell'asserzione. | Daniele Albrizio[6]<br>Maurizio Festi[7]<br>Giuliano Latini[8]<br>Fabio Spelta[9] |

[6] Università di Trieste <daniele.albrizio@units.it>
[7] Università di Trento <maurizio.festi@unitn.it>
[8] Università Politecnica delle Marche <giuliano.latini@univpm.it>
[9] Università degli Studi di Milano - Bicocca <fabio.spelta@unimib.it>

**Premessa**

Per la segnalazione di suggerimenti, errori o inesattezze relative a questo documento, vi preghiamo di scrivere a idem@garr.it

**Abbreviazioni**

STA = Specifiche Tecniche - Compilazione e Uso degli Attributi

NdP = Norme di Partecipazione

IPRR= Identity Provider Registration Request

RRR = Resource Registration Request

IdP = Identity Provider

SP = Service Provider

CA = Certification Authority

WAYF = Where Are You From

CoCo = Code of Conduct Entity Category

R&S = Research and Scholarship Entity Category

**Contatti**

Sito IDEM = https://www.idem.garr.it

Federazione IDEM: idem@garr.it

Servizio IDEM GARR AAI: idem-help@garr.it

# Indice

# 1 Introduzione

La federazione IDEM utilizza lo standard SAML2 per effettuare il Single Sign-On. Una delle funzionalità di questa tecnologia è la possibilità di far pervenire ai servizi federati un insieme di *caratteristiche* relative all'utente, oltre che assicurarne la corretta autenticazione.

Queste *caratteristiche* possono essere di vario tipo: informazioni personali (nome, cognome), relative all'affiliazione dell'utente (per esempio, personale docente presso un determinato ateneo), alla lingua e molte altre ancora. *Queste caratteristiche prendono il nome di attributi.*

Lo scopo di questo documento è quello di standardizzare l'uso degli attributi tra i partecipanti alla federazione IDEM. La procedura di standardizzazione riguarda la denominazione, la sintassi, la semantica, le politiche di rilascio ed eventuali valorizzazione degli attributi che i Fornitori di identità (Identity Provider o **IdP**) delle Organizzazioni con cui l'utente è affiliato (Organizzazioni di Appartenenza) devono o possono rilasciare ai Fornitori di Servizi (Service Provider o **SP**). Per comodità gli attributi sono definiti utilizzando schemi standard LDAP.

Spetta all'Organizzazione di Appartenenza dell'utente, responsabile dell'IdP, il compito di trasferire solo gli attributi giudicati meritevoli di trasferimento in conformità alla legislazione vigente, gli accordi tra i membri, la volontà dell'utente.

La risorsa che viene acceduta (SP) dovrebbe richiedere soltanto gli attributi che le sono necessari per decidere riguardo l'autorizzazione all'accesso e per erogare il servizio.

Nella tabella del capitolo "Panoramica sugli attributi" si può notare che questi sono divisi in 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 e di accounting. Quasi tutti gli attributi sono dati personali ai sensi del D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" e il loro trattamento è soggetto alla normativa citata.

Per gli SP nella maggior parte dei casi è sufficiente sapere che l'utente è registrato nella Federazione, che l'accesso è discriminabile in base all'organizzazione di appartenenza dell'utente e al suo tipo di affiliazione con essa (attributo "eduPersonScopedAffiliation"). Gli SP possono individuare univocamente l'utente in forma pseudo-anonima, per fornirgli un servizio personalizzato (asserzione NameID nel subject).

L'Organizzazione di Appartenenza è responsabile della protezione dei dati forniti per conto dei propri utenti.

In questo documento vengono citati alcuni esempi di configurazione usando la sintassi dell'IdP Shibboleth 3.

## 1.1 Rilascio degli attributi

### 1.1.1 Policy sul rilascio degli attributi

Nel rispetto del principio di necessità[10] nel trattamento dei dati personali, gli IdP devono rilasciare in maniera automatica agli SP solo gli attributi strettamente necessari per l'erogazione del servizio.
E' d'obbligo per gli IdP il rilascio a tutti gli SP degli attributi classificati come "obbligatori" in questo documento.

[10] Art.3 L.196/2003 : 1. I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità' che permettano di identificare l'interessato solo in caso di necessità.

Oltre agli attributi obbligatori, affinché gli utenti appartenenti alla federazione IDEM possano accedere ai servizi di federazione, è necessario che gli IdP rilascino anche gli attributi *richiesti* dagli SP, fidandosi di quanto dichiarato nei metadati firmati e distribuiti dalla federazione IDEM.

Il rilascio degli attributi agli SP avviene tramite opportune regole (Attribute Release Policies o ARP) costruite e mantenute da parte del gestore dell'IdP. A tal proposito l'onere della gestione tecnica aumenta con l'aumentare degli attributi opzionali distribuibili, numero di SP federati, granularità dei meccanismi di consenso informato disponibili agli utenti appartenenti all'IdP gestito.
Tale onere può essere alleggerito sostanzialmente con la corretta valorizzazione dell'asserzione RequestedAttribute da parte degli SP nei propri metadati, così come indicato nel documento "IDEM Metadata Profile" e tramite l'adozione delle Entity Category dettagliato nel paragrafo dedicato.

La definizione delle politiche di rilascio degli attributi opzionali, che non ricadono nei casi precedenti, è a discrezione dell'ente a cui appartiene l'IdP, previo consenso informato dell'utente, come previsto dalla normativa attualmente in vigore. Nei paragrafi seguenti si suggeriscono alcuni meccanismi tra quelli disponibili.

L'adozione di queste linee-guida, insieme alla corretta valorizzazione degli attributi generati e all'uso del Resource Registry[11], consente d'implementare automatismi per generare le regole di rilascio degli attributi, e automatizzarne l'aggiornamento e l'adozione da parte dell'IdP .

```
<util:list id="shibboleth.AttributeFilterResources">
    <!-- Filtri acquisiti dalla federazione -->
    <ref bean="FileBacked_RR_Garr_ARP"/>
    <!-- Filtri locali IDP -->
    <value>
        "%{idp.home}/conf/attribute-filter.xml"
    </value>
</util:list>
<bean id="FileBacked_RR_Garr_ARP"
class="net.shibboleth.ext.spring.resource.FileBackedHTTPResource"
c:client-ref="shibboleth.FileCachingHttpClient"
c:url="https://registry.idem.garr.it/rr3/arp/format3exp/[parte relativa al singolo IdP]/arp.xml"
c:backingFile="%{idp.home}/conf/cache/RRgarrARP.xml"/>

<!--
Il bean definito scarica i filtri dal resource registry del Garr.
Gli aggiornamenti vengono controllati periodicamente secondo quanto definito dalla chiave
idp.service.attribute.filter.checkInterval nel file conf/services.properties.
-->
```

Esempio di caricamento automatico dei filtri in Shibboleth nel file services.xml

L'attuazione delle buone prassi suggerite è necessaria al buon ed efficace funzionamento della federazione.

### 1.1.2 Entity Category

Per semplificare la gestione degli attributi richiesti, la federazione si avvale delle Entity Category[12].
La loro funzione è il raggruppamento di servizi aderenti secondo caratteristiche specifiche.

[11] Resource Registry IDEM: https://registry.idem.garr.it/
[12] Entity category usate nella Fererazione IDEM:
Code of conduct: https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home
Research&Scholaship: https://refeds.org/category/research-and-scholarship

A seguire un caso d'uso reale nella federazione europea eduGAIN, come esempio.

Standard entity attribute for R&S (Service Provider):

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
    entityID="https://service.example.com/sp">
    <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
        <mdattr:EntityAttributes xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml:Attribute
                Name="http://macedir.org/entity-category"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml:AttributeValue>
                    http://refeds.org/category/research-and-scholarship
                </saml:AttributeValue>
            </saml:Attribute>
        </mdattr:EntityAttributes>
    </Extensions>
    ...
</EntityDescriptor>
```

Standard entity attribute for R&S (Identity Provider):

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
    entityID="https://service.example.com/idp">
    <Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
        <mdattr:EntityAttributes xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml:Attribute
                Name="http://macedir.org/entity-category-support"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml:AttributeValue>
                    http://refeds.org/category/research-and-scholarship
                </saml:AttributeValue>
            </saml:Attribute>
        </mdattr:EntityAttributes>
    </Extensions>
    ...
</EntityDescriptor>
```

Esempio di Research and Scholarship Entity Category da ReFeds

Entity Category support attribute (Service Provider):

```
<EntityAttributes xmlns="urn:oasis:names:tc:SAML:metadata:attribute">
    <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="http://macedir.org/entity-category">
        <AttributeValue>
            http://www.geant.net/uri/dataprotection-code-of-conduct/v1
        </AttributeValue>
    </Attribute>
</EntityAttributes>
```

Entity Category support attribute (Identity Provider):

```
<EntityAttributes xmlns="urn:oasis:names:tc:SAML:metadata:attribute">
    <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="http://macedir.org/entity-category-support">
        <AttributeValue>
            http://www.geant.net/uri/dataprotection-code-of-conduct/v1
        </AttributeValue>
    </Attribute>
</EntityAttributes>
```

Esempio di Code of Conduct Entity Category da GÉANT

### 1.1.3 Espressione del consenso informato

Può essere conveniente permettere all'utente di scegliere quali dei propri attributi l'organizzazione di appartenenza deve mantenere privati e conseguentemente non deve trasmettere a certi SP piuttosto che ad altri.
In linea con la normativa italiana ed europea sulla privacy viene caldamente raccomandato agli IdP l'uso di opportuni meccanismi d'espressione del consenso informato al trattamento dei dati da parte degli utenti finali ad esempio attraverso i meccanismi di Consent di Shibboleth 3.
La situazione ottimale prevede che i vincoli espressi dall'utente vengano applicati dopo l'autenticazione e prima del rilascio degli attributi all'SP.
Nel documento "IDEM Metadata Profile"[13] sono riportati i riferimenti per la configurazione di metadati specifici (mdui:PrivacyStatementUR) per l'esposizione delle privacy policy di SP e IdP.

[13] IDEM Metadata Profile: https://www.idem.garr.it/documenti/idem-metadata-profile.pdf

# 2 Panoramica sugli attributi

Gli attributi selezionati provengono dall'insieme degli attributi di base definiti per il protocollo LDAPv3 (RFC 4519 Lightweight Directory Access Protocol (LDAP): Schema for User Application) e dagli schemi Cosine, inetOrgPerson, eduPerson e Schac.

Ogni attributo prevede uno stato che può assumere uno fra i valori *obbligatorio*, *raccomandato* e *opzionale*.

L'insieme degli attributi *obbligatori* costituisce quindi il set minimo per aderire alla federazione nell'ipotesi di preservare al massimo la riservatezza dell'utente. Sono **obbligatori** la **generazione** e il **rilascio** del solio attributo **eduPersonScopedAffiliation** e dell'asserzione NameID in modalità persistente che permettono al Service Provider di verificare l'affiliazione dell'utente all'interno dell'organizzazione di appartenenza e poterlo riconoscere (in forma pseudo anonima) durante gli accessi successivi.

L'insieme degli attributi *raccomandati* è costituito da attributi richiesti frequentemente dagli SP e necessari per l'erogazione del servizio. Per fruire appieno delle risorse federate è necessario che questi attributi vengano generati dagli IdP e rilasciati agli SP quando previsto.

L'insieme degli attributi *opzionali* è costituito da attributi la cui necessità di generazione è influenzata da un effettivo uso da parte degli SP, vengono riportati con la dicitura "*opzionale*" allo scopo di suggerirne la corretta sintassi e semantica.

Gli attributi selezionati dalla federazione sono elencati di seguito.

## 2.1 Tipi di attributi

Gli attributi possono descrivere diversi tipi di caratteristiche dell'utente e si dividono in tre categorie principali: caratteristiche personali, informazioni di contatto, e dati per autorizzazione e accounting.

### 2.1.1 Caratteristiche personali

Ad esempio il nome, il cognome, e il titolo dell'utente.

### 2.1.2 Contatti

Attributi utilizzati per contattare personalmente l'utente al fine di fornirgli il servizio o parte di esso mediante strumenti diversi dal web.

### 2.1.3 Autorizzazioni e Accounting

Attributi sull'affiliazione il ruolo dell'utente nella propria organizzazione, identificativi personali persistenti, attributi di sottoscrizione del servizio o autorizzazioni aggiuntive.

#### Scope degli attributi

Alcuni attributi sono di tipo "scoped". La rappresentazione dell'organizzazione di appartenenza (<organizzazione>) deve essere un dominio DNS registrato dall'organizzazione di appartenenza. Nel caso un'organizzazione abbia registrato più di un dominio DNS, per gli scopi della federazione ne deve scegliere uno, comunicarlo alla federazione e quindi usarlo nella valorizzazione degli attributi.

## 2.2 Elenco attributi

Di seguito gli attributi in ordine di maggior utilizzo e rilevanza in federazione IDEM nel 2016.

| Nome LDAP | Origine | Descrizione | Stato | Uso [14] | R&S [15] |
|---|---|---|---|---|---|
| **eduPersonTargetedID** | eduPerson | Identificativi anonimi persistenti per l'utente relativi ai diversi Servizi | deprecato in favore di SAML 2.0 NameID | A | Full |
| **eduPersonScopedAffiliation** | eduPerson | Affiliazione secondo le convenzioni descritte nell'Appendice A | obbligatorio racc. eduGAIN | A | Full |
| **mail** | Cosine rfc4524 | Indirizzo eMail | raccomandato racc. eduGAIN | C | Min |
| **eduPersonPrincipalName** | eduPerson | Identificativo unico persistente dell'utente | raccomandato racc. eduGAIN | A | Min |
| **displayName** | RFC2798 eduPerson | The name(s) that should appear in white-pages-like applications for this person. From RFC2798 description: "preferred name of a person to be used when displaying entries." | raccomandato racc. eduGAIN | P | Min [16] |
| **orcid** | eduPerson | identificativo utente registrato su ORCID.org | opzionale | P | |

[14] Uso prevalente dell'attributo. Vedi paragrafo sui tipi di attributi. (da quale singola tabella originale proviene):
P: caratteristiche personali
C: contatti
A: autorizzazione e accounting

[15] Entity category Research and Scholarship:
Min: previsto dal set minimo dell'entity category, obbligatorio per l'entity category
Full: previsto dal set completo dell'entity category, raccomandato

[16] ① per l'entity category Research and Scholarship displayName è previsto in alternativa a sn + givenName: "displayName OR (givenName AND sn)"

| | | | | | |
|---|---|---|---|---|---|
| **sn**[17] | LDAPv3 rfc4519 eduPerson | Cognome | raccomandato | P | Min [18] |
| **givenName** | LDAPv3 rfc4519 | Nome | raccomandato | P | Min [19] |
| **eduPersonEntitlement** | eduPerson | Uno o più URI (URN o URL). Valori concordati con il fornitore di servizi. | raccomandato | A | |
| **cn**[20] | LDAPv3 rfc4519 eduPerson | Nome seguito da Cognome | raccomandato racc. eduGAIN | P | |
| **eduPersonOrgDN**[21] | eduPerson | Il Distinguished Name (DN) della entry che rappresenta l'organizzazione di appartenenza alla quale la persona è associata | opzionale | C | |
| **title** | LDAPv3 rfc4519 | Titolo nel contesto dell'organizzazione (es. "Direttore", "Responsabile Reparto X" ecc.) | opzionale | P | |
| **telephoneNumber** | LDAPv3 rfc4519 | Recapito telefonico | opzionale | C | |
| **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 | C | |
| **schacPersonalTitle** | schac | Titolo usato per salutare il soggetto. | opzionale | P | |

[17] ② sn, cn e ediPersonOrgDn sono i 3 attributi che costituiscono la "core" application utility class di eduPerson: http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201310.html
[18] vedi nota 16
[19] vedi nota 16
[20] vedi nota 17
[21] vedi nota 17

| | | | | | |
|---|---|---|---|---|---|
| | | Es: Sig., Sig.ra, Dott., Prof. | | | |
| **schacPersonalPosition** | LDAPv3 rfc4519 | Il codice rappresentativo dell'inquadramento della persona all'interno dell'organizzazione seconodo le convenzioni descritte nell'appendice B | opzionale | P | |
| **schacUserPresenceID** | schac | Recapiti relativi a diversi protocolli di rete | opzionale | C | |
| **mobile** | Cosine rfc4524 | Recapito cellulare | opzionale | C | |
| **schacMotherTongue** | schac | Lingua madre del soggetto | opzionale | P | |
| **preferredlanguage** | inetOrgPerson rfc2798 | Lingua scritta o parlata preferita dal soggetto | opzionale | P | |

# 3 Attributi: definizioni

## 3.1 Attributi: definizione dei meta-dati e notazione

Per tutti gli attributi sono definiti i seguenti meta-dati:

- **Descrizione:** una breve descrizione dell'attributo;
- **Identificativo SAML2:** URN SAML2 che identifica in maniera univoca l'attributo[22]
- **Semantica:** la semantica dell'attributo
- **Riferimenti:** standard di riferimento
- **Sintassi LDAP:** la sintassi LDAP dell'attributo (si veda RFC 2252)
- **# di valori:**
  - singolo;
  - multiplo;
- **Valori permessi:** una lista di valori permessi. Dove possibile la lista di valori è basata su standard nazionali o internazionali.
- **Classificazione:**

[22] L'urn è necessario nella configurazione di Shibboleth.

**-** *obbligatorio*: un IdP deve fornire questo attributo per poter fare parte della federazione;

**-** *raccomandato*: è fortemente raccomandato che un IdP generi questo attributo.

**-** *opzionale*: attributi poco utilizzati in federazione.

**-** *deprecato:* attributi il cui uso è da dismettere da parte di SP e IdP.

- **Note:** informazioni aggiuntive relative all'attributo;
- **Esempi:** esempi nel formato LDIF (RFC2849 LDAP Data Interchange Format);
- **Uso tipico:** ambito di utilizzo dell'attributo.

## 3.2 Dettaglio degli attributi in ordine alfabetico

In questa sezione sono elencati in ordine alfabetico gli attributi con le loro specifiche di dettaglio.

### 3.2.1 cn

| | |
|---|---|
| **Descrizione** | CommonName |
| **Identificativo SAML2** | urn:oid:2.5.4.3 |
| **Semantica** | Indica il nome completo della persona |
| **Riferimenti** | [RFC 4519] |
| **Sintassi LDAP** | Directory String 1.3.6.1.4.1.1466.115.121.1.15 |
| **# di valori** | Singolo |
| **Valori permessi** | n/d |
| **Classificazione** | Raccomandato |
| **Note** | [RFC 4519] prevede una molteplicità di valori per questo attributo. Tuttavia all'interno della federazione, l'Organizzazione di Appartenenza deve fornire un solo valore, ossia quello utilizzato per le comunicazioni ufficiali con la persona. |
| **Esempi** | `cn: Andrea Rossi` |
| **Uso tipico** | Informazioni aggiuntive sull'utente |

### 3.2.2 displayName

| | |
|---|---|
| **Descrizione** | Display Name |
| **Identificativo SAML2** | urn:oid:2.16.840.1.113730.3.1.241 |
| **Semantica** | Il nome della persona da usare in fase di visualizzazione della descrizione della sua entry, in particorlare in elenchi, rubriche e liste in generale. |
| **Riferimenti** | [RFC 2798] |
| **Sintassi LDAP** | Directory String 1.3.6.1.4.1.1466.115.121.1.15 |
| **# di valori** | Singolo |
| **Valori permessi** | n/d |
| **Classificazione** | Raccomandato |
| **Note** | Dove non già definito, questo attributo è valorizzabile in modo semplice utilizzando commonName o sn + givenName. Utilizzabile anche nei casi riferiti a persone la cui cultura di origine non distingue nome da |

| | |
|---|---|
| | cognome o non prevede uno dei due. Può contenere soprannomi o abbreviazioni differenti da sn e givenName. |
| **Esempi** | `displayName: Andrea Rossi` |
| **Uso tipico** | Informazioni aggiuntive sull'utente |

### 3.2.3 eduPersonEntitlement

| | |
|---|---|
| **Descrizione** | URI (URN o URL) che indica il diritto di accesso ad una risorsa. |
| **Identificativo SAML2** | urn:oid:1.3.6.1.4.1.5923.1.1.1.7 |
| **Semantica** | I valori contenuti sono tipicamente delle URI che individuano una risorsa o una particolare proprietà dell'utente stesso.<br>L'utente è autorizzato ad accedere ad una risorsa solo se eduPersonEntitlement contiene una particolare e predefinita URI. |
| **Riferimenti** | [EDUPER] |
| **Sintassi LDAP** | DirectoryString 1.3.6.1.4.1.1466.115.121.1.15 |
| **#di valori** | Multiplo |
| **Valori permessi** | n/d |
| **Classificazione** | Raccomandato |
| **Note** | Sebbene la maggior parte delle decisioni sull'autorizzazione all'accesso vengano prese basandosi semplicemente su uno o più attributi, per alcuni servizi l'accesso sarà consentito solo se viene soddisfatto un insieme più complesso di condizioni difficilmente determinabili a priori dal Service Provider.<br>A questo scopo è stato introdotto l'attributo eduPersonEntitlement: il fornitore del servizio definisce un valore specifico (formattato come URI) da assegnare a eduPersonEntitlement per marcare gli utenti che soddisfano determinate condizioni stabilite dal Fornitore.<br>L'organizzazione di appartenenza è responsabile del controllo sui propri utenti, affinché a coloro che soddisfano le condizioni venga assegnato il valore opportuno.<br>Con questo attributo il Fornitore di un Servizio, di fatto, delega l'Organizzazione di Appartenenza a decidere su quali utenti autorizzare per l'accesso al servizio in quanto è proprio l'Organizzazione dell'utente che valorizza questo attributo in accordo con i valori predefiniti con il fornitore del servizio. |
| **Esempi** | `eduPersonEntitlement: http://nilde.bo.cnr.it`<br>`eduPersonEntitlement: urn:mace:internet2:terena.nl:garr:service` |
| **Uso tipico** | Autorizzazione |

### 3.2.4 eduPersonOrcid

| | |
|---|---|
| **Descrizione** | Identificativi ricercatore ORCID appartenenti all'utente assegnati e gestiti da orcid.org |
| **Identificativo SAML2** | urn:oid:1.3.6.1.4.1.5923.1.1.1.16 |
| **Semantica** | Ogni valore rappresenta un identificativo ORCID registrato su ORCID.org e appartenente all'utente |
| **Riferimenti** | [RFC 4512];[EDUPER] |
| **Sintassi LDAP** | Directory String 1.3.6.1.4.1.1466.115.121.1.15 |
| **# di valori** | Multiplo |
| **Valori permessi** | n/d |
| **Classificazione** | Opzionale |
| **Note** | Gli identificativi ORCID iD sono identificativi digitali persistenti per singoli ricercatori. Lo scopo principale e collegare i ricercatori in maniera definitiva e non ambigua ai propri prodotti e pubblicazioni. Gli identificativi sono registrati e mantenuti da ORCID.org |
| **Esempi** | `eduPersonOrcid: http://orcid.org/0000-0002-1825-0097` |
| **Uso tipico** | NIH/NLM SciENcv self-service web application |

### 3.2.5 eduPersonOrgDN

| | |
|---|---|
| **Descrizione** | L'organizzazione dell'utente |
| **Identificativo SAML2** | urn:oid:1.3.6.1.4.1.5923.1.1.1.3 |
| **Semantica** | Il Distinguished Name (DN) della entry che rappresenta l'organizzazione di appartenenza alla quale la persona è associata |
| **Riferimenti** | [EDUPER] |
| **Sintassi LDAP** | Distinguished Name syntax 1.3.6.1.4.1.1466.115.121.1.12 |
| **# di valori** | Singolo |
| **Valori permessi** | n/d |
| **Classificazione** | Opzionale |
| **Note** | |
| **Esempi** | `eduPersonOrgDN: o=unimore,dc=unimore,dc=it`<br>`eduPersonOrgDN: o=Istituto di Fisiologia Clinica,dc=ifc,dc=cnr,dc=it` |
| **Uso tipico** | Informazioni aggiuntive sull'utente |

### 3.2.6 eduPersonOrgUnitDN

| | |
|---|---|
| **Descrizione** | L'unità organizzativa di appartenenza alla quale la persona è associata |
| **Identificativo SAML2** | urn:oid:1.3.6.1.4.1.5923.1.1.1.4 |
| **Semantica** | Il Distinguished Name (DN) della entry che rappresenta l'unità organizzativa di appartenenza alla quale la persona è associata (ad esempio Dipartimento) |
| **Riferimenti** | [EDUPER], [RFC 4524] |
| **Sintassi LDAP** | Distinguished Name syntax 1.3.6.1.4.1.1466.115.121.1.12 |
| **# di valori** | Multiplo |
| **Valori permessi** | n/d |
| **Classificazione** | Opzionale |
| **Note** | |
| **Esempi** | `eduPersonOrgUnitDN: ou=Dipartimento di Fisica,o=unimore,dc=unimore,dc=it` |
| **Uso tipico** | Informazioni aggiuntive sull'utente |

### 3.2.7 eduPersonPrincipalName

| | |
|---|---|
| **Descrizione** | Identificativo unico persistente dell'utente. |
| **Identificativo SAML2** | urn:oid:1.3.6.1.4.1.5923.1.1.1.6 |
| **Semantica** | Un identificativo che permette di riconoscere univocamente un utente in maniera coerente tra servizi diversi, nella forma: <identificativo>@<organizzazione> |
| **Riferimenti** | [EDUPER] |
| **Sintassi LDAP** | DirectoryString 1.3.6.1.4.1.1466.115.121.1.15 |
| **# di valori** | Singolo. |
| **Valori permessi** | n/d |
| **Classificazione** | Raccomandato |
| **Esempi** | `eduPersonPrincipalName: 132lk1j2l@biblio.bo.cnr.it`<br>`eduPersonPrincipalName: mrossi@esempio.it` |
| **Uso tipico** | Autorizzazione, Accounting |

### 3.2.8 eduPersonScopedAffiliation

| | |
|---|---|
| **Descrizione** | Indica l'affiliazione dell'utente presso l'organizzazione di appartenenza, nella forma: |

| | |
|---|---|
| | <affiliazione>@<organizzazione> |
| **Identificativo SAML2** | urn:oid:1.3.6.1.4.1.5923.1.1.1.9 |
| **Semantica** | Affiliazione secondo le convenzioni descritte nell'Appendice B in congiunzione con l'Organizzazione di Appartenenza indicata nella forma <organizzazione>. |
| **Riferimenti** | [EDUPER], [UK2] 3.2.2, [UK3] 7.1.2, Appendice B |
| **Sintassi LDAP** | Directory String 1.3.6.1.4.1.1466.115.121.1.15 |
| **# di valori** | Multiplo |
| **Valori permessi** | <affiliazione>: solo i valori permessi per eduPersonAffiliation (si veda Appendice B). <organizzazione>: nome DNS |
| **Classificazione** | Obbligatorio |
| **Note** | EduPersonScopedAffiliation permette la minima intrusione nella privacy dell'utente pur essendo sufficiente per decidere riguardo l'autorizzazione all'accesso nella maggior parte delle situazioni.<br>Il fornitore di servizio deve progettare il proprio sistema di autorizzazione in modo da usare questo attributo ovunque possibile. [UK2] |
| **Esempi** | `eduPersonScopedAffiliation: staff@biblio.bo.cnr.it`<br>`eduPersonScopedAffiliation: faculty@unica.it` |
| **Uso tipico** | Autorizzazione |

### 3.2.9 eduPersonTargetedID (deprecato)

| | |
|---|---|
| **Descrizione** | Identificativo anonimo, persistente e non riassegnabile di un utente, differente per ogni fornitore di servizio.<br>L'Organizzazione di Appartenenza comunica ad ogni Fornitore di Servizio (oppure ad un gruppo di Fornitori) solo il valore appropriato e non rivela tale valore ad altri Fornitori di Servizi. |
| **Identificativo SAML2** | urn:oid:1.3.6.1.4.1.5923.1.1.1.10 |
| **Semantica** | Ogni valore è un identificativo anonimo persistente associato all'utente per la fruizione di uno specifico servizio ed è composto da tre parti, nella forma:<br><organizzazione>!<servizio>!<stringa opaca><br>Per organizzazione si intende l'identificativo dello IdP dell'utente.<br>La stringa opaca deve essere univoca all'interno dell'organizzazione e generata con un meccanismo di hashing di dati univoci relativi all'utente. Gli identificativi persistenti definiti in SAML 2.0 sono conformi a queste specifiche. |
| **Riferimenti** | [EDUPER], [UK3] (par. 7.1.3.2) e [UK2] (par. 3.2.2), [SAML-CORE] (par. 8.3.7) |

| | |
|---|---|
| **Sintassi LDAP** | Directory String 1.3.6.1.4.1.1466.115.121.1.15 |
| **# di valori** | Multiplo |
| **Valori permessi** | stringa di lunghezza massima 256 caratteri |
| **Classificazione** | **Deprecato**<br>Usare al suo posto SAML 2.0 NameID di tipo persistent nel subject dell'asserzione. |
| **Note** | La stringa opaca non deve permettere al servizio di risalire direttamente all'identità dell'utente ma consentire solo il suo riconoscimento nelle sessioni successive di accesso al servizio. Una volta utilizzato per un utente il valore non può essere riutilizzato per un altro utente o servizio. |
| **Esempi** | `eduPersonTargetedID: biblio.bo.cnr.it!servizio_1!1304asf2rsfs`<br>`eduPersonTargetedID: unica.it!servizio_n!alskdj92920alsk` |
| **Uso tipico** | Autorizzazione, Accounting, servizio personalizzato |

### 3.2.10 givenName

| | |
|---|---|
| **Descrizione** | Nome |
| **Identificativo SAML2** | urn:oid:2.5.4.42 |
| **Semantica** | Nome proprio della persona come usato nelle comunicazioni ufficiali |
| **Riferimenti** | [RFC 4519];[EDUPER] |
| **Sintassi LDAP** | Directory String 1.3.6.1.4.1.1466.115.121.1.15 |
| **# di valori** | Singolo |
| **Valori permessi** | n/d |
| **Classificazione** | Raccomandato |
| **Note** | [RFC 4519] prevede una molteplicità di valori per questo attributo. Tuttavia all'interno della federazione, l'Organizzazione di Appartenenza deve fornire un solo valore, ossia quello utilizzato per le comunicazioni ufficiali con la persona. |
| **Esempi** | `givenName: Andrea` |
| **Uso tipico** | Informazioni aggiuntive sull'utente |

### 3.2.11 mail

| | |
|---|---|
| **Descrizione** | Indirizzo e-mail |
| **Identificativo SAML2** | urn:oid:0.9.2342.19200300.100.1.3 |
| **Semantica** | Indica la casella di posta elettronica dell'utente |

| | |
|---|---|
| **Riferimenti** | [RFC 4524] |
| **Sintassi LDAP** | IA5 String 1.3.6.1.4.1.1466.115.121.1.26 |
| **# di valori** | Multiplo |
| **Valori permessi** | n/d |
| **Classificazione** | Raccomandato |
| **Note** | I valori dovrebbero essere editabili dall'utente stesso. |
| **Esempi** | `mail: andrea.rossi@unimi.it` |
| **Uso tipico** | Informazioni aggiuntive sull'utente |

### 3.2.12 mobile

| | |
|---|---|
| **Descrizione** | Recapito cellulare |
| **Identificativo SAML2** | urn:oid:0.9.2342.19200300.100.1.41 |
| **Semantica** | Indica il numero di cellulare associato all'utente, indicato in accordo al formato internazionale dei numeri di telefono |
| **Riferimenti** | [RFC 4524] |
| **Sintassi LDAP** | Telephone Number 1.3.6.1.4.1.1466.115.121.1.50 |
| **# di valori** | Multiplo |
| **Valori permessi** | n/d |
| **Classificazione** | Opzionale |
| **Note** | Particolari servizi potrebbero voler contattare l'utente al telefono via voce oppure via SMS. Occorre fare attenzione alla privacy dell'utente quando si trasferiscono numeri telefonici privati. Non ci dovrebbero essere problemi nel trasferimento di numeri telefonici di servizio. I valori dovrebbero essere editabili dall'utente stesso. |
| **Esempi** | `mobile: +39 347 379 15 71` |
| **Uso tipico** | Informazioni aggiuntive sull'utente |

### 3.2.13 preferredLanguage

| | |
|---|---|
| **Descrizione** | Lingua Preferita dall'utente |
| **Identificativo SAML2** | urn:oid:2.16.840.1.113730.3.1.39 |
| **Semantica** | Lingua scritta o parlata preferita dall'utente |
| **Riferimenti** | [RFC2798], [RFC5646],[ISO 639], [ISO 3166] |
| **Sintassi LDAP** | Directory String 1.3.6.1.4.1.1466.115.121.1.15 |

| | |
|---|---|
| **# di valori** | Singolo |
| **Valori permessi** | I language-tag sono formati da un primary-tag e da più subtag<br>Questi ultimi posso anche essere vuoti.<br>language-tag = primary-tag *( "-" subtag)<br>primary-tag = 1*8ALPHA<br>subtag = 1*8ALPHA<br>Non sono consentiti gli spazi bianchi tra i tag. I tag sono case unsensitive. I name space dei language-tag sono amministrati da IANA. |
| **Classificazione** | Opzionale |
| **Note** | |
| **Esempi** | `preferredLanguage: it`<br>`preferredLanguage: it-ch` |
| **Uso tipico** | Informazioni aggiuntive sull'utente |

### 3.2.14 schacMotherTongue

| | |
|---|---|
| **Descrizione** | Lingua madre dell'utente |
| **Identificativo SAML2** | urn:oid:1.3.6.1.4.1.25178.1.2.1 |
| **Semantica** | È la prima lingua che una persona impara |
| **Riferimenti** | [SCHAC], [RFC5646], [ISO 639] |
| **Sintassi LDAP** | Directory String 1.3.6.1.4.1.1466.115.121.1.15 |
| **# di valori** | Singolo |
| **Valori permessi** | |
| **Classificazione** | Opzionale |
| **Note** | |
| **Esempi** | `schacMotherTongue: it`<br>`schacMotherTongue: fr-ch` |
| **Uso tipico** | Informazioni aggiuntive sull'utente |

### 3.2.15 schacPersonalPosition

| | |
|---|---|
| **Descrizione** | Il codice rappresentativo dell'inquadramento della persona all'interno dell'organizzazione secondo le convenzioni descritte nell'appendice B |
| **Identificativo SAML2** | urn:oid:1.3.6.1.4.1.25178.1.2.13 |
| **Semantica** | Specifica la posizione (ruolo) all'interno dell'organizzazione |
| **Riferimenti** | [SCHAC] |
| **Sintassi LDAP** | Directory String 1.3.6.1.4.1.1466.115.121.1.15 |

| | |
|---|---|
| **# di valori** | Multiplo |
| **Valori permessi** | I valori sono definiti (o la loro definizione è esplicitamente delegata) da TERENA URN Registry. Si veda: http://www.terena.org/registry/terena.org/schac/personalPosition/ |
| **Classificazione** | Opzionale |
| **Note** | |
| **Esempi** | `urn:schac:personalPosition:pl:umk.pl:programmer` |
| **Uso tipico** | Informazioni aggiuntive sull'utente |

### 3.2.16 schacPersonalTitle

| | |
|---|---|
| **Descrizione** | Titolo usato per salutare il soggetto |
| **Identificativo SAML2** | urn:oid:1.3.6.1.4.1.25178.1.2.8 |
| **Semantica** | Specifica il titolo personale dell'utente |
| **Riferimenti** | [SCHAC], [RFC4524] |
| **Sintassi LDAP** | Directory String 1.3.6.1.4.1.1466.115.121.1.15 |
| **# di valori** | Singolo |
| **Valori permessi** | n/d |
| **Classificazione** | Opzionale |
| **Note** | |
| **Esempi** | `schacPersonalTitle: Sig.` |
| **Uso tipico** | Informazioni aggiuntive sull'utente |

### 3.2.17 schacUserPresenceID

| | |
|---|---|
| **Descrizione** | Insieme di recapiti relativi alla presenza della persona in rete |
| **Identificativo SAML2** | urn:oid:1.3.6.1.4.1.25178.1.2.12 |
| **Semantica** | Recapiti relativi a diversi protocolli in rete |
| **Riferimenti** | [SCHAC] |
| **Sintassi LDAP** | Directory String 1.3.6.1.4.1.1466.115.121.1.15 |
| **# di valori** | Multiplo |
| **Valori permessi** | n/d |
| **Classificazione** | Opzionale |
| **Note** | I valori dovrebbero essere editabili dall'utente stesso. |

| | |
|---|---|
| **Esempi** | `schacUserPresenceID = xmpp:a.rossi@unimi.it`<br>`schacUserPresenceID = sip:rossi@myweb.com`<br>`schacUserPresenceID = sip:+39-95-505-6600@unimi.it;transport=TCP;user=phone`<br>`schacUserPresenceID = sips:alice@atlanta.com?subject=project%20x&priority=urgent`<br>`schacUserPresenceID = h323:andy@myweb.it:808;params`<br>`schacUserPresenceID = skype:andrea.rossi` |
| **Uso tipico** | Informazioni aggiuntive sull'utente |

### 3.2.18 sn

| | |
|---|---|
| **Descrizione** | Cognome |
| **Identificativo SAML2** | urn:oid:2.5.4.4 |
| **Semantica** | Cognome della persona come usato nelle comunicazioni ufficiali |
| **Riferimenti** | [RFC 4519];[eduPerson] |
| **Sintassi LDAP** | Directory String 1.3.6.1.4.1.1466.115.121.1.15 |
| **# di valori** | Singolo |
| **Valori permessi** | n/d |
| **Classificazione** | Raccomandato |
| **Note** | [RFC 4519] prevede una molteplicità di valori per questo attributo. Tuttavia all'interno della federazione, l'Organizzazione di Appartenenza deve fornire un solo valore, ossia quello utilizzato per le comunicazioni ufficiali con la persona. |
| **Esempi** | `sn: Rossi` |
| **Uso tipico** | Informazioni aggiuntive sull'utente |

### 3.2.19 telephoneNumber

| | |
|---|---|
| **Descrizione** | Recapito telefonico |
| **Identificativo SAML2** | urn:oid:2.5.4.20 |
| **Semantica** | Numero di telefono dell'utente, indicato in accordo al formato internazionale dei numeri di telefono |
| **Riferimenti** | [RFC 4519] |
| **Sintassi LDAP** | Telephone Number 1.3.6.1.4.1.1466.115.121.1.50 |
| **# di valori** | Multiplo |
| **Valori permessi** | n/d |
| **Classificazione** | Opzionale |
| **Note** | Particolari servizi potrebbero voler contattare l'utente al telefono. |

| | |
|---|---|
| | Occorre fare attenzione alla privacy dell'utente quando si trasferiscono numeri telefonici privati. Non ci dovrebbero essere problemi nel trasferimento di numeri telefonici di servizio. I valori dovrebbero essere editabili dall'utente stesso. |
| **Esempi** | `telephoneNumber: +39 02 779 160 81` |
| **Uso tipico** | Informazioni aggiuntive sull'utente |

### 3.2.20 title

| | |
|---|---|
| **Descrizione** | Titolo della persona nel contesto dell'organizzazione |
| **Identificativo SAML2** | urn:oid:2.5.4.12 |
| **Semantica** | Indica il titolo di una persona nel contesto della propria organizzazione |
| **Riferimenti** | [RFC 4519] |
| **Sintassi LDAP** | Directory String 1.3.6.1.4.1.1466.115.121.1.15 |
| **# di valori** | Multiplo |
| **Valori permessi** | n/d |
| **Classificazione** | Opzionale |
| **Note** | |
| **Esempi** | `title: Direttore` |
| **Uso tipico** | Informazioni aggiuntive sull'utente |

# 4 Appendice A: affiliazione

## 4.1 Capire l'affiliazione

L'affiliazione definisce la relazione che esiste tra l'utente e la propria Organizzazione di Appartenenza. Per descrivere l'affiliazione, all'interno delle comunità scientifiche, Internet2 propone lo schema **eduPerson** [EDUPER], nella fattispecie con gli attributi **eduPersonAffiliation**, **eduPersonScoperdAffiliation**, e **eduPersonPrimaryAffiliation**.

L'attributo di riferimento in IDEM è **eduPersonScopedAffiliation**.

A questi attributi è associabile soltanto un insieme predefinito di valori elencati nel documento di riferimento. I valori usati in IDEM sono:**, student, staff, alum, member, affiliate, e library-walk-in.**

Volutamente non sono stati inclusi i valori "**other**" o "**misc**" perché sono semanticamente equivalenti a "nessuno dei precedenti". Volendo indicare tale proprietà per una specifica persona, l'attributo dovrà essere "non valorizzato".

I valori elencati individuano delle *classi* di persone; alcune classi sono specializzazioni di altre.

**Member** contiene tutte le persone che hanno un rapporto istituzionale con l'organizzazione di appartenenza e ai quali viene dato un insieme base di privilegi. Sono member tutti gli appartenenti a staff student, ma tipicamente non gli alum.

**Student** e **staff** sono quindi due specializzazione distinte di member:

Il valore **staff** va utilizzato per 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.

Con **student** si indicano gli studenti regolarmente iscritti ad uno dei corsi dell'organizzazione di appartenenza.

**Affiliate** si applica alle persone con le quali l'organizzazione di appartenenza ha una qualsiasi forma di rapporto ed alle quali è necessario attribuire un'identità di utente, ma alle quali non vengono estesi i privilegi derivanti dall'essere membri dell'organizzazione stessa. Potrebbero rientrare in questa categoria i fornitori di servizi o materiali delle organizzazioni, ricercatori di altre organizzazioni che collaborano con un gruppo interno, persone per le quali è necessaria l'identificazione per servizi molto particolari riservati ad esterni all'università stessa. *Normalmente gli **affiliate** non sono **member***, se non in casi eccezionali: ad esempio uno studente che sia anche dipendente di una ditta che fornisce servizi ad un'università.

**Alum** comprende gli ex studenti dell'organizzazione di appartenenza che hanno completato almeno il primo livello di studi. E' possibile che un **alum** sia anche **staff** oppure **affiliate** dell'organizzazione.

**Library-walk-in** indica i frequentatori di una biblioteca ed è pensato per semplificare la gestione di frequenti accordi contrattuali con i fornitori di risorse. Il valore è indipendente dagli altri valori indicanti l'affiliazione, ciò vuol dire che il possedere tale requisito non influisce o pregiudica l'avere un altro tipo di affiliazione e viceversa.

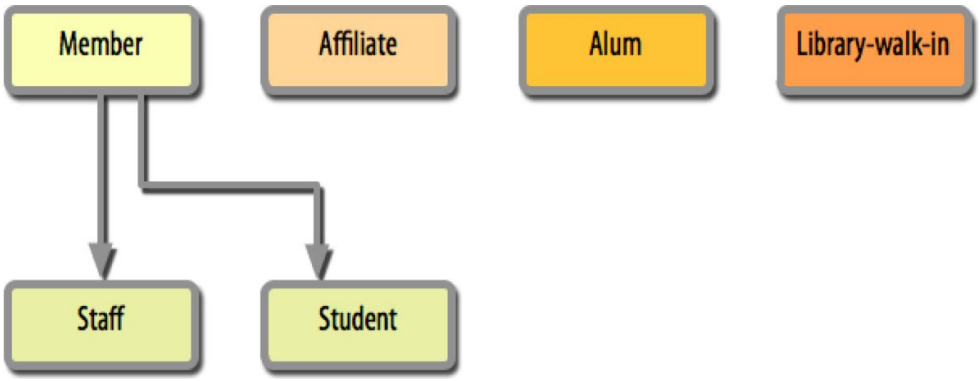


Figura 3: Valori per eduPersonAffiliation

La figura 3 rappresenta le classi sopra descritte e le relative specializzazioni.

L'attributo **eduPersonAffiliation** assume valori multipli quando una persona appartiene ad una classe specializzata.

## 4.2 Esempi pratici

Ecco alcuni scenari comuni. Un docente avrà sempre:

```
eduPersonAffiliation: staff
eduPersonAffiliation: member
```

Uno studente avrà sempre:

```
eduPersonAffiliation: student
eduPersonAffiliation: member
```

Se uno studente ha anche una borsa di studio, oppure un contratto con l'organizzazione stessa per svolgere un compito istituzionale; egli avrà:

```
eduPersonAffiliation: student
eduPersonAffiliation: staff
eduPersonAffiliation: member
```

Se un dipendente amministrativo si è anche laureato nella stessa università, avrà:

```
eduPersonAffiliation: staff
eduPersonAffiliation: member
eduPersonAffiliation: alum
```

Ad eccezione di **library-walk-in**, che come detto è compatibile con qualsiasi altro valore, solo in casi veramente eccezionali un **affiliate** avrà anche un altro valore per **eduPersonAffiliation**, così come solo una minoranza tra tutti gli **alum** avranno anche altri valori per lo stesso attributo.

Per gli scopi della federazione anziché usare **eduPersonAffiliation** si preferisce usare **eduPersonScopedAffiliation**, perché nello stesso attributo è specificata l'organizzazione di appartenenza, oltre al tipo di affiliazione. In questo modo si ottengono informazioni anche sull'organizzazione di appartenenza dell'utente ed il tipo di rapporto che questi ha con la corrispondente organizzazione.

Per definire l'attributo **eduPersonScopedAffiliation** occorre considerare per ciascun utente i valori di eduPersonAffiliation ed aggiungere in coda ai valori il carattere @ e l'indicazione dell'organizzazione nella forma di security domain, che per convenzione è il dominio registrato (secondo la convenzione per il Domain Name Service) per l'organizzazione di appartenenza. Ad esempio, un tecnico dell'Università di Modena e Reggio Emilia avrà:

```
eduPersonScopedAffiliation: staff@unimore.it
eduPersonScopedAffiliation: member@unimore.it
```

## 4.3 Corrispondenza tra le categorie note e le possibili affiliazioni

La seguente tabella di corrispondenze consente ai membri della federazione di assegnare ai propri utenti valori semanticamente uniformi per l'attributo **eduPersonScopedAffiliation**. La tabella si riferisce a ruoli censiti in ambito universitario e negli istituti di ricerca.

N.B. Qualora per alcuni contesti esistessero ruoli non previsti nelle tabelle successive occorrerà darne comunicazione agli organi della federazione, che provvederanno alla modifica delle stesse, evitando di assegnare a tali utenti ruoli inappropriati.

| Ruolo | eduPersonAffiliation |
|---|---|
| assistente universitario | staff, member |
| associato (ad es. CNR) | member |
| cessato | (none) |
| 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 |
| dipendente azienda ospedaliera/policlinico | member |
| dipendente di altra azienda sanitaria | member |
| direttore amministrativo | staff, member |
| dirigente | staff, member |
| dirigente a contratto | staff, member |
| dirigente di ricerca | staff, member |
| dirigente tecnologo | staff, member |
| docente a contratto | staff, member |
| dottorando | staff, member, student |
| dottorando di altra università (consorziata) | member |

| | |
|---|---|
| esperto linguistico | staff, member |
| fornitore (dipendente o titolare delle ditte fornitrici) | affiliate |
| interinale | staff, member |
| ispettore generale | affiliate |
| laureato frequentatore/collaboratore di ricerca (a titolo gratuito) | member |
| lavoratore occasionale (con contratto personale senza partita iva) | staff, member |
| lettore di scambio | member |
| libero professionista (con contratto personale con partita iva) | staff, member |
| ospite / visitatore | affiliate |
| personale tecnico-amministrativo a tempo determinato | staff, member |
| personale tecnico-amministrativo | staff, member |
| primo ricercatore | staff, member |
| primo tecnologo | staff, member |
| professore associato | staff, member |
| professore emerito | member |
| professore incaricato interno | staff,member |
| professore incaricato esterno | staff,member |
| professore fuori ruolo | affiliate (era errato) |
| professore ordinario | staff, member |
| ricercatore | staff, member |
| specializzando | staff, member, student |
| studente | student, member |
| studente erasmus in ingresso | student |
| studente fuori sede (tesista, tirocinante, …) | student, member |
| studente laurea specialistica | student, member |
| studente master | student, member |
| studente siss | student, member |
| supervisore siss | staff, member |
| supplente docente | staff, member |
| titolare di assegno di ricerca | staff, member |
| titolare di borsa di studio | member |

| | |
|---|---|
| tecnologo | staff, member |
| tutor | staff, member |
| volontario servizio civile nazionale | member |

N.B. Le affiliazioni Alum e Library Walk-In possono essere aggiunte a tutti i ruoli, ove risultasse applicabile.

## 4.4 Configurazione di Shibboleth

Una volta compreso il significato dell'affiliazione e avendo chiaro in quale delle precedenti categorie rientrano i propri utenti occorre configurare Shibboleth in maniera che restituisca tali valori. Come descritto in precedenza, l'attributo utilizzato in IDEM è **eduPersonScopedAffiliation**. La configurazione di Shibboleth può essere effettuata in due modi diversi in funzione del fatto che i valori da restituire siano o no già presenti nel backend (LDAP o DBMS).

Per la configurazione di **eduPersonScopedAffiliation**, come risulta evidente dalla stessa denominazione dell'attributo, è conveniente utilizzare un attributo di tipo scoped, indicando come scope il proprio dominio.

**N.B.** È importante fare attenzione che lo **scope** utilizzato **coincida** con quello **dichiarato nei metadati**.

Nel caso in cui i valori di affiliazione siano già presenti nel backend è sufficiente configurare *sourceAttributeID* con il nome dell'attributo contente tali valori, avendo cura di indicare anche il riferimento alla sorgente di tali attributi (`resolver:Dependency ref="myLDAP"`). La configurazione potrebbe quindi essere:

```
<resolver:AttributeDefinition id="eduPersonScopedAffiliation" xsi:type="ad:Scoped"
               scope="example.org" sourceAttributeID="eduPersonAffiliation">
   <resolver:Dependency ref="myLDAP" />
   <resolver:AttributeEncoder xsi:type="enc:SAML2ScopedString"
               name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9"
               friendlyName="eduPersonScopedAffiliation" />
</resolver:AttributeDefinition>
```

Nella maggior parte dei casi avere l'attributo relativo all'affiliazione già presente in maniera esplicita nel proprio backend può risultare un inutile spreco di spazio oltre che di tempo (necessario per valorizzare l'attributo ad ogni nuovo inserimento di un utente). In genere è conveniente generare dinamincamente l'attributo in Shibboleth a partire da attributi *già esistenti nel proprio backend*. Per fare ciò, nell'attribute-resolver.xml, è necessario definire un *mapped attribute*, che mappi i valori nel backend con i valori previsti per l'affiliazione come indicato nella tabella vista nel paragrafo precedente. Nell'ipotesi che questo attributo fosse ad esempio *employeeType* la configurazione potrebbe essere:

```
<resolver:AttributeDefinition id="eduPersonAffiliation" xsi:type="ad:Mapped"
       sourceAttributeID="employeeType">
   <resolver:Dependency ref="myLDAP" />
   <resolver:AttributeEncoder xsi:type="enc:SAML2String"
               name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
      friendlyName="eduPersonAffiliation" />
   <ad:DefaultValue>affiliate</ad:DefaultValue>
   <!-- da definire laddove necessario
```

```
   <ad:ValueMap>
       <ad:ReturnValue>alum</ad:ReturnValue>
   </ad:ValueMap>
   -->
   <!-- da completare con i ruoli all'interno del proprio ente -->
   <ad:ValueMap>
       <ad:ReturnValue>affiliate</ad:ReturnValue>
       <ad:SourceValue>convenzionato</ad:SourceValue>
       <ad:SourceValue>fornitore</ad:SourceValue>
       <ad:SourceValue>ospite</ad:SourceValue>
   </ad:ValueMap>
   <ad:ValueMap>
       <ad:ReturnValue>member</ad:ReturnValue>
       <ad:SourceValue>dirigente tecnologo</ad:SourceValue>
       <ad:SourceValue>dirigente di ricerca</ad:SourceValue>
       <ad:SourceValue>primo tecnologo</ad:SourceValue>
       <ad:SourceValue>primo ricercatore</ad:SourceValue>
       <ad:SourceValue>tecnologo</ad:SourceValue>
       <ad:SourceValue>ricercatore</ad:SourceValue>
       <ad:SourceValue>personale tecnico-amministrativo</ad:SourceValue>
       <ad:SourceValue>specializzando</ad:SourceValue>
   </ad:ValueMap>
   <ad:ValueMap>
       <ad:ReturnValue>staff</ad:ReturnValue>
       <ad:SourceValue>dirigente tecnologo</ad:SourceValue>
       <ad:SourceValue>dirigente di ricerca</ad:SourceValue>
       <ad:SourceValue>primo tecnologo</ad:SourceValue>
       <ad:SourceValue>primo ricercatore</ad:SourceValue>
       <ad:SourceValue>tecnologo</ad:SourceValue>
       <ad:SourceValue>ricercatore</ad:SourceValue>
       <ad:SourceValue>personale tecnico-amministrativo</ad:SourceValue>
       <ad:SourceValue>specializzando</ad:SourceValue>
   </ad:ValueMap>
   <ad:ValueMap>
       <ad:ReturnValue>student</ad:ReturnValue>
       <ad:SourceValue>studente</ad:SourceValue>
       <ad:SourceValue>studente laurea specialistica</ad:SourceValue>
       <ad:SourceValue>specializzando</ad:SourceValue>
   </ad:ValueMap>
</resolver:AttributeDefinition>

<resolver:AttributeDefinition id="eduPersonScopedAffiliation"
              xsi:type="ad:Scoped"
```

```
                scope="ifc.cnr.it">
   <resolver:Dependency ref="eduPersonAffiliation" />
   <resolver:AttributeEncoder xsi:type="enc:SAML2ScopedString"
            name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9"
                friendlyName="eduPersonScopedAffiliation" />
</resolver:AttributeDefinition>
```

Nell'esempio precedente è stato definito l'attributo **eduPersonAffiliation** utilizzato poi da **eduPersonScopedAffiliation**. In base alla precedente configurazione, nel caso in cui una determinata posizione non fosse prevista, l'utente verrebbe considerato come *affiliate* (DefaultValue). **N.B.** Il valore di default viene assegnato solo con il campo valorizzato. Nel caso in cui l'attributo di origine non fosse definito o prevedesse una stringa nulla il "mapped attribute" non verrebbe definito.

# 5 Appendice B: Identificativi univoci (NameID e eduPersonTargetedID)

Un Fornitore di Servizi usa un identificativo univoco per realizzare, tramite pseudonimo, la persistenza fra diverse sessioni dello stesso utente, offrendogli così una personalizzazione del servizio nel rispetto della privacy.

Per implementare questa funzionalità è necessario che l'IdP rilasci questo identificativo all'SP in modo da creare una relazione uno-a-molti, anonima e permanente fra lo stesso utente ed i Fornitori di Servizi. La **generazione** e il **rilascio** sono **obbligatori** nella federazione IDEM.

Generalmente la gestione di tale identificativo comporta qualche difficoltà a causa della sua dipendenza da altri attributi (ad esempio da **eduPersonPrincipalName**). La generazione dei valori, conseguente ad una richiesta, può essere effettuata con tre modalità:

- **Temporaneo o di tipo Transient** . In questo modo, per gli SP che lo richiedono, l'identificativo unico viene generato in maniera casuale, diverso per ogni SP e con una durata breve determinata. Tale identificativo, se viene tracciato nei log dell'IdP, può essere usato per ottemperare alle funzioni di accountability delle operazioni di un utente di un IdP presso un SP. Tale identificativo preserva in maniera massima i dati personali dell'utente in federazione. Risulta però inutile in tutti quelli scenari in cui è necessario riconoscere l'utente anche a distanza di tempo.
- **Algoritmica o di tipo computed (deprecata)**. In questo modo i valori vengono generati ad ogni richiesta partendo da valori dipendenti dall'utente, dall'IdP e dal SP, come esemplificato in precedenza. In questo modo si eviterebbe la necessità, da parte dell'IdP, di memorizzare i valori dell'attributo.
  Questo metodo implica tuttavia alcuni svantaggi che hanno portato a deprecarlo:
  - Al variare dell'algoritmo di hashing (anche a causa di eventuali vulnerabilità o semplicemente a causa della indisponibilità di librerie e metodi software) il valore cambia invalidando la persistenza dell'identità presso tutti gli SP che ne fanno uso.
  - Costituendo di fatto uno dei dati personali dell'utente, lo stesso può potenzialmente richiederne la cancellazione o la variazione (ad esempio in seguito a un furto di identità). Tale operazione non può essere effettuata efficientemente su questo tipo di identificativi se non nel caso di seguito descritto.
- **Per memorizzazione - StoredID (consigliata)**. L'alternativa al metodo precedente è quella di memorizzare in una base di dati tutti i valori generati in maniera algoritmica (come nel caso del computed) o casuale per l'Identificativo. Si ottiene così un identificativo univoco, persistente e modificabile/revocabile in caso di necessità. La gestione comporta lo svantaggio di dover amministrare un database dedicato (e condiviso tra più nodi dell'IdP qualora lo IdP fosse in cluster). Questo database consiste di una sola tabella "shibpid".
  Utilizzando questo approccio, quando un utente si autentica presso un servizio, Shibboleth verifica nel database se esiste già una entry relativa a **quell'utente presso quel servizio.** In caso negativo l'identificativo viene generato e memorizzato nel database per gli accessi

futuri allo stesso SP. Se invece trova una entry già salvata, restituisce il valore di quest'ultima.

## Salt

Il salt, quando usato nell'algoritmo di generazione della stringa opaca di Shibboleth, è un valore unico per tutti gli utenti ma che deve essere sufficientemente complesso, ad esempio il risultato di 'openssl rand -base64 36' o salt="adn9tkalnci2f09fjs3v981298fkfjkgri"

e mantenuto segreto per evitare che, conoscendo l'algoritmo utilizzato ed i parametri su cui viene applicato, si possa risalire ai valori dell'identificativo. Nel caso di un cluster di IdP, questo valore deve essere identico su tutti i nodi.

## Persistenza/Riassegnamento

Ogni valore dell'Identificativo deve essere unico all'interno dell'IdP e non dovrà essere riassegnato ad un diverso utente neanche in tempi diversi. Questo vincolo dovrebbe essere soddisfatto se i valori vengono generati con un buon algoritmo di hash che garantisce una probabilità di collisione prossima alla zero o se l'attributo utilizzato per la generazione dei valori non viene a sua volta riassegnato. I valori dell'attributo dovrebbero rimanere immodificati fino a che non ci sia l'effettiva necessità di farlo.

In tale caso la necessità di modificare un valore non dovrebbe comportare la modifica di tutti gli altri valori di uno stesso utente. Come già evidenziato la sola generazione algoritmica dei valori (senza memorizzazione in database) rende difficile il rispetto di tale caratteristica.

La scelta su come l'identificativo univoco debba essere generato e/o trattato, al netto delle considerazioni fatte, resta a carico dell'IdP.

Nelle implementazioni IdP Shibboleth 2.X per rilasciare l'identificativo univoco veniva usato comunemente *l'attributo* **eduPersonTargetedID** definito nella versione del 2006 di [EDUPER].

A partire dalla versione 3 di Shibboleth, viene incoraggiata la rappresentazione del dato all'interno dell'oggetto dell'**asserzione** come *SAML 2.0* **NameID** anziché come **attributo eduPersonTargetedID**. Tale funzionalità era già presente in Shibboleth nelle versioni 2.x e in altre implementazioni molto diffuse di SAML.

La maggior parte dei Service Provider supporta l'utilizzo di entrambi (asserzione NameID oppure attributo eduPersonTargetedID), ma si raccomanda l'utilizzo del primo.

Il rilascio dell'attributo eduPersonTargetedID è infatti sconsigliato, salvo non sia indispensabile concedere l'accesso a un SP che ancora lo richieda in maniera obbligatoria - in attesa che anche questo si adegui all'uso di NameID. Per la configurazione di eduPersonTargetedID si rimanda alle vecchie guide IDEM per Shibboleth 2.x.

# Bibliografia

## Documentazione federazione Inglese

[UK1] Rules of membership for the federation

http://www.ukfederation.org.uk/library/uploads/Documents/rules-of-membership.pdf

[UK2] Recommendations for use of personal data

http://www.ukfederation.org.uk/library/uploads/Documents/recommendations-for-use-of-personal-data.pdf

[UK3] Technical Recommendations for participants

http://www.ukfederation.org.uk/library/uploads/Documents/technical-recommendations-for-participants.pdf

[UK4] Federation technical specifications

http://www.ukfederation.org.uk/library/uploads/Documents/federation-technical-specifications.pdf

[UK5] Federation operator procedures

http://www.ukfederation.org.uk/library/uploads/Documents/federation-operator-procedures.pdf

## Documentazione federazione Svizzera

[SW1] AAI Service Agreement

http://www.switch.ch/aai/docs/AAI_Service_Agreement.pdf

[SW2] AAI Service Agreement exhibits

http://www.switch.ch/aai/docs/AAI_Service_Agreement_exhibits.pd

[SW3] AAI Federation Partner Agreement

http://www.switch.ch/aai/docs/AAI_Partner_Agreement.pdf

[SW4] AAI Federation Partner Agreement Policy

http://www.switch.ch/aai/docs/AAI_Policy.pdf

[SW5] Authorization Attribute Specification

http://www.switch.ch/aai/docs/AAI_Attr_Specs.pdf

[SW6] swissedu.schema

http://www.switch.ch/aai/docs/swissedu.schema

## Documentazione federazione Spagnola

[ES1] irisUserPrivateAttribute

http://www.rediris.es/ldap/esquemas/iris/irisUserPrivateAttribute/

## Documentazione federazione Norvegese

[NO1] norEdu* Object Class Specification

http://www.feide.no/feide/sites/drupal.uninett.no.feide/files/documents/norEdu_spec.pdf

[NO2] Feide eduPersonAffiliation

http://rnd.feide.no/attribute/edupersonaffiliation/

## RFC, Schemi LDAP e ISO

[RFC4512] RFC 4512 Lightweight Directory Access Protocol (LDAP): Directory Information Models

https://tools.ietf.org/html/rfc4512

[RFC4519] RFC 4519 Lightweight Directory Access Protocol (LDAP): Schema for User Applications

http://tools.ietf.org/html/rfc4519

[RFC2798] RFC 2798 Definition of the inetOrgPerson LDAP Object Class

http://tools.ietf.org/html/rfc2798

[RFC4524] RFC 4524 COSINE LDAP/X.500 Schema

http://tools.ietf.org/html/rfc4524

[RFC3986] Uniform Resource Identifier (URI): Generic Syntax

http://tools.ietf.org/html/rfc3986

[RFC1737] Functional Requirements for Uniform Resource Names

http://tools.ietf.org/html/rfc1737

[RFC2141] URN Syntax

http://tools.ietf.org/html/rfc2141

[RFC3305] Report from the Joint W3C/IETF URI Planning Interest Group: Uniform Resource Identifiers (URIs), URLs, and Uniform Resource Names (URNs): Clarifications and Recommendations

http://tools.ietf.org/html/rfc3305

[RFC5646] Tags for Identifying Languages

http://tools.ietf.org/html/rfc5646

[EDUPER] EduPerson Object Class Specification

http://middleware.internet2.edu/eduperson/

[SHAC] SCHAC - SCHema for ACademia - Attribute Definition For Individual Data

http://www.terena.org/activities/tf-emc2/schacreleases.html

[ISO 639] ISO 639-4:2010 Codes for the representation of names of languages -- Part 4: General principles of coding of the representation of names of languages and related entities, and application guidelines
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=39535

[ISO 3166] ISO 3166-3:2013 Codes for the representation of names of countries and their subdivisions -- Part 3: Code for formerly used names of countries
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63547

## SAML

[SAML-ATTR] MACE-Dir SAML Attribute Profiles

http://middleware.internet2.edu/dir/docs/internet2-mace-dir-saml-attributes-200604.pdf

[SAML-CORE] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0

http://www.oasis-open.org/committees/download.php/22385/sstc-saml-core-errata-2.0-wd-04-diff.pdf

## Protezione dei dati personali e sensibili

[DL19603] Decreto Legislativo 30/6/2003 n.196: Codice in materia di protezione dei dati personali

http://www.parlamento.it/parlam/leggi/deleghe/03196dl.htm

[EU1] Protezione dei dati nell'Unione Europea

http://ec.europa.eu/justice_home/fsj/privacy/docs/guide/guide-italy_it.pdf

[EU2] Direttive Europee

http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

## Shibboleth

[SHIB] Shibboleth

http://shibboleth.internet2.edu/

[SHIBATTR] Define and Release a New Attribute in an IdP

https://spaces.internet2.edu/display/SHIB2/IdPAddAttribute

[SHIBFILT] Define a New Attribute Filter

https://spaces.internet2.edu/display/SHIB2/IdPAddAttributeFilter