



# From LDAP to IdM

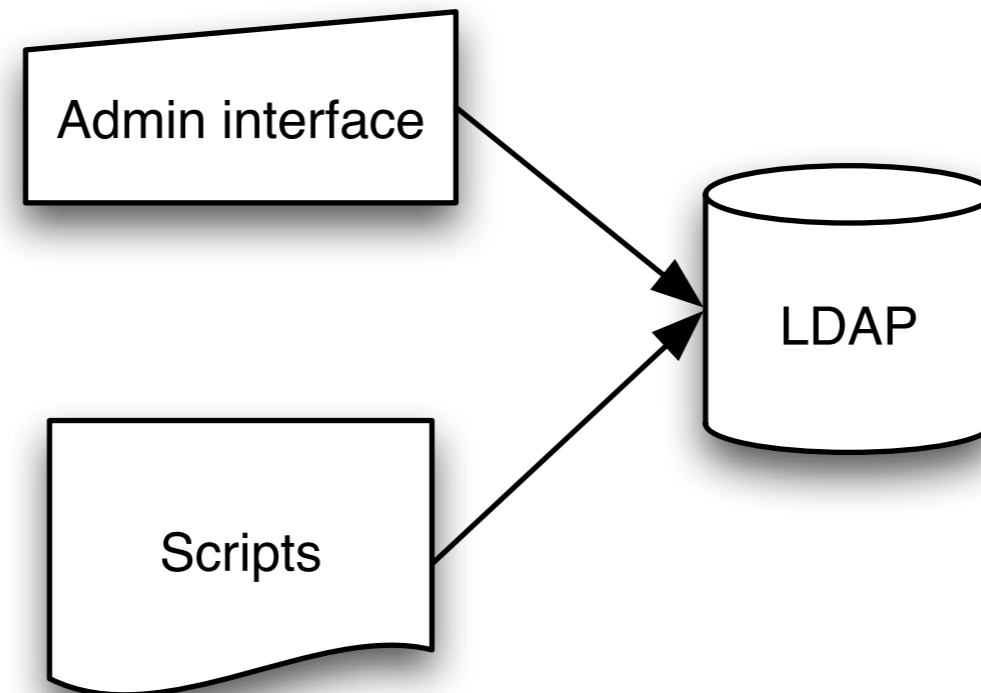
Presentation at the Athens Eurocamp 2008

by Roland Hedberg

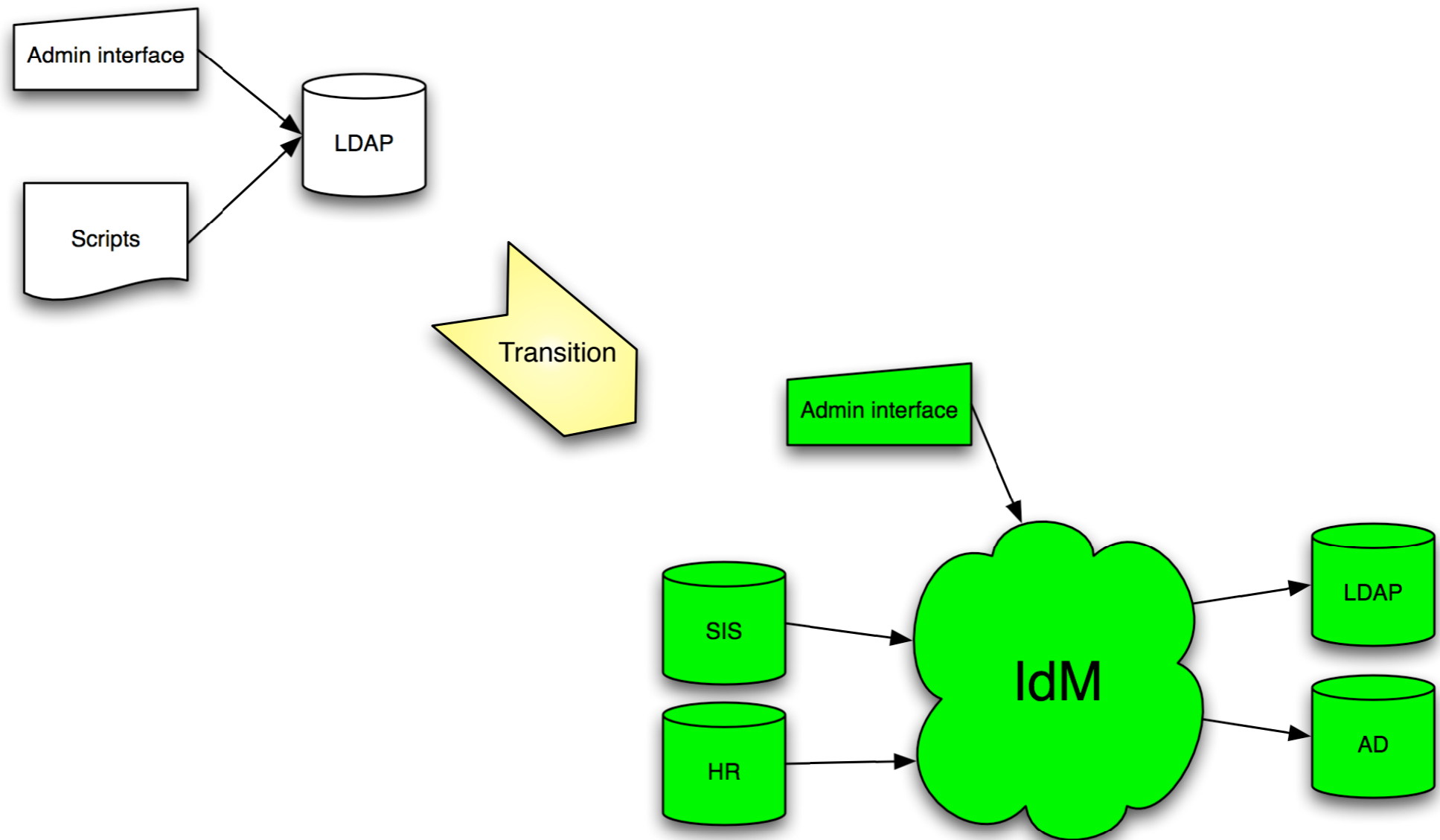
<roland.hedberg@adm.umu.se>



# The transition -starting point



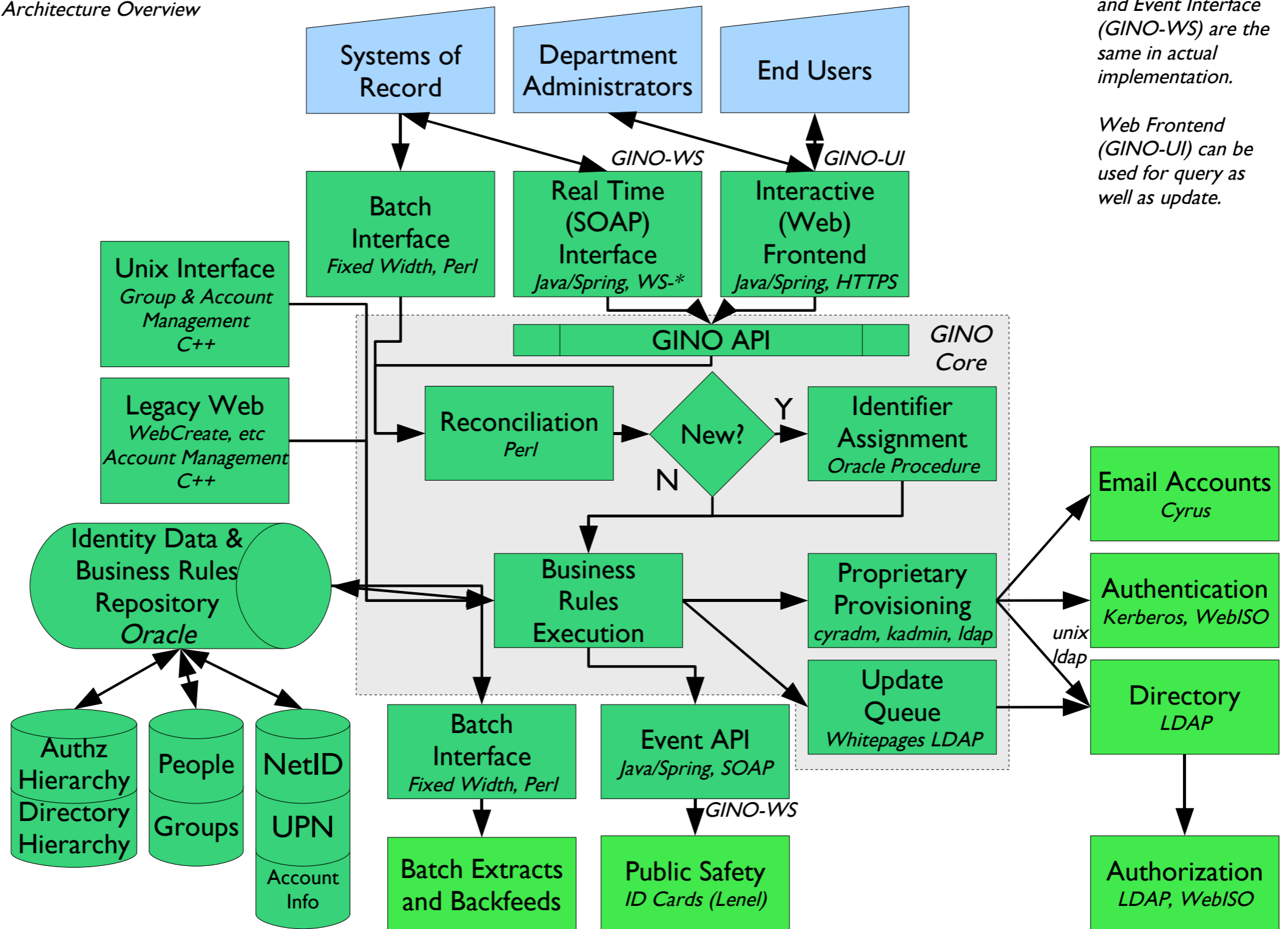
# The transition - toward nirvana





# Columbia University Identity Management (May 2008)

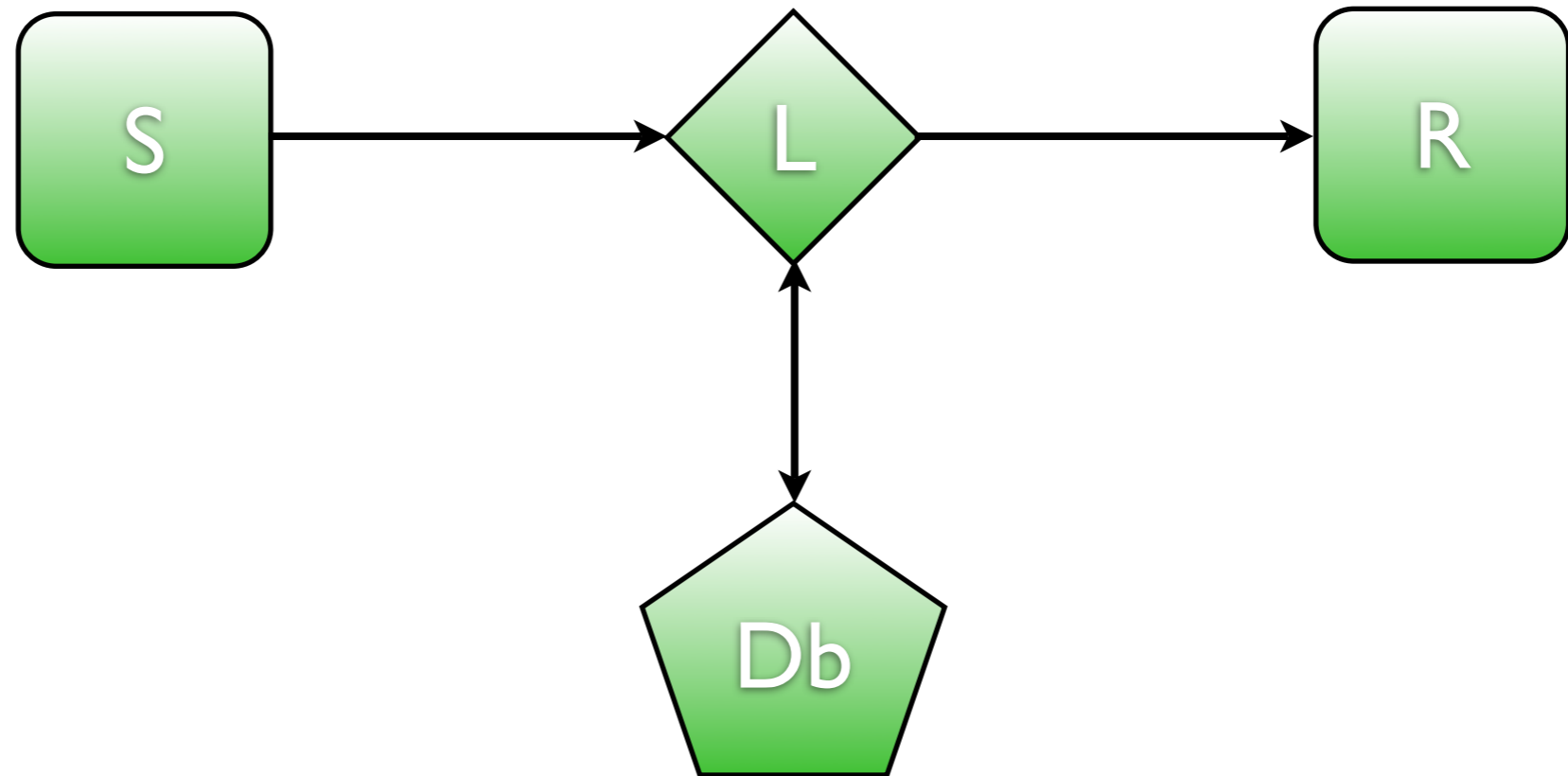
## Architecture Overview



Real Time Interface and Event Interface (GINO-WS) are the same in actual implementation.

Web Frontend (GINO-UI) can be used for query as well as update.

# The basic model





# What's IdM ?

“Identity management is the management of the identity life cycle of entities.”

Establish → Describe → Destroy



# Where the big challenge is !

Establish → **Describe** → Destroy





# Francis Bacon

1561-1626

- knowledge of the essence of things
  - the way things really are
- Ideals of the mind
  - ideal of the tribe (human nature)
  - ideal of the cave (hobby horse, prejudice)
  - ideal of the market place (social interaction, language)
  - ideals of the theater (learned)



# Ontology

Ontology deals with questions concerning what entities exist or can be said to exist, and how such entities can be grouped, related within a hierarchy, and subdivided according to similarities and differences

# Data models

- LDAP
- Ontology language (OWL)

# LDAP

- Object class
  - set of must/may attributes
- Attribute
  - value type
  - $\leq 1$  or  $\geq 0$
  - size
- Object relationship
  - DIT
  - seeAlso, Alias, ...

# LDAP limitations

- Simple inheritance
- You can not have objects as values
- No value sets
- *No meta-information*



# OWL

## Web Ontology Language

- Object classes
  - set of properties
  - property restrictions
- Properties
  - domain / range
- Multiple inheritance
- Version control
- ontology meta information

# Our present model

## • Basic objects

- person, collection, unit, user, course, ...

## • Relation objects

- employee, student, partOf, belongsTo, ...

# The information

## • Who owns it ?

- Responsibility
- Accountability
- Stability

## • What does it mean ?

- Special / Universal
- Usage uncoupled from definition

# Leads up to

- Information services
- Service definitions

# Business rules

## • Examples

- Life cycles
- Source priorities
- Value construction algorithms
- Object matching/reconciliation
- Harmonization

## • Features

- Declarative
- Atomic
- Distinct, independent

# Repositories

## • Identifiers

- Any identifier an object has ever had

## • State

- The complete state of an object

## • Messages

- All messages ever seen by the system

# Views

- Different applications - different needs
  - \* There are so many ways of doing things, that we can not mandate one.
    - LDAP/AD
    - WS
    - Provisioning
  - \* Transformation between data models



# Information security

## • Confidentiality

- Ensuring that information is accessible only to those authorised to have access

## • Integrity

- Data cannot be modified without authorisation

## • Availability

- the information must be available when it is needed

## • Correctness/Coherence



**That's it !**  
**Questions ?**