FIDERN

FIDERN – Federated ID for Education and Research Network

Attibute Specification

Authors	ZAMREN
Last Modified	04/10/2018
Version	4.0

Table of Contents

1 Introduction

The Attribute Specification is crucial for the data exchange within the FIDERN federation. It provides the common basis on which two communicating entities are able to share information they know to interpret identically. This document standardizes the attributes among all organizations participating in FIDERN.

The format of the attribute definition is based on the eduPerson LDAP schema (see 3.0: “Attribute definitions” for further details). eduPerson and eduOrg are Lightweight Directory Access Protocol (LDAP) schema designed to include widely-used person and organizational attributes in higher education. The eduPerson object class provides a common list of attributes and definitions, drawing on the existing standards in higher education.

The set of attributes is adapted depending on requirements of consumers (the resources) and the ability of the home organizations to supply them.

1.1 Privacy and data protection

The home organization administrator's and resource owner's first and foremost duty regarding attributes is privacy and data protection. Users perceive many of the attributes specified in this document as very sensitive information. The persons responsible for the systems that process attributes must fully respect user privacy and the relevant data protection laws and regulations which define how to deal with personal data.

1.2 Security

Revealing attribute values can be a security risk. Administrators of home organisations should take extra care when releasing attributes and should only release those attributes as are required by the resource provider. Conversely resource providers should only request user attributes as much as will be required to provide the service to prospective users.

Note that FIDERN is designed to transfer information about authentication but not the credentials themselves.

2 Implementing the Attribute Specification

2.1 Responsibilities of Home Organisation

The information to be made available through attributes gets collected and maintained by the home organization. It is stored in a user directory, which can either be implemented using an LDAP compatible directory (e.g. OpenLDAP or Active Directory) or an SQL database.

The home organization is responsible for proper identity management and up-to-date personal data. In addition, it is also responsible for proper configuration of the Simplesamlphp attribute filter policy defining which attributes may be released to which resources in order to protect the privacy of its users.

Each home organization participating in the FIDERN Federation has to implement at least the core attributes as defined in section 3.0 below.

2.2 Responsibilities of Resource Owners

The set of attributes needed by a resource depends on the service it offers to its users. The set may be minimal for anonymous services and rather large for highly personalized services with granular authorization. Keep in mind: according to the data protection principles, as few as possible personal data should be processed!

In addition, a resource owner should carefully consider which information to store across user sessions. The fewer information is stored, the smaller impact a potential misuse has in case of an incident.

So it is the duty of the resource owner to specify which attributes are really required to offer the service and which additional optional attributes might allow him/her to offer optional advanced services.

When defining their attribute requirements, resource owners should always check the attribute implementation status as defined on the FIDERN website (url: www.fidern.ac.zm). If a resource requires an attribute not (yet) implemented in the home organization of its prospective users, these users will not be able to access the resource.

Resource owners have to maintain the attribute requirements of their resource in the FIDERN Resource Registry.

3 Attribute Definitions

For all attributes, the following metadata is defined:

Name	The name of the attribute
Description	A short description of the attribute
Permissible values	A list of permissible value (Where possible, the list of values is based on international or national standards.)
References	Reference to a standard the attribute is based on (where available)
OID	Object Identifier
LDAP Syntax	The LDAP syntax of an attribute, see [RFC4517], "Directory String" and "Postal Address" are the most often used syntaxes, they both use UTF-8 encoding.
# of values	single or multi
Example values	Example values in the LDIF format, see [RFC2849]

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3.1 Surname

Name	surname
Description	Surname or family name
Vocabulary	not applicable, no controlled vocabulary
References	[RFC4519], [eduPerson]
OID	2.5.4.4
LDAP Syntax	Directory String
# of values	single (multi in [RFC4519], see notes)
Example values	Mwanza Zulu

Description
This is the X.500 surname attribute, which contains the family name of a person. The [eduPerson] specification says: 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.

Notes

- Within FIDERN Federation, home organizations MUST provide a single value only: the surname which is used for official communication with that person.

3.2 Given name

Name	givenName
Description	Given name of a person

Vocabulary	not applicable, no controlled vocabulary
References	[RFC4519], [eduPerson]
OID	2.5.4.42
LDAP	Syntax Directory String
# of values	single (multi in [RFC4519], see notes)
Example values	Jane Peter

Description
The givenName attribute is used to hold the part of a person's name which is not their surname. The [eduPerson] specification says: 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.

Notes
- Within FIDERN Federation, home organizations MUST provide a single value only: the given name which is used for official communication with that person.

3.3. Display Name

Name	displayName
Description	Preferred name of a person to be used when displaying entries
Vocabulary	not applicable, no controlled vocabulary
References	RFC2798
OID	2.16.840.1.113730.3.1.241
LDAP Syntax	Directory String
# of values	multi
Example values	Jane Mwanza Peter Zulu

Description
A single string value indicating the preferred name of a person to be used for display purposes, for example a greeting or a descriptive listing.

3.4. Principal name

Name	eduPersonPrincipalName
Description	A scoped identifier for a person. It should be represented in the form"user@scope" defines a local security domain. Each value of 'scope' defines a namespace within which the assigned identifiers MUST be unique. Given this rule, if two eduPersonPrincipalName (ePPN) values are the same at a given point in time, they refer to the same person.
Vocabulary	not applicable, no controlled vocabulary
References	[eduPerson]
OID	1.3.6.1.4.1.5923.1.1.1.6

LDAP Syntax	Directory String
# of values	single
Example values	hputter@hsww.wiz

Description
EPPN is the eduPerson equivalent of a username. It typically has most of the properties usually associated with usernames (such as uniqueness and a naming convention of some sort), with the added property of global uniqueness through the use of a scope. An application that tracks information based on it can therefore interact with users via any number of identity providers without fear of duplicates, although the possibility for recycling/reassignment does still exist within the domain of a given identity provider.Note that at some Identity Providers a user can freely change their local account name (in the case of a name change due to marriage, for example), and the corresponding EPPN will typically change as well. This can cause a loss of service until name changes propagate throughout every application storing the value.

Notes
- Syntactically, ePPN looks like an email address but is not intended to be a person's published email address or be used as an email address. In general, namebased identifiers tend to be subject to some degree of expected change and/or reassignment.
- Could be equivalent to userPrincipalName.

3.5. E-mail address

Name	mail
Description	Preferred address for the "To:" field of e-mail to be sent to this person
Vocabulary	not applicable, no controlled vocabulary
References	[RFC5321]
OID	0.9.2342.19200300.100.1.3
LDAP Syntax	IA5 String {256}
# of values	multi
Example values	peter.mwanza@education-instititon.zm dumbledore@hsww.wiz

Description
The 'mail' attribute type holds Internet mail addresses in Mailbox [RFC5321] of the form.
Mailbox = Local-part "@" Domain

Notes
- For purposes of the FIDERN Federation, the correctness of this attribute can not be guaranteed by the home organization since mailboxes may be changed by the user without informing the home organization (private mailboxes). If a person has more than one e-mail address, it is recommended to provide a single address only (the address used by the home organization itself when sending e-mails to that person).

3.6 Home organization

Name	schacHomeOrganization
Description	The fully qualified domain name of the person's organisation.

Vocabulary	Domain name according to RFC 1035
References	SHAC
OID	1.3.6.1.4.1.25178.1.2.9
LDAP Syntax	Directory String
# of values	single
Example values	university.ac.zm college.edu.zm

Description
The 'schacHomeOrganization' attribute specifies DNS name that is associated with the institution.

3.7. Affiliation

Name	eduPersonAffiliation
Description	Type of affiliation
Vocabulary	faculty, student, staff, alum, member, affiliate, employee, library-walk-in
References	[eduPerson]
OID	1.3.6.1.4.1.5923.1.1.1.1
LDAP Syntax	Directory String
# of values	multi
Example values	student staff

Description
Specifies the user's relationship(s) to the home organization in broad categories such as student, faculty, employee, etc. (see controlled vocabulary).

The member affiliation MUST be asserted for people carrying one or more of the following affiliations: faculty or staff or student or employee. affiliate for eduPersonAffiliation indicates that the holder has some definable affiliation to the university not captured by any of faculty, staff, student, employee, alum and/or member. Typical examples might include event volunteers, parents of students, guests and external auditors. There are likely to be widely varying definitions of affiliate across institutions. Given that, affiliate is of dubious value in federated, inter-institutional use cases.

Library-walk-in: This term was created to cover the case where physical presence in a library facility grants someone access to electronic resources typically licensed for faculty, staff and students.

References

[eduPerson] EduPerson Object Class Specification (201203). EduPerson. Internet2 Middleware Architecture Committee for Education, Directory Working Group. 02.2016. http://middleware.internet2.edu/eduperson/ .

[RFC1035] Domain names—implementation and specification, November 1987 P Mockapetris - URL http://www. ietf. org/rfc/rfc1035.txt.

[RFC2119] Key words for use in RFCs to Indicate Requirement Levels. RFC 2119. IETF. March 1997. http://www.ietf.org/rfc/rfc2119.txt

[RFC2798] Definition of the inetOrgPerson LDAP Object Class. RFC 2798. IETF. April 2000. http://www.ietf.org/rfc/rfc2798.txt .

[RFC2849] The LDAP Data Interchange Format (LDIF) - Technical Specification. RFC 2849. IETF. June 2000. http://www.ietf.org/rfc/rfc2849.txt .

[RFC4517] Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules. RFC 4517. IETF. June 2006. http://www.ietf.org/rfc/rfc4517.txt .

[RFC4519] Lightweight Directory Access Protocol (LDAP): Schema for User Applications. RFC 4519. IETF. June 2006. http://www.ietf.org/rfc/rfc4519.txt .

[RFC5321] Simple Mail Transfer Protocol. RFC 5321. IETF. October 2008. http://www.ietf.org/rfc/rfc5321.txt .