



Attribute Definitions for Individual Data

Working Draft v: 1.4.0 - 2009-03-26

Document: schac-schema-IAD-1.4.0.pdf
Location: <http://www.terena.org/activities/tf-emc2/schacreleases.html>
Editor: Javi Masa (javier.masa@rediris.es), RedIRIS
Comments to: schac@terena.org

Table of Contents

1 About SCHAC.....	3
2 Normative References.....	3
3 Attribute Metainformation.....	3
4 Attribute Classification.....	4
5 Attributes defined by SCHAC.....	5
5.1 Personal Characteristics.....	5
5.1.1 schacMotherTonge.....	5
5.1.2 schacGender.....	5
5.1.3 schacDateOfBirth.....	6
5.1.4 schacYearOfBirth.....	6
5.1.5 schacPlaceOfBirth.....	7
5.1.6 schacCountryOfCitizenship.....	7
5.1.7 schacSn1.....	8
5.1.8 schacSn2.....	8
5.1.9 schacPersonalTitle.....	9
5.2 Contact / Location Information.....	10
5.2.1 schacHomeOrganization.....	10
5.2.2 schacHomeOrganizationType.....	10
5.2.3 schacCountryOfResidence.....	11
5.2.4 schacUserPresenceID.....	11
5.3 Student Information.....	11
5.4 Employee Information.....	12
5.4.1 schacPersonalPosition.....	12
5.5 Linkage Identifiers / Foreign Keys.....	13
5.5.1 schacPersonalUniqueCode.....	13
5.5.2 schacPersonalUniqueID.....	14
5.6 Entry Metadata / Administration Information.....	15
5.6.1 schacExpiryDate.....	15
5.7 Security Attributes and Keys.....	15
5.8 Confidentiality / Attribute Release (Visibility).....	16
5.8.1 schacUserPrivateAttribute.....	16
5.9 Authorization, Entitlements.....	17
5.9.1 schacUserStatus.....	17
5.10 Group-related Attributes.....	18
5.10.1 schacProjectMembership.....	18
5.10.2 schacProjectSpecificRole.....	18
6 Appendix.....	19
6.1 SCHAC LDAP Schema.....	19
6.1.1 Object identifiers.....	19
6.1.2 Object classes.....	19
6.1.3 Attribute types.....	21
6.1.4 Experimental object class.....	25
6.1.5 Experimental attribute types.....	25
7 List of Changes.....	26
8 Alphabetical Index of attributes.....	28

1 About SCHAC

The SCHEMA for ACademia, SCHAC, is the result of the work in the area of attributes coordination carried out within the TERENA Task Force on Middleware, TF-EMC2.

SCHAC aims to define and promote common schemas in the field of higher education to facilitate inter-institutional data exchange.

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

SCHAC documents can be found on SCHAC web page, under the section called "SCHAC Releases".

For more information about SCHAC, please refer to the SCHAC web page.

2 Normative References

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 other document.

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

- The eduPerson schema v. 200806, as defined at <http://middleware.internet2.edu/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

3 Attribute Metainformation

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
Format	The syntax for the representation of the attribute's values
# of values	<ul style="list-style-type: none"> ● 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 # of values
RFC 4517 definition	Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules
Examples	Example of values used within the attribute

4 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 and discussions with the International Schema Archives (Feb, 2004). The categories are:

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

A detailed description of these categories can found in the document: Higher-Education Person: A Comparative Analysis of Collaborative Public LDAP Person Object Classes in Higher-Education <draft-internet2-mace-dir-higher-ed-person-analysis-06.htm>, <<http://middleware.internet2.edu/dir/docs/draft-internet2-mace-dir-higher-ed-person-analysis-latest.htm>>

5 Attributes defined by SCHAC

5.1 Personal Characteristics

Personal characteristics describe the individual person represented by the entry.

5.1.1 schacMotherTonge

Name	schacMotherTonge
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.
Format	See RFC 3066 Tags for the Identification of Languages
# of values	Single
References	<ul style="list-style-type: none"> ● 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 'schacMotherTonge' DESC 'RFC 3066 code for preferred language of communication' EQUALITY caseExactMatch SINGLE-VALUE SYNTAX 1.3.6.1.4.1.1466.115.121.1.15)
Examples	<ul style="list-style-type: none"> ● schacMotherTonge = fr ● schacMotherTonge = es-ES

5.1.2 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)
Format	<ul style="list-style-type: none"> ● 0 Not known ● 1 Male ● 2 Female ● 9 Not specified
# of values	Single
References	<ul style="list-style-type: none"> ● RFC 2985 – PKCS #9: Selected Object Classes and Attribute Types Version 2.0. Sections 5.2.6, B.3.10 ● 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 integerMatch SINGLE-VALUE SYNTAX 1.3.6.1.4.1.1466.115.121.1.27)
Examples	<ul style="list-style-type: none"> ● schacGender = 2

5.1.3 schacDateOfBirth

Name	schacDateOfBirth
Description	The date of birth for the subject it is associated with
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.
# of values	Single
References	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● schacDateOfBirth = 19660412

5.1.4 schacYearOfBirth

Name	schacYearOfBirth
Description	The year of birth for the subject it is associated with
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.
# of values	Single
References	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● schacYearOfBirth = 1966

5.1.5 schacPlaceOfBirth

Name	schacPlaceOfBirth
Description	The schacPlaceOfBirth attribute specifies the place of birth for the subject it is associated with.
Format	Free string
# of values	Single
References	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● schacPlaceOfBirth = Algeciras, Spain

5.1.6 schacCountryOfCitizenship

Name	schacCountryOfCitizenship
Description	The schacCountryOfCitizenship attribute specifies the (claimed) countries of citizenship for the subject it is associated with.
Format	Two-letter country acronym in accordance with ISO 3166.
# of values	Multi
References	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● schacCountryOfCitizenship = es

5.1.7 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.
Format	Free string
# 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	<ul style="list-style-type: none"> ● In Spain, if sn = Lopez de la Moraleda y de Las Altas Alcornias 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

5.1.8 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.
Format	Free string
# 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	<ul style="list-style-type: none"> ● In Spain, if sn = Lopez de la Moraleda y de Las Altas Alcornias and that person uses de Las Altas Alcornias as the second component of the surname we can write: schacSn2 = de Las Altas Alcornias ● In Poland, if sn = Gorecka-Wolniewicz and we decide to use the national convention for the sn attribute, we can write: schacSn2 = Gorecka

5.1.9 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".
Format	Free format string
# of values	Single
References	<ul style="list-style-type: none"> ● RFC 1274 - The COSINE and Internet X.500 Schema personal title 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	<ul style="list-style-type: none"> ● schacPersonalTitle = Prof

5.2 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.

5.2.1 schacHomeOrganization

Name	schacHomeOrganization
Description	Specifies a person's home organization using the domain name of the organization
Format	Domain name according to RFC 1035
# of values	Single
References	<ul style="list-style-type: none"> ● RFC 1035 – Domain names – implementation and specification
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	<ul style="list-style-type: none"> ● schacHomeOrganization = tut.fi

5.2.2 schacHomeOrganizationType

Name	schacHomeOrganizationType
Description	Type of a Home Organization
Format	urn:mace:terena.org:schac:homeOrganizationType:<country-code>:<string> <ul style="list-style-type: none"> ● The <country-code> must be a valid two-letter ISO 3166 country code identifier or the string "int", and assigned by the TERENA URN Registry* for this attribute at http://www.terena.org/registry/terena.org/schac/homeOrganizationType/ ● <string> from a nationally controlled vocabulary, published through the URI identified at the above mentioned TERENA URN registry.
# of values	Single
References	<ul style="list-style-type: none"> ● RFC 2141 – URN Syntax ● ISO 3166 – Codes for the representation of names of countries and their subdivisions ● TERENA URN Registry: http://www.terena.org/registry/terena.org/
RFC 4517 definition	(schacAttributeType:10 NAME 'schacHomeOrganizationType' DESC 'Type of the home organization' EQUALITY caseIgnoreMatch SINGLE-VALUE SYNTAX 1.3.6.1.4.1.1466.115.121.1.15)
Examples	Common values: <ul style="list-style-type: none"> ● urn:mace:terena.org:schac:homeOrganizationType:eu:higherEducationallInstitution ● urn:mace:terena.org:schac:homeOrganizationType:eu:educationallInstitution ● urn:mace:terena.org:schac:homeOrganizationType:int:NREN ● urn:mace:terena.org:schac:homeOrganizationType:int:universityHospital ● urn:mace:terena.org:schac:homeOrganizationType:int:NRENAffiliate ● urn:mace:terena.org:schac:homeOrganizationType:int:other National extensions: <ul style="list-style-type: none"> ● urn:mace:terena.org:schac:homeOrganizationType:ch:vho ● urn:mace:terena.org:schac:homeOrganizationType:es:opi

* The SCHAC community has applied for a URN NID (urn:schac) to the IETF recently. Once it is approved the URN based attribute values will be able to use the new prefix and the registry and values shall be updated accordingly.

5.2.3 schacCountryOfResidence

Name	schacCountryOfResidence
Description	The schacCountryOfResidence attribute specifies the (claimed) country of residence for the subject is associated with.
Format	Two-letter country acronym in accordance with ISO 3166 country code identifier.
# of values	Multi
References	<ul style="list-style-type: none"> ● 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 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	<ul style="list-style-type: none"> ● schacCountryOfResidence = es

5.2.4 schacUserPresenceID

Name	schacUserPresenceID
Description	To store a set of values related to network presence protocols
Format	URI
# of values	Multi
References	<ul style="list-style-type: none"> ● RFC 2396 – Uniform Resource Identifiers (URI): Generic Syntax ● RFC 3508 – H.323 URL Schema ● RFC 3261 – SIP: Session Initiation Protocol
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	<ul style="list-style-type: none"> ● 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 ● schacUserPresenceID = skype:pepe.perez

5.3 Student Information

Student information includes attributes that have relevance to the student role, such as curriculum, major, and degree.

No attributes defined

5.4 Employee Information

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

5.4.1 schacPersonalPosition

Name	schacPersonalPosition
Description	The Personal Position attribute type specifies a personal position inside an institution.
Format	<p>urn:mace:terena.org:schac:personalPosition:<country-code>:<domain>:<iNSS></p> <ul style="list-style-type: none"> ● The <country-code> must be a valid two-letter ISO 3166 country code identifier or the string "int", and assigned by the TERENA URN Registry for this attribute at http://www.terena.org/registry/terena.org/schac/personalPosition/ ● <domain> is the institution domain name according to RFC 1035 ● <iNSS> is a Namespace Specific String as defined in RFC 2141 but case insensitive. Valid components for it are those specified (or explicitly delegated) by the TERENA URN Registry for this attribute at http://www.terena.org/registry/terena.org/schac/personalPosition/
# 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	<ul style="list-style-type: none"> ● RFC 1035 – Domain names – implementation and specification ● RFC 2141 – URN Syntax ● TERENA URN Registry: http://www.terena.org/registry/terena.org/ ● 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	<p>National extensions:</p> <ul style="list-style-type: none"> ● urn:mace:terena.org:schac:personalPosition:pl:umk.pl:programmer

5.5 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.

5.5.1 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,...
Format	urn:mace:terena.org:schac:personalUniqueCode:<country-code>:<iNSS> <ul style="list-style-type: none"> ● The <country-code> must be a valid two-letter ISO 3166 country code identifier or the string "int", and assigned by the TERENA URN Registry for this attribute at http://www.terena.org/registry/terena.org/schac/personalUniqueCode/ ● <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 TERENA URN registry.
# of values	Multi
References	<ul style="list-style-type: none"> ● RFC 2141 – URN Syntax ● ISO 3166 – Codes for the representation of names of countries and their subdivisions ● TERENA URN Registry: http://www.terena.org/registry/terena.org/ ● HEP rev 06 – Nov 21, 2005 (6.5.2 Student System Identification Code) http://middleware.internet2.edu/dir/docs/draft-internet2-mace-dir-higher-ed-person-analysis-latest.htm
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: <ul style="list-style-type: none"> ● urn:mace:terena.org:schac:personalUniqueCode:int:studentID:<country-code>:<code> National extensions: <ul style="list-style-type: none"> ● urn:mace:terena.org:schac:personalUniqueCode:fi:tut.fi:hetu:010161-995A ● urn:mace:terena.org:schac:personalUniqueCode:es:uma:estudiante:a3b123c12 ● urn:mace:terena.org:schac:personalUniqueCode:se:LIN:87654321

5.5.2 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,...
Format	<p>urn:mace:terena.org:schac:personalUniqueID:<country-code>:<idType>:<idValue></p> <ul style="list-style-type: none"> ● The <country-code> must be a valid two-letter ISO 3166 country code identifier or the string "int", and assigned by the TERENA URN Registry for this attribute at http://www.terena.org/registry/terena.org/schac/personalUniqueID/ ● <idType>. Acceptable values must be declared per each country code through the URI identified at the above mentioned TERENA URN registry. ● <idValue>
# of values	Multi
References	<ul style="list-style-type: none"> ● RFC 2141 – URN Syntax ● ISO 3166 – Codes for the representation of names of countries and their subdivisions ● TERENA URN Registry: http://www.terena.org/registry/terena.org/
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	<p>National extensions</p> <ul style="list-style-type: none"> ● urn:mace:terena.org:schac:personalUniqueID:fi:FIC:260667-123F ● urn:mace:terena.org:schac:personalUniqueID:es:NIF:31241312L ● urn:mace:terena.org:schac:personalUniqueID:se:NIN:12345678

5.6 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.

5.6.1 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.
Format	Values MUST be expressed Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDhhmmssZ), even where the number of seconds is zero. GeneralizedTime values MUST NOT include fractional seconds.
# of values	Single
References	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● schacExpiryDate = 20051231125959Z

5.7 Security Attributes and Keys

Security attributes are used to assist in authentication-related activities such as password self-reset. Security attributes that contain sensitive data such as passwords should be carefully protected, highly restricted, and probably encrypted using a one-way hash algorithm such as MD5 or SHA1 so that in the event that the directory server is compromised in an attack the attribute values are not useful to an attacker.

No attributes defined.

5.8 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.

5.8.1 schacUserPrivateAttribute

Name	schacUserPrivateAttribute
Description	Used to model privacy requirements, as expressed by the user and/or the 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.
Format	An attribute type identifier. Operational semantics may imply specific values as wildcards.
# of values	Multi
References	<ul style="list-style-type: none"> ● http://www.rediris.es/ldap/doc/irisUserPrivateAttribute/tnc2005-irisUserPrivateAttribute.pdf ● 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	<ul style="list-style-type: none"> ● Attributes mail and telephoneNumber are considered private schacUserPrivateAttribute = mail schacUserPrivateAttribute = telephoneNumber

5.9 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://middleware.internet2.edu/dir/groups>>).

Applications such as Shibboleth (see <<http://shibboleth.internet2.edu>>) can make use of entitlement attributes in an entry to provide authorization information to requesting services.

5.9.1 schacUserStatus

Name	schacUserStatus
Description	Used to store a set of status of a person as user of services
Format	<p>urn:mace:terena.org:schac:userStatus:<country-code>:<domain>:<iNSS></p> <ul style="list-style-type: none"> ● The <country-code> must be a valid two-letter ISO 3166 country code identifier or the string "int", and assigned by the TERENA URN Registry for this attribute at http://www.terena.org/registry/terena.org/schac/userStatus/ ● <domain> is the institution domain name according to RFC 1035 ● <iNSS> is a Namespace Specific String as defined in RFC 2141 but case insensitive
# of values	Multi
References	<ul style="list-style-type: none"> ● 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	<p>To store different user activity states at University of Málaga (uma.es):</p> <ul style="list-style-type: none"> ● urn:mace:terena.org:schac:userStatus:es:uma.es:affiliation:expired ● urn:mace:terena.org:schac:userStatus:es:uma.es:sendMail:expired ● urn:mace:terena.org:schac:userStatus:es:uma.es:getMail:active <p>A parameter in the URN can be used to represent the temporal validity of the statement.</p> <ul style="list-style-type: none"> ● urn:mace:terena.org:schac:userStatus:si:ujl.si:webmail:active+ttl=20060531235959

5.10 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>

5.10.1 schacProjectMembership

Name	schacProjectMembership
Description	The name of the project the user belongs to
Format	<p><project-name></p> <ul style="list-style-type: none"> The <project-name> must be a name assigned by the TERENA URN Registry for this attribute at http://www.terena.org/registry/terena.org/schac/projectSpecificRole/
# 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	<ul style="list-style-type: none"> schacProjectMembership = perfsonar

5.10.2 schacProjectSpecificRole

Name	schacProjectSpecificRole
Description	Used to store a set of roles inside specific projects
Format	<p>urn:mace:terena.org:schac:projectSpecificRole:<project-name>:<iNSS></p> <ul style="list-style-type: none"> The <project-name> must be a name assigned by the TERENA URN Registry for this attribute at http://www.terena.org/registry/terena.org/schac/projectSpecificRole/ <iNSS> is a Namespace Specific String as defined in RFC 2141 but case insensitive
# of values	Multi
References	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> schacProjectSpecificRole = urn:mace:terena.org:schac:projectSpecificRole:perfsonar:developer

6 Appendix

6.1 SCHAC LDAP Schema

Definitions of the object class 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:

<http://www.terena.org/activities/tf-emc2/schacreleases.html>

6.1.1 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
```

6.1.2 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
  )
)
```

6.1.3 Attribute types

schacMotherTongue

```
(
  schacAttributeType:1
  NAME 'schacMotherTongue'
  DESC 'RFC 3066 code for preferred 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
  SINGLE-VALUE
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
)
```

schacCountryOfResidence

```
(
  schacAttributeType:11
  NAME 'schacCountryOfResidence'
  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
)
```

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
)
```


6.1.4 Experimental object class

schacExperimentalOC

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

6.1.5 Experimental attribute types

schacProjectMembership

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

schacProjectSpecificRole

Attribute changed to official branch below schacGroupMembership object class. OID schacExpAttr:2 is obsolete 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
)
```

7 List of Changes

March 26, 2009. V:1.4.0

- Added a footnote related to "TERENA 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 TERENA URN registry.
- Clarify schacExpiryDate scope.

March 27, 2006. V: 1.1.2

- Changed from urn:SCHACPREFIX string to urn:mace:terena.org: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

8 Alphabetical Index of attributes

schacCountryOfCitizenship.....	7
schacCountryOfResidence.....	11
schacDateOfBirth.....	6
schacExpiryDate.....	15
schacGender.....	5
schacHomeOrganization.....	10
schacHomeOrganizationType.....	10
schacMotherTongue.....	5
schacPersonalPosition.....	12
schacPersonalTitle.....	9
schacPersonalUniqueCode.....	13
schacPersonalUniqueID.....	14
schacPlaceOfBirth.....	7
schacProjectMembership.....	18
schacProjectSpecificRole.....	18
schacSn1.....	8
schacSn2.....	8
schacUserPresenceID.....	11
schacUserPrivateAttribute.....	16
schacUserStatus.....	17
schacYearOfBirth.....	6