Authentication and Authorization Infrastructure (AAI)

Authorization Attribute Specification

11-Dec-02

Document management

Version/status:	1.0 / final	
Date:	11-Dec-02	
Author(s):	Serge Droz	PSI
	Pascal Jacot-Guillarmod	University of Lausanne
	Thomas Lenggenhager	SWITCH
	Christian Heim	University of Bern
	David McLaughlin	ETH
	Pascal Py	University of Zurich
	André Redard	at rete ag
	Alexandre Roy	University of Lausanne
	Marc-Alain Steinemann	University of Bern
File name:	AAI_Attr_Specs_v07.doc	
Replacing:	0.6 / 7-Nov-02	
Approved by:		

Change Log:

1.0

- surname, givenname, mail, homePostalAddress, postalAddress: usage within AAI changed
- swissEduPersonOrgDN, swissEduPersonOrgUnitDN, swissEduPersoneEntitlement, mobileTelephoneNumber: attribute name changed
- swissEduPersonDateOfBirth, swissEduPersonGender: format changed
- code lists for UAS study branches added (appendix B)

Table of Content

Figures

Tables

1. Introduction

Authorization Attributes are the user data owned by the Home Organization and needed by the Resource Owner for access control decisions (see “AAI Preparatory Study”, 15 July 2002, www.switch.ch/aai).

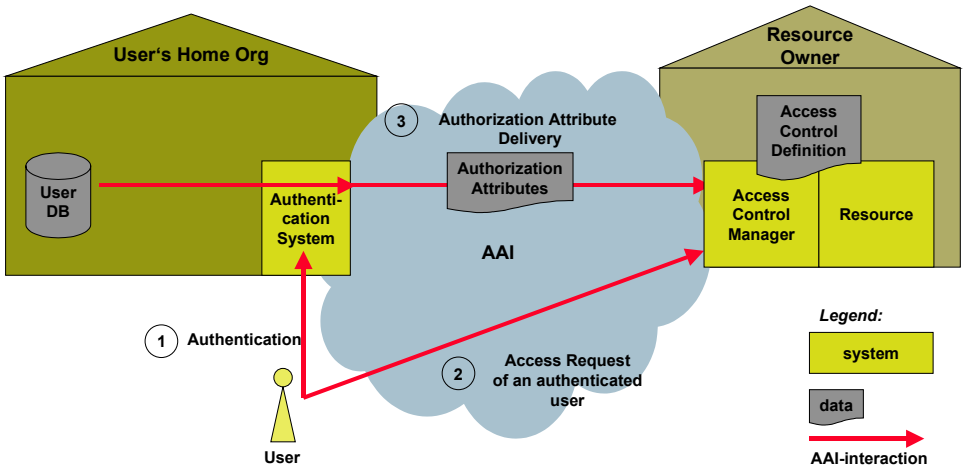

Figure 1 AAI architectural overview

The purpose of this document is to standardize the attributes among all organizations participating in the AAI. The format of the attribute definition is close to the LDAP syntax (see chapter 3 for further details). A schema for an LDAP implementation by the Home Organization is available at http://www.switch.ch/aai/docs/.

We start with a basic set of attributes which may have to be extended during the deployment of the AAI, depending on the requirements of the Resource Owners. Therefore, a clear change management to track the implementation of new standardized attributes will be installed. The AAI Service Provider will be responsible for this change process management in cooperation with the organizations. The details of this change process are not part of this document.

The technical implementation of the interfaces at the Home Organization and at the Resource depend on the chosen architecture (e.g. SAML for Shibboleth) and will be described in the technical detail specification.

Not all attributes defined within this document are always needed; the resource that is accessed should only ask for the attributes that are needed and the Home Organization should transfer only those attributes that were asked for.

2. Attribute Overview

Individual attributes of a user:

Attribute	LDAP Name	derived /adapted from
unique ID	*swissEduPersonUniqueID*	*eduPerson*
Surname	*surname*	*person*
Given name	*givenName*	*inetOrgPerson*
Date of birth	*swissEduPersonDateOfBirth*	
Gender	*swissEduPersonGender*	
Preferred language	*preferredLanguage*	*inetOrgPerson*
E-mail	*mail*	*inetOrgPerson*
Home postal address	*homePostalAddress*	*inetOrgPerson*
Business postal address	*postalAddress*	*orgPerson*
Private phone number	*homePhone*	*inetOrgPerson*
Business phone number	*telephoneNumber*	*person*
Mobile phone number	*mobile*	*inetOrgPerson*

Table 1: Individual attributes

Attributes defining the group membership of users:

Attribute	LDAP Name	Derived / adapted from
Home Organization	*swissEduPersonHomeOrganization*	
Home Organization Type	*swissEduPersonHomeOrganiza-tionType*	
Affiliation	*eduPersonAffiliation*	*eduPerson*
Study branch 1 *Study branch 2* *Study branch 3*	*swissEduPersonStudyBranch1* *swissEduPersonStudyBranch2* *swissEduPersonStudyBranch3*	
Study level	*swissEduPersonStudyLevel*	
Staff category	*swissEduPersonStaffCategory*	*eduPerson*
Organization Path	*eduPersonOrgDN*	*eduPerson*
Organizational unit path	*eduPersonOrgUnitDN*	*eduPerson*
Member of	*eduPersonEntitlement*	*eduPerson*

Table 2: Group membership attributes

3. Attribute Meta-Information and Notation

For all attributes, the following meta-data is defined:

Description	A short description of the attribute	
Semantics	The semantics of the attribute	
LDAP Syntax	The LDAP syntax of an attribute (see RFC 2252)	
#of values	single multiple	
Permissible values (if controlled)	A list of permissible values. Where possible, the list of values is based on international or national standards (e.g. ISO country codes)	
Classification	mandatory	A Home Organization has to be able to provide this attribute in order to be part of the AAI community (only if applicable for a specific user)
	recommended	It is strongly recommended that a Home Organization is able to provide this attribute (only if applicable for a specific user)
	optional	Some resources may need this attribute
	Independent of the classification, attributes should only be transferred to resources with a valid case to use it.	
Notes	Additional information about the attribute	
Examples (LDIF Fragment)	Examples in the LDIF Format (LDIF = LDAP Data Interchange Format, see RFC 2849)	
Typical usage	authorization	Typically, a resource uses this attribute to make the access control decision
	accounting	This attribute is used for accounting reasons
	additional user information	Information which is typically not used for authorization or accounting, but may be used to offer a better service to the user (e.g. Given Name, Surname used within a personalized portals)
	AAI internal (not used yet)	Used for AAI internal purposes; attribute is not accessible by the resource

4. Attribute Definitions

4.1 Unique ID (*swissEduPersonUniqueID*)

Description	A unique identifier for a person, mainly for inter-institutional user identification.
Semantics	<unique-local-ID>@<Internet-domain> The format used is derived from e-mail addresses. The 'domain part' is equivalent to the registered Internet domain the home organization uses, i.e the same value as the content of the attribute swissEduPersonHomeOrganization. The 'local part' is an ID uniquely allocated by the home organization for a user they correctly authenticated according to the local authentication policy. Every time the same user re-authenticates, the same 'local part' should be used.
LDAP Syntax	Directory String Note: The length of the local part should be minimum 6 and maximum 12 characters.
#of values	single
Permissible values (if controlled)	n/a
Classification	mandatory
Notes	One should never expose the Unique ID to end users; especially one should not require a user to provide his Unique ID manually! It is up to the local policy to define how long the same 'local part' represents the same user. However, a minimum duration (of e.g. a semester or a year) should be agreed upon by all participants of the AAI. Unlike the 'Matrikelnummer' or the 'AHV-Nummer', the 'local part' should not carry visible semantics. However, a home organization has to be able to identify the person matching that 'local part'. The 'local part' could be a hash value based on information about the user. University of Berne already uses a hash algorithm to generate pseudo IDs.
Examples (LDIF Fragment)	`swissEduPersonUniqueID: 84593872749492@ethz.ch` `swissEduPersonUniqueID: 7382940224@unil.ch`
Typical usage	authorization, accounting

4.2 Surname (*surname)*

Description	Surname or family name (defined in person)
Semantics	According to RFC 2256, this is the X.500 surname attribute, which contains the family name of a person.
LDAP Syntax	Directory String
#of values	multiple
Permissible values (if controlled)	n/a
Classification	mandatory
Notes	The following notes have been taken from the inetOrgPerson specification > If the person has a multi-part surname (whether hyphenated or not), store the multi-part name as one value and each component as separate values in this multi-valued attribute. That yields the best results for the broadest range of clients doing name searches. Within AAI, HomeOrganizations should provide only one value: the surname which is used for official communication with that person. Resource has to be able to support UTF-8 encoded accented character strings.
Examples (LDIF Fragment)	`surname: Meier-Müller`
Typical AAI usage	additional user information

4.3 Given Name (*givenName*)

Description	Given name of a person (defined in inetOrgPerson)
Semantics	RFC 2256 description: "The givenName attribute is used to hold the part of a person's name which is not their surname nor middle name."
LDAP Syntax	Directory String
#of values	multiple
Permissible values (if controlled)	n/a
Classification	mandatory
Notes	The following notes have been taken from the inetOrgPerson specification > If the person has a multi-part given name (whether hyphenated or not), store the multi-part name as one value and each component as separate values in this multi-valued attribute. That yields the best results for the broadest range of clients doing name searches. Within AAI, HomeOrganizations should provide only one value: the given name which is used for official communication with that person. Resource has to be able to support UTF-8 encoded accented character strings

Examples (LDIF Fragment)	`givenName: Hans-Peter`
Typical AAI usage	additional user information

4.4 Date of Birth (*swissEduPersonDateOfBirth*)

Description	The date of birth of the person

Semantics	Based on RFC 3339 'Date and Time on the Internet: Timestamps'. Using the 'full-date' format from paragraph 5.6:
	`full-date = date-fullyear date-month date-mday`
	`date-fullyear = 4DIGIT`
	`date-month = 2DIGIT` ; 01-12
	`date-mday = 2DIGIT` ; 01-28, 01-29, 01-30, 01-31 based on month/year

LDAP Syntax	Numeric String {8}
#of values	single
Permissible values (if controlled)	date-mday must be within the proper range depending on the values of date-month and date-fullyear
Classification	optional
Notes	The birthdate is sensitive in the eyes of many users.
Examples (LDIF Fragment)	`swissEduPersonDateOfBirth: 19871022` `swissEduPersonDateOfBirth: 20021010`
Typical usage	additional user information

4.5 Gender (*swissEduPersonGender)*

Description	The state of being male or female
Semantics	"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)
LDAP Syntax	Integer {1}
#of values	single
Permissible values (if controlled)	The following codes are used (see ISO 5218): Not known 0 Male 1 Female 2 Not specified 9
Classification	optional
Notes	

Examples (LDIF Fragment)	`swissEduPersonGender: 1` `swissEduPersonGender: 2`
Typical usage	additional user information

4.6 Preferred Language (*preferredLanguage*)

Description	Preferred language of a user (defined in inetOrgPerson)
Semantics	Preferred written or spoken language for a user
LDAP Syntax	Directory String
#of values	single

Permissible values
(if controlled)
	The syntax and registry of language tags is the same as that defined by RFC 1766. In summary, a language tag is composed of 1 or more parts: A primary language tag and a possibly empty series of subtags:
	`language-tag = primary-tag *( "-" subtag )`
	`primary-tag = 1*8ALPHA`
	`subtag = 1*8ALPHA`
	Whitespace is not allowed within the tag and all tags are case-insensitive. The name space of language tags is administered by the IANA. Example tags are:
	`en, en-us`
	`de, de-ch`
	where any two-letter primary-tag is an ISO 639 language abbreviation and any two-letter initial subtag is an ISO 3166 country code.

Classification	optional
Notes	

Examples
(LDIF Fragment)
	`preferredLanguage: en-us`
	`preferredLanguage: de-ch`
	`preferredLanguage: it-ch`
	`preferredLanguage: fr-ch`

Typical AAI usage	additional user information

4.7 E-mail Address (*mail*)

Description	Preferred address for the "to:" field of e-mail to be sent to this person (defined in inetOrgPerson)
Semantics	Follow inetOrgPerson definition of RFC 1274: "The [mail] attribute type specifies an electronic mailbox attribute following the syntax specified in RFC 822. Note that this attribute should not be used for greybook or other non-Internet order mailboxes."
LDAP Syntax	IA5 string {256}
#of values	multiple
Permissible values (if controlled)	n/a

Classification	recommended
Notes	The following notes have been taken from the inetOrgPerson specification RFC 1274 uses the longer name 'rfc822Mailbox' and syntax OID of 0.9.2342.19200300.100.3.5. All recent LDAP documents and most deployed LDAP implementations refer to this attribute as 'mail' and define the IA5 String (ASCII string) syntax using the OID 1.3.6.1.4.1.1466.115.121.1.26. Within AAI, the correctness of this attribute cannot be guaranteed by the Home Organization since the mailboxes may be changed by the user without informing the Home Organization (privat mailboxes). If a person has more than one e-mail address, it is recommended to provide only one address (the address used by the HomeOrganization itself when sending e-mails to that person)
Examples (LDIF Fragment)	`mail: peter.meier@unizh.ch`
Typical AAI usage	additional user information

4.8 Home Postal Address (*homePostalAddress*)

Description	Home address of the user (defined in inetOrgPerson)
Semantics	From RFC 1274 description: "The Home postal address attribute type specifies a home postal address for an object. This should be limited to up to 6 lines of 30 characters each." Within AAI, the limitation to up to 6 lines of 30 characters is not relevant.
LDAP Syntax	Postal Address
#of values	multiple
Permissible values (if controlled)	n/a
Classification	optional
Notes	
Examples (LDIF Fragment)	`homePostalAddress: Bernerstrasse 45$CH-8048 Zürich`
Typical usage	additional user information

4.9 Business Postal Address (*postalAddress*)

Description	Campus or office address (defined in orgPerson)
Semantics	Campus or office address; derived from orgPerson X.520(2000): "The Postal Address attribute type specifies the address information required for the physical postal delivery to an object." Within AAI, the limitation to up to 6 lines of 30 characters as defined in the X.520 standard is not relevant.
LDAP Syntax	Postal Address

#of values	multiple
Permissible values (if controlled)	n/a
Classification	recommended
Notes	
Examples (LDIF Fragment)	`postalAddress: ETH Zentrum$CH-8092 Zürich`
Typical usage	additional user information

4.10 Private Phone Number (*homePhone*)

Description	Private phone number (defined in inetOrgPerson)
Semantics	Private phone number of the user. Attribute values should follow the agreed format for international telephone numbers: i.e., "+44 71 123 4567."
LDAP Syntax	Telephone Number
#of values	multiple
Permissible values (if controlled)	n/a
Classification	optional
Notes	
Examples (LDIF Fragment)	`homePhone: +41 1 234 5678`
Typical usage	additional user information

4.11 Business Phone Number (*telephoneNumber*)

Description	Office/campus phone number (defined in person)
Semantics	Office/campus phone number of the user. Attribute values should follow the agreed format for international telephone numbers: i.e., "+44 71 123 4567."
LDAP Syntax	Telephone Number
#of values	multiple
Permissible values (if controlled)	n/a
Classification	recommended
Notes	
Examples (LDIF Fragment)	`telephoneNumber: +41 1 234 5678`
Typical usage	additional user information

4.12 Mobile Phone Number (*mobile*)

Description	Mobile phone number (defined in inetOrgPerson)
Semantics	Follow inetOrgPerson definition of RFC 1274: "The [mobile] attribute type specifies a mobile telephone number associated with a person. Attribute values should follow the agreed format for international telephone numbers: i.e., "+41 79 123 4567."
LDAP Syntax	Telephone Number
#of values	multiple
Permissible values (if controlled)	n/a
Classification	optional
Notes	This attribute may be useful if resource has the ability to send SMS (short message service).
Examples (LDIF Fragment)	`mobileTelephoneNumber: +41 79 234 5678`
Typical usage	additional user information

4.13 Home Organization (*swissEduPersonHomeOrganization*)

Description	Name of a Home Organization
Semantics	Domain Name of a Home Organization
LDAP Syntax	Directory String
#of values	single
Permissible values (if controlled)	SWITCH maintains a register of organizations participating in the AAI with their domain names and swissEduPersonHomeOrganizationType
Classification	mandatory
Notes	

Examples (LDIF Fragment)	`swissEduPersonHomeOrganization: unil.ch`
	`swissEduPersonHomeOrganization: switch.ch`
	`swissEduPersonHomeOrganization: ethz.ch`
	`swissEduPersonHomeOrganization: library.ethz.ch`

Typical usage	authorization, accounting

4.14 Home Organization Type (*swissEduPersonHomeOrganizationType*)

Description	Type of a Home Organization
Semantics	Domain Name of a Home Organization
LDAP Syntax	Directory String
#of values	single
Permissible values (if controlled)	university; uas; hospital; library; vho; others

Classification	mandatory
Notes	“vho” stands for virtual home organization.

Examples (LDIF Fragment)	`swissEduPersonHomeOrganizationType: university`
	`swissEduPersonHomeOrganizationType: vho`
	`swissEduPersonHomeOrganizationType: hospital`

Typical usage	authorization

4.15 Affiliation (*eduPersonAffiliation*)

Description	Type of affiliation (defined in eduPerson)
Semantics	Specifies the user's relationship(s) to the Home Organization in broad categories such as student, faculty, employee, etc. (See controlled vocabulary).
LDAP Syntax	Directory String
#of values	multiple
Permissible values (if controlled)	faculty, student, staff, alum, member, affiliate, employee
Classification	mandatory
Notes	The following notes have been taken from the eduPerson specification 1.5: > The list of allowed values in the current version 1.0 of the object class is CERTAINLY incomplete. We felt that any additional values should come out of discussions with the stakeholder communities. Any agreed-upon additional values will be included as part of the post-1.0 versions of eduPerson. > > We also deliberately avoided including a value such as "other" or "misc" because it would be semantically equivalent to "none of the above." To indicate "none of the above," for a specific person, leave the attribute empty. > > "Member" is intended to include faculty, staff, student, and other persons with a basic set of privileges that go with membership in the university community (e.g., library privileges). It could be glossed as "member in good standing of the university community." > > "Affiliate" is intended to apply to people with whom the university has dealings, but to whom no general set of "community membership" privileges are extended. Within AAI, we will not use the value “employee”. Use “staff” instead.
Examples (LDIF Fragment)	`eduPersonAffiliation: student` `eduPersonAffiliation: faculty`
Typical usage	authorization

4.16 Study Branch 1 (*swissEduPersonStudyBranch1*)

Description	Study branch of a student, first level of classification.
Semantics	This attribute follows the catalog of study branch of the SIUS/SHIS[1]. It is classified in branch, domain of branch and group of domain. This attribute is a code corresponding to the group of domain.
LDAP Syntax	Integer {6}
#of values	multiple
Permissible values (if controlled)	If `swissEduPersonOrganizationType = uni` : possible value can be found in the first column of the uniStudyBranch1.csv file (see also Appendix A). If `swissEduPersonOrganizationType = uas` : possible value can be found in the first column of the uasStudyBranch1.csv file (see also Appendix B).
Classification	optional
Notes	This attribute has a meaning only if the person is a student (`eduPersonAffiliation = student`). The uniStudyBranch1.csv file (uasStudyBranch1.csv) lists possible values of this attribute and the corresponding meaning in German and French. Example: the value 1 means that the student is studying in a branch belonging to “Geistes + Sozialwiss.” (“Sciences humaines + socials”).
Examples (LDIF Fragment)	`swissEduPersonStudyBranch1: 4`
Typical usage	authorization

4.17 Study Branch 2 (*swissEduPersonStudyBranch2*)

Description	Study branch of a student, intermediate level of classification.
Semantics	This attribute follows the catalog of study branch of the SIUS/SHIS. It is classified in branch, domain of branch and group of domain. This attribute is a code corresponding to the domain of branch.
LDAP Syntax	Integer {6}
#of values	multiple
Permissible values (if controlled)	If `swissEduPersonOrganizationType` = uni : possible value can be found in the first column of the uniStudyBranch2.csv file (see also Appendix A). If `swissEduPersonOrganizationType = uas` : possible value can be found in the first column of the uasStudyBranch2.csv file (see also Appendix B).
Classification	optional
Notes	This attribute has a meaning only if the person is a student (`eduPersonAffiliation = student`). The uniStudyBranch2.csv file (uasStudyBranch2.csv) lists possible values of this

[1] SIUS/SHIS = Service d'Information Universitaire Suisse/Schweizerisches Hochschulinformationssystem, http://www.statistik.admin.ch/stat_ch/ber15/dber15.htm

	attribute and the corresponding meaning in German and French. Example: the value 42 means that the student is studying in a branch belonging to “Naturwissenschaften” (“Sciences naturelles”). If a value of this attribute is set, it always implies a value of swissEduPersonStudyBranch1 even if it is not explicitly defined; it is the value given on the fourth column of the csv file. Example: `swissEduPersonStudyBranch2 = 42` means that `swissEduPersonStudyBranch1 = 4`
Examples (LDIF Fragment)	`swissEduPersonStudyBranch2: 42`
Typical usage	authorization

4.18 Study Branch 3 (*swissEduPersonStudyBranch3*)

Description	Study branch of a student.
Semantics	This attribute follows the catalog of study branch of the SIUS/SHIS. It is classified in branch, domain of branch and group of domain. This attribute is the SIUS/SHIS code of the study branch.
LDAP Syntax	Integer {6}
#of values	multiple
Permissible values (if controlled)	If `swissEduPersonOrganizationType = uni` : possible value can be found in the first column of the uniStudyBranch3.csv file (see also Appendix A). If `swissEduPersonOrganizationType = uas` : possible value can be found in the first column of the uasStudyBranch3.csv file (see also Appendix B). The possible values of this attribute and their meaning correspond exactly to the coding used by the SIUS/SHIS; this coding is already used by every University and ETH for the data that is regularly sent to SIUS/SHIS.
Classification	recommended
Notes	This attribute has a meaning only if the person is a student (`eduPersonAffiliation = student`). The uniStudyBranch3.csv file (uasStudyBranch3.csv) lists possible values of this attribute and the corresponding meaning in German and French. Example: the value 7450 means that the student is studying in the branch “Mikrotechnik” (“Microtechnique”). If a value of this attribute is set, it implies always a value of swissEduPersonStudyBranch1 even if it is not explicitly defined; it is the value given on the seventh column of the csv file. It also implies (not always) a value of swissEduPersonStudyBranch2. Example: `swissEduPersonStudyBranch3 = 7450` means that `swissEduPersonStudyBranch2 = 62` and `swissEduPersonStudyBranch1 = 6`. Change process: SHIS/SIUS may add new study branches, but will not delete or modify existing ones. Home Organizations are obliged to implement new branches until the statistical data records have to be delivered to SHIS/SIUS (i.e. every year on Nov 15).

Examples (LDIF Fragment)	`swissEduPersonStudyBranch3: 7905`
Typical usage	authorization

4.19 Study Level (*swissEduPersonStudyLevel*)

Description	Study level of a student in a particular Study Branch 3.
Semantics	This attribute follows the definition of study branch 3 and study level of the SIUS/SHIS. The format is <swissEduPersonStudyBranch3> - <study level>
LDAP Syntax	Directory String
#of values	multiple
Permissible values (if controlled)	for <swissEduPersonStudyBranch3>: see chapter 4.18 for <study level>: the permissible values are 0, 10, 15, 20, 25, 26, 31, 32, 39. A more detailed explanation is given in Appendix C.
Classification	recommended
Notes	This attribute has a meaning only if the person is a student (`eduPersonAffiliation = student`). A student may study in more than one study branch and may have reached a different study level in each of these study branches. Therefore, this attribute may have multiple values, defining the study level for each study branches 3. Make sure that the content of the attribute swissEduPersonStudyBranch3 and swissEduPersonStudyLevel are consistent (swissEduPersonStudyBranch3 should contain at least the study branch part of each study level).
Examples (LDIF Fragment)	`swissEduPersonStudyLevel: 7905-15`
Typical usage	authorization

4.20 Staff Category (*swissEduPersonStaffCategory*)

Description	Workbranch of a staff member
Semantics	The classification is based on the Staff Categories of the SIUS/SHIS Documents, suitably expanded to include non-school categories.
LDAP Syntax	Integer {3}
#of values	multiple
Permissible values (if controlled)	There are three main Categories: 100 Teachers 200 Researchers 300 Others (Support, Admin and technical staff) The last two digits detail the category, as explained in Appendix D.
Classification	recommended

Notes	
Examples (LDIF Fragment)	`swissEduPersonStaffCategory: 101` `swissEduPersonStaffCategory: 305`
Typical usage	authorization, accounting

4.21 Organization Path (*eduPersonOrgDN*)

Description	The distinguished name (DN) of the directory entry representing the organization with which the person is associated (defined in eduPerson).
Semantics	The directory entry pointed to by this dn should be represented in the X.521(1993) "organization" object class
LDAP Syntax	DN
#of values	single
Permissible values (if controlled)	
Classification	optional
Notes	With a distinguished name, the client can do an efficient lookup in the institution's directory to find out more about the organization with which the person is associated. The value of SwissEduPersonHomeOrganization attribute is better suited for authorization based on about the organization with which the person is associated.
Examples (LDIF Fragment)	`o=Universite de Lausanne, c=CH`
Typical usage	authorization

4.22 Organizational Unit Path (*eduPersonOrgUnitDN*)

Description	The distinguished name (DN) of the directory entries representing the person's Organizational Unit(s) (defined in eduPerson).
Semantics	The directory entry pointed to by this dn should be represented in the X.521(1993) "organizational unit" object class.
LDAP Syntax	DN
#of values	multiple
Permissible values (if controlled)	
Classification	optional
Notes	With a distinguished name, the client can do an efficient lookup in the institution's directory for information about the person's organizational unit(s). It also possible to use this attribute to give some authorization to persons that belong to a known Organizational Unit.

Examples (LDIF Fragment)	`ou=Faculte des sciences, o=Universite de Lausanne, c=CH`
Typical usage	authorization

4.23 Group Membership (*eduPersonEntitlement*)

Description	URI (either URL or URN) that indicates a set of rights to specific resources. (defined in eduPerson)
Semantics	With eduPersonEntitlement, a home organisation declares that the user whose record contains this attribute is in their opinion entitled to access the SPECIFIC resource described by the URI. I.e. the group membership is restricted to authorized users of that resource.
LDAP Syntax	Directory String
#of values	multiple
Permissible values (if controlled)	URIs only
Classification	optional
Notes	This attribute is suitable for cases where a home organization knows to which resources their students, staff etc. should have access. A typical case is a home organization having signed a contract with a resource which defines the range of allowed users. The home organization knows their users and can therefore authorize them to access the resource. This attribute is of no use for resources without close ties to the home organizations. Home organizations are not in the position to keep track of all group memberships their students and staff may require. For this, more flexible solutions as described in chapter 5 are needed.
Examples (LDIF Fragment)	`eduPersonEntitlement: http://unil.ch/aai/resources/biblio92`
Typical usage	authorization, accounting

5. Group Membership Independent of Home Organizations

Being able to support more flexible group membership criteria, especially for inter-institutional groups without close ties to the administration of the home organizations of their members, is a necessity for AAI. Examples would be special interest groups coordinated by a volunteer who knows the group members or researchers in a specific field sharing their resources within their group via the network. The administration of such a group can be compared with the administration of an e-mail list with restricted subscription.

A model for such group memberships could follow the eduPersonEntitlement attribute. However, the resource would not automatically receive the attribute via the AAI because the home organization does not know about that group membership. Since the AAI is able to provide the unique ID of a user the resource has only to know where to look for group membership confirmation regarding that unique ID. A resource can check that e.g. via LDAP or a web service with the pre-configured 'group registry' for membership of that unique ID. In case of success, the user gets access to the AAI-protected resource.

A closer look at how group membership confirmation could be implemented by re-using elements of the Shibboleth architecture:

- The resources sends a SAML (Security Assertion Markup Language) message with the unique ID to the Attribute Authority (AA) of the group membership server.
- The AA then checks for existing group membership of the user identifyed by the unique ID and answers with a SAML message. The Attribute Release Policy of the group member, configured at the group membership server, could release further attributes to be sent to the resource.

5.1 Managing Group Membership

The group membership administration could be either done completely outside the AAI or the group registry could be an AAI-enabled resource for itself. The group administrator authenticates via AAI and gets admin access.

New group members connect initially to an AAI-enabled registration page and submit their uniqueID plus additional attributes as required by the resource. Further information about the applicant can be collected on that web page. After positive review of the application information by the group administrator, he or she adds the unique ID to the list of group members in the group registry. That's where resources could later on check for membership.

Groups can either maintain their own group registry integrated with other resources they provide or they could use a shared group registry specialized for that purpose. SWITCH will in conjunction with virtual home organization services look into possible offerings for shared group registries.

Appendix A Study Branches for Swiss Universities

Permissible Values for *StudyBranches1*
(for the entire list see **http://www.switch.ch/aai/docs/uniStudyBranch1.csv**)

Study-branch1	German	French
1	GEISTES-+ SOZIALWISS.	SCIENCES HUMAINES + SOCIALES
2	WIRTSCHAFTSWISSENSCHAFTEN	SCIENCES ÉCONOMIQUES
3	RECHT	DROIT
…	...	…

Permissible Values for *StudyBranches2*
(for the entire list see **http://www.switch.ch/aai/docs/uniStudyBranch2.csv**)

Study-branch2	German	French	Study-branch1
11	THEOLOGIE	THÉOLOGIE	1
12	SPRACH-+ LITERATURW. (SLW)	LANGUES + LITTÉRATURE (LL)	1
13	HISTORISCHE + KULTURW.	SCIENCES HISTORIQUES + CULTURE	1
…	…	…	…

Permissible Values for *StudyBranches3*
(for the entire list see **http://www.switch.ch/aai/docs/uniStudyBranch3.csv**)

Study-branch3	German	French	Study-branch1	Study-branch2
1205	PROTESTANTISCHE THEOLO-GIE	THÉOLOGIE PROTESTANTE	1	11
1210	RÖMISCH-KATHOLISCHE THE-OLOGIE	THÉOLOGIE CATHOLIQUE-ROMAINE	1	11
1215	CHRISTKATHOLISCHE THE-OLOGIE	THÉOLOGIE CATHOLIQUE-CHRÉTIENNE	1	11
…	…	…	…	…

Appendix B Study Branches for Swiss Universities of Applied Science

Permissible Values for *StudyBranches1* (uasStudyBranch1.csv)

(for the entire list see **http://www.switch.ch/aai/docs/uasStudyBranch1.csv**)

Study-branch1	German	French
10000	Bauwesen	Sciences de la construction
20000	Technik	Technique
30000	Chemie	Chimie
40000	Landwirtschaft	Agriculture

Permissible Values for *StudyBranches2* (uasStudyBranch2.csv)

(for the entire list see **http://www.switch.ch/aai/docs/uasStudyBranch2.csv**)

Study-branch2	German	French	Study-branch1
10100	Architektur	Architecture	10000
10200	Bauingenieurwesen	Génie civil	10000
10300	Planung und Geomatik	Mensuration et géomatique	10000
10400	Holztechnik	Technique du bois	10000
10900	Bauwesen	Sciences de la construction	10000

Permissible Values for *StudyBranches3*

(for the entire list see **http://www.switch.ch/aai/docs/uasStudyBranch3.csv**)

Study-branch3	German	French	Study-branch1	Study-branch2
10199	Architektur allgemein	Architecture en général	10000	10100
10201	Bauprozessmanagement	Bauprozessmanagement	10000	10200
10299	Bauingenieurwesen allgemein	Génie civil en général	10000	10200
…	…	…	…	…

Appendix C Study Levels

STUDIENSTUFE

Diplomstudien:

Als Diplomstudien gelten alle Ausbildungsgänge, die zu einem Lizentiat, Diplom, Bachelor, Master, Gymnasial-, Sekundar- oder Primarlehrpatent führen. Ebenfalls einbegriffen sind Kurzstudiengänge.

00 = Studierende auf Diplomstufe, die nur vorübergehend an der betreffenden Hochschule eingeschrieben sind (Fremdsprachenaufenthalt, Fortbildung) und hier keine Abschlussprüfungen ablegen werden (Gaststudierende).
Studierende, die im Rahmen eines von der Hochschule durchgeführten Vorbereitungskurses auf die Zulassung zum eigentlichen Studium hinarbeiten (z.B. Cours de mathématiques spéciales EPFL).

10 = Studierende in der Studienphase, die zu einem der folgenden Abschlüsse führt: Lizentiat, Diplom, Gymnasial-, Sekundar- oder Primarlehrpatent, Abschlussprüfung bei Kurzstudiengängen.
Studierende der Medizin und der Eidg. Technischen Hochschulen: Hier werden nur die Vorkliniker/innen bzw. die Studierenden vor dem 2. Vordiplom mit der Studienstufe 10 bezeichnet.

15 = Studierende in der Studienphase, die zum Bachelor führt.

20 = Medizinstudierende in den klinischen Semestern, d.h. Medizinstudierende, die das 2. Propädeutikum bestanden haben.
Studierende der Eidg. Technischen Hochschulen, die das 2. Vordiplom absolviert haben.

25 = Studierende, die den Bachelortitel erworben haben und einen Master anstreben.

26 = «Direkter Master»: Studierende in gestuften Studiengängen, die einen Master anstreben, ohne zuvor den Bachelortitel erwerben zu müssen.

Nachdiplomstudien:

31 = Studien, die auf das Doktorat vorbereiten und einen akademischen Titel (Master, Lizentiat, Diplom) oder einen gleichwertigen Abschluss voraussetzen.

32 = Im Rahmen eines strukturierten Lehrplanes zu besuchende Spezialisierungsstudien, welche als Eintrittsbedingung einen akademischen oder gleichwertigen Titel erfordern und die zur Erlangung eines Diploms/Nachdiploms führen.

39 = Andere Nachdiplomstudiengänge von individuellem Charakter, mit oder ohne Abschlussdiplom, insbesondere:
- Immatrikulation im selben Fach nach einem Erstabschluss (Lizentiat, Diplom) ohne bestimmtes Studienziel
- Weiterbildung auf Stufe Nachdiplom
- Studien nach dem Doktorat

NIVEAU D'ÉTUDES

Etudes diplômes:

Les études diplôme sont tous les cursus d'études qui conduisent à une licence, un diplôme, un titre de Bachelor, un titre de Master, un titre de maître ou maîtresse de gymnase ou de maître ou maîtresse primaire ou secondaire. Y sont comprises aussi les filières de cycle court.

00 = Etudiants au niveau d'études diplôme qui sont inscrits temporairement à la haute école concernée (séjour linguistique, perfectionnement) et qui n'y subiront pas d'examen (auditeurs libres).
Etudiants fréquentant des cours organisés par la haute école préparant aux études supérieures proprement dites (p. ex. cours de mathématiques spéciales EPFL).

10 = Etudiants réguliers se trouvant dans une phase d'études qui les conduit à un des examens finals suivants: licence, diplôme, titre de maître ou maîtresse de gymnase ou de maître ou maîtresse primaire ou secondaire, examen final pour des filières de cycle court.
Etudiants en médecine et des écoles polytechniques fédérales: seuls les pré-cliniciens, c'est-à-dire les étudiants n'ayant pas subi le deuxième examen propédeutique sont recensés sous le niveau 10.

15 = Etudiants réguliers se trouvant dans une phase d'études qui les conduit au titre de Bachelor.

20 = Etudiants en médecine en semestres d'études cliniques.
Etudiants des écoles polytechniques fédérales qui ont passé le deuxième examen propédeutique.

25 = Etudiants réguliers, ayant obtenu le titre de Bachelor et qui aspirent au titre de Master.

26 = «Master direct»: étudiants dans des cursus d'études échelonnées qui aspirent au titre de Master sans devoir acquérir au préalable le titre de Bachelor.

Etudes postgrades:

31 = études préparant au doctorat, après avoir obtenu un diplôme académique (Master, licence, diplôme) ou un titre équivalent

32 = études de spécialisation suivies dans le cadre d'un programme précis exigeant comme condition d'entrée un titre universitaire ou un titre jugé équivalent et débouchant normalement sur un diplôme/diplôme postgrade

39 = autres études post-diplôme, à caractère individuel, avec ou sans diplôme final, notamment:
- inscription dans la même filière après un premier titre universitaire (licence, diplôme) sans but défini
- formation continue postdiplôme
- études postdoctorat

Appendix D Staff Categories

The permissible values of the swissEduPersonStaffCategory attribute are, where possible, obtained from the SIUS/SHIS Documents:

[1] Technisches Handbuch für universitäre Hochschulen, pp. 62-64

[2] Technisches Handbuch für die Erhebung des Personals der FH, sec 3.9 p.13

100 Teaching

Designates staff with teaching duties (including physicians working at unviersity hospitals). Completely based on the SIUS/SHIS documents.

Code	Name	Example	Remark
101	Professors	Ordinary Profs.	[1] Cat I-II [2] Cat 10
102	Oberer Mittelbau/Corps intermediaire superieur	Lectures	[1] Cat III-VI [2] Cat 20
103	Unterer Mittelbau/Corps intermediaire inferieur	Assistants	[1] Cat VII-X [2] Cat 30

200 Research

Designates staff with research duties. Similar to the Teaching category, but for researchers only.

Code	Name	Example	Remark
201	Permanent Researchers	Ordinary Profs.	[1] Cat I-II [2] Cat 10
202	Oberer Mittelbau/Corps intermediaire superieur	Lectures	[1] Cat III-VI [2] Cat 20
203	Unterer Mittelbau/Corps intermediaire inferieur	Assistants	[1] Cat VII-X [2] Cat 30

300 Admin/Support/technical

This section does not contain a direct correspondence to the SIUS/SHIS documents.

It's based though on the categories XI-XVII of [1].

If needed more categories should be added. This category needs still some discussion.

Code	Name	Example	Remark
301	Administrative Personnel	Members of HR	[1] Cat XI
302	Administrative Personnel: Apprentices and Interns		[1] Cat XII
303	Technical Personnel	Sysadmins	[1] Cat XIII
304	Technical Personnel: Apprentices and Interns		[1] Cat XIV
305	Janitors, Building Managers		[1] Cat XV
306	Social and Wellness Personnel		[1] Cat XVI
307	Library Personnel		[1] Cat XVII
308	Safety Personnel	Radiation, Firefighters, Guards?	