eduGAIN Policy Framework Attribute Profile (RECOMMENDED)

Version date	Editor	Change
20.9.2010	ML	Changes based on the Call for Comments

This is the recommended profile for end users' attributes exchanged ~~in~~ throughout the eduGAIN service.

Initially, this profile covers only the Web Single Sign-On scenario. The profile may later be amended by additional scenarios with different requirements e.g. on recommended attributes.

1. Attributes for Web Single Sign-On

Attributes defined in eduPerson [eduPerson] and ~~Schac~~ SCHAC [SCHAC] MAY be used in eduGAIN.

Other attributes MAY be used based on a bilateral agreement between the ~~Identity and Service Providers~~Members.

The syntax for expressing attributes MUST follow MACE-Dir SAML Attribute Profiles [MACEDir].

Identity Providers SHOULD NOT release all attributes to all Service Providers for all end users. ~~For eduGAIN confederation~~service~~, a~~ A procedure for controlled attribute release and minimal disclosure is defined in the data protection profile [eduGAIN-DPP].

The technical representation of an attribute during the transfer is presented in the SAML 2.0 WebSSO protocol profile document [WebSSO].

1.1. Recommended Attributes

It is RECOMMENDED that eduGAIN P~~p~~articipant ~~f~~Federations make sure that Identity Providers ~~have~~ supply the following attributes~~ populated~~:

Friendly name	Defined in	Notes
displayName	[eduPerson]	
common name (cn)	[eduPerson]	Syntax may be culturally dependent (e.g. Firstname Lastname or Lastname Firstname)
mail	[eduPerson]	If populated, must be the end user’s valid personal

Friendly name	Defined in	Notes
		mail address (i.e. not a shared mailbox)
eduPersonAffiliation and eduPersonScopedAffiliation	[eduPerson]	see also 1.2.1
schacHomeOrganization	[SCHAC]	
schacHomeOrganizationType	[SCHAC]	see also 1.2.2

Table 1: Recommended Attributes.

~~SAML2 Persistent NameID vs eduPersonTargetedID - ? what happened to it? Should it be here?~~

- ~~common name~~
- ~~mail (if populated, must be the end user's valid and personal mail address)~~
- ~~eduPersonAffiliation and eduPersonScopedAffiliation~~
- ~~schacHomeOrganization~~
- ~~schacHomeOrganizationType~~
- ~~Open issue: displayName (for UI purposes? For what purpose is cn, then?)~~

A RECOMMENDED attribute means that it is available, in general, for most end users. However, it can be left empty for those end users who do not qualify ~~to~~ for any of the values in the vocabulary.

Application developers are advised to ~~make~~ produce fail-safe code, i.e. implementing appropriate fall-back mechanism, if an Identity Provider is unable to provide an attribute the Service Provider ~~is asking for~~requests.

1.2. Controlled Vocabularies

1.2.1 eduPersonAffiliation and eduPersonScopedAffiliation

eduPersonAffiliation and derivatives have a controlled vocabulary, as defined in eduPerson.

Participant Federations MUST ensure that Identity Providers use the semantics defined in **bold** face in the document "REFEDs ePSA usage comparison~~ v0.13~~" [ePSACompare] for the following attribute values:

- member
- faculty
- student
- alum
- affiliate
- library-walk-in

Following values are unreliable and SHOULD NOT be used by Service Providers, unless their semantics has been verified bilaterally with the Home Organisation or Home Federation:

- employee
- staff

~~The reader should notice that, currently, there is no way to express an organisation's end user who is neither student nor faculty.~~

1.2.2. schacHomeOrganizationType

schacHomeOrganizationType attribute has an international vocabulary, known by the prefix *urn:mace:terena.org:schac:homeOrganizationType:int*. The vocabulary MAY be amended by national, more specific values.

At least one value from the international vocabulary SHOULD be populated for each end user.

1.3. Unique Identifiers

1.3.1. SAML2 Persistent NameID

It is RECOMMENDED that Identity Providers support SAML2 Persistent Identifier as the unique opaque identifier for their end users. To ensure proper functioning of (possible) consent modules for attribute release, SAML2 Persistent Identifier MUST be placed both ~~to~~ in the subject/nameID element and ~~to~~ the attribute statement of a SAML assertion.

1.3.1. eduPersonPrincipalName (ePPN)

ePPN MAY be used as a unique identifier, but ~~Providers~~ Entities who decide to use it, MUST recognise that:

- Identity Providers in Participant Federations may decide to reassign ePPN values, according to local policies

- ePPN ~~is~~ may not be ~~less~~ privacy preserving ~~attribute that~~unlike SAML2 persistent NameID

References

~~**[SCHAC]** URL~~

~~[SAML2REFERENCE]~~ ~~URLthe SAML 2.0 WebSSO protocol profile document~~

[eduPerson~~REFERENCE~~] eduPerson(200806), ~~URL~~ http://middleware.internet2.edu/eduperson/

[eduGAIN-DPP] **eduGAIN Policy Framework: Data Protection Profile,**

[ePSACompare] ~~URL~~ REFEDs ePSA usage comparison v0.13,
http://www.terena.org/activities/refeds/docs/ePSAcomparison_0_13.pdf

[homeOrgType] TERENA Registry,
~~http://www.terena.org/registry/terena.org/schac/homeOrganizationType/index.html~~http://www.terena.org/registry/terena.org/schac/homeOrganizationType/index.html

[SCHAC] SCHAC 1.4.1.b1, http://www.terena.org/activities/tf-emc2/schacreleases.html

[WebSSO] eduGAIN Policy Framework. SAML2 WebSSO Protocol Profile

~~**[SAML2Int]**~~ **[MACEDir]** MACE-Dir SAML Attribute Profiles (200804),
http://middleware.internet2.edu/dir/docs/internet2-mace-dir-saml-attributes-200804.pdf

~~Glossary~~

~~**eduGAIN**~~ ~~Definition – which should automatically wrap to align correctly if the definition is longer than a single line, as this line should demonstrate~~

~~**ACRONYMSCHAC**~~ ~~Definition~~

~~**eduPersonACRONYM**~~ ~~Definition~~

~~**ACRONYMWebSSO**~~ ~~Definition~~

~~**SAML**~~ ~~Definition~~

~~**REFEDs**~~ ~~Research and Education Federations~~