Specifiche tecniche per la compilazione e l'uso degli attributi

v. 3.0

29 novembre 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	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>

		Modificata descrizione, semantica e riferimenti di 4.2.6 eduPersonOrgDN e 4.2.7 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. 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.	
2.2	19/06/12	Traduzione inglese Revisioni minori	Alessandra De Nicola M.L.M.
3.0	05/10/16	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, schacHomeOrganization, schacHomeOrganizationType, 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	Daniele Albrizio[6] Maurizio Festi[7] Giuliano Latini[8] 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>

		a raccomandato Tolta la definizione di persistenza nell'eduPersonPrincipalName per essere compliant allo schema eduPerson. Introduzione all'uso di SAML 2.0 NameID nel 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

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 Titolare del trattamento dei dati dei propri utenti. Tali dati possono essere trasmessi a terzi, tipicamente ai fornitori di servizi. Il fornitori di servizi è Responsabile del trattamento dei dati che il SP riceve dagli IdP tramite le asserzioni SAML.

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: attributi riguardanti le caratteristiche personali del soggetto; attributi riguardanti le modalità per contattare il soggetto; 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 necessità[10] 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 rilasciano 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 Registry[11], 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="[registry attribute release policy url
per lo specifico idp]" 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 Category[12].
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 quando richiesto (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 dei servizi. Per fruire appieno delle risorse federate è necessario che questi attributi vengono 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 di questo documento come obbligatori per l'erogazione del servizio è sconsigliato in quanto non è prevedibile 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]

[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] Per l'entity category Research and Scholarship displayName è previsto in alternativa a sn + givenName.

3.3.1 eduPersonOrcid	eduPerson	identificativo utente registrato su ORCID.org	opzionale	P	
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	opzionale	C	

[17] 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

		rappresenta l'unità organizzativa di appartenenza alla quale la persona è 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	
schacHomeOrganization	schac	Rappresenta il nome a dominio dell'organizzazione di appartenenza.	raccomandato racc. eduGAIN	C	
schacHomeOrganizationType	schac	Rappresenta il tipo di organizzazione alla quale la persona è associata.	raccomandato racc. eduGAIN	C	
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'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:** 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 *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

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	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. 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. L'organizzazione di appartenenza è responsabile del controllo sui propri utenti, affinché a coloro che soddisfano le condizioni venga assegnato il valore opportuno. 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: 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 e non riassegnabile 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
Note	Una volta assegnato un valore a questo attributo, lo stesso valore non può essere assegnato ad altri utenti
Esempi	`eduPersonPrincipalName: 132lk1j2l@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 il 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 posso 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 schacHomeOrganization

Descrizione	Il nome a dominio dell'organizzazione di appartenenza dell'utente
Identificativo SAML2	urn:oid:1.3.6.1.4.1.25178.1.2.9
Semantica	Corrisponde al nome a dominio dell'organizzazione
Riferimenti	[SCHAC]
Sintassi LDAP	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# di valori	Singolo
Valori permessi	
Classificazione	Raccomandato
Note	

Esempi	`units.it`
	`unitn.it`
	`unimib.it`

Uso tipico	Informazioni aggiuntive sull'utente

4.2.15 schacHomeOrganizationType

Descrizione	Tipo di organizzazione di appartenenza dell'utente
Identificativo SAML2	urn:oid:`1.3.6.1.4.1.25178.1.2.10`
Semantica	Definisce la tipologia dell'organizzazione di appartenenza dell'utente secondo il formato urn:schac:homeOrganizationType:<country-code>:<string>
Riferimenti	[schac], [ISO3166]
Sintassi LDAP	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# di valori	Multiplo
Valori permessi	urn:schac:homeOrganizationType:<country-code>:<string> Dove il <country-code> deve essere un codice paese ISO 3166 valido a due lettere o la stringa "int", e assegnato dallo SCHAC URN Registry per questo attributo su

	https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry e <string> froma un vocabolario controllato su base nazioale, pubblicato attraverso una URI identificata nel sopra citato SCHAC URN registry.
Classificazione	Raccomandato
Note	

Esempi	`urn:schac:homeOrganizationType:eu:higherEducationInstitution`
	`urn:schac:homeOrganizationType:int:universityHospital`
	`urn:schac:homeOrganizationType:eu:educationInstitution`
	`urn:schac:homeOrganizationType:eu:higherEducationInstitution`

Uso tipico	Informazioni aggiuntive sull'utente

4.2.16 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

4.2.17 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

4.2.18 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. L'attributo viene usato comunemente per gli scopi di account linking e rilascio del dato codice fiscale.

Esempi	`urn:schac:personalUniqueID:it:CF:LBRDNL89S09D704H`
	`urn:schac:personalUniqueID:fi:FIC:260667-123F`
	`urn:schac:personalUniqueID:es:DNI:31241312L`
	`urn:schac:personalUniqueID:se:NIN:12345678`

Uso tipico	Informazioni aggiuntive sull'utente

4.2.19 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`
	`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`

Uso tipico	Informazioni aggiuntive sull'utente

4.2.20 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

4.2.21 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

4.2.22 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.

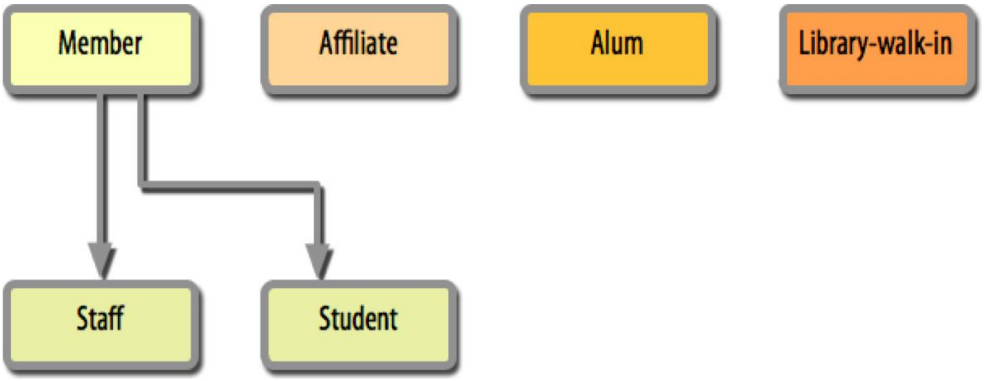

Figura 3: Valori per eduPersonAffiliation

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
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 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 SP usa un identificativo univoco persistente per collegare sessioni iniziate in tempi diversi dallo stesso utente, al fine di offrirgli servizi personalizzati. Quando l'IdP rilascia a diversi SP uno stesso identificativo per lo stesso utente, offre ai diversi SP la possibilità di collegare le diverse attività dell'utente avvenute su più fornitori di servizio. Per garantire all'utente un maggior rispetto della sua privacy, l'IdP crea per uno stesso utente una molteplicità di identificativi univoci e persistenti (pseudonimi), ciascuno dedicato ad uno specifico SP, costruendo una relazione uno-a-uno, anonima e permanente fra lo stesso utente e ognuno dei Fornitori di Servizio.

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,** quando previsto, 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 specifica un NameID:persistent.
- Alternativamente rilasciato nell'attributo **eduPersonTargetedID** qualora l'SP lo richieda e non supporti ancora l'uso del NameID.

Si raccomanda di evitare il rilascio di entrambe le forme [SAML2INT].

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 il medesimo attributo multivalore (persistent-id). L'SP che utilizza un identificativo persistente, per essere compatibile con gli IdP nell'interfederazione, deve richiedere il NameID:persistent nel subject dell'asserzione, l'eduPersonTargetedID come opzionale fra gli attributi e deve alternativamente:

- trattare l'attributo 'persistent-id' del software SP come multiplo e risolvere i conflitti dei valori all'interno dell'applicazione.
- 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 allo 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 consumati da altri SP. La sola generazione algoritmica dei valori senza memorizzazione in database (transient-id) 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 *in modo predefinito* verso gli 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

Technical Specifications for the Compilation and Use of Attributes

v. 3.0

29 November 2016

Revisions

Version	Data	Description	Authors
1.0	24/10/2008	Initial version	Raffaele Conte[23] Maria Laura Mantovani[24] Contribution of: Roberto Gaffuri[25] Francesco Malvezzi[26] Giacomo Tenaglia[27]
2.0	26/01/2010	Text general revision. Adapting the terminology according to Shibboleth 2.0. Inserting identifiers (urn) in the "Attributes: metadata definition and notation." Change paragraph "Confidentiality / Visibility." Minor corrections.	Ra. C.

[23] Istituto di Fisiologia Clinica, CNR, Pisa <raffaele.conte@cnr.it>
[24] GARR e Università di Modena e Reggio Emilia <marialaura.mantovani@garr.it>
[25] Politecnico di Milano <roberto.gaffuri@ceda.polimi.it>
[26] Università di Modena e Reggio Emilia <francesco.malvezzi@unimore.it>
[27] CNR, Biblioteca Area della Ricerca di Bologna <giacomo.tenaglia@area.bo.cnr.it>

Version	Data	Description	Authors
2.1	07/05/2011	Chapter 2 "Overview of Attributes": little changes (second and third paragraph). Par. 2.3 eduPersonEntitlement table: Modified description. Chap 3: Modified description of recommended and optional. Chapter "Attributes": modified organisation. Changed obsolete "References" for 4.1.4. preferredLanguage, 4.1.5 schacMotherTongue and 4.1.7 schacPersonalTitle. 4.1.5 definition of schacMotherTongue and 4.2.5 schacUserPresenceID: added reference to [SCHAC. 4.1.8 schacPersonalPosition:modified "Semantics", "References" and "allowed values". 4.2.6 eduPersonOrgDN and 4.2.7 EduPersonOrgUnitDN: modified description, semantics and references. 4.3.1 eduPersonScopedAffiliation: changed "References" and "allowed values". 4.3.2 eduPersonTargetedID: changed "Notes". 4.3.3 eduPersoPrincipalName: fixed "ID" and added value in "References". Bibliography moved at the end of the document. Appendix B minor corrections and new values in the corresponding affiliations. Added reference to [RFC5646] and updated links [NO1] [NO2], [EDUPER] and [SCHAC] in Bibliografy. Shibboleth bibliography added.	Ra. C. M.L.M.

Version	Data	Description	Authors
2.2	19/06/12	English Translation Minor revisions	Alessandra De Nicola M.L.M.
3.0	05/10/16	General text revision after the adoption of SAML 2, Entity Category, Resource Registry and Shibboleth 3. Rewriting of the introduction with upgrade about the European privacy and data protection concepts, and further definition of range of competence. In-depth analysis about attribute filtering. Added a paragraph about the informed consent about the attribute. Refined the brief list of attributes, ordered by the importance and the effective usage among the Federation. Deleting of facsimileTelephoneNumber e schacPersonalPosition. Added the attributes DisplayName, eduPersonOrcid, schacHomeorganisation, schacHomeorganisationType, schacPersonalUniqueID. Deleted the persistence definition in eduPersonPrincipalName to be compliant to the eduPerson schema. eduPersonTargetedID become recommended instead of mandatory. Introduction to the use of SAML 2.0 NameID in the assertion subject.	Daniele Albrizio[28] Maurizio Festi[29] Giuliano Latini[30] Fabio Spelta[31]

[28] Università di Trieste <daniele.albrizio@units.it>
[29] Università di Trento <maurizio.festi@unitn.it>
[30] Università Politecnica delle Marche <giuliano.latini@univpm.it>
[31] Università degli Studi di Milano - Bicocca <fabio.spelta@unimib.it>

Preamble

To report suggestions, errors or inaccuracies in this document, please write to: idem@garr.it

Abbreviations

STA = Technical Specifications for Compilation and Use of Attributes

NdP = Rules of participation

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

Contacts

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

IDEM Federation: idem@garr.it

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

Index

1 Introduction

IDEM Federation uses the SAML2 standard for Single Sign-On operations. In addition to assure a correct user authentication, federated services may receive a set of information related to the user..

These information, referred to as "attributes", includes personal information (name, surname), user affiliation (for example professor staff ofat theone Uuniversity of Trieste), language, and possibly others.

The scope of this document is to standardise the attribute usage and encourage common practices among the IDEM federation participants. This would guarantee the correct conduct and operations also in line with IDEM participation in the eduGAIN inter-federation.

Attributes are defined using the standard LDAP schemas.

The standardisation applies to the naming, syntax, semantics (see chapter "Attributes: definitions"), release policies (see chapter "Releasing Attributes"), and to the possible attribute values that the Identity Provider (IdP) of an organisation could or should release to Service Providers (SP).

The organisation is the Data Controller for its users' data. These data can be sent to third parties, who are usually service providers. Service providers are data processors for the data received from IdPs through SAML assertions.

It is the duty of the organization responsible for the IdP to send to service providers only the attributes that are deemed necessary to perform the authentication and authorization procedure and to do so in compliance with contracts, the current legislation, membership agreements and the users' preferences.

The accessed resource (SP) should only ask for the attributes that are mandatory for the authentication and the supply of the requested service.

In the chapter "Attribute overview", the table of attributes is organised in three categories: personal user data, user contacts, authorization and accounting attributes. Almost all these attributes are considered as personal data in accordance with the Italian law D.LGS. 196/2003 "Codice in materia di protezione dei dati personali" and their management must be in compliance with this law.

For most SPs it is sufficient to know the users' organisation and the affiliation ("eduPersonScopedAffiliation" attribute). The SPs could also need to identify a user through a persistent and pseudo-anonymous identification attributes and, where possible, we recommend to support them.

In this document there are some configuration examples that use the syntax of Shibboleth 3.x IdP .

2 Attribute release

2.1 Attribute release policy

In compliance with the data minimisation principle in processing of personal data IdPs must release only the attributes that are necessary to the SPs.
IdPs in the Federation are committed to release to SPs all the attributes defined as "mandatory"in this document .
In addition to the mandatory attributes, in order for a user to access the federated and inter-federated

services, IdPs should also release the attributes required by the SPs, trusting the signed Federation metadata supplied by IDEM Federation and eduGAIN inter-Federation.

The release process follows well-defined rules (Attribute Release Policies or ARP) that are deployed and managed by the IdP operator. The effort required to perform this process can increase in time, due to the growth of released attributes, the growing number of SPs, and the management of users' consent.. This process could be simplified by inserting the correct value in the RequestedAttribute assertion, as specified in the "IDEM Metadata Profile" document, and by correctly implementing the EntityCategory features, as specified below in this document .

The adoption of these policies, along with a correct attributes assessment and the use of Resource Registry[32], allows to automate the generation of the attribute release policies.

```
<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="[registry attribute release policy url
per lo specifico idp]" 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.
-->
```

Example of configuration for the automatic loading of the attribute filter files in services.xml

2.2 Entity Category

In order to automate the attribute release process for the SPs, the IDEM Federation make use of Entity Categories[33].

Entity Categories group services that share common characteristics. The adoption by SPs and IdPs is accomplished by inserting additional information in their respective metadata fragments.

In the following, aa real use case from the European inter-Federation eduGAIN, is provided as an example.

[32] Resource Registry IDEM: https://registry.idem.garr.it/
[33] Entity category used among IDEM Federation: 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

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>
```

Example for di Research and Scholarship Entity Category from 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>
```

Example of the GÉANT “Code of Conduct” Entity Category

2.3 Consent

It could be useful to let the user choose which attributes should remain private inside his organisation

and if an attribute could or could not be sent to a SP.

According to Italian and European laws it is recommended that IdPs provide users with a *consent* mechanism allowing them to make choices about the release of their attributes to the SP (for example the "Consent" feature in Shibboleth 3).

The best approach to implement the consent, is to let the user gives her consent after the authentication phase and before the releasing of the user's attributes to the SP.
For this reason, the only way a SP can inform the user about its attribute management, is to provide its data processing policy to the IdP, which can in turn present it to the user as a part of the user consent to the attribute release.

The document "IDEM Metadata Profile" [34] describes the specific metadata configuration (mdui:PrivacyStatementURL) to expose the privacy policies both for the IdP and the SP.

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

3 Overview on Attributes

The following selected attributes come from the set defined in the LDAPv3 protocol standard [RFC4519] and from the following schemas: Cosine, inetOrgPerson, eduPerson [EDUPER] and Schac [SCHAC].

Each attribute has a status that can be either **mandatory, recommended** or **optional**.

The set of **mandatory** attributes defines the minimum set required to join the Federation. Among these attributes, it is **mandatory** to **generate** and **release** the **eduPersonScopedAffiliation** attribute and the NameID assertion in a persistent mode. The latter is an opaque pairwise ID, specific for each SP obtained by using **NameID:Persistent** in the assertion subject upon request (see Appendix B about unique ID). With these two, the service provider is able to verify the users' affiliation and to identify them (in a pseudo-anonymous form).

The set of **recommended** attributes consists of frequently requested attributes. In order to make full use of the federated resources it is necessary that IdPs generate and release these attributes, if foreseen.

The set of **optional** attributes consists of attributes that could be supported by IdPs only if they are effectively used by the federated SPs. If a SP requests an optional attribute implemented by the IdP, it is appropriate that the attribute is released as well, in order to have the full usage of the SP. A SP is discouraged to request optional attributes as mandatory..

3.1 Attribute types

The attributes describe many user characteristics and are divided in three categories: personal data, contact information, authorization and accounting data.

Personal data (P): for example user name, surname, title.

Contacts (C): used to personally contact the user in order to supply the service

Authorization and Accounting (A): affiliation, role, persistent IDs, entitlements, service subscribing attributes or additional authorizations.

3.2 Attribute Scope

Some attributes are scoped. The organisation representation (<organisation>) must be a DNS registered domain that belongs to the organisation. If an organisation registered more than one DNS domain, it must choose one, and use it in its attribute value assessment.

3.3 Attribute List

IDEM Federation attributes ordered by their use and importance in 2016.

LDAP name	Origin	Description	Status	Use[35]	R&S[36]
eduPersonTargetedID	eduPerson	Persistent, anonymous, pairwise identifier for the user.	recommended	A	Yes
eduPersonScopedAffiliation	eduPerson	Affiliation according to the conventions described in Appendix A	mandatory recommended in eduGAIN	A	Yes
mail	Cosine rfc4524	e-mail address	recommended racc. eduGAIN	C	Yes
eduPersonPrincipalName	eduPerson	Persistent unique identifier for the user	recommended racc. eduGAIN	A	Yes
LDAP name	**Origin**	**Description**	**Status**	**Use[37]**	**R&S[38]**
displayName	RFC2798 eduPerson	From RFC2798 description: "preferred name of a person to be used when displaying entries."	recommended racc. eduGAIN	P	Yes[39]
eduPersonOrcid	eduPerson	User ID registered in ORCID.org	optional	P	
sn[40]	LDAPv3 rfc4519 eduPerson	Last name	recommended	P	Yes[41]
givenName	LDAPv3 rfc4519	Name	recommended	P	Yes[42]

[35] Main use of the attribute. See paragraph on attribute types::
P: personal information
C: contact information A: authorization and accounting
[36] "Research and Scholarship" Entity Category.
[37] See note 14.
[38] See note 14.
[39] For the "Research and Scholarship" entity category, the displayName attribute can be provided as alternative to sn + givenName.
[40] sn, cn and eduPersonOrgDn are the three attributes that constitute the "core" application utility class for eduPerson: http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201310.html
[41] See note 17
[42] See note 17

LDAP name	Origin	Description	Status	Use[43]	R&S[44]
eduPersonEntitlement	eduPerson	One or more URIs (either URN or URL), agreed with the service provider, generally used to indicate a set of rights to a specific resources.	recommended	A	
cn[45]	LDAPv3 rfc4519 eduPerson	Name followed by Last name	recommended racc. eduGAIN	P	
eduPersonOrgDN[46]	eduPerson	The distinguished name (DN) of the directory entry representing the home organisation with which the person is associated.	optional	C	
title	LDAPv3 rfc4519	Title in the context of the organisation (i.e.: "Director", "Head of Department X" etc.)	optional	P	

[43] See note 13.

[23] See note 14.

[24] See note 17.

[25] Sn, cn and eduPersonOrgDn are the three attributes that constitute the "core" application utility class for eduPerson: http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201310.html

[44]

[45]

[46]

LDAP name	Origin	Description	Status	Use[47]	R&S[48]
telephoneNumber	LDAPv3 rfc4519	Telephone number	optional	C	
eduPersonOrgUnitDN	eduPerson	The distinguished name(s) (DN) of the directory entries representing the organisational Unit(s). to which the user is associated.	optional	C	
schacPersonalTitle	schac	A salutation title for a person. Examples of personal titles are "Ms", "Dr", "Prof", "Rev", "Sr".	optional	P	
schacPersonalUniqueID	schac	The user's "Legal unique ID"	Optional	P	
LDAP name	**Origin**	**Description**	**Status**	**Use[49]**	**R&S[50]**
schacHomeorganisation	schac	Organization DNS name	recommended racc. eduGAIN	C	
schacHomeorganisationType	schac	The organisation type	recommended racc. eduGAIN	C	

[47] MainThe prevalent use of the attribute. See paragraph about the attribute types. (from which table it come from):
P: Personal informationdata
C: contact informations A: authorization and accounting

[27] Entity category 'Research and Scholarship' Entity category :
Min: foreseen inexpected by the entity category minimum set, mandatory for the entity category
Full: foreseen inexpected by the entity category full set, recommended

[48]

[49] TMain use of the attribute. See paragraph about the attribute types:
P: Personal information
C: contact information A: authorization and accounting
he prevalent use of the attribute. See paragraph about the attribute types. (from which table it come from):
P: Personal data
C: contacts A: authorization and accounting

[29] Entity category Research and Scholarship,:
Min: foreseen inexpected by the entity category minimum set, mandatory for the entity category
Full: foreseen inexpected by the entity category full set, recommended.

[50]

schacUserPresenceID	schac	To store a set of values related to network presence protocol	optional	C	
mobile	Cosine rfc4524	Mobile number	optional	C	
schacMotherTongue	schac	User's mother tongue	optional	P	
preferredlanguage	inetOrgPerson rfc2798	User's preferred written or spoken language	optional	P	

4 Attributes: definitions

4.1 Attributes: meta-data definition and notation

All attributes are defined by the following meta-data:

- **Description:** a brief description of the attribute
- **SAML2 Identifier:** SAML2 URN that uniquely identifies the attribute[51]
- **Semantics:** the semantics of the attribute
- **References:** reference to current standards
- **Syntax LDAP:** the LDAP attribute syntax (see RFC 2252)
- **# of values:**
  - - single;
  - - multiple;
- **Allowed values:** a list of allowed values. Where possible the list of values is based on national or international standards.
- **Classification:**
  - **mandatory:** an IdP must provide this attribute to be part of the Federation;
  - **recommended:** it is highly recommended that an IdP provides this attribute because there are SP who request it
  - **- optional:** although there are no SP in the Federation requesting it explicitly, the attribute might be useful
- **Notes:** additional information related to the attribute
- **Examples:** examples in LDIF format (LDIF=LDAP Data Interchange Format, see RFC2849)
- **Typical use:** attribute area of interest.

4.2 Attribute details (in alphabetical order)

This section provides a list of attribute details in alphabetical order.

4.2.1 cn

Description	CommonName
SAML2 Identifier	urn:oid:2.5.4.3
Semantics	Indicate the full name of the person
References	[RFC 4519]
LDAP syntax	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# of values	Multiple

[51] the urn is necessary in Shibboleth configuration.

Values permitted	n/d
Classification	Recommended
Notes	The attribute is defined as multi-values. However within the Federation, the Home organisation should provide a single value, eg. the one used for official communications with the person
Examples	`cn: Andrea Rossi`
Typical use	Additional information about the user

4.2.2 displayName

Description	Display Name
SAML2 Identifier	urn:oid:2.16.840.1.113730.3.1.241
Semantics	The name of the person, to be displayed in the visualisation of the description of his entry, in particular in directories, address books and other lists.
References	[RFC 2798]
LDAP syntax	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# of values	Single
Values permitted	n/d
Classification	Recommended
Notes	Where not defined, this attribute can simply assume the value of *commonName* or *sn* + *givenName.* Can be used also in those cases where there is no clear distinction between first name and last name or when one of the two is missing. It could contain nicknames or abbreviations different from *sn* and *givenName.*
Examples	`displayName: Andrea Rossi`
Typical use	Additional information about the user

4.2.3 eduPersonEntitlement

Description	URI (either URN or URL) that indicates a set of access rights to specific resources.
SAML2 Identifier	urn:oid:1.3.6.1.4.1.5923.1.1.1.7
Semantics	The values are typically URIs, which identify resources or a particular user property. The user is authorised to access a resource only if the attribute a specific URI.
References	[EDUPER]

LDAP syntax	DirectoryString 1.3.6.1.4.1.1466.115.121.1.15
# of values	Multiple
Values permitted	n/d
Classification	Recommended
Notes	Although most of the access authorization decisions are made simply on the basis of one or more attributes, for some services access will be allowed only if a more complex set of conditions is satisfied, which may be difficult to determine in advance by the service provider. In the past this type of applications have forced the service provider to maintain the list of usernames for authorised users, which is difficult to maintain and can pose privacy risks. The attribute eduPersonEntitlement was introduced to solve this issue: the service provider defines a unique value (formatted as a URI) to be assigned to eduPersonEntitlement to mark users who meet certain conditions. The Home organisation is responsible for the control of its users, so that those who meet the conditions are assigned an appropriate entitlement. In general eduPersonEntitlement is not considered as personal data, however where there are only a few holders of entitlements in an organisation their identification is possible bycrossing the data with other information. For example, if eduPersonEntitlement is used to grant access to sensitive data, such value can be treated only after having obtained the written approval of the user. So, before assigning an eduPersonEntitlement value to a user, the organisation has to determine whether it is necessary to get the user's consent. In any case the eduPersonEntitlement attribute must be issued only to service providers for which the value is relevant to access control. With this attribute, the service provider in fact delegates the Home organisation to decide which users are authorised to access the service. The attribute may also contain values that identify a user's property (not defined byother attributes) based on which the permission to access the service may be granted.
Examples	`eduPersonEntitlement: urn:mace:dir:entitlement:common-lib-terms` `eduPersonEntitlement: urn:mace:internet2:terena.nl:garr:service`
Typical use	Authorization

4.2.4 eduPersonOrcid

Description	Researcher ORCID identifier assigned and managed by orcid.org
SAML2 Identifier	urn:oid:1.3.6.1.4.1.5923.1.1.1.16
Semantics	Each value is a persistent ID that univocally identifies the person.

References	[RFC 4512];[EDUPER]
LDAP syntax	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# of values	Multiple
Values permitted	n/d
Classification	Optional
Notes	ORCID ID are digital persistent identifiers for a single researcher. Their principal objective is to connect persistently and uniquely researchers to their products and publications. The identifiers are registered and managed by ORCID.org
Examples	`eduPersonOrcid: http://orcid.org/0000-0002-1825-0097`
Typical use	NIH/NLM SciENcv self-service web application

4.2.5 eduPersonOrgDN

Description	User's home organisation
SAML2 Identifier	urn:oid:1.3.6.1.4.1.5923.1.1.1.3
Semantics	The Distinguished Name (DN) of the entry that represents the home organisation of the person
References	[EDUPER]
LDAP syntax	Distinguished Name syntax 1.3.6.1.4.1.1466.115.121.1.12
# of values	Single
Values permitted	n/d
Classification	Optional
Notes	
Examples	`eduPersonOrgDN: o=unimore,dc=unimore,dc=it` `eduPersonOrgDN: o=Istituto di Fisiologia Clinica,dc=ifc,dc=cnr,dc=it`
Typical use	Additional information about the user

4.2.6 eduPersonOrgUnitDN

Description	Organisational Unit
SAML2 Identifier	urn:oid:1.3.6.1.4.1.5923.1.1.1.4
Semantics	The distinguished name(s) (DN) of the directory entries representing the person's organisational Unit(s). (for example Department)
References	[EDUPER], [RFC 4524]
LDAP syntax	Distinguished Name syntax 1.3.6.1.4.1.1466.115.121.1.12

# of values	Multiple
Values permitted	n/d
Classification	Optional
Notes	
Examples	`eduPersonOrgUnitDN: ou=Dipartimento di Fisica,o=unimore,dc=unimore,dc=it`
Typical use	Additional information about the user

4.2.7 eduPersonPrincipalName

Description	Unique and persistent identifier of the user
SAML2 Identifier	urn:oid:1.3.6.1.4.1.5923.1.1.1.6
Semantics	An ID which permits to recognize uniquely a user in a coherent manner between different services, in the form of: <identification>@<organisation>
References	[EDUPER]
LDAP syntax	DirectoryString 1.3.6.1.4.1.1466.115.121.1.15
# of values	Single
Values permitted	n/d
Classification	Recommended
Notes	When a value for this attribute is assigned to a specific user, the same value cannot be assigned to any other user, not even after user departing.
Examples	`eduPersonPrincipalName: 132lk1j2l@biblio.bo.cnr.it` `eduPersonPrincipalName: mrossi@esempio.it`
Typical use	Authorization, Accounting

4.2.8 eduPersonScopedAffiliation

Description	Indicate the affiliation of the user with his/her home organisation, in the following form. <affiliation>@<organisation>
SAML2 Identifier	urn:oid:1.3.6.1.4.1.5923.1.1.1.9
Semantics	Affiliation according to the conventions described in appendix B in conjunction with the Home organisation indicated in <organisation>
References	[EDUPER], [UK2] 3.2.2, [UK3] 7.1.2, Appendice B
LDAP syntax	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# of values	Multiple

Values permitted	<affiliation>: see Appendix B for a list of allowed values for this attribute <organisation>: DNS name
Classification	Mandatory
Notes	eduPersonScopedAffiliation allows minimal intrusion into user privacy while being sufficient to decide on the access authorization in many situations. The Home organisation should release the least intrusive value regarding the user involved and the accessed service; the service provider should design its own authorization system to be able to use this attribute wherever possible [UK2]
Examples	`eduPersonScopedAffiliation: staff@biblio.bo.cnr.it` `eduPersonScopedAffiliation: faculty@unica.it`
Typical use	Authorization

4.2.9 eduPersonTargetedID

Description	A persistent, non-reassignable, privacy-preserving identifier for a user shared between the identity provider and the service provider (or a group of service providers). An identity provider uses the appropriate value of this attribute when communicating with a particular service provider or group of service providers, and does not reveal that value to any other service provider. Organisation defines the ID of the user's IdP.
SAML2 Identifier	urn:oid:1.3.6.1.4.1.5923.1.1.1.10
Semantics	Each value is an anonymous, persistent, pairwise and non-reassignable identifier, which is associated to the user for the access to a specific service. It is composed by three parts: <organisation>!<service>!<opaque string> <organisation> stands for the user's IdP entityID. <service> stands for the SP entityID. <opaque string> is computed by IdP through a hashing mechanism on univocal user data. The persistent identifiers defined in SAML 2.0 are compliant with these specifications
References	[EDUPER], [UK3] (par. 7.1.3.2) e [UK2] (par. 3.2.2), [SAML-CORE] (par. 8.3.7)
LDAP syntax	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# of values	Multiple
Values permitted	Maximum length 256 characters
Classification	Recommended The generation of this attribute is still necessary for SPs currently not

	complying with the usage of SAML 2.0 persistent NameID in the assertion subject.
Notes	The opaque string must not allow the service to trace directly the identity of the user but it should only allow the recognition of the user in the successive sessions after the first access to the service. Once used for a user, the value cannot be reassigned to another user or service.
Examples	`eduPersonTargetedID: biblio.bo.cnr.it!servizio_1!1304asf2rsfs` `eduPersonTargetedID: unica.it!servizio_n!alskdj92920alsk`
Typical use	Authorization, Accounting, personalised service

4.2.10 givenName

Description	Name
SAML2 Identifier	urn:oid:2.5.4.42
Semantics	Given name of the person as used in official communications
References	[RFC 4519];[EDUPER]
LDAP syntax	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# of values	Single
Values permitted	n/d
Classification	Recommended
Notes	The definition of "givenName" in [RFC 4519] includes several values for this attribute in order to speed up the research for most LDAP clients. However within the Federation, the Home organisation must provide a single value, e.g. the one used for official communications with the person.
Examples	`givenName: Andrea`
Typical use	Additional information about the user

4.2.11mail

Description	e-Mail Address
SAML2 Identifier	urn:oid:0.9.2342.19200300.100.1.3
Semantics	Indicate the user email address
References	[RFC 4524]
LDAP syntax	IA5 String 1.3.6.1.4.1.1466.115.121.1.26
# of values	Multiple
Values permitted	n/d

Classification	Recommended
Notes	The values should be editable by the user
Examples	`mail: andrea.rossi@unimi.it`
Typical use	Additional information about the user

4.2.12 mobile

Description	Mobile number
SAML2 Identifier	urn:oid:0.9.2342.19200300.100.1.41
Semantics	The mobile number associated with the user, indicated according the international telephone numbers format
References	[RFC 4524]
LDAP syntax	Telephone Number 1.3.6.1.4.1.1466.115.121.1.50
# of values	Multiple
Values permitted	n/d
Classification	Optional
Notes	Some services may want to contact the user on the phone by voice or through SMS. Be careful with user's privacy terms and conditions when transferring private telephone numbers. There should not be any problem when transferring business telephone numbers. Values should be editable by the user.
Examples	`mobile: +39 347 379 15 71`
Typical use	Additional information about the user

4.2.13preferredLanguage

Description	Language preferred by the user
SAML2 Identifier	urn:oid:2.16.840.1.113730.3.1.39
Semantics	Written or spoken language preferred by the user
References	[RFC2798], [RFC5646],[ISO 639], [ISO 3166]
LDAP syntax	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# of values	Single
Values permitted	The language-tags are formed by a primary-tag and by more subtags The latters can also be empty. language-tag = primary-tag *("-" subtag) primary-tag = 1*8ALPHA subtag = 1*8ALPHA

	No white spaces are allowed between the tags. The tags are case insensitive. The namespace of the language-tags is administered by IANA
Classification	Optional
Notes	
Examples	`preferredLanguage: it` `preferredLanguage: it-ch`
Typical use	Additional information about the user

4.2.14schacHomeorganisation

Description	The DNS name of the user's organisation
SAML2 Identifier	urn:oid:1.3.6.1.4.1.25178.1.2.9
Semantics	The DNS name of the user's organisation
References	[SCHAC]
LDAP syntax	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# of values	Single
Values permitted	
Classification	Recommended
Notes	

Examples	`units.it`
	`unitn.it`
	`unimib.it`

Typical use	Additional information about the user

4.2.15schacHomeorganisationType

Description	Type of organisation the user belongs to
SAML2 Identifier	urn:oid:`1.3.6.1.4.1.25178.1.2.10`
Semantics	Defines the type of the organisation to which the user belongs. Format: urn:schac:homeorganisationType:<country-code>:<string>
References	[schac], [ISO3166]
LDAP syntax	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# of values	Multiple
Values permitted	urn:schac:homeorganisationType:<country-code>:<string> Where <country-code> is a valid ISO 3166 country code, of two letters, or the "int" string, assigned by SCHAC URN registry for this attribute on: https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry and <string> is a national controlled vocabulary form, published by an URI identified by SCHAC URN registry.

Classification	Recommended
Notes	

Examples	`urn:schac:homeorganisationType:eu:higherEducationInstitution`
	`urn:schac:homeorganisationType:int:universityHospital`
	`urn:schac:homeorganisationType:eu:educationInstitution`
	`urn:schac:homeorganisationType:eu:higherEducationInstitution`

Typical use	Additional information about the user

4.2.16schacMotherTongue

Description	Mother tongue of the user
SAML2 Identifier	urn:oid:1.3.6.1.4.1.25178.1.2.1
Semantics	Is the language a person learns first
References	[SCHAC], [RFC5646], [ISO 639]
LDAP syntax	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# of values	Single
Values permitted	
Classification	Optional
Notes	
Examples	`schacMotherTongue: it` `schacMotherTongue: fr-ch`
Typical use	Additional information about the user

4.2.17schacPersonalTitle

Description	Salutation title for a person.
SAML2 Identifier	urn:oid:1.3.6.1.4.1.25178.1.2.8
Semantics	A personal title or salutation for a person
References	[SCHAC], [RFC4524]
LDAP syntax	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# of values	Single
Values permitted	n/d
Classification	Optional
Notes	
Examples	`urn:schac:personalTitle: Sig.`
Typical use	Additional information about the user

4.2.18schacPersonalUniqueID

Description	"Legal unique ID" associated to the person
SAML2 Identifier	urn:oid:1.3.6.1.4.1.25178.1.2.15

Semantics	Specifies a "legal unique ID" associated to the person. Such as the DNI in Spain, FIC in Finland, NIN in Sweden,...
References	[SCHAC]
LDAP syntax	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# of values	multiple
Values permitted	The values are in the form: urn:schac:personalUniqueID:<country-code>:<idType>:<idValue>, where: <country-code> ID country code, a two letter code as described in ISO 3166 country code identifier; <idType> type of ID. The acceptable value are described for each country code by an URI registered in TERENA URN registry; <idValue> is the value.
Classification	Optional
Notes	The national extension “it” is being registered in TERENA URN registry. At the moment the only usage for the attribute in Italy is for the Tax Identification Number (Codice Fiscale).

Examples	`urn:schac:personalUniqueID:it:CF:LBRDNL89S09D704H`
	`urn:schac:personalUniqueID:fi:FIC:260667-123F`
	`urn:schac:personalUniqueID:es:DNI:31241312L`
	`urn:schac:personalUniqueID:se:NIN:12345678`

Typical use	Additional information about the user

4.2.19 schacUserPresenceID

Description	To store a set of values related to network presence protocol.
SAML2 Identifier	urn:oid:1.3.6.1.4.1.25178.1.2.12
Semantics	To store a set of values related to network presence protocol.
References	[SCHAC]
LDAP syntax	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# of values	Multiple
Values permitted	n/d
Classification	Optional
Notes	Values should be editable by the user.

Examples	`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`

Typical use	Additional information about the user

4.2.20 sn

Description	Last name
SAML2 Identifier	urn:oid:2.5.4.4
Semantics	Last name of the person as used in official communications
References	[RFC 4519];[eduPerson]
LDAP syntax	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# of values	Single
Values permitted	n/d
Classification	Recommended
Notes	The definition of "sn" in [RFC 4519] includes several values for this attribute in order to speed up the research for most LDAP client. However within the Federation, the Home organisation must provide a single value, eg. the one used for official communications with the person
Examples	`sn: Rossi`
Typical use	Additional information about the user

4.2.21 telephoneNumber

Description	Telephone number
SAML2 Identifier	urn:oid:2.5.4.20
Semantics	User's phone number, indicated according to the international phone numbers format
References	[RFC 4519]
LDAP syntax	Telephone Number 1.3.6.1.4.1.1466.115.121.1.50
# of values	Multiple
Values permitted	n/d
Classification	Optional
Notes	Special services may want to contact the user by phone. Be careful with user's privacy when transferring private telephone numbers. There shouldn't be any problems when transferring business telephone numbers. The values should be editable by the user
Examples	`telephoneNumber: +39 02 779 160 81`
Typical use	Additional information about the user

4.2.22 title

Description	Title of the person within organisational context
SAML2 Identifier	urn:oid:2.5.4.12
Semantics	Indicate the title of a person within his/her own organisational context
References	[RFC 4519]
LDAP syntax	Directory String 1.3.6.1.4.1.1466.115.121.1.15
# of values	Multiple
Values permitted	n/d
Classification	Optional
Notes	
Examples	`title: Director`
Typical use	Additional information about the user

5 Bibliography

English Federation Documentation

[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

Norwegian Federation Documentation

[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, LDAP Schemas 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/

Protection of personal and sensitive data

[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] Data protection in the European Union

http://ec.europa.eu/justice/data-protection/index_en.htm

[EU2] European directives

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