

Política d'emissió d'atributs en la federació

1. Introducció

L'objectiu d'aquesta pàgina és la definició de la política d'emissió d'atributs que estarà disponible en la federació.

2. Definició de la Política d'emissió d'atributs

La **política d'emissió d'atributs** (ARP) de la federació defineix aquells atributs que estaran disponibles en la interoperabilitat amb els Proveïdors de Servei. Això no implica que sempre s'enviïn tots els atributs a un SP de la federació, sinó que a més s'haurà d'enviar el mínim conjunt possible preservant així la reexpedició d'informació de l'usuari a tercers entitats.

La política té 3 categories de tipus d'atributs:

- **Identificació d'usuari:** són aquells atributs que proporcionen informació sobre la identitat que té l'usuari en la seva organització.
- **Estat de l'usuari:** són aquells atributs que descriuen situacions o condicions que en aquest moment té associat l'usuari en la seva organització.
- **Informació de l'organització:** són aquells atributs que descriuen i defineixen a l'organització de l'usuari.

Un atribut en la política està definit pels següents aspectes:

- **Nom:** identificador de l'atribut, on per a facilitar la interoperabilitat normalment s'utilitzaran aquells que es troben en esquemes de LDAP.
- **Descripció:** informa de l'objecte i semàntica de l'atribut.
- **OID:** conegut com a identificador d'objecte, és una seqüència de números que s'assignen jeràrquicament i que permet identificar objectes en la xarxa.
- **Multivaluat:** defineix si un atribut admet més d'un valor.
- **Emissor:** defineix qui ha de generar o emetre els valors de l'atribut. Existeixen dues possibilitats:
 - **Proveïdor d'Identitat:** és el propi IdP on l'usuari s'ha autenticat el que ha d'enviar l'atribut.
 - **HUB:** és el component HUB de la federació el que ha de generar els valors de l'atribut sobre la base de la informació rebuda o que d'alguna manera té emmagatzemada.
- **Estat:** en el cas que l'emissor sigui el Proveïdor d'Identitat defineix si l'emissió d'un atribut ha de ser obligatori (*MUST*) o opcional (*MAY*), mentre que si l'emissor és el HUB indica si l'atribut estaria sempre disponible (*MUST*) per al Proveïdor de Servei si així ho necessités o *MAY* en cas contrari

2.1. ARP de la federació

Nom	Descripció	OID	Multivaluat	Emissor	Estat
-----	------------	-----	-------------	---------	-------

Identificació de l'usuari					
displayName	Nom complet a mostrar de l'usuari	2.16.840.1.113730.3.1.241	No	IdP	MUST
eduPersonPrincipalName	Identificador de l'usuari dins de l'organització	1.3.6.1.4.1.5923.1.1.1.6	No	IdP	MUST
eduPersonTargetedID	Pseudònim de l'identificador d'usuari	1.3.6.1.4.1.5923.1.1.1.10	Sí	IdP	MUST
givenName	Nom propi de l'usuari	2.5.4.42	No	IdP	MAY
mail	Correu electrònic de l'usuari en l'organització	0.9.2342.19200300.100.1.3	Sí	IdP	MAY
preferredLanguage	Idioma preferit per l'usuari	2.16.840.1.113730.3.1.39	No	IdP	MAY
schacPersonalUniqueCode	Especifica un valor únic per a l'entrada a la qual s'associa	1.3.6.1.4.1.25178.1.2.14	Sí	IdP	MAY
schacPersonalUniqueID	Especifica un identificador legal únic de l'usuari	1.3.6.1.4.1.25178.1.2.15	No	IdP	MAY
schacSn1	Primer cognom de l'usuari	1.3.6.1.4.1.25178.1.2.6	No	IdP	MAY
schacSn2	Segon cognom de l'usuari	1.3.6.1.4.1.25178.1.2.7	No	IdP	MAY
sn	Cognoms de l'usuari	2.5.4.4	No	HUB	MAY
Estat de l'usuari en l'organització					
eduPersonEntitlement	Drets de l'usuari	1.3.6.1.4.1.5923.1.1.1.7	Sí	IdP	MAY
eduPersonScopedAffiliation	Pertinença i tipus d'associació a una unitat de l'organització	1.3.6.1.4.1.5923.1.1.1.9	Sí	IdP	MUST
eduPersonAssurance	Conjunt d'URIs per garantir la identitat	1.3.6.1.4.1.5923.1.1.1.11	Sí	IdP	MAY
Informació de l'organització					
schacHomeOrganization	Identificador únic de l'organització en la federació	1.3.6.1.4.1.25178.1.2.9	No	HUB	MUST
schacHomeOrganizationType	Tipus d'organització	1.3.6.1.4.1.25178.1.2.10	Sí	HUB	MUST

2.2. Atributs

2.2.1. Atribut "displayName"

Nom	displayName
Descripció	Nom complet de l'usuari a mostrar en una aplicació. No té per què ser una concatenació del nom i els cognoms de l'usuari, sinó una preferència de l'usuari a l'hora que l'identifiquin a través del seu nom i cognoms. Per exemple, és possible que l'usuari no vulgui que s'utilitzi el seu segon nom i el seu segon cognom.
OID	2.16.840.1.113730.3.1.241
URN	SAML2: urn:oid:2.16.840.1.113730.3.1.241 SAML1: urn:mace:dir:attribute-def:displayName
Format	Cadena de text.
Nombre de valors	1 o més valors.
Emissor	IdP
Estat	MUST

Exemples	Manuel Pérez
	John R. Stone
	Carmela Stockwell Pérez

2.2.2. Atribut "eduPersonPrincipalName"

Nom	eduPersonPrincipalName
Descripció	Identificador de l'usuari dins de l'organització.
OID	1.3.6.1.4.1.5923.1.1.1.6
URN	SAML2: urn:oid:1.3.6.1.4.1.5923.1.1.1.6 SAML1: urn:mace:dir:attribute-def:eduPersonPrincipalName
Format	El valor d'aquest atribut ha de tenir el format <i>id@domini_organització</i> , on id és un identificador de l'usuari i domini_organització és el domini principal de l'organització a la qual pertany l'usuari.
Nombre de valors	1
Emissor	IdP
Estat	<i>MUST</i>
Exemples	u17823@csuc.cat
	candido.rodolfo@prise.es

2.2.3. Atribut "eduPersonTargetedID"

Nom	eduPersonTargetedID
Descripció	Pseudònim de l'identificador d'usuari, amb l'objectiu de proporcionar un identificador opac diferent per a cada Proveïdor de Servei (SP) de la federació. D'aquesta manera, com per a cada SP el valor de l'atribut és diferent per a un mateix usuari, s'impedeix relacionar comportaments d'un mateix usuari en diferents serveis.
OID	1.3.6.1.4.1.5923.1.1.1.10
URN	SAML2: urn:oid:1.3.6.1.4.1.5923.1.1.1.10 SAML1: urn:mace:dir:attribute-def:eduPersonTargetedID
Format	Cadena alfanumèrica.
Nombre de valors	1 o més valors
Emissor	IdP
Estat	<i>MUST</i>
Exemples	21b0d36949acd6fd54 para la siguiente condición: (usuario=juan,IdP=CSUC,SP=Confluence)
	f2f0dcf57f06fbb9d171 para la siguiente condición: (usuario=juan,IdP=CSUC,SP=ScienceDirect.com)

2.2.4. Atribut "givenName"

Nom	givenName
Descripció	Nom propi de l'usuari així com els noms intermedis (middle names en anglès) que tingui.

OID	2.5.4.42
URN	SAML2: urn:oid:2.5.4.42 SAML1: urn:mace:dir:attribute-def:givenName
Formato	Cadena de text amb el nom propi de l'usuari.
Nombre de valors	0 o 1 valor
Emissor	IdP
Estat	MAY
Exemples	Manuel
	John R.

2.2.5. Atribut "mail"

Nom	mail
Descripció	Correu electrònic de l'usuari en l'organització.
OID	0.9.2342.19200300.100.1.3
URN	SAML2: urn:oid:0.9.2342.19200300.100.1.3 SAML1: urn:mace:dir:attribute-def:mail
Format	Correo electrónico
Nombre de valors	0 o més valors
Emissor	IdP
Estat	MAY
Exemples	juan@csuc.cat
	candido.rodolfo@prise.es

2.2.6. Atribut "preferredLanguage"

Nom	preferredLanguage
Descripció	Idioma preferit per l'usuari.
OID	2.16.840.1.113730.3.1.39
URN	SAML2: urn:oid:2.16.840.1.113730.3.1.39 SAML1: urn:mace:dir:attribute-def:preferredLanguage
Format	Una abreviatura de dues lletres per al llenguatge preferit segons la taula de codi d'abreviació de llenguatge ISO 639; no hi ha subcodis.
Nombre de valors	0 o 1 valor
Emissor	IdP
Estat	MAY
Exemples	ca
	es

2.2.7. Atribut "schacPersonalUniqueCode"

Nom	schacPersonalUniqueCode
Descripció	Un codi únic associat a un subjecte, que no ha de correspondre's necessàriament amb cap altre identificador fora de l'àmbit dels directoris que usin aquest esquema.
OID	1.3.6.1.4.1.25178.1.2.14
URN	SAML2: urn:oid:1.3.6.1.4.1.25178.1.2.14 SAML1: urn:schac:attribute-def:schacPersonalUniqueCode
Format	urn:schac:personalUniqueID:<country-code>:<id_type>:<id_value> urn:schac:personalUniqueID:int:passport:<country-code>:<passport_code> • <country-code> ha de ser o un codi de país vàlid, de dues lletres, segons l'ISO 3166 o la cadena "int", i ha d'haver estat assignat pel registre de URNs de TERENA per a aquest atribut a https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry#SCHACURNRegistry-personalUniqueCode • <id_type> ha de ser un valor seleccionat d'un vocabulari controlat nacional i publicat en el registre d'URNs de TERENA a dalt indicat. ○ Valors definits per Espanya: ■ urn:schac:personalUniqueID:es:DNI • Documento nacional de identidad de una persona ■ urn:schac:personalUniqueID:es:NIE • Número de identificación de extranjeros ■ urn:schac:personalUniqueID:es:UNK • Identificador de documento desconocido. Suele ser utilizado para extranjeros cuando el identificador del documento no se encuentra registrado en el registro de urn:schac:personalUniqueID de su país de origen. • <id_value> valor de l'id seleccionat • <passport_code> valor del passaport
No mbr e de valo rs	0 o més valors
Emissor	IdP
Estat	MAY
Exemples	urn:schac:personalUniqueCode:int:studentID:es:1234567890
	urn:schac:personalUniqueCode:es:upf.edu:estudiant:a3b123c12
	urn:schac:personalUniqueCode:es:esi:upf.edu:1234567890

2.2.8. Atribut "schacPersonalUniqueID"

Nom	schacPersonalUniqueID
Descripció	Especifica un identificador legal únic de l'usuari
OID	1.3.6.1.4.1.25178.1.2.15

URN	SAML2: urn:oid:1.3.6.1.4.1.25178.1.2.15 SAML1: urn:schac:attribute-def:schacPersonalUniqueID
Format	urn:schac:personalUniqueCode:<country-code>:<iNSS> • <country-code> ha de ser o un codi de país vàlid, de dues lletres, segons l'ISO 3166 o la cadena "int", i ha d'haver estat assignat pel registre de URNs de TERENA per a aquest atribut a https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry#SCHACURNRegistry-personalUniqueCode • <iNSS> és un Namespace Specific String tal com es defineix en el RFC2141 però no sensible al cas. Ha de ser triat d'una vocabulari controlat nacional i publicat en la direcció indicada en el registre de URNs de TERENA a dalt indicat. En el cas particular de MyAcademicID, es requereix que el valor enviat tingui el format següent: urn:schac:personalUniqueCode:es:esi:<sh0>:<identificador>
No mbr e de valo rs	0 o més valors
Emissor	IdP
Estat	MAY
Exemples	urn:schac:personalUniqueID:es:DNI:31241312L
	urn:schac:personalUniqueID:it:CF:XXXXXX00Z00Z000Z
	urn:schac:personalUniqueID:se:NIN:12345678

2.2.9. Atribut "schacSn1"

Nom	schacSn1
Descripció	Primer cognom de l'usuari.
OID	1.3.6.1.4.1.25178.1.2.6
URN	SAML2: urn:oid:1.3.6.1.4.1.25178.1.2.6 SAML1: urn:schac:attribute-def:schacSn1
Format	Cadena de text amb el primer cognom de l'usuari.
Nombre de valors	0 o 1 valor
Emissor	IdP
Estat	MAY
Exemples	Rodríguez
	Schmidt

2.2.10. Atribut "schacSn2"

Nom	schacSn2
Descripció	Segon cognom de l'usuari.
OID	1.3.6.1.4.1.25178.1.2.7
URN	SAML2: urn:oid:1.3.6.1.4.1.25178.1.2.7 SAML1: urn:schac:attribute-def:schacSn2
Format	Cadena de text amb el segon cognom de l'usuari. En el cas que l'usuari no tingui un segon cognom, el IdP no ha d'enviar cap valor per a aquest atribut.
Nombre de valors	0 o 1 valor
Emissor	IdP
Estat	MAY
Exemples	Sánchez
	Pérez

2.2.11. Atribut "sn"

Nom	sn
Descripció	Primer i segon (si tingués) cognoms de l'usuari
OID	2.5.4.4
URN	SAML2: urn:oid:2.5.4.4 SAML1: urn:mace:dir:attribute-def:sn
Format	Cadena de text amb els cognoms de l'usuari. Es generarà utilitzant els valors rebuts dels atributs schacSn1 i schacSn2
Nombre de valors	0 o 1 valor
Emissor	HUB
Estat	MAY
Exemples	Rodríguez Sánchez
	Schmidt

2.2.12. Atribut "eduPersonEntitlement"

Nom	eduPersonEntitlement
Descripció	Drets de l'usuari respecte als serveis que estan disponibles en la federació. Aquests drets li permeten a l'aplicació decidir tant si oferir-li el servei com un conjunt total o parcial de les característiques d'aquest.
OID	1.3.6.1.4.1.5923.1.1.1.7
URN	SAML2: urn:oid:1.3.6.1.4.1.5923.1.1.1.7 SAML1: urn:mace:dir:attribute-def:eduPersonEntitlement
Format	URI (URN o URL) que indica un conjunt de drets per a recursos específics, segons <i>RFC 2141</i>
Nombre de valors	0 o més valors
Emissor	IdP

Estat	MAY
Exemples	urn:mace:dir:entitlement:common-lib-terms

2.2.13. Atribut "eduPersonScopedAffiliation"

Nom	eduPersonScopedAffiliation
Descripció	Pertinença i tipus d'associació a una unitat de l'organització.
OID	1.3.6.1.4.1.5923.1.1.1.9
URN	SAML2: urn:oid:1.3.6.1.4.1.5923.1.1.1.9 SAML1: urn:mace:dir:attribute-def:eduPersonScopedAffiliation
Format	Ha de ser expressat sota el format <i>rol@domini_unitat_organització</i>. Els valors permesos per a <i>rol</i> estan definits sota una estructura jeràrquica: • Conjunt de valors per a indicar que és membre d'una unitat de l'organització amb un rol determinat: ◦ faculty: membre investigador (caso PDI). ◦ staff: membre de la plantilla (caso PAS). ◦ employee: membre que presta els seus serveis en l'organització però pertany a una altra organització externa. ◦ student: estudiant. • alum: antic estudiant. • affiliate: indica que l'usuari té algun tipus de relació amb l'organització però no està cobert per cap de les anteriors. Per exemple: pares d'estudiants, convidats, usuaris que són faculty o staff en una altra organització però que disposen d'identitat en l'organització a causa d'un projecte en comú, etc. • library-walk-in: indica aquells usuaris que poden gaudir dels serveis de biblioteca de l'organització. El <i>domini_unitat_organització</i> referencia sota format domini a una unitat de l'organització, podent ser la pròpia organització o un centre d'aquest
Nombre de valors	1 o més valors
Emissor	IdP
Estat	MUST
Exemples	student@informatica.univ.edu staff@univ.edu affiliate@csuc.cat

2.2.14. Atribut "eduPersonAssurance"

Nom	eduPersonAssurance
Descripció	Conjunt d'URIs que afirmen el compliment d'estàndards específics per garantir la identitat. Requerit per MyAcademicID (https://wiki.geant.org/display/MyAccessID/MyAccessID+Home)
OID	1.3.6.1.4.1.5923.1.1.1.11
URN	SAML2: urn:oid:1.3.6.1.4.1.5923.1.1.1.11 SAML1: urn:mace:dir:attribute-def:eduPersonAssurance
Format	No controlat
Nombre de valors	1 o més valors
Emissor	IdP
Estat	MAY
Exemples	urn:mace:incommon:IAQ:sample
	urn:mace:feide.no:auth:level:fad08:3
	http://idm.example.org/LOA#sample

2.2.15. Atribut "schacHomeOrganization"

Nom	schacHomeOrganization
Descripció	Identificador únic en l'organització.
OID	1.3.6.1.4.1.25178.1.2.9
URN	SAML2: urn:oid:1.3.6.1.4.1.25178.1.2.9 SAML1: urn:schac:attribute-def:schacHomeOrganization
Format	Domini segons <i>RFC 1035</i> . El domini ha de ser un domini de nivell secundari que estigui sota control de la institució. Preferiblement, s'ha d'utilitzar el nom de domini principal de la institució.
Nombre de valors	Un
Emissor	HUB
Estat	MUST
Exemples	csuc.cat
	prise.es

2.2.16. Atribut "schacHomeOrganizationType"

Nom	schacHomeOrganizationType
Descripció	Tipus d'organització
OID	1.3.6.1.4.1.25178.1.2.10

URN	SAML2: urn:oid:1.3.6.1.4.1.25178.1.2.10 SAML1: urn:mace:terena.org:attribute-def:schacHomeOrganizationType
Format	URN amb el valor que representa el tipus d'organització de l'usuari. La llista dels valors permesos és gestionada per TERENA i està disponible en https://wiki.refeds.org/display/stan/schac+URN+*Registry . A Espanya el vocabulari és gestionat per RedIRIS i la llista dels valors permesos està disponible en http://wiki.rediris.es/gtschema/iriseduperson#schacHomeOrganizationType . Els valors definits a Espanya són: • urn:schac:homeOrganizationType:es:university (Universitat) • urn:schac:homeOrganizationType:es:pri (Organisme públic de recerca) • urn:schac:homeOrganizationType:es:company (Empresa)
Nombre de valors	Un
Emissor	HUB
Estat	<i>MUST</i>
Exemples	urn:schac:homeOrganizationType:int:NRENAffiliate