Attribute definitions for individual data

Version 1.0.0

November 22, 2005

1 Introduction

These schema definitions are intended to facilitate information exchange among European, and possibly international, academic and research institutions.

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. Appropriate profiles, at least for LDAP and XML, will be defined in other documents.

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

- The **eduPerson** schema v. 200312, as defined at http://www.educause.edu/eduperson/
- The **person** schema, as defined by X.521 (2001)
- The **organizationalPerson** schema, as defined by X.521 (2001)
- The **inetOrgPerson** schema, as defined by RFC 2798

2 Attribute meta-information and notation

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	● 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
Examples	Example of values used within the attribute

3 Attribute's 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 were compiled 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

Descriptions of these categories have been compiled from 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.doc>, <http://middleware.internet2.edu/dir/docs/draft-internet2-mace-dir-higher-ed-person-analysis-latest.htm>

4 Attributes defined by SCHAC

4.1 Personal Characteristic

Personal characteristics describe the individual person represented by the entry.

4.1.1 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.
Format	- ISO 639: 2-letter codes if the code is defined for our language - ISO 639: 3-letter codes if the 2-letter code is not defined - If ISO 639: 3-letter codes is not defined for our language we need to use a code defined in another classification. All values must be lower case.
# 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
Examples	schacMotherTongue = fr

4.1.2 schaGender

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	• 0 Not known • 1 Male • 2 Female • 9 Not specified
# of values	Single
References	● **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 standar 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
Examples	schacGender = f

4.1.3 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	● **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
Examples	schacDateOfBirth = 19660412

4.1.4 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	● **RFC 2985** - PKCS #9: Selected Object Classes and Attribute Types Version 2.0. Sections 5.2.5, B.3.9
Examples	schacPlaceOfBirth = Algeciras, Spain

4.1.5 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. All values must be lower case.
# 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
Examples	schacCountryOfCitizenship = es

4.1.6 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
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

4.1.7 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
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

4.1.8 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	● **RFC1274** - The COSINE and Internet X.500 Schema personal title Sections 9.3.30
Examples	schacPersonalTitle = Prof

4.2 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.

4.2.1 schacHomeOrganization

Name	**schacHomeOrganization**
Description	Specifies a person´s home organization using the domain name of the organization
Format	Domain name acording to RFC 1035. All values must be lower case.
# of values	Single
References	● **RFC 1035** - Domain names - implementation and specification
Examples	schacHomeOrganization = terena.nl

4.2.2 SchacHomeOrganizationType

Name	**schacHomeOrganizationType**
Description	Type of a Home Organization
Format	urn:SCHACPREFIX:homeOrgType:<country-code>:<string> ● The <country-code> must be a valid two-letter ISO 3166 country code identifier. ● <string> from a nationally controlled vocabulary
# of values	Single
References	● **ISO 3166** - Codes for the representation of names of countries and their subdivisions
Examples	schacHomeOrganizationType = urn:SCHACPREFIX:homeOrgType:ch:vho schacHomeOrganizationType = urn:SCHACPREFIX:homeOrgType:es:opi

4.2.3 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. All values must be lower case.
# 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
Examples	schacCountryOfResidence = es

4.2.4 schacUserPresenceID

Name	**schacUserPresenceID**
Description	To store a set of values related to network presence protocols
Format	urn:SCHACPREFIX:presence:<NSS> <NSS> is a Namespace Specific String as defined in RFC 2141
# of values	Multi
References	● **RFC 2141** - URN Syntax
Examples	schacUserPresenceID = urn:SCHACPREFIX:presence:xmpp:pepe@im.univx.es schacUserPresenceID = urn:SCHACPREFIX:presence:sip:pepe@myweb.com schacUserPresenceID = urn:SCHACPREFIX:presence:sip:jose.perez@univx.es schacUserPresenceID = urn:SCHACPREFIX:presence:h323:pepe@myweb.fi:808;pars

4.3 Student Information

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

No attributes defined.

4.4 Employee Information

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

4.4.1 schacPersonalPosition

Name	**schacPersonalPosition**
Description	The Personal Position attribute type specifies a personal position inside an institution
Format	urn:SCHACPREFIX:position:<NSS> <NSS> is a Namespace Specific String as defined in RFC 2141
# of values	Multi
References	● **RFC 2141** - URN Syntax ● **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	schacPersonalPosition = urn:SCHACPREFIX:position:umk.pl:programmer

4.5 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.

4.5.1 schacPersonalPublicUniqueID

Name	**schacPersonalPublicUniqueID**
Description	Specifies a "pub lic unique identifier" for the subject it is associated with. This might be Student number, Employee number,...
Format	urn:SCHACPREFIX:publicUniqueID:<country-code>:<NSS> ● <NSS> is a Namespace Specific String as defined in RFC 2141 ● The <country-code> must be a valid two-letter ISO 3166 country code identifier.
# of values	Multi
References	● **ISO 3166** - Codes for the representation of names of countries and their subdivisions ● *HEP rev 06 – Nov 21, 2005 (6.5.2 Student System Identification Code)*
Examples	schacPersonalPublicUniqueID = urn:SCHACPREFIX:publicUniqueID:fi:tut.fi:student:165934 schacPersonalPublicUniqueID = urn:SCHACPREFIX:publicUniqueID:es:uma:estudiante:a3b123c12 schacPersonalPublicUniqueID = urn:SCHACPREFIX:publicUniqueID:se:LIN:87654321

4.5.2 schacPersonalUniqueID

Name	**schacPersonalUniqueID**
Description	Specifies a "legally unique identifier" for the subject it is associated with. This might be DNI in Spain, FIC in Finland, NIN in Sweden,...
Format	urn:SCHACPREFIX:uniqueID:<country-code>:<idType>:<idValue> ● The <country-code> must be a valid two-letter ISO 3166 country code identifier. ● <idType>. Acceptable values must be declared per each country code. ● <idValue>
# of values	Multi
References	● **ISO 3166** - Codes for the representation of names of countries and their subdivisions
Examples	schacPersonalUniqueID = urn:SCHACPREFIX:uniqueID:es:NIF:31241312L schacPersonalUniqueID = urn:SCHACPREFIX:uniqueID:fi:FIC:260667-123F schacPersonalUniqueID = urn:SCHACPREFIX:uniqueID:se:NIN:12345678

4.5.3 schacUUID

Name	**schacUUID**
Description	Specifies a "universally unique identifier" for an entity representing a person.
Format	urn:uuid:<UUID> ● <UUID>. A UUID is essentially a 16-byte number and in its canonical form a UUID may look like this: f81d4fae-7dec-11d0-a765-00a0c91e6bf6. UUID generation requires no central registration process
# of values	Single
References	● **RFC4122** - A Universally Unique IDentifier (UUID) URN Namespace
Examples	schacUUID = urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6

4.6 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.

4.6.1 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)
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	● **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
Examples	schacExpiryDate = 20051231

4.7 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.

4.8 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.

4.8.1 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	● http://www.rediris.es/ldap/doc/irisUserPrivateAttribute/ tnc2005-irisUserPrivateAttribute.pdf
Examples	● Attributes mail and telephoneNumber are considered private schacUserPrivateAttribute = mail schacUserPrivateAttribute = telephoneNumber

4.9 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

4.9.1 schacUserStatus

Name	**schacUserStatus**
Description	Used to store a set of status of a person as user of services
Format	urn:SCHACPREFIX:status:<NSS> ● <NSS> is a Namespace Specific String as defined in RFC 2141
# of values	Multi
References	● **RFC 2141** - URN Syntax
Examples	● To store different user activity states at University of Málaga (uma.es): schacUserStaus = urn:SCHACPREFIX:status:uma.es:affiliation:expired schacUserStaus = urn:SCHACPREFIX:status:uma.es:sendMail:expired schacUserStaus = urn:SCHACPREFIX:status:uma.es:getMail:active ● A parameter in the URN can be used to represent the temporal validity of the satus: schacUserStatus = urn:SCHACPREFIX:status:ujl.si:webmail:active?ttl=20060531

4.10 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 DSA's 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>

No attributes defined.