

A Reference Schema for LDAP-based Identity Management Systems

Frank Tröger

`frank.troeger@rrze.uni-erlangen.de`

Regional Computing Center Erlangen (RRZE)

Department of Computer Science 6
Friedrich-Alexander University of Erlangen-Nuremberg

1st International Conference on LDAP



Project IDMonE

IDMonE



The project IDMonE aims at reconstructing the existent user management.

- Novell as the solution partner
- LDAP is the key technology
- One task: **schema design for metadirectory**



Four Steps of Schema Design

- 1 Locate application, standard and directory vendor-provided schemas
- 2 Choose other predefined schema elements
- 3 Develop schema extensions
- 4 Document the whole schema design



Step 2 – Choose other predefined schema elements

Provides a basis for a decision through . . .

- 1 gathering information about existing LDAP schemas
- 2 consolidating gathered LDAP schemas

Problems

- multiple schemas define equivalent elements
- own schema extensions apply better



The Idea of a Reference Schema

Idea – What is it?

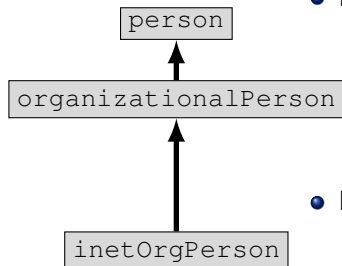
- **IDM-related** reference schema
- focus on higher education
- one place for
 - ▶ finding public schemas
 - ▶ comparing public schemas
 - ▶ derivating own schema extensions



Standard Schemas defined by RFCs

White Pages Schema

A basis for many other so called white pages schemas.



- RFC 2256

- ▶ “A Summary of the X.500(96) User Schema for use with LDAPv3”
- ▶ provides a basic set of attributes
- ▶ defines `person`, `organizationalPerson`, et al.

- RFC 2789

- ▶ “Definition of the `inetOrgPerson` LDAP Object Class”
- ▶ found in most user management directories
- ▶ defines `inetOrgPerson`, et al.



Middleware Arena

Two schemas with rather generic characteristics.

- Internet2 – MACE-Dir: eduPerson
 - ▶ de facto standard in higher education
 - ▶ focus on the U.S. → still attributes missing
 - ▶ defines `eduPerson`, et al.
- TERENA – TF-EMC2: SChema Harmonisation Committee (SCHAC)
 - ▶ Task Force European Middleware Coordination and Collaboration
 - ▶ refers to `inetOrgPerson` and `eduPerson`



Higher Education

Schemas for a single domain of purposes.

- WA Libraries Authentication Project (WALAP)
 - ▶ extensive use of subtypes
- Integrierende Benutzer- und Ressourcenverwaltung an den Thüringer Hochschulen (Codex – Meta Directory)
 - ▶ good documentation
- Higher Education Information System (HIS)
 - ▶ deployed in the majority of German universities



Step 2 – Choose other predefined schema elements

Provides a basis for a decision through ...

- 1 Gathering information about existing LDAP schemas ✓
 - ▶ sources and tools available
 - 2 Consolidating gathered LDAP schemas
 - ▶ available tools provide no help
-
- This drawback should be eliminated as part of the IDMone project in the sector of identity management.
 - Perhaps in collaboration with already existing tools.



A Reference Schema

What is it not?

- not yet another schema
 - ▶ already enough schemas available
 - ▶ no unique schema for all circumstances
- not a general purpose schema

What is it?

- IDM-related reference schema
- an assistance for directory architects in
 - ▶ finding public schemas
 - ▶ comparing public schemas
 - ▶ getting an overview



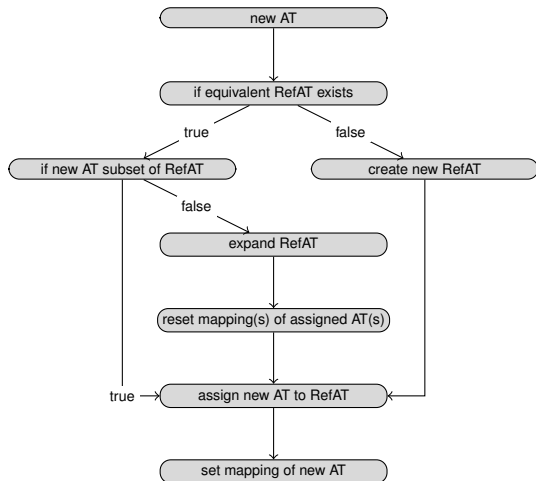
Reference Schema – Basics

- attribute-based, object classes are not considered
 - ▶ no problem in most cases
 - ▶ either structural with `inetOrgPerson` as superior
 - ▶ or auxiliary
- matching rules are not taken into account
 - ▶ subordinate in the decision process

The reference schema emerges from integrating attribute types of existing schemas.



Method of Integration



At Present each step is executed manually.



Categories

- 1 Personal Characteristics
- 2 Contact / Local Information
- 3 Student Information
- 4 Employee Information
- 5 Linkage Identifiers / Foreign Keys
- 6 Entry Metadata / Administration Information
- 7 Security Attributes and Keys
- 8 Confidentiality / Attribute Release (Visibility)
- 9 Authorization, Entitlements
- 10 Group-related Attributes
- 11 Other Miscellaneous Attributes

helps in

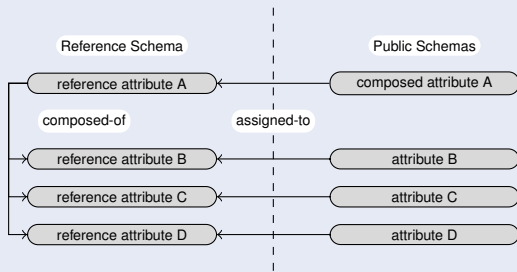
- locating the searched for attribute
- giving a first anticipation about the semantics



Single-valued vs Multi-valued & Atomic vs Decomposable

- Single-valued vs Multi-valued
 - ▶ if at least one attribute is multi-valued → reference attribute is multi-valued
 - ▶ exceptions: attribute that are single-valued by nature
- Atomic vs Decomposable
 - ▶ handle composed attributes

A Composed Attribute



Mapping – Basics

At present all mappings are described informal.

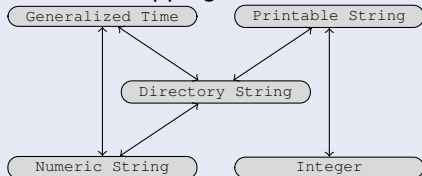
- reference schema is always a superset
- reference schema \leftarrow public schema: lossless
- reference schema \rightarrow public schema: possible with loss



Mapping – Directory Syntax & Additional Constraints

Directory Syntax

occurred mappings:



Additional Constraints

- rule-based constraints (proprietary or RFCs)
- controlled vocabularies (enumeration types)



Usage and Examples – Date Of Birth

Example (Date Of Birth)

- single-valued
- lossless mapping

s	single-valued	Reference Schema	WALAP	Codex	HIS	eduPerson	SCHAC
	composed						
	loss						
		Date Of Birth		X	X		X

- Codex: YYYY-MM-DD (Directory String syntax; RFC 3339)
- SCHAC: YYYYMMDD (Numeric String syntax)
- HIS: YYYYMMDD00Z (Generalized Time syntax; 00Z is constant)



Usage and Examples – Affiliation

Example (Affiliation)

- “controlled vocabulary”
- mapping with loss

single-valued		Reference Schema	WALAP	Codex	HIS	eduPerson	SCHAC
composed							
loss							
s		Date Of Birth		X	X		X
	loss	Affiliation	(X)	(X)		(X)	

- WALAP: student, staff, others
- Codex: Mitarbeiter, Student, Bibliotheksbenutzer, Gast, Alumni
- eduPerson: faculty, student, staff, alum, member, affiliate, employee



Conclusions

Summary

The **reference schema** supports the reuse of common schema elements and provides mappings for locally adapted ones.

- Outlook
 - ▶ formal mapping of equivalent attributes
 - ▶ translate values automatically on the fly



Reference Schema Online

Reference Schema

A pilot service is linked on the project's website.

Project's Website

<http://www.rrze.uni-erlangen.de/forschung/laufende-projekte/idm.shtml>

Mailingliste

send subscribe to

`refschema-request@rrze.uni-erlangen.de`

