The way to IdM at uma.es

Identity Management Workshop

Victoriano Giralt

Central Computing Facility
University of Málaga, Spain

Chişinău, Replublic of Moldova
May, 15th 2007

The corporate directory
is
the cornerstone
for
the middleware infrastructure

Overview

1. Past
   - Preliminaries
   - Design
   - Research work

Overview

1. Past
   - Preliminaries
   - Design
   - Research work
2. Present
   - Data load
   - Applications
   - Mailsystem redesign

Overview

1. Past
   - Preliminaries
   - Design
   - Research work
2. Present
   - Data load
   - Applications
   - Mailsystem redesign
3. Future
   - Classifications
   - Tree stabilising
   - Evolving the schema

Coordinated work

Joining efforts and seeding

Our main aim was that our work could be useful to others.

Coordinated work

Joining efforts and seeding

Our main aim was that our work could be useful to others.

- Esquema IRIS (Spanish coordinated schema effort)
- Schema comitee
- TF-EMC^2
- SCHAC

Tree structure and attributes

On pine trees, bonsais and forests

Main points of our Directory Information Tree design

Tree structure and attributes

On pine trees, bonsais and forests

Main points of our Directory Information Tree design

- Shallow tree

The fewer the branches, the fewer the problems

One branch for each kind of object with a reduced count, greatly simplifies administration. Above all, objects do not usually change kind.

Tree structure and attributes

On pine trees, bonsais and forests

Main points of our Directory Information Tree design

- Shallow tree
- One branch for persons

Persons are persons

Regardless of their relationship to the University at a given moment in time. And they often have more than one kind of relationship.

Tree structure and attributes

On pine trees, bonsais and forests

Main points of our Directory Information Tree design

- Shallow tree
- One branch for persons
- Classifications

Overlaid hierarchies

The use of classification codes allows an object to be at different places in different hierarchies and even in the same hierarchy.

Tree structure and attributes

On pine trees, bonsais and forests

Main points of our Directory Information Tree design

- Shallow tree
- One branch for persons
- Classifications
- Privacy

Opaque DNs

Opaque data are used to build DNs that can't be associated to the persons described in the directory entries, in order to avoid privacy *leaks*: idnc,dc=uma,dc=es, idnc being an UUID we produce when the entry is created.

Tree structure and attributes

On pine trees, bonsais and forests

Main points of our Directory Information Tree design

- Shallow tree
- One branch for persons
- Classifications
- Privacy

I own my data

We designed the privacy attribute, now schacUserPrivateAttribute, to allow users control on publishing of certain publically accesable information.

Tree structure and attributes

On pine trees, bonsais and forests

Main points of our Directory Information Tree design

- Shallow tree
- One branch for persons
- Classifications
- Privacy
- Authorisation

Who does what

Granting privileges through URNs allows for fine grained control of access levels, both for persons to applications and for applications to persons data.

Source identification

Are all bases covered?

We know for certain were all data about our University members are

Source identification

Are all bases covered?

We know for certain were all data about our University members are, don't we?

Source identification

Are all bases covered?

We know for certain were all data about our University members are, don't we?

- Staff.

Source identification

Are all bases covered?

We know for certain were all data about our University members are, don't we?

- Staff. Researching staff?

Source identification

Are all bases covered?

We know for certain were all data about our University members are, don't we?

- Staff. Researching staff? Really fashionable

Source identification

Are all bases covered?

We know for certain were all data about our University members are, don't we?

- Staff. Researching staff? Really fashionable
- Faculty.

Source identification

Are all bases covered?

We know for certain were all data about our University members are, don't we?

- Staff. Researching staff? Really fashionable
- Faculty. Scholarships?

Source identification

Are all bases covered?

We know for certain were all data about our University members are, don't we?

- Staff. Researching staff? Really fashionable
- Faculty. Scholarships? Paid by

Source identification

Are all bases covered?

We know for certain were all data about our University members are, don't we?

- Staff. Researching staff? Really fashionable
- Faculty. Scholarships? Paid by whom?

Source identification

Are all bases covered?

We know for certain were all data about our University members are, don't we?

- Staff. Researching staff? Really fashionable
- Faculty. Scholarships? Paid by whom? . . .

Source identification

Are all bases covered?

We know for certain were all data about our University members are, don't we?

- Staff. Researching staff? Really fashionable
- Faculty. Scholarships? Paid by whom? . . .
- Students.

Source identification

Are all bases covered?

We know for certain were all data about our University members are, don't we?

- Staff. Researching staff? Really fashionable
- Faculty. Scholarships? Paid by whom? . . .
- Students. Graduate?

Source identification

Are all bases covered?

We know for certain were all data about our University members are, don't we?

- Staff. Researching staff? Really fashionable
- Faculty. Scholarships? Paid by whom? . . .
- Students. Graduate? Foreign?

Source identification

Are all bases covered?

We know for certain were all data about our University members are, don't we?

- Staff. Researching staff? Really fashionable
- Faculty. Scholarships? Paid by whom? . . .
- Students. Graduate? Foreign?
- Emeriti
- Affiliates
- Unclassifiables

Source identification

Are all bases covered?

We know for certain were all data about our University members are, don't we?

- Staff. Researching staff? Really fashionable
- Faculty. Scholarships? Paid by whom? . . .
- Students. Graduate? Foreign?
- Emeriti
- Affiliates
- Unclassifiables

Who . . . does this address belong to?

External data maintenance

Perennial tree

Entries are created, but never destroyed.

External data maintenance

Perennial tree

Entries are created, but never destroyed.
(except for blatant errors).

External data maintenance

Perennial tree

Entries are created, but never destroyed.
(except for blatant errors).

- Status transitions

Entries evolve

We load directory stored data changes as transitions from a previous state to a new one.

External data maintenance

Perennial tree

Entries are created, but never destroyed.
(except for blatant errors).

- Status transitions
- SQL *Triggers*

Sytems of record log their changes

Functions and triggers have been programmed to log the changes that the SoRs make to data that affect the directory. This log is stored into a state transition table that keeps the same data for all persosns, but with different states for each system.

External data maintenance

Perennial tree

Entries are created, but never destroyed.
(except for blatant errors).

- Status transitions
- SQL *Triggers*
- The linkage problem

Linking entries to their origin

A unique code that links directory entries to the registers in the various systems of record is fundamental.

The IRIS schema lacked a proper solution to this, but it is properly dealt with in SCHAC.

Changes in authentication methods

The directory as the authorisation centre

This is the way to a real Authentication and Authorisation Infrastructure.

Changes in authentication methods

The directory as the authorisation centre

This is the way to a real Authentication and Authorisation Infrastructure.

- Web applications

Old applications

We have developed a classic web authentication mechanism for our web server, that validates against the directory, similar to Apache mod_authz_ldap, which allows applications to run unmodified.

Changes in authentication methods

The directory as the authorisation centre

This is the way to a real Authentication and Authorisation Infrastructure.

- Web applications

New applications

New applications do authN and authR against the directory, as preliminary step for federation mechanisms.

Changes in authentication methods

The directory as the authorisation centre

This is the way to a real Authentication and Authorisation Infrastructure.

- Web applications
- Non web applications

Directory validation

Conventional applications like mailbox access, authenticated mail sending or wireless access, do direct validation against the directory, for a better usr experience.

The first big project

An owner for each mail address

This process has been key both to directory advancement as to data cleansing.

The first big project

An owner for each mail address

This process has been key both to directory advancement as to data cleansing.

- AA

Authenticate and Authorise

We have opted for virtual users, which bring some nice features and allow users to authenticate with any of their mail addresses.

It is used for mailbox access and mail sending through the University MTA.

The first big project

An owner for each mail address

This process has been key both to directory advancement as to data cleansing.

- AA
- Routing

Deliver mail to its recipient

The system is very flexible thanks to the use if mail routing recomendations from the IRIS schema.

The first big project

An owner for each mail address

This process has been key both to directory advancement as to data cleansing.

- AA
- Routing
- Storing

A permanent mailbox

Using the entryUUID to identify mailboxes associated to entries, instead of other attributes that may change, allows for moving and modifying entries at will without loosing track of the mail store.

Organise persons
in diverse ways

We are working in several classifications at present.

Organise persons
in diverse ways

We are working in several classifications at present.
Though, there is little automated information.

Organise persons
in diverse ways

We are working in several classifications at present.
Though, there is little automated information.

- White pages
- Departments
- Geographical location
- Subject areas

Not all branches are healthy

Time for prunning and grafting

We have been able to achieve a reasonable health in the persons branch.

Not all branches are healthy

Time for prunning and grafting

We have been able to achieve a reasonable health in the persons branch.
There is still some work to do on branches with non-person entries.

Not all branches are healthy

Time for prunning and grafting

We have been able to achieve a reasonable health in the persons branch.
There is still some work to do on branches with non-person entries.

- Clear definitions of University roles.
- Place non-person entries at their final locations.
- Delete the transient branches.

Schemas are not static

like wine, they improve with time

Our aim is to apply new development we deem valuable.

Schemas are not static

like wine, they improve with time

Our aim is to apply new development we deem valuable.

- We are transitioning from iris* to SCHAC, were applicable.
- Improve authorisation management. eduPermissions?
- We are worknig on a URN registry.

Summary

- The directory is the liveliest of the services

Summary

- The directory is the liveliest of the services, the never ending project.

Summary

- The directory is the liveliest of the services, the never ending project.
- Persons are persons.

Summary

- The directory is the liveliest of the services, the never ending project.
- Persons are persons.
- The directory can be organised in may ways through classifications.