SCHAC

SCHema for ACademia

v: 1.5.0 - 2015-04-12

Document: schac_1.5.0.pdf
Location: https://wiki.refeds.org/display/STAN/SCHAC+Releases

Editor: Heather Flanagan, SCHAC Shepherd
Comments to: refeds@terena.org

Table of Contents

About SCHAC

The SCHema for ACademia, SCHAC <https://wiki.refeds.org/display/STAN/SCHAC>, aims to define and promote common schemas in the field of higher education to facilitate inter-institutional data exchange. This schema is originally the result of the work in the area of attributes coordination carried out within the now-discontinued TERENA Task Force on Middleware, TF-EMC2 <http://www.terena.org/activities/tf-emc2and is now being maintained under the auspices of REFEDS <https://refeds.org> and the SCHAC Editorial Board.

SCHAC work started in 2005; the first release of "SCHAC Individual Attributes Specification" was issued in May 2006.

Current as well as older SCHAC specifications can be found on SCHAC web page <https://wiki.refeds.org/display/STAN/SCHAC>, under the section called "SCHAC Releases" <https://wiki.refeds.org/display/STAN/SCHAC+Releases>.

For more information about SCHAC, please refer to the SCHAC web page <https://wiki.refeds.org/display/STAN/SCHAC>.

Related Work

In its current version, the SCHAC schemas are not oriented to any particular technology. They define a set of attributes to describe individuals in the academic and research institutions. An appropriate LDAP profile is included as an appendix of this document. An XML profile will be defined in Appendix B at the end of this document.

These definitions assume that other attributes describing individuals are already available and properly encoded, according to the following standards:

The eduPerson schema v. 201310, as defined at http://macedir.org/specs/eduperson/
The person schema, as defined by X.521 (2001) - [RFC 4517, RFC 4519]
The organizationalPerson schema, as defined by X.521 (2001) - [RFC 4517, RFC 4519]
The inetOrgPerson schema, as defined by RFC 2798

Please note that where newer versions of the references exist, only the versions referred to in the current SCHAC specifications normatively apply.

Attribute Information

For all attributes, the following metadata is defined:

Name	**A label used to identify and distinguish one attribute from another**
Description	A short description of the attribute
OID	Registered OID of the attribute
Format	The syntax for the representation of the attribute's values
Number of values	Single Only one value is permitted for describing a given individual Multi An indefinite number of values can be used
References	Additional information used to clarify some properties of attributes like format, description or number of values
RFC 4517 definition	`Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules`
Examples	Example of values used within the attribute

Attribute Classification

The attributes considered in this document are designed to contain information specifically about people. It is helpful to consider this information within broad categories. The ten categories used in this document have been collected from the NMI LocalDomainPerson survey <http://www.nmi-edit.org/CAMP/EDIT_IdM/docs/internet2-mace-dir-localdomainperson-200505.html> and discussions with the International Schema Archives (Feb, 2004; no longer available online). The categories are:

- Personal Characteristics
- Contact / Location Information
- Student Information
- Employee Information
- Linkage Identifiers / Foreign Keys
- Entry Metadata / Administration Information
- Confidentiality / Attribute Release (Visibility)
- Authorization, Entitlements
- Group-related Attributes

Attributes defined by SCHAC

Personal Characteristics

Personal characteristics describe the individual person represented by the entry.

schacMotherTongue

Name	**schacMotherTongue**
Description	Is the language a person learns first. Correspondingly, the person is called a native speaker of the language. Usually a child learns the basics of their first language from their family.
OID	1.3.6.1.4.1.25178.1.2.1
Format	See RFC 3066 Tags for the Identification of Languages
Number of values	Single
References	ISO 639 - Language Codes RFC 2798 - Definition of the inetOrgPerson LDAP Object Class RFC 3066 - Tags for the Identification of Languages

RFC 4517 definition	`( schacAttributeType:1`
	`NAME 'schacMotherTongue'`
	`DESC 'RFC 3066 code for prefered language of communication'`
	`EQUALITY caseExactMatch`
	`SINGLE-VALUE`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )`

Examples	schacMotherTongue = fr schacMotherTongue = es-ES

schacGender

Name	**schacGender**
Description	The state of being male or female. The gender attribute specifies the legal gender of the subject it is associated with. "Either of the two groups that people, animals and plants are divided into according to their function of producing young" (Oxford Advanced Learner's Dictionary)
OID	1.3.6.1.4.1.25178.1.2.2
Format	0 Not known 1 Male 2 Female 9 Not specified
Number of values	Single
References	ISO 5218 - Information interchange -- Representation of human sexes.The standard ISO 5218 defines the representation of the human sexes by a numeric digital code. It was created by the Data Management and Interchange Technical Committee and proposed in November 1976

RFC 4517 definition	`( schacAttributeType:2`
	`NAME 'schacGender'`
	`DESC 'Representation of human sex (see ISO 5218)'`
	`EQUALITY integerMatchSINGLE-VALUE`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 )`

Examples	schacGender = 2

schacDateOfBirth

Name	**schacDateOfBirth**
Description	The date of birth for the subject it is associated with
OID	1.3.6.1.4.1.25178.1.2.3
Format	Numeric value YYYYMMDD, using 4 digits for year, 2 digits for month and 2 digits for day as described in RFC 3339 'Date and Time on the Internet: Timestamps' as reference using the 'full-date' format from paragraph 5.6 but without the dashes.
Number of values	Single
References	RFC 2985 - PKCS #9: Selected Object Classes and Attribute Types Version 2.0.Sections 5.2.4, B.3.8 RFC 3339 - Date and Time on the Internet: Timestamps.'Date and Time on the Internet: Timestamps' as reference using the 'full-date' format from paragraph 5.6 but without the dashes ISO 8601 - Data elements and interchange formats - Information interchange - Representation of dates and times

RFC 4517 definition	`( schacAttributeType:3`
	`NAME 'schacDateOfBirth'`
	`DESC 'Date of birth (format YYYYMMDD, only numeric chars)'`
	`EQUALITY numericStringMatch`
	`ORDERING numericStringOrderingMatch`
	`SUBSTR numericStringSubstringsMatch`
	`SINGLE-VALUE`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.36 )`

Examples	schacDateOfBirth = 19660412

schacYearOfBirth

Name	**schacYearOfBirth**
Description	The year of birth for the subject it is associated with
OID	1.3.6.1.4.1.25178.1.0.2.3
Format	Numeric value YYYY, using 4 digits for the year, as described in RFC 3339 'Date and Time on the Internet: Timestamps' as reference using the 'full-date' format from paragraph 5.6 but without the dashes.
Number of values	Single
References	RFC 2985 - PKCS #9: Selected Object Classes and Attribute Types Version 2.0.Sections 5.2.4, B.3.8 RFC 3339 - Date and Time on the Internet: Timestamps.'Date and Time on the Internet: Timestamps' as reference using the 'full-date' format from paragraph 5.6 but without the dashes ISO 8601 - Data elements and interchange formats - Information interchange - Representation of dates and times

RFC 4517 definition	`( schacExpAttr:3`
	`NAME 'schacYearOfBirth'`
	`DESC 'Date of birth (format YYYY, only numeric chars)'`
	`EQUALITY numericStringMatch`
	`ORDERING numericStringOrderingMatch`
	`SUBSTR numericStringSubstringsMatch`
	`SINGLE-VALUE`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.36 )`

Examples	schacYearOfBirth = 1966

schacPlaceOfBirth

Name	**schacPlaceOfBirth**
Description	The schacPlaceOfBirth attribute specifies the place of birth for the subject it is associated with.
OID	1.3.6.1.4.1.25178.1.2.4
Format	Free format string
Number of values	Single
References	RFC 2985 - PKCS #9: Selected Object Classes and Attribute Types Version 2.0.Sections 5.2.5, B.3.9

RFC 4517 definition	`( schacAttributeType:4`
	` NAME 'schacPlaceOfBirth'`
	` DESC 'Birth place of a person'`
	` EQUALITY caseIgnoreMatch`
	` ORDERING caseIgnoreOrderingMatch`
	` SUBSTR caseIgnoreSubstringsMatch`
	` SINGLE-VALUE`
	` SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )`

Examples	schacPlaceOfBirth = Algeciras, Spain

schacCountryOfCitizenship

Name	**schacCountryOfCitizenship**
Description	The schacCountryOfCitizenship attribute specifies the (claimed) countries of citizenship for the subject it is associated with.
OID	1.3.6.1.4.1.25178.1.2.5
Format	Two-letter country acronym in accordance with ISO 3166.
Number of values	Multi
References	RFC 2985 - PKCS #9: Selected Object Classes and Attribute Types Version 2.0.Sections 5.2.7, B.3.11 ISO 3166 - Codes for the representation of names of countries and their subdivisions

RFC 4517 definition	`( schacAttributeType:5`
	` NAME 'schacCountryOfCitizenship'`
	` DESC 'Country of citizenship of a person. Format two-letter acronym according to ISO 3166'`
	` EQUALITY caseIgnoreMatch`
	` SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )`

Examples	schacCountryOfCitizenship = es

schacSn1

Name	schacSn1
Description	First surname of a person ("the surname" in international terms). schacSn1 would contain whatever values the described person thinks they should contain. Splitting shall be done by humans. That means that, when filling a SCHAC-based description that allows the use of schacSn1 and schacSn2, the administrators must ask for 1st surname and 2nd surname (if applicable) as well as they do for givenName, surname, etc.
OID	1.3.6.1.4.1.25178.1.2.6
Format	Free format string
Number of values	Multi

RFC 4517 definition	`( schacAttributeType:6`
	`NAME 'schacSn1'`
	`DESC 'First surname of a person'`
	`EQUALITY caseIgnoreMatch`
	`ORDERING caseIgnoreOrderingMatch`
	`SUBSTR caseIgnoreSubstringsMatch`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )`

Examples	In Spain, if sn = Lopez de la Moraleda y de Las Altas Alcurnias and that person uses Lopez de la Moraleda as the first component of the surname we can write: schacSn1 = Lopez de la Moraleda In Poland, if sn = Gorecka-Wolniewicz and we decide to use the national convention for the sn attribute, we can write: schacSn1 = Wolniewicz

schacSn2

Name	schacSn2
Description	Second surname of a person (how this is assigned is a local matter). schacSn2 would contain whatever values the described person thinks they should contain. Splitting shall be done by humans. That means that, when filling a SCHAC-based description that allows the use of schacSn1 and schacSn2, the administrators must ask for 1st surname and 2nd surname (if applicable) as well as they do for givenName, surname, etc.
OID	1.3.6.1.4.1.25178.1.2.7
Format	Free format string
Number of values	Multi

RFC 4517 definition	`( schacAttributeType:7`
	`NAME 'schacSn2'`
	`DESC 'Second surname of a person'`
	`EQUALITY caseIgnoreMatch`
	`ORDERING caseIgnoreOrderingMatch`
	`SUBSTR caseIgnoreSubstringsMatch`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )`

Examples	In Spain, if sn = Lopez de la Moraleda y de Las Altas Alcurnias and that person uses de Las Altas Alcurnias as the second component of the surname we can write: schacSn2 = de Las Altas Alcurnias In Poland, if sn = Gorecka-Wolniewicz and we decide to use the national convention for the sn attribute, we can write: schacSn2 = Gorecka

schacPersonalTitle

Name	schacPersonalTitle
Description	The Personal Title attribute type specifies a personal title or salutation for a person. Examples of personal titles are "Ms", "Dr", "Prof", "Rev", “Sr”.
OID	1.3.6.1.4.1.25178.1.2.8
Format	Free format string
Number of values	Single
References	RFC 1274 - The COSINE and Internet X.500 Schema, Sections 9.3.30

RFC 4517 definition	`( schacAttributeType:8`
	`NAME 'schacPersonalTitle'`
	`DESC 'RFC1274: personal title'`
	`EQUALITY caseIgnoreMatch`
	`SUBSTR caseIgnoreSubstringsMatch`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )`

Examples	schacPersonalTitle = Prof

Contact / Location Information

Higher education’s established history of openness and collaboration gives rise to the use of institutional directories as a primary means of locating and contacting potential collaborators and other persons-of-interest at peer institutions.

schacHomeOrganization

Name	schacHomeOrganization
Description	Specifies a person´s home organization using the domain name of the organization. Issuers of schacHomeOrganization attribute values via SAML are strongly encouraged to publish matching shibmd:Scope elements as part of their IDP's SAML metadata. Relaying Parties recieving schacHomeOrganization values via SAML are strongly encouraged to check attribute values against the Issuer's published shibmd:Scope elements in SAML metadata, and may discard any non-matching values.
OID	1.3.6.1.4.1.25178.1.2.9
Format	Domain name according to RFC 1035
Number of values	Single
References	RFC 1035 - Domain names - implementation and specification ShibMetaExt 1.0: https://wiki.shibboleth.net/confluence/display/SC/ShibMetaExt+V1.0

RFC 4517 definition	`( schacAttributeType:9`
	`NAME 'schacHomeOrganization'`
	`DESC 'Domain name of the home organization'`
	`EQUALITY caseIgnoreMatch`
	`SUBSTR caseIgnoreSubstringsMatch`
	`SINGLE-VALUE`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )`

Examples	schacHomeOrganization = tut.fi

schacHomeOrganizationType

Name	**schacHomeOrganizationType**
Description	Type of a Home Organization
OID	1.3.6.1.4.1.25178.1.2.10
Format	**urn:schac:homeOrganizationType:<country-code>:<string>** The <country-code> must be a valid two-letter ISO 3166 country code identifier or the string "int", and assigned by the SCHAC URN Registry for this attribute at https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry <string> from a nationally controlled vocabulary, published through the URI identified at the above mentioned TERENA URN registry.
Number of values	Multi
References	RFC 2141 - URN Syntax ISO 3166 - Codes for the representation of names of countries and their subdivisions SCHAC URN Registry: https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry

RFC 4517 definition	`( schacAttributeType:10`
	`NAME 'schacHomeOrganizationType'`
	`DESC 'Type of the home organization'`
	`EQUALITY caseIgnoreMatch`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )`

Examples	Common values: urn:schac:homeOrganizationType:eu:higherEducationalInstitution urn:schac:homeOrganizationType:eu:educationalInstitution urn:schac:homeOrganizationType:int:NREN urn:schac:homeOrganizationType:int:universityHospital urn:schac:homeOrganizationType:int:NRENAffiliate urn:schac:homeOrganizationType:int:other National extensions: urn:schac:homeOrganizationType:ch:vho urn:schac:homeOrganizationType:es:opi

schacCountryOfResidence

Name	**schacCountryOfResidence**
Description	The schacCountryOfResidence attribute specifies the (claimed) country of residence for the subject is associated with.
OID	1.3.6.1.4.1.25178.1.2.11
Format	Two-letter country acronym in accordance with ISO 3166 country code identifier.
Number of values	Multi
References	RFC 2985 - PKCS #9: Selected Object Classes and Attribute Types Version 2.0.Sections 5.2.8, B.3.12 ISO 3166 - Codes for the representation of names of countries and their subdivisions

RFC 4517 definition	`( schacAttributeType:11`
	`NAME 'schacCountryOfResidence'`
	`DESC 'Country of residence of a person. Format two-letter acronym according to ISO 3166'`
	`EQUALITY caseIgnoreMatch`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )`

Examples	schacCountryOfResidence = es

schacUserPresenceID

Name	schacUserPresenceID
Description	To store a set of values related to network presence protocols
OID	1.3.6.1.4.1.25178.1.2.12
Format	URI
Number of values	Multi
References	RFC 2396 - Uniform Resource Identifiers (URI): Generic Syntax RFC 3508 - H.323 URL Schema RFC 3261 - SIP: Session Initiation Protocol RFC 5122 - IRIs and URIs for XMPP

RFC 4517 definition	`( schacAttributeType:12`
	`NAME 'schacUserPresenceID'`
	`DESC 'Used to store a set of values related to the network presence'`
	`EQUALITY caseExactMatch`
	`SUBSTR caseExactSubstringsMatch`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )`

Examples	schacUserPresenceID = xmpp:pepe@im.univx.es schacUserPresenceID = sip:pepe@myweb.com schacUserPresenceID = sip:+34-95-505-6600@univx.es;transport=TCP;user=phone schacUserPresenceID = sips:alice@atlanta.com?subject=project%20x&priority=urgent schacUserPresenceID = h323:pepe@myweb.fi:808;params

Student Information

Student information includes attributes that have relevance to the student role, such as curriculum, major, and degree.
No attributes defined

Employee Information

Employee information includes attributes that have relevance to the employee role, such as position, office hours, and job title

schacPersonalPosition

Name	**schacPersonalPosition**
Description	The Personal Position attribute type specifies a personal position inside an institution.
OID	1.3.6.1.4.1.25178.1.2.13
Format	**urn:schac:personalPosition:<country-code>:<domain>:<iNSS>** The <country-code> must be a valid two-letter ISO 3166 country code identifier or the string “int”, and assigned by the SCHAC URN Registry for this attribute at https://wiki.refeds.org/display/STAN/SCHAC+Registry <domain> is the institution domain name according to RFC 1035 <iNSS> is a Namespace Specific String as defined in RFC 2141 but case insenstitive. Valid components for it are those specified (or explicitly delegated) by the SCHAC URN Registry for this attribute at https://wiki.refeds.org/display/STAN/SCHAC+Registry
Number of values	Multi

RFC 4517 definition	`( schacAttributeType:13`
	`NAME 'schacPersonalPosition'`
	`DESC 'Position inside an institution'`
	`EQUALITY caseIgnoreMatch`
	`SUBSTR caseIgnoreSubstringsMatch`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )`

References	RFC 1035 - Domain names - implementation and specification RFC 2141 - URN Syntax SCHAC URN Registry: https://wiki.refeds.org/display/STAN/SCHAC+Registry RFC 2256 - A Summary of the X.500(96) User Schema for use with LDAPv3. Section: 5.13 title This attribute contains the title, such as "Vice President", of a person in their organizational context. The "personalTitle" attribute would be used for a person's title independent of their job function.
Examples	National extensions: urn:schac:personalPosition:pl:umk.pl:programmer

Linkage Identifiers / Foreign Keys

Linkage attributes are those identifiers used to link a directory entry with records in external data stores or other directory entries. The use of linkage identifiers can obviate the need to synchronize data elements between systems of record and the enterprise directory. Linkage attributes are also used in the implementation of metadirectory services.

schacPersonalUniqueCode

Name	**schacPersonalUniqueCode**
Description	Specifies a “unique code” for the subject it is associated with. Its value does not necessarily correspond to any identifier outside the scope of the directories using this schema. This might be Student number, Employee number,...
OID	1.3.6.1.4.1.25178.1.2.14
Format	**urn:schac:personalUniqueCode:<country-code>:<iNSS>** The <country-code> must be a valid two-letter ISO 3166 country code identifier or the string “int”, and assigned by the SCHAC URN Registry for this attribute at https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry <iNSS> is a Namespace Specific String as defined in RFC 2141 but case insensitive, from a nationally controlled vocabulary, published through the URI identified at the above mentioned SCHAC URN registry.
Number of values	Multi
References	RFC 2141 - URN Syntax ISO 3166 - Codes for the representation of names of countries and their subdivisions SCHAC URN Registry: https://wiki.refeds.org/display/STAN/SCHAC+Registry

RFC 4517 definition	`( schacAttributeType:14`
	`NAME 'schacPersonalUniqueCode'`
	`DESC 'Unique code for the subject'`
	`EQUALITY caseIgnoreMatch`
	`ORDERING caseIgnoreOrderingMatch`
	`SUBSTR caseIgnoreSubstringsMatch`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )`

Examples	Common values: urn:schac:personalUniqueCode:int:studentID:<country-code>:<code> National extensions: urn:schac:personalUniqueCode:fi:tut.fi:hetu:010161-995A urn:schac:personalUniqueCode:es:uma:estudiante:a3b123c12 urn:schac:personalUniqueCode:se:LIN:87654321

schacPersonalUniqueID

Name	**schacPersonalUniqueID**
Description	Specifies a "legal unique identifier" for the subject it is associated with. This might be DNI in Spain, FIC in Finland, NIN in Sweden,...
OID	1.3.6.1.4.1.25178.1.2.15
Format	**urn:schac:personalUniqueID:<country-code>:<idType>:<idValue>** The <country-code> must be a valid two-letter ISO 3166 country code identifier or the string “int”, and assigned by the SCHAC URN Registry for this attribute at https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry <idType>. Acceptable values must be declared per each country code through the URI identified at the above mentioned SCHAC URN registry. <idValue>
Number of values	Multi
References	RFC 2141 - URN Syntax ISO 3166 - Codes for the representation of names of countries and their subdivisions SCHAC URN Registry: https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry

RFC 4517 definition	`( schacAttributeType:15`
	`NAME 'schacPersonalUniqueID'`
	`DESC 'Unique code for the subject'`
	`EQUALITY caseExactMatch`
	`ORDERING caseExactOrderingMatch`
	`SUBSTR caseExactSubstringsMatch`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )`

Examples	National extensions urn:schac:personalUniqueID:fi:FIC:260667-123F urn:schac:personalUniqueID:es:DNI:31241312L urn:schac:personalUniqueID:se:NIN:197104058289

Entry Metadata / Administration Information

Entry metadata attributes are used to contain information about the entry itself, often its status, birth, and death. Such attributes can be critical to metadirectory processing. While the object classes discussed here were designed to accommodate person entries, metadata attributes can also be useful with non-person entry types such as groups. In such cases the metadata attributes may be best defined in an auxiliary object class independent of the person object class.

schacExpiryDate

Name	**schacExpiryDate**
Description	The date from which the set of data is to be considered invalid (specifically, in what refers to rights and entitlements). This date applies to the entry as a whole.
OID	1.3.6.1.4.1.25178.1.2.17
Format	Values must be expressed in UTC and must include seconds (i.e., times are YYYYMMDDhhmmssZ), even where the number of seconds is zero. GeneralizedTime values must not include fractional seconds.
Number of values	Single
References	RFC 2630 - Cryptographic Message Syntax. Section 11.3 RFC 2985 - PKCS #9: Selected Object Classes and Attribute Types Version 2.0.Sections 5.2.4, B.3.8 RFC 3339 - Date and Time on the Internet: Timestamps.'Date and Time on the Internet: Timestamps' as reference using the 'full-date' format from paragraph 5.6 but without the dashes ISO 8601 - Data elements and interchange formats - Information interchange - Representation of dates and times

RFC 4517 definition	`( schacAttributeType:17`
	`NAME 'schacExpiryDate'`
	`DESC 'Date from which the set of data is to be considered invalid (format YYYYMMDDhhmmssZ)'`
	`EQUALITY generalizedTimeMatch`
	`ORDERING generalizedTimeOrderingMatch`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.24 )`

Examples	schacExpiryDate = 20051231125959Z

Confidentiality / Attribute Release (Visibility)

Confidentiality attributes are commonly used to indicate whether an entry is visible publicly, visible only to affiliates of the institution, or not visible at all. In some cases only specific attributes, such as phone, address, and email address, are restricted, in other cases all attributes are restricted.

schacUserPrivateAttribute

Name	**schacUserPrivateAttribute**
Description	Used to model privacy requirements, as expressed by the user and/or organizational policies. The values are intended to be attribute type names and applies to the attribute and any subtypes of it for a given entity. In what respects to data exchange, it applies to the expression of privacy requirements. This attribute can also have specific operational semantics (one has already been applied to LDAP servers: see references below), that will be defined in a separate document.
OID	1.3.6.1.4.1.25178.1.2.18
Format	An attribute type identifier. Operational semantics may imply specific values as wildcards.
Number of values	Multi
References	http://www.rediris.es/ldap/schema/iris/irisUserPrivateAttribute/

RFC 4517 definition	`( schacAttributeType:18`
	`NAME 'schacUserPrivateAttribute'`
	`DESC 'Set of denied access attributes'`
	`EQUALITY caseIgnoreIA5Match`
	`SUBSTR caseIgnoreIA5SubstringsMatch`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )`

Examples	Attributes mail and telephoneNumber are considered private: schacUserPrivateAttribute = mail schacUserPrivateAttribute = telephoneNumber

Authorization, Entitlements

Authorization for services is generally implemented in LDAP directories either through the use of entry attributes or group memberships. (For information regarding LDAP groups please see the MACE Best Practices for Directory Groups document at <http://web.archive.org/web/20111204210114/http://middleware.internet2.edu/dir/groups/>).
Applications such as Shibboleth (see <https://shibboleth.net>) can make use of entitlement attributes in an entry to provide authorization information to requesting services.

schacUserStatus

Name	**schacUserStatus**
Description	Used to store a set of status of a person as user of services
OID	1.3.6.1.4.1.25178.1.2.19
Format	**urn:schac:userStatus:<country-code>:<domain>:<iNSS>** The <country-code> must be a valid two-letter ISO 3166 country code identifier or the string “int”, and assigned by the SCHAC URN Registry for this attribute at https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry <domain> is the institution domain name according to RFC 1035 <iNSS> is a Namespace Specific String as defined in RFC 2141 but case insensitive
Number of values	Multi
References	RFC 1035 - Domain names - implementation and specification RFC 2141 - URN Syntax

RFC 4517 definition	`( schacAttributeType:19`
	`NAME 'schacUserStatus'`
	`DESC 'Used to store a set of status of a person as user of services'`
	`EQUALITY caseIgnoreMatch`
	`SUBSTR caseIgnoreSubstringsMatch`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )`

Examples	To store different user activity states at University of Málaga (uma.es): urn:schac:userStatus:es:uma.es:affiliation:expired urn:schac:userStatus:es:uma.es:sendMail:expired urn:schac:userStatus:es:uma.es:getMail:active A parameter in the URN can be used to represent the temporal validity of the statement. urn:schac:userStatus:si:ujl.si:webmail:active+ttl=20060531235959

Group-related Attributes

Directory groups are often used to provide authorization to entries and attributes, as well as to restrict or provide access to services. There are benefits to having group memberships described in members' entries as well as in a group entry. Because not all directory servers provide this functionality (Microsoft Active Directory and Novell eDirectory do) local attributes are often defined to meet organizational needs. For a complete treatment of issues concerning LDAP groups please see the MACE Best Practices for Directory Groups document at http://middleware.internet2.edu/dir/groups

schacProjectMembership

Name	**schacProjectMembership**
Description	The name of the project the user belongs to
OID	1.3.6.1.4.1.25178.1.2.20
Format	**<project-name>** The <project-name> must be a name assigned by the SCHAC URN Registry for this attribute at https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry
Number of values	Multi

RFC 4517 definition	`( schacAttributeType:20`
	`NAME 'schacProjectMembership'`
	`DESC 'Name of the project'`
	`EQUALITY caseIgnoreMatch`
	`SUBSTR caseIgnoreSubstringsMatch`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )`

Examples	schacProjectMembership = perfsonar

schacProjectSpecificRole

Name	**schacProjectSpecificRole**
Description	Used to store a set of roles inside specific projects
OID	1.3.6.1.4.1.25178.1.2.21
Format	**urn:schac:projectSpecificRole:<project-name>:<iNSS>** The <project-name> must be a name assigned by the SCHAC URN Registry for this attribute at https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry <iNSS> is a Namespace Specific String as defined in RFC 2141 but case insensitive
Number of values	Multi
References	RFC 2141 - URN Syntax

RFC 4517 definition	`( schacAttributeType:21`
	`NAME 'schacProjectSpecificRole'`
	`DESC 'Used to store a set of roles of a person inside a project'`
	`EQUALITY caseIgnoreMatch`
	`SUBSTR caseIgnoreSubstringsMatch`
	`SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )`

Examples	schacProjectSpecificRole = urn:schac:projectSpecificRole:perfsonar:developer

Appendix A: SCHAC LDAP Schema

Definitions of the object classes and attribute types specified in this document have been done in accordance with RFC 4517, in an attempt to ease integration with LDAP-accessible Directory systems. Lines have been folded in some cases to improve readability.

The latest version of the SCHAC LDAP Schema is available at:
https://wiki.refeds.org/display/STAN/SCHAC+Releases

Object identifiers

```
objectIdentifier TERENA 1.3.6.1.4.1.25178

 objectIdentifier schac TERENA:1
 objectIdentifier schacExperimental schac:0
 objectIdentifier schacObjectClass schac:1
 objectIdentifier schacAttributeType schac:2
 objectIdentifier schacExpObjClass schacExperimental:1
 objectIdentifier schacExpAttr schacExperimental:2
```

Object classes

schacPersonalCharacteristics

```
(
    schacObjectClass:1
    NAME 'schacPersonalCharacteristics'
    DESC 'Personal characteristics describe individual person represented by the entry'
    AUXILIARY
    MAY (
       schacMotherTongue $ schacGender $ schacDateOfBirth $ schacPlaceOfBirth $
       schacCountryOfCitizenship $ schacSn1 $ schacSn2 $ schacPersonalTitle
    )
 )
```

schacContactLocation

```
(
    schacObjectClass:2
    NAME 'schacContactLocation'
    DESC 'Primary means of locating and contacting potential collaborators
       and other persons-of-interest at peer institutions'
    AUXILIARY
    MAY (
       schacHomeOrganization $ schacHomeOrganizationType $
       schacCountryOfResidence $ schacUserPresenceID
    )
 )
```

schacEmployeeInfo

```
(    schacObjectClass:3
     NAME 'schacEmployeeInfo'
     DESC 'Employee information includes attributes that have relevance to the employee
        role, such as position, office hours, and job title'
     AUXILIARY
     MAY ( schacPersonalPosition )
 )
```

schacLinkageIdentifiers

```
(
     schacObjectClass:4
     NAME 'schacLinkageIdentifiers'
     DESC 'Used to link a directory entry with records in external
        data stores or other directory entries'
     AUXILIARY
     MAY (
        schacPersonalUniqueCode $ schacPersonalUniqueID
     )
 )
```

schacEntryMetadata

```
(
     schacObjectClass:5
     NAME 'schacEntryMetadata'
     DESC 'Used to contain information about the entry itself, often
        its status, birth, and death'
     AUXILIARY
     MAY (
        schacExpiryDate
     )
 )
```

schacEntryConfidentiality

```
(
     schacObjectClass:6
     NAME 'schacEntryConfidentiality'
     DESC 'Used to indicate whether an entry is visible publicly, visible only to
        affiliates of the institution, or not visible at all'
     AUXILIARY
     MAY (
        schacUserPrivateAttribute
     )
 )
```

schacUserEntitlements

```
(
     schacObjectClass:7
     NAME 'schacUserEntitlements'
     DESC 'Authorization for services'
     AUXILIARY
     MAY (
     schacUserStatus
     )
 )
```

schacGroupMembership

```
(
    schacObjectClass:8
    NAME 'schacGroupMembership'
    DESC 'Groups used to provide/restrict authorization to entries and attributes'
    AUXILIARY
    MAY (
    schacProjectMembership $ schacProjectSpecificRole
    )
 )
```

Attribute types

schacMotherTongue

```
(
    schacAttributeType:1
    NAME 'schacMotherTongue'
    DESC 'RFC 3066 code for prefered language of communication'
    EQUALITY caseExactMatch
    SINGLE-VALUE
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 )
```

schacGender

```
(
    schacAttributeType:2
    NAME 'schacGender'
    DESC 'Representation of human sex (see ISO 5218)'
    EQUALITY integerMatch
    SINGLE-VALUE
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
 )
```

schacDateOfBirth

```
(
    schacAttributeType:3
    NAME 'schacDateOfBirth'
    DESC 'Date of birth (format YYYYMMDD, only numeric chars)'
    EQUALITY numericStringMatch
    ORDERING numericStringOrderingMatch
    SUBSTR numericStringSubstringsMatch
    SINGLE-VALUE
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.36
 )
```

schacPlaceOfBirth

```
(
    schacAttributeType:4
    NAME 'schacPlaceOfBirth'
    DESC 'Birth place of a person'
    EQUALITY caseIgnoreMatch
    ORDERING caseIgnoreOrderingMatch
    SUBSTR caseIgnoreSubstringsMatch
    SINGLE-VALUE
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 )
```

schacCountryOfCitizenship

```
(
    schacAttributeType:5
    NAME 'schacCountryOfCitizenship'
    DESC 'Country of citizenship of a person. Format two-letter
       acronym according to ISO 3166'
    EQUALITY caseIgnoreMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 )
```

schacSn1

```
(
    schacAttributeType:6
    NAME 'schacSn1'
    DESC 'First surname of a person'
    EQUALITY caseIgnoreMatch
    ORDERING caseIgnoreOrderingMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 )
```

schacSn2

```
(
    schacAttributeType:7
    NAME 'schacSn2'
    DESC 'Second surname of a person'
    EQUALITY caseIgnoreMatch
    ORDERING caseIgnoreOrderingMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 )
```

schacPersonalTitle

```
(
    schacAttributeType:8
    NAME 'schacPersonalTitle'
    DESC 'RFC1274: personal title'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 )
```

schacHomeOrganization

```
(
    schacAttributeType:9
    NAME 'schacHomeOrganization'
    DESC 'Domain name of the home organization'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SINGLE-VALUE
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 )
```

schacHomeOrganizationType

```
(
    schacAttributeType:10
    NAME 'schacHomeOrganizationType'
    DESC 'Type of the home organization'
    EQUALITY caseIgnoreMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 )
```

schacCountryOfResidence

```
(
    schacAttributeType:11
    NAME 'schacCountryOfResidence'
    DESC 'Country of residence of a person. Format two-letter
       acronym according to ISO 3166'
    EQUALITY caseIgnoreMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 )
```

schacUserPresenceID

```
(
    schacAttributeType:12
    NAME 'schacUserPresenceID'
    DESC 'Used to store a set of values related to the network presence'
    EQUALITY caseExactMatch
    SUBSTR caseExactSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 )
```

schacPersonalPosition

```
(
    schacAttributeType:13
    NAME 'schacPersonalPosition'
    DESC 'Position inside an institution'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 )
```

schacPersonalUniqueCode

```
(
    schacAttributeType:14
    NAME 'schacPersonalUniqueCode'
    DESC 'Unique code for the subject'
    EQUALITY caseIgnoreMatch
    ORDERING caseIgnoreOrderingMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 )
```

schacPersonalUniqueID

```
(
    schacAttributeType:15
    NAME 'schacPersonalUniqueID'
    DESC 'Unique code for the subject'
    EQUALITY caseExactMatch
    ORDERING caseExactOrderingMatch
    SUBSTR caseExactSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 )
```

schacUUID

Attribute deleted after Málaga TF-EMC2 meeting.

schacExpiryDate

```
(
    schacAttributeType:17
    NAME 'schacExpiryDate'
    DESC 'Date from which the set of data is to be considered
       invalid (format YYYYMMDDhhmmssZ)'
    EQUALITY generalizedTimeMatch
    ORDERING generalizedTimeOrderingMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
 )
```

schacUserPrivateAttribute

```
(
    schacAttributeType:18
    NAME 'schacUserPrivateAttribute'
    DESC 'Set of denied access attributes'
    EQUALITY caseIgnoreIA5Match
    SUBSTR caseIgnoreIA5SubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
 )
```

schacUserStatus

```
(
    schacAttributeType:19
    NAME 'schacUserStatus'
    DESC 'Used to store a set of status of a person as user of services'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 )
```

schacProjectMembership

```
(
    schacAttributeType:20
    NAME 'schacProjectMembership'
    DESC 'Name of the project'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 )
```

schacProjectSpecificRole

```
(
    schacAttributeType:21
    NAME 'schacProjectSpecificRole'
    DESC 'Used to store a set of roles of a person inside a project'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 )
```

Experimental object class

schacExperimentalOC

```
(
    schacExpObjClass:1
    NAME 'schacExperimentalOC'
    DESC 'Experimental Object Class'
    AUXILIARY
    MAY (
       schacYearOfBirth
    )
 )
```

Experimental attribute types

schacProjectMembership
Attribute changed to official branch below schacGroupMembership object class. OID schacExpAttr:1 is obsoleted and will not be reused ever.

schacProjectSpecificRole
Attribute changed to official branch below schacGroupMembership object class. OID schacExpAttr:2 is obsoleted and will not be reused ever.

schacYearOfBirth

```
(
    schacExpAttr:3
    NAME 'schacYearOfBirth'
    DESC 'Year of birth (format YYYY, only numeric chars)'
    EQUALITY numericStringMatch
    ORDERING numericStringOrderingMatch
    SUBSTR numericStringSubstringsMatch
    SINGLE-VALUE
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.36
 )
```

Appendix B: SAML 2.x Profile

The rules defined by the SAML 2.0 X.500/LDAP attribute profile [SAML-X500] are to be applied, with the exception that the XML attribute named Encoding defined by that profile is NOT specified for use with this profile.

[SAML-X500] S.Cantor., SAML V2.0 X.500/LDAP Attribute Profile, Committee Specification 01. OASIS SSTC, March 2008. Document ID sstc-saml-attribute-x500-cs-01. See http://wiki.oasis-open.org/security/

Appendix C: List of Changes

March 31, 2015. V:1.5.0 final

- Added SAML 2.x profile (appendix B)
- Removed SAML2.0 names from tables
- Removed 'Security Attributes and Keys' (not applicable to today's security needs)

March 10, 2015. V:1.5.0 final-proposed

- added additional information to schacHomeOrganization

December 29, 2014. V:1.5.0.c

- All pointers to www.terena.org, including static registry, have been updated to point to the new wiki.refeds.org space
- Minor wording cleanup
- Removal of pointers to documents no longer online
- Clarified what RFCs are normative when a newer RFC is available than what is listed
- Added SAML 2.0 name to each table
- Adjusted overall page layout
- Fixed example in `schacPersonalUniqueId`
- Added clear URLs in introduction to aid with accessibility

September 24, 2012. V:1.5.0.b1

- Changed SCHAC URN prefix from urn:mace:terena.org:schac to urn:shac following RFC 6338
- Added sHO as a second name for schacHomeOrganization
- Added sPUC as a second name for schacPersonalUniqueCode
- Added sPUID as a second name for schacPersonaUniqueID
- Added sUPA as a second name for schacUserPrivateAttribute

June 2, 2011. V:1.4.1.b2

- Changed the example of attribute schacPersonalUniqueID from “NIF” to “DNI”.

September 16, 2010. V:1.4.1.b1

- Changed “Number of values” from single-valued to multivalued in schacHomeOrganizationType.

March 26, 2009. V:1.4.0

- Added a footnote related to "SCHAC URN Registry" and URN NID urn:schac

March 18, 2009. V:1.4.0 b4

- Links no longer underlined.
- schacYearOfBirth placed near schacDateOfBirth.
- Corrected a copy/paste error in schacYearOfBirth

March 16, 2009. V:1.4.0 b3

- Added section "About SCHAC".
- Suppression of the first paragraph in section "Normative References".
- Changed section name from "Introduction" to "Normative References".

March 13, 2009. V:1.4.0 b2

- Added schacYearOfBirth experimental attribute.
- Changed references to RFC 2252 by RFC 4517.
- Changed erroneous reference from RFC 2131 to RFC 2141 in schacProjectSpecificRole.
- Added name, location, editor and contact information.
- Added table of content with page references and alphabetical index of attributes.
- Added the date of the document to all pages.
- Made all useful URLs in the PDF clickable.

March 4, 2009. V:1.4.0 b1

- Added schacGroupMembership objectclass.
- Changed schacProjectMembership and schacProjectSpecificRole from experimental OID branch to official branch below schacGroupMembership object class.
- OIDs schacExpAttr:1 and schacExpAttr:2 are obsoleted and will not be reused ever.

September 30, 2007. V:1.3.1 b1

- Added an experimental OID branch 1.3.6.1.4.1.25178.0.
- Defined an experimental schacExpObjClass objectclass.

- Added schacProjectMembership and schacProjectSpecificRole experimental attributes.
- Changed schacHomeOrganizationType values below namespaces "eu" and "int".

December 12, 2006. V:1.3.0

- Changed references from terena.nl to terena.org.

November 25, 2006. V:1.3.0 b3

- Changed schacPersonalPosition and schacUserStatus format and samples.

October 17, 2006. V:1.3.0 b2

- Deleted schacUUID attribute.

September 28, 2006. V:1.3.0 b1

- Changed schacHomeOrganization syntax OID.
- New definition of shacUUID attribute.
- Changed “?” by “+” in schacUserStatus sample.

May 4, 2006. V: 1.2.0

- Changed schacUserPresenceID syntax from URN to URI.
- Added references to the SCHAC URN registry.
- Clarify schaExpiryDate scope.

March 27, 2006. V: 1.1.2

- Changed from urn:SCHACPREFIX string to urn:schac:
- URN reserved for SCHAC: urn:mace:terena.org:schac:

March 10, 2006. V: 1.1.1

- Added TERENA OID.
- Branch reserved for SCHAC: 1.3.6.1.4.1.25178.1

February 10, 2006. V: 1.1.0

- Added appendix with LDAP schema.

November 22, 2005. V: 1.0.0

- Added attribute's classification according to HEP categories.

September 5, 2005. V: 1.0.0 RC3
June 24, 2005. V: 1.0.0 RC2
June 1, 2005. V: 1.0.0 RC1
May 24, 2005. V: 0.2
April 25, 2005. V: 0.1
