Entity Category attribute release in SWAMID

Entity categories are used for data release minimization and scalable attribute release from an Identity Provider within SWAMID to a Service Provider in SWAMID and/or eduGAIN.

If an owner of a Service and the Identity Provider Home Organisation has a bilateral agreement the attribute release can be extended with additional attributes based on the agreement.

Please note that the old entity categories SWAMD Research and Education and SWAMID SFS 1993:1153 is deprecated and will removed from all services metadata at the end of 2022.

Best Practice attribute release based on entity categories

x - Attribute is released if it's available in the Home Organisation Identity Provider.
o - Attribute is released only if requested and required in the metadata for the service and if it's available in the Home Organisation Identity Provider.

SAML2 Attribute Identifier	Friendly Name	Without enitity category	Data protection Code of Conduct (REFEDS CoCo v2 and GÉANT CoCo v1)	REFEDS Personalized Access Entity Category	REFEDS Pseudonymous Access Entity Category	REFEDS Anonymous Access Entity Category	REFEDS Research and Scholarship Entity Category (R&S)	European Student Identifier Entity Category
			⚠ **Restriction** Attribute released "only if requested and required" in metadata[1]. Note that norEduPersonNIN and personalIdentity Number has additional restrictions[2].					
urn:oasis:names:tc:SAML:attribute:pairwise-id	pairwise-id		o		x			
urn:oasis:names:tc:SAML:attribute:subject-id	subject-id		o	x				
urn:oid:1.3.6.1.4.1.5923.1.1.1.10	eduPersonTargetedID		o				(x[3])	
urn:oid:1.3.6.1.4.1.5923.1.1.1.6	eduPersonPrincipalName		o				x	
urn:oid:1.3.6.1.4.1.5923.1.1.1.16	eduPersonOrcid		o[4]					
urn:oid:1.3.6.1.4.1.2428.90.1.5	norEduPersonNIN		o[2]					
urn:oid:1.2.752.29.4.13	personalIdentityNumber		o[2]					
urn:oid:1.3.6.1.4.1.25178.1.2.3	schacDateOfBirth		o					
urn:oid:0.9.2342.19200300.100.1.3	mail		o	x			x	
urn:oid:2.16.840.1.113730.3.1.13	mailLocalAddress		o[5]					
urn:oid:2.5.4.42	givenName		o[6]	x[6]			x[6]	
urn:oid:2.5.4.4	sn *(aka surname)*		o[6]	x[6]			x[6]	
urn:oid:2.16.840.1.113730.3.1.241	displayName		o[6]	x[6]			x[6]	
urn:oid:1.3.6.1.4.1.2428.90.1.10	norEduPersonLegalName		o[6]					

urn:oid:2.5.4.3	cn *(aka commonName)*		o[6]					
urn:oid:1.3.6.1.4.1.5923.1.1.1.11	eduPersonAssurance		o	x	x		x[7]	
urn:oid:1.3.6.1.4.1.5923.1.1.1.9	eduPersonScopedAffiliation		o	x	x	x	x	
urn:oid:1.3.6.1.4.1.5923.1.1.1.1	eduPersonAffiliation		o					
urn:oid:2.5.4.10	o *(aka organizationName)*		o					
urn:oid:1.3.6.1.4.1.2428.90.1.6	norEduOrgAcronym		o					
urn:oid:2.5.4.6	c *(aka countryName)*		o					
urn:oid:0.9.2342.19200300.100.1.43	co *(aka friendlyCountryName)*		o					
urn:oid:1.3.6.1.4.1.25178.1.2.9	schacHomeOrganization		o	x	x	x		
urn:oid:1.3.6.1.4.1.25178.1.2.10	schacHomeOrganizationType		o					
urn:oid:1.3.6.1.4.1.25178.1.2.14	schacPersonalUniqueCode							x[8]

1. The entity category the REFEDS and GÉANT Code of Conduct entity categories does not have a specific attribute bundle. Instead of an attribute bundle it uses attribute request in metadata for specific required attributes.
2. norEduPersonNIN and personalIdentityNumber shall only be released when required by entities registered with in SWAMID (registrationAuthority="http://www.swamid.se/").
    - personalIdentityNumber must only contain Swedish Personal Numbers or Swedish Co-ordination Numbers.
    - norEduPersonNIN can besides Swedish Personal Numbers and Swedish Co-ordination Numbers also contain Interim Personal Numbers from the student documentation system Ladok and the Swedish national study enrolment system.
3. eduPersonTargetedID should only be released with the entity category REFEDS Research & Scholarship if eduPersonPrincipalName is reassignable. All Identity Providers in SWAMID must by the SWAMID Assurance Profiles be longterm unique and therefore it should not be released.
4. eduPersonOrcid should only be released if and only if the IdP organization has retrived the ORCID iD via the ORCID Collect & Connect service. ORCID iDs are persistent digital identifiers for individual researchers. Their primary purpose is to unambiguously and definitively link them with their scholarly work products. ORCID iDs are assigned,managed and maintained by the ORCID organization.
5. mailLocalAddress is used for services that may need access to more than one mail address for the user, for example mail aliases and secondary mail addresses. A use case for this is when a person is invited by another mail address than the one in released in the mail attribute.
6. Name attribute are expected to be released as following:
    - givenName is the legal first name of the person. If the person has more than one legal first name it's possible to only release the default name (sw. tilltalsnamn) or the person can choose which one of the legal first names they want to be released.
    - sn (aka surname) is the legal last name (or family name) of the person.
    - displayName shall always be the combination of givenName and sn.
    - norEduPersonLegalName must always be the full legal name from the population registry or the passport, otherwise it must not be released.
    - cn (aka commonName) must be the persons full name, not the attribute value from Active Directory.
7. Within SWAMID the REFEDS Research and Scholarship Entity Category is extended to also include eduPersonAssurance.
8. This entity category should only trigger release of the European Student Identifier (ESI) value as specified by https://wiki.geant.org/display/SM/European+Student+Identifier

URI for all entity categories used within SWAMID

Entity category	Unique identifier	
GÉANT Data Protection Code of Conduct Entity Category	http://www.geant.net/uri/dataprotection-code-of-conduct/v1	
REFEDS Data Protection Code of Conduct Entity Category	https://refeds.org/category/code-of-conduct/v2	
REFEDS Personalized Access Entity Category	https://refeds.org/category/personalized	
REFEDS Pseudonymous Access Entity Category	https://refeds.org/category/pseudonymous	
REFEDS Anonymous Access Entity Category	https://refeds.org/category/anonymous	

REFEDS Research and Scholarship Entity Category (R&S)	http://refeds.org/category/research-and-scholarship	
European Student Identifier Entity Category (ESI)	https://myacademicid.org/entity-categories/esi	
SWAMID R&E	http://www.swamid.se/category/research-and-education	Deprecated and decommisoned
SWAMID SFS-1993-1153	http://www.swamid.se/category/sfs-1993-1153	Deprecated and decommisoned
SWAMID EU-Adequate-Protection	http://www.swamid.se/category/eu-adequate-protection	Deprecated and decommisoned
SWAMID NREN-Service	http://www.swamid.se/category/nren-service	Deprecated and decommisoned
SWAMID HEI-Service	http://www.swamid.se/category/hei-service	Deprecated and decommisoned

URI for all assurance profiles used within SWAMID

Entitetskategori	**Unik identifierare**	
SWAMID AL1	http://www.swamid.se/policy/assurance/al1	
SWAMID AL2	http://www.swamid.se/policy/assurance/al2	
SWAMID AL3	http://www.swamid.se/policy/assurance/al3	
SWAMID AL2-MFA-HI	https://www.swamid.se/policy/authentication/swamid-al2-mfa-hi	Deprecated and decommisoned
REFEDS Assurance Framework	https://refeds.org/assurance/*	
REFEDS Security Incident Response Trust Framework for Federated Identity (SIRTFI) version 1	https://refeds.org/sirtfi	
REFEDS Security Incident Response Trust Framework for Federated Identity (SIRTFI) version 2	https://refeds.org/sirtfi2	