Internet2 EduPerson

2nd TF-LSD meeting, Amsterdam, 2. February 2001

Peter Gietz

Peter.gietz@DAASI.de

Agenda

- EduPerson Working Group
- EduPerson Objectclass
- New developments
- What shall we do about it?

EduPerson WG bodies

- **Internet2 (www.internet2.edu)**
  - **Consortium led by > 180 Universities in cooperation with industry and government**
  - **20 WGs, 3 of Middleware Architecture Commitee for Education (MACE), 1: MACE-DIR**
- **EDUCAUSE (www.educause.edu)**
  - **International nonprofit association**
  - **Transforming education through information technology**
  - **1800 people from > 190 corporations (edu and a few coms) world wide**

EduPerson WG bodies contd.

- Net@EDU (www.educause.edu/netatedu)
  - Part of EDUCAUSE
  - Merger of:
    - Networking and Telecommunications Task Force (NTTF)
    - Federation of American Research Networks (FARNET)
  - EduPerson WG part of Net@EDU PKI efforts
- EduPerson WG
  - Members from Univ. of Wisconsin, Georgetown Univ., Univ. of Washington, MIT
  - Chair: Keith Hazelton (Univ. of Wisconsin)

Edu-Person WG Charter

- **Deliverables:**
  - **Proposed definition of an edu-Person object class, version 0.9**
  - **Explanatory documents**
  - **Schema registration / IETF standardization**
  - **Proposal for maintanance and update od edu-Person definition**

Edu-Person WG Charter

- inetOrgPerson (RFC 2798)
- plus additional attributes
- Needed to support:
  - Role-based access to services and resources
  - Anonymous access to licensed resources
  - PKI-enabled functions
  - X.509 certificate standard and extensions for educational environment

EduPerson OC definition

- **Structure:**
  - **Name**
  - **OID**
  - **Syntax**
  - **Semantics**
  - **Controlled vocabulary**
  - **Advice on**
    - **Usage, management and application context**
    - **Group and certificate-based access control**
    - **Indexing and update procedures**

InetOrgPerson Attributes

- **displayName, givenName, initials, uid, cn, sn**
- **telephoneNumber, facsimileTelephoneNumber, mobile, pager, homePhone**
- **homePostalAddress, postalAddress, postalCode, postOfficeBox, street**
- **ou, o, st, l**
- **Mail, labeledURI, description, jpegPhoto**
- **userCertificate, userSMIMECertificate**
- **preferredLanguage, seeAlso**

New attributes

- **eduPersonAffiliation (1.3.6.1.4.1.5923.1.1.1)**
  - **Relationship(s) to institution in broad categories:**
    - **Faculty, student, staff, alum, member, affiliate, employee**
    - **For „none of the above“: empty attribute**
    - **Only „member“ and „affiliate“ described**
    - **„a reasonable person should find the listed relationships commonsensical“**
  - **Usage: Dir of Dirs, WP, access control**
  - **Syntax: CIS, multivalue**
  - **Indexing pres, eq, sub**

New attributes contd.

- **eduPersonPrimaryAffiliation (1.3.6.1.4.1.5923.1.1.5)**
  - **Primary relationship to institution in broad categories**
  - **(same as eduPersonAffiliation)**
  - **Usage: Dir of Dirs, WP, access control**
  - **Syntax: CIS, singlevalue**
  - **Indexing pres, eq, sub**

New attributes contd.

- **eduPersonAlternateName (1.3.6.1.4.1.5923.1.1.2)**
  - **Persons nickname**
  - **Self-maintained attribute**
    - **hence not additional cn**
    - **But: „editorial oversight advisable“**
  - **Usage: Dir. Of Dirs., WP**
  - **Syntax: CIS, multivalue**
  - **Indexing: pres, eq, sub**

DAASI International
Directory Applications for Advanced Security and Information Management

New attributes contd.

- eduPersonPrincipalName (1.3.6.1.4.1.5923.1.1.6)
  - „NetID“ of the person
    - for inter-institutional authentication
    - Shoud be stored in the form: user@univ.edu
    - Authentication ID for local services
    - Local authentication systems should be able to affirm (to local and remote applications) this ID
    - Uid use is not prescribed sufficiantly precise and consistent for cross domain authorization
  - Usage: controlling access to resources
  - Syntax: CES, singlevalue
  - Indexing: pres, eq, sub

New attributes contd.

- **eduPersonOrgDN** (1.3.6.1.4.1.5923.1.1.3)
  - „DN of the directory entry representing the institution with which the person is associated“
  - For efficient lookup in the institutions directory
  - „We recommend using the attribute searchGuide“ since Org doesn‘t include labeledURI
  - Usage, DoD, WP
  - Syntax: CIS [SIC!], singlevalue
  - Indexing: none

New attributes contd.

- **eduPersonOrgUnitDN** (1.3.6.1.4.1.5923.1.1.3)
  - **„DN of the directory entry representing the person‘s Organizational Unit(s)“**
  - **For efficient lookup for information on OUs**
  - **„We recommend using the attribute searchGuide“ since OU doesn‘t include labeledURI**
  - **Usage, DoD, WP**
  - **Syntax: CIS [SIC!], multivalue**
  - **Indexing: pres, eq, sub**

searchGuide

- X.521, 5.5.2
  - information of suggested search criteria
  - For entries that are convenient base-objects for the search operation (e.g.: C or O)
  - Includes:
    - Optional objectclass id for type of object sought
    - Search criteria for constructing filters:
      - attribute types
      - logical operators
      - matching level
  - 5.5.3 enhancedSearchGuide
    - adds search depth (base, one, sub)

searchGuide

- **LDAP RFC 2256 5.15, 5.48, 6.2, 6.3**
  - **For use by X.500 clients in constructing search filters**
  - **enhancedSearchGuide obsoletes searchGuide**

searchGuide contd.

- **EduPerson WG proposal** (axle.doit.wisc.edu/~haz/mware/eduPerson/eduPerson%20OrgRelated.pdf)
  - **replace syntax by labeledURI**
  - **Use not only as ldap filter**
    - **(e.g., ldap://host:389/basedn?attrs?depth?(filter)**
  - **But also for web URLs**
    - **(e.g., http://www.univ.edu)**
- Newest development:
    - **We have opted not to redefine searchGuide**
    - **Going with the labeledURIobject**

EduPerson FAQ

- Basic Questions
- Technical Issues
  - Only a pointer to The LDAP Recipe document
- Policy Issues
  - Technical details
  - Data management issues
- Process Issues
  - „Characteristics of eduPerson will be dynamic“

General remarks

- V 1.0 Dec 3, 2000 still looks very incomplete
  - Flaws (CIS instead of DN), Typos
  - Some wordings unspecific
  - „commonsensical“ as argument
  - No formal definitions (ASN.1 or
- V 0.9 was sent out to the world for comments, but not to Europe
- V 1.0. Jan 22, 2001 not yet published

What shall we do about it?

- Give comments to V1.0 Dec. 3, 2000
- Wait for V 1.0 Jan 22, 2001 to comment
- Specify own EUEduPerson (project?)
  - Look at other specs, e.g.:
    - NIH nihInetOrgPerson (www.alw.nih.gov/amgtech/docs/schema/current.html)
    - IBM ePerson (www.as400.ibm.com/ldap/schema)
- Try to co-work on V 2.0