



1 **eduGAIN Policy Framework**
2 **Attribute Profile**
3 **(RECOMMENDED)**



4

Version	Version date	Editor	Change
1.0	29.4.2011	Mikael Linden	Approved by SA3 T3 task leader 28.4.2011

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

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

8 1. Attributes for Web Single Sign-On

9 Attributes defined in eduPerson [eduPerson] and SCHAC [SCHAC] MAY be used in eduGAIN. Other attributes
10 MAY be used based on a bilateral agreement between the Members.

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

12 Identity Providers SHOULD NOT release all attributes to all Service Providers for all end users. A procedure for
13 controlled attribute release and minimal disclosure is defined in the Data protection good practice profile
14 document [eduGAIN-DPP].

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

17 1.1. Recommended Attributes

18 It is RECOMMENDED that eduGAIN Participant Federations ensure that Identity Providers supply the following
19 attributes:

Friendly name	Defined in	Notes
displayName	[eduPerson]	
common name (cn)	[eduPerson]	Syntax may be culturally dependent (for example, Firstname Lastname or Lastname Firstname).
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.

Friendly name	Defined in	Notes
schacHomeOrganization	[SCHAC]	
schacHomeOrganizationType	[SCHAC]	See section 1.2.2.

20 Table 1: Recommended Attributes

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

23 Application developers are advised to produce fail-safe code, such as implementing an appropriate fall-back
24 mechanism if an Identity Provider is unable to provide an attribute that the Service Provider requests.

25 1.2. Controlled Vocabularies

26 1.2.1 eduPersonAffiliation and eduPersonScopedAffiliation

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

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

- 30 • member
- 31 • faculty
- 32 • student
- 33 • alum
- 34 • affiliate
- 35 • library-walk-in

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

- 38 • employee
- 39 • staff

40 1.2.2. schacHomeOrganizationType

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

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

45 1.3. Unique Identifiers

46 1.3.1. SAML2 Persistent NameID

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

51 1.3.1. eduPersonPrincipalName (ePPN)

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

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

56 References

57	[eduPerson]	eduPerson(200806), http://middleware.internet2.edu/eduperson/
58	[eduGAIN-DPP]	eduGAIN Policy Framework: Data Protection Good Practice Profile
59	[ePSACompare]	REFEDs ePSA usage comparison v0.13, http://www.terena.org/activities/refeds/docs/ePSAcomparison_0_13.pdf
60	[homeOrgType]	TERENA Registry, http://www.terena.org/registry/terena.org/schac/homeOrganizationType/index.html
61	[SCHAC]	SCHAC 1.4.1.b1, http://www.terena.org/activities/tf-emc2/schacreleases.html
62	[WebSSO]	eduGAIN Policy Framework. SAML2 WebSSO Protocol Profile
63	[MACEDir]	MACE-Dir SAML Attribute Profiles (200804), http://middleware.internet2.edu/dir/docs/internet2-mace-dir-saml-attributes-200804.pdf
64		
65		
66		
67		
68		
69		