



Specifiche tecniche per la compilazione e l'uso degli attributi

v. 3.0 - Proposta

5 ottobre 2016

Revisioni

Versione	Data	Descrizione	Note
1.0	24/10/2008	Versione iniziale	Raffaele Conte ¹ Maria Laura Mantovani ² contributi di: Roberto Gaffuri ³ Francesco Malvezzi ⁴ Giacomo Tenaglia ⁵
2.0	26/01/2010	Revisione generale del testo. Adeguamento della terminologia in funzione di Shibboleth 2.0. Inserimento identificativi (urn) in "Attributi: definizione dei metadati e notazione". Modifica paragrafo "Confidenzialità/Visibilità". Riorganizzazione delle Appendici A e B con indicazioni su configurazione di Shibboleth adeguate alla versione 2.x ed esempi. Correzioni minori.	Ra. C.
2.1	07/05/2011	Piccole modifiche capitolo 2 "Panoramica sugli attributi" (secondo e terzo capoverso). Modificata descrizione di eduPersonEntitlement in tabella al paragrafo 2.3. Modificata descrizione di attributo raccomandato e opzionale (capitolo 3). Modificata organizzazione capitolo "Attributi". Modificati "Riferimenti" obsoleti per 4.1.4 preferredLanguage, 4.1.5 schacMotherTongue e 4.1.7 schacPersonalTitle Aggiunto riferimento a [SCHAC] su definizione di 4.1.5 schacMotherTongue, 4.2.5 schacUserPresenceID Modificati "Semantica", "Riferimenti" e "Valori permessi" per 4.1.8 schacPersonalPosition Modificata descrizione, semantica e riferimenti di 4.2.6 eduPersonOrgDN e 4.2.7	Ra. C. 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>

		<p>EduPersonOrgUnitDN. Modificati "Riferimenti" e "Valori permessi" per 4.3.1 eduPersonScopedAffiliation. Modificate "Note" per 4.3.2 eduPersonTargetedID . Corretto "Identificativo" per 4.3.3 eduPersoPrincipalName e aggiunto valore in "Riferimenti" per 4.3.4 eduPersonEntitlement. Spostata Bibliografia in fondo al documento.</p> <p>Piccole correzioni Appendice B e nuovi valori di corrispondenza nelle affiliazioni. Aggiunto riferimento a [RFC5646] e aggiornati i link [NO1], [NO2], [EDUPER] e [SCHAC] in Bibliografia. Aggiunta bibliografia relativa a Shibboleth.</p>	
2.2	19/06/12	<p>Traduzione inglese Revisioni minori</p>	Alessandra De Nicola M.L.M.
3.0	05/10/16	<p>Revisione generale del testo alla luce dell'adozione di SAML 2, Entity Category, Resource Registry e Shibboleth 3. Riscrittura dell'introduzione con aggiornamento sui concetti di privacy e data protection europei e definizione ulteriore degli ambiti di competenza. Approfondimento sul filtraggio degli attributi. Aggiunta di un paragrafo sul consenso informato dell'utente al rilascio degli attributi. Eliminazione di facsimileTelephoneNumber e schacPersonalPosition. Aggiunti gli attributi eduPersonOrcid, schacPersonalUniqueID e DisplayName. Elenco sintetico degli attributi ripulito, rivisto e ordinato con un criterio misto di importanza ed effettivo utilizzo degli attributi in federazione. eduPersonTargetedID passa da obbligatorio a raccomandato Tolta la definizione di persistenza nell'eduPersonPrincipalName per essere compliant allo schema eduPerson. Introduzione all'uso di SAML 2.0 NameID nel</p>	<p>Daniele Albrizio⁶ Maurizio Festi⁷ Giuliano Latini⁸ Fabio Spelta⁹</p>

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>

		subject dell'asserzione.	
--	--	--------------------------	--

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 = Data Protection 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

Introduzione	7
Rilascio degli attributi	8
Policy sul rilascio degli attributi	8
Entity Category	9
Espressione del consenso informato	10
Panoramica sugli attributi	11
Tipi di attributi	11
Scope degli attributi	11
Elenco attributi	12
eduPersonOrcid	12
Attributi: definizioni	15
Attributi: definizione dei meta-dati e notazione	15
Dettaglio degli attributi in ordine alfabetico	16
cn	16
displayName	16
eduPersonEntitlement	17
eduPersonOrcid	17
eduPersonOrgDN	18
eduPersonOrgUnitDN	18
eduPersonPrincipalName	19
eduPersonScopedAffiliation	19
eduPersonTargetedID	20
givenName	21
mail	21
mobile	21
preferredLanguage	22
schacMotherTongue	23
schacPersonalTitle	23
schacPersonalUniqueID	23
schacUserPresenceID	24
sn	25
telephoneNumber	25
title	26
Appendice A: affiliazione	27
Capire l'affiliazione	27
Esempi pratici	28
Corrispondenza tra le categorie note e le possibili affiliazioni	29
Configurazione di Shibboleth	31

Appendice B: Identificativi univoci (NameID e eduPersonTargetedID)	33
Identificativo pseudonimo univoco	33
Uso lato SP	33
Persistenza/Riassegnamento	33
Tipologie del NameID	34
Salt	35
Bibliografia	36

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 e favorire l'adozione di pratiche uniformi tra i partecipanti alla federazione IDEM al fine di garantirne il buon funzionamento anche in relazione alla partecipazione all'interfederazione eduGAIN.

Gli attributi sono definiti utilizzando schemi standard LDAP.

La procedura di standardizzazione riguarda la denominazione, la sintassi, la semantica (si veda il capitolo "Attributi: definizioni"), le politiche di rilascio (si veda il capitolo "Rilascio degli Attributi") ed eventuale 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**). L'Organizzazione di Appartenenza è responsabile della protezione dei dati forniti per conto dei propri utenti. Spetta all'Organizzazione di Appartenenza dell'utente, responsabile dell'IdP, il compito di trasferire alle risorse solo gli attributi giudicati meritevoli di trasferimento in conformità alla legislazione vigente, agli accordi tra i membri, alla volontà dell'utente.

La risorsa che viene acceduta (SP) deve 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 rappresentano 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'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 anche mediante un identificativo persistente pseudo-anonimo e, quando questo è possibile, se ne consiglia l'uso.

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

2 Rilascio degli attributi

2.1 Policy sul rilascio degli attributi

Nel rispetto del principio di necessità¹⁰ nel trattamento dei dati personali, gli IdP devono rilasciare agli SP solo gli attributi strettamente necessari per l'erogazione del servizio.

E' d'obbligo per gli IdP il rilascio a tutti gli SP IDEM degli attributi classificati come "obbligatori" in questo documento.

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

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 rilasciabili, del numero di SP federati, della 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.

L'adozione di queste policy, insieme alla corretta valorizzazione degli attributi e all'uso del Resource Registry¹¹, consente di implementare automatismi scalabili per generare le regole di rilascio degli attributi, e automatizzare l'aggiornamento e l'adozione delle stesse da parte degli 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

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.

¹¹ Resource Registry IDEM: <https://registry.idem.garr.it/>

2.2 Entity Category

Per automatizzare il rilascio in maniera scalabile degli attributi richiesti dagli SP, la federazione si avvale delle Entity Category¹².

La loro funzione è il raggruppamento di servizi secondo caratteristiche specifiche. L'adozione da parte degli SP e degli IdP si concretizza nell'inserimento di ulteriori informazioni nei rispettivi metadati.

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>
```

¹² Entity category usate nella Federazione IDEM:

Data Protection Code of conduct: <https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home>

Research&Scholaship: <https://refeds.org/category/research-and-scholarship>

```
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

2.3 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 che permettano di informare puntualmente gli utenti riguardo al trattamento dei propri dati personali e di esprimere il consenso alla loro trasmissione all'SP (ad esempio mediante la funzionalità Consent di Shibboleth 3).

La situazione ottimale prevede che i vincoli espressi dall'utente vengono applicati dopo l'autenticazione e prima del rilascio degli attributi all'SP.

Per tale motivo, l'unico modo che ha l'SP di informare l'utente sull'uso dei dati è quello di rendere disponibile all'IdP l'informativa sul proprio trattamento in modo che l'IdP stesso possa presentarla all'utente contestualmente alla richiesta di autorizzazione al rilascio degli attributi.

Nel documento "IDEM Metadata Profile"¹³ sono riportati i riferimenti per la configurazione di metadati specifici (mdui:PrivacyStatementURL) per l'esposizione delle privacy policy di SP e IdP.

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

3 Panoramica sugli attributi

Gli attributi selezionati provengono dall'insieme degli attributi di base definiti per il protocollo LDAPv3 [RFC4519] e dagli schemi Cosine, inetOrgPerson, eduPerson [EDUPER] e Schac [SCHAC].

Ogni attributo prevede uno stato che può assumere uno tra i valori **obbligatorio**, **raccomandato** e **opzionale**, questi valori si riferiscono alla capacità di gestione che si richiede da parte dell'IdP.

L'insieme degli attributi **obbligatori** costituisce quindi il set minimo per aderire alla federazione. Sono **obbligatori** la **generazione** e il **rilascio** dell'attributo **eduPersonScopedAffiliation** e di un identificativo opaco, persistente e specifico per ogni SP (targeted) preferibilmente tramite il **NameID:persistent** nel subject dell'asserzione (vedi appendice B sugli Identificativi Univoci). Ciò permette 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 in federazione. Se l'SP richiede un attributo opzionale che l'IdP implementa, è opportuno che tale attributo venga rilasciato a vantaggio della fruizione ottimale del servizio. Lato SP, dichiarare gli attributi opzionali come obbligatori per l'erogazione del servizio è sconsigliato in quanto non è detto che gli IdP li generino.

Gli attributi selezionati dalla federazione sono elencati di seguito.

3.1 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.

Caratteristiche personali (P): Ad esempio il nome, il cognome e il titolo dell'utente.

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

Autorizzazioni e Accounting (A): Attributi sull'affiliazione, il ruolo dell'utente nella propria organizzazione, identificativi personali persistenti, attributi di sottoscrizione del servizio o autorizzazioni aggiuntive.

3.2 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.

3.3 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	raccomandato	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
3.3.1 eduPersonOrcid	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)"

sn¹⁷	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	
cn²⁰	LDAPv3 rfc4519 eduPerson	Nome seguito da Cognome	raccomandato racc. eduGAIN	P	
eduPersonOrgDN²¹	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	opzionale	C	

¹⁷ ② sn, cn e eduPersonOrgDn 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

		associata (ad esempio Dipartimento)			
schacPersonalTitle	schac	Titolo usato per salutare il soggetto. Es: Sig., Sig.ra, Dott., Prof.	opzionale	P	
schacPersonalUniqueID	schac	"Identificativo Univoco Legale" associato alla persona.	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	

4 Attributi: definizioni

4.1 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'attributo²²
- **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:** obbligatorio, raccomandato, opzionale. Vedi paragrafo *"Panoramica sugli attributi"*
- **Note:** informazioni aggiuntive relative all'attributo
- **Esempi:** esempi nel formato LDIF (RFC2849 LDAP Data Interchange Format)
- **Uso tipico:** ambito di utilizzo dell'attributo

²² L'urn è necessario nella configurazione di Shibboleth.

4.2 Dettaglio degli attributi in ordine alfabetico

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

4.2.1 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

4.2.2 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 particolare 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 <i>commonName</i> o <i>sn + givenName</i> . 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 <i>sn</i> e <i>givenName</i> .

Esempi	displayName: Andrea Rossi
Uso tipico	Informazioni aggiuntive sull'utente

4.2.3 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. 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	<p>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.</p> <p>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.</p> <p>L'organizzazione di appartenenza è responsabile del controllo sui propri utenti, affinché a coloro che soddisfano le condizioni venga assegnato il valore opportuno.</p> <p>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.</p>
Esempi	eduPersonEntitlement: urn:mace:dir:entitlement:common-lib-terms eduPersonEntitlement: urn:mace:internet2:terena.nl:garr:service
Uso tipico	Autorizzazione

4.2.4 eduPersonOrcid

Descrizione	Identificativi ricercatore ORCID dell'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 persistente che individua univocamente la persona.
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 è 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

4.2.5 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 eduPersonOrgDN: o=Istituto di Fisiologia Clinica,dc=ifc,dc=cnr,dc=it
Uso tipico	Informazioni aggiuntive sull'utente

4.2.6 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

4.2.7 eduPersonPrincipalName

Descrizione	Identificativo unico 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: 1321k1j21@biblio.bo.cnr.it eduPersonPrincipalName: mrossi@esempio.it
Uso tipico	Autorizzazione, Accounting

4.2.8 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. Il fornitore del servizio deve progettare il proprio sistema di autorizzazione in modo da usare questo attributo ovunque possibile. [UK2]
Esempi	eduPersonScopedAffiliation: staff@biblio.bo.cnr.it eduPersonScopedAffiliation: faculty@unica.it
Uso tipico	Autorizzazione

4.2.9 eduPersonTargetedID

Descrizione	Identificativo anonimo, persistente e non riassegnabile di un utente, differente per ogni fornitore di servizio. 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 e non riassegnabile associato all'utente per la fruizione di uno specifico servizio ed è composto da tre parti, nella forma: <organizzazione>!<servizio>!<stringa opaca> Per <organizzazione> si intende l'identificativo dello IdP dell'utente. 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	Raccomandato In attesa di usare al suo posto SAML 2.0 NameID di tipo persistent nel subject dell'asserzione, è ancora necessaria la generazione di questo

	attributo per gli SP non compatibili
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 eduPersonTargetedID: unica.it!servizio_n!alskdj92920alsk
Uso tipico	Autorizzazione, Accounting, servizio personalizzato

4.2.10 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

4.2.11 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

4.2.12 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

4.2.13 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. Questi ultimi possono anche essere vuoti. language-tag = primary-tag *("-" subtag) primary-tag = 1*8ALPHA subtag = 1*8ALPHA 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 preferredLanguage: it-ch
Uso tipico	Informazioni aggiuntive sull'utente

4.2.14 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 schacMotherTongue: fr-ch
Uso tipico	Informazioni aggiuntive sull'utente

4.2.15 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	urn:schac:personalTitle: Sig.

Uso tipico	Informazioni aggiuntive sull'utente
-------------------	-------------------------------------

4.2.16 schacPersonalUniqueID

Descrizione	"Identificativo Univoco Legale" associato alla persona.
Identificativo SAML2	urn:oid:1.3.6.1.4.1.25178.1.2.15
Semantica	Specifica un "Identificativo Univoco Legale" associato alla persona. Questo può essere DNI in Spagna, FIC in Finlandia, NIN in Svezia,...
Riferimenti	[SCHAC]
Sintassi LDAP	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# di valori	multiplo
Valori permessi	I valori hanno il formato: urn:schac:personalUniqueID:<country-code>:<idType>:<idValue>, dove: <country-code> è un codice identificativo di due lettere valido descritto in ISO 3166 country code identifier; <idType> tipo di identificativo i cui valori accettabili sono dichiarati per ogni country code attraverso una URI registrata nel TERENA URN registry; <idValue> è il valore. Per quanto riguarda il codice fiscale, tale valore è da assumersi case insensitive.
Classificazione	Opzionale
Note	L'estensione Nazionale "it" è in via di registrazione presso il TERENA URN registry. Allo stato attuale il solo utilizzo dell'attributo in Italia è relativo all'estensione CF per il codice fiscale.
Esempi	urn:schac:personalUniqueID:it:CF:LBRDNL86B23L223Z urn:schac:personalUniqueID:fi:FIC:260667-123F urn:schac:personalUniqueID:es:DNI:31241312L urn:schac:personalUniqueID:se:NIN:12345678
Uso tipico	Account linking, rilascio codice fiscale.

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

4.2.18 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

4.2.19 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

4.2.20 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

5 Appendice A: affiliazione

5.1 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 specializzazioni 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 per cui non vengono estesi i privilegi derivanti dall'essere membri dell'organizzazione stessa. Potrebbero rientrare in questa categoria i fornitori di servizi o di 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.

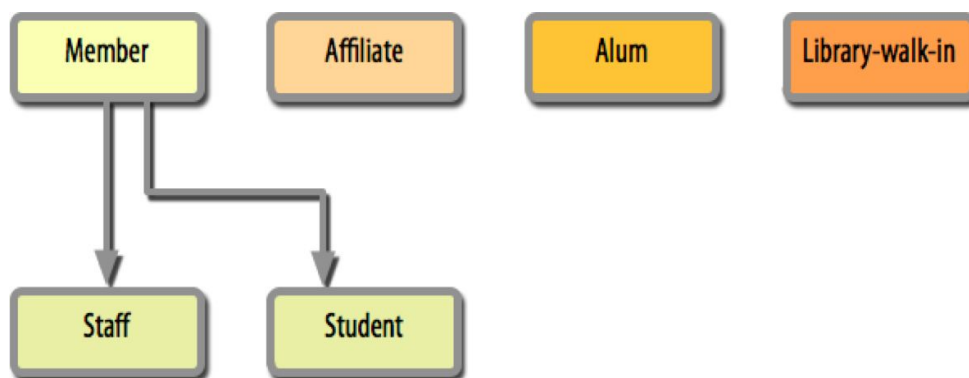


Figura 3: Valori per eduPersonAffiliation

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.

5.2 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, 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
```

5.3 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
consorzio (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.

5.4 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 contenente 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 dinamicamente 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="example.org">
  <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.

6 Appendice B: Identificativi univoci (NameID e eduPersonTargetedID)

Un Fornitore di Servizi usa un identificativo univoco per realizzare la persistenza fra diverse sessioni dello stesso utente, offrendogli così una personalizzazione del servizio. Accettando come identificativo univoco uno pseudonimo, realizza un servizio maggiormente rispettoso della privacy dell'utente.

Per consentire agli SP di implementare in questo modo questa funzionalità è necessario che l'IdP rilasci un identificativo pseudonimo all'SP in modo da creare una relazione uno-a-molti, anonima e permanente fra lo stesso utente ed i Fornitori di Servizi.

Di seguito vengono indicati i requisiti per una migrazione efficace dall'attributo eduPersonTargetedID all'uso del SAML2:NameID:persistent nel subject dell'asserzione.

6.1 Identificativo pseudonimo univoco

La **generazione** e il **rilascio** di un identificativo pseudonimo univoco diverso per ogni SP è **obbligatorio** nella federazione IDEM.

Questo identificativo opaco, persistente e differente per ogni SP (targeted) va:

- Rilasciato come **NameID:persistent** nel subject dell'asserzione qualora l'SP richieda in maniera generica un NameID ovvero richieda in maniera specifica un NameID:persistent.
- Alternativamente rilasciato nell'attributo **eduPersonTargetedID** qualora l'SP non supporti ancora l'uso del NameID.

Si raccomanda di evitare il rilascio di entrambe le forme.

6.2 Uso lato SP

Alcuni software SP, come ad esempio uno Shibboleth SP nella configurazione di default rimappano **NameID:persistent** e **eduPersonTargetedID** verso l'applicazione valorizzando un singolo attributo multivalore (PersistentID). L'SP che fruisca di un identificativo persistente, per essere compatibile con gli IdP in interfederazione, deve richiedere il NameID:persistent nel subject dell'asserzione, l'eduPersonTargetedID come opzionale fra gli attributi e deve alternativamente:

- trattare nell'applicazione l'attributo PersistentID del software SP come multiplo e risolvere i conflitti dei valori.
- configurare il software SP per presentare attributi distinti verso l'applicazione adottando in prima analisi il NameID:persistent rimappando su questo eventuali contesti assegnati in precedenza all'eduPersonTargetedID corrispondente.

6.3 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 immutati 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. La sola generazione algoritmica dei valori (senza memorizzazione in database) rende impossibile 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 incoraggiato l'utilizzo del dato come **SAML 2.0 NameID** nel subject dell'asserzione anziché come **attributo eduPersonTargetedID**. Tale funzionalità era già presente in altre implementazioni molto diffuse di SAML.

Per la configurazione di **eduPersonTargetedID** si rimanda alle vecchie guide IDEM per Shibboleth 2.x.

Per quanto riguarda l'uso di identificativi persistenti lato SP, si raccomanda l'uso di **NameID:persistent** o **eduPersonTargetedID** e di evitare a tale scopo **eduPersonPrincipalName** che è potenzialmente considerato riassegnabile in federazioni diverse da IDEM.

6.4 Tipologie del NameID

La generazione, conseguente ad una richiesta, dei valori del **NameID** nel subject dell'asserzione può essere effettuata con due modalità:

- **Transient o di tipo temporaneo.** In questo modo, per gli SP che lo richiedono, l'identificativo unico viene generato in maniera casuale e di breve durata. 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 quegli scenari in cui è necessario riconoscere l'utente anche a distanza di tempo. Tale identificativo va rilasciato in federazione usando il **NameID:transient** nel subject dell'asserzione *solo se esplicitamente richiesto* dall'SP.
- **Persistent o di tipo persistente.** I valori di questa tipologia possono essere generati nelle seguenti modalità:
 - **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 l'IdP fosse in cluster).

Nel caso di Shibboleth 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.

6.5 Salt

Il salt, comunemente 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.

7 Bibliografia

Documentazione federazione Inglese

[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>

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

<https://www.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

<https://www.internet2.edu/products-services/trust-identity/eduperson-eduorg/#service-features>

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

<https://wiki.refeds.org/display/STAN/SCHAC>

[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-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>

[SAML2INT] SAML 2.0 Interoperability Deployment Profile

<http://saml2int.org/profile/current/>

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/data-protection/index_en.htm

[EU2] Direttive Europee

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

Shibboleth

[SHIB] Shibboleth

<http://shibboleth.net/>

[SHIBATTR] Shibboleth Attribute Definition

<https://wiki.shibboleth.net/confluence/display/IDP30/AttributeResolverConfiguration>

[SHIBFILT] Shibboleth Attribute Filtering

<https://wiki.shibboleth.net/confluence/display/IDP30/AttributeFilterConfiguration>

IDEM

[IDEMTUTOR] IDEM Tutorials

<https://github.com/ConsortiumGARR/idem-tutorials>

[IDEMREG] Resource Registry IDEM

<https://registry.idem.garr.it/>

Entity Categories

[ECRS] Research and Scholarship Entity Category

<https://refeds.org/category/research-and-scholarship>

[ECCOCO] Code of Conduct Entity Category

<https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home>