eduGAIN Policy Framework Attribute Profile

Version	Version date	Editor	Change
1.0	29.4.2011	Mikael Linden	Approved by SA3 T3 task leader 28.4.2011
1.1	14.11.2012	Mikael Linden	Policy review. A new Schac namespace and a scope check for scoped attributes.
1.2	28.11.2012	Mikael Linden	Fixed the attribute name used for the SAML2 persistent identifier in an attribute statement. Relation of displayName and cn.
1.3	5.12.2012	Mikael Linden	
1.4	24 Feb 2015	Brook Schofield	Corrected undefined SCHAC attribute.

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

Initially, this profile covers only the Web Single Sign-On scenario. The profile may be amended later by adding scenarios with different requirements, such as recommended attributes.

1. Attributes for Web Single Sign-On

Attributes defined in eduPerson [eduPerson] and SCHAC [SCHAC] MAY be used in eduGAIN. Other attributes MAY be used based on a bilateral agreement between the 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. A procedure for controlled attribute release and minimal disclosure is defined in the GÉANT Data protection Code of Conduct [GÉANT-CoC].

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 Participant Federations ensure that Identity Providers supply the following attributes:

Friendly name	Defined in	Notes
displayName	[eduPerson]	Since other attribute types such as 'cn' are multivalued, an additional attribute type is needed. Display name is defined for this purpose. Syntax may be culturally dependent (for example, Firstname Lastname or Lastname Firstname).
common name (cn)	[eduPerson]	Syntax may be culturally dependent (for example, Firstname Lastname or Lastname Firstname).

Friendly name	Defined in	Notes
mail	[eduPerson]	If populated, this must be the end user's valid personal mail address (not a shared mailbox).
eduPersonAffiliation and eduPersonScopedAffiliation	[eduPerson]	See section 1.2.1.
eduPersonPrincipalName	[eduPerson]	See section 1.3.2.
SAML2 Persistent NameID (eduPersonTargetedID)	[SAMLCore, eduPerson]	See section 1.3.1.
schacHomeOrganization	[SCHAC]	

Table 1: Recommended Attributes

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 for any of the values in the vocabulary.

Application developers are advised to produce fail-safe code, such as implementing an appropriate fall-back mechanism if an Identity Provider is unable to provide an attribute that the Service Provider 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*" [ePSACompare] for the following attribute values:

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

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

- employee
- staff

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 in the subject/nameID element and the attribute statement of a SAML assertion. The attribute name used in the attribute statement MUST be eduPersonTargetedID as defined in section 3.3.1.1 of [MACEDir].

1.3.2. eduPersonPrincipalName (ePPN)

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

- Identity Providers in Participant Federations may decide to re-assign ePPN values according to local policies.
- ePPN may not be privacy preserving, unlike SAML2 persistent NameID.

1.4. Scoped Attributes

If a Service Provider makes use of a scoped attribute (such as eduPersonScopedAffiliation or eduPersonPrincipalName), it is encouraged to use available mechanisms to ensure the “scope” value of the attribute matches one permitted to the Identity Provider asserting the value.

References

[eduPerson]	eduPerson(200806), http://middleware.internet2.edu/eduperson/
[ePSACompare]	REFEDs ePSA usage comparison v0.13, http://www.terena.org/activities/refeds/docs/ePSAcomparison_0_13.pdf
[GÉANT-CoC]	GÉANT Data protection Code of Conduct
[homeOrgType]	TERENA Registry, http://www.terena.org/registry/terena.org/schac/homeOrganizationType/index.html
[SAMLCore]	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, 15 March 2005.
[SCHAC]	SCHAC 1.4.1.b1, http://www.terena.org/activities/tf-emc2/schacreleases.html

[WebSSO] eduGAIN Policy Framework. SAML2 WebSSO Protocol Profile
[MACEDir] MACE-Dir SAML Attribute Profiles (200804), http://middleware.internet2.edu/dir/docs/internet2-mace-dir-saml-attributes-200804.pdf