

The Role of an AAI in Campus System Integration



+46705778807

Torbjörn Wiberg
CIO, Umeå Universitet

EuroCAMP, Ljubljana 060403

The Reason to Deploy an AuthN and AuthZ Infrastructure - AAI



☞ The introduction of web interfaces to applications, and of self services, drives the cost of user management up into the sky!

☞ This fact alone motivates an AAI!

☞ By the way:
An AAI shall provide

- ☞ Authentication
- ☞ Authorization and
- ☞ Enterprise information (Attribute Release)

☞ services to the university and its partners

Electronic Identity

Planning for a new study programme



- Programme planning committee
 - eMail account, project "wiki"
 - meeting room
- New courses - Course spec group
 - draft, processed
- Planning committee suggests a new programme
- Project Support System
- eMail List Server
- Facilities Reservation System
- Financial system
- Calendar server,
- Course Specification System
- possibly with external
- Content Management System
- Workflow System
- Goal Systems for publishing
- ...

Electronic Identity

Observations



- A lot of systems involved, perhaps 50
 - There is a need to share data between them
- A lot of users
 - it could be "anyone"
- ... mostly simple self service privileges
 - if you are a member of ...
- The involved applications need
 - AuthN, AuthZ and Attribute Release Services

Electronic Identity

We need an AAI



- ☛ Identity management for networked entities
 - ☛ people, systems, org. units, courses, projects
- ☛ AuthN
 - ☛ Single signon through a webiso
 - ☛ AuthN of communicating entities - certificates
- ☛ Privilege management
 - ☛ Mgmt of privilege info shall be done by those who have the authority to delegate or appoint

Electronic Identity

We need an AAI ... cont



☞ AuthZ

- ☞ when ids are centralised the implicit right to use a system has to be replaced by explicit access control
- ☞ to keep costs of privilege mgmt down, most authz has to be based on general enterprise information

Electronic Identity

Expected Results



- Lower costs for user mgmt (80kEur/yr -> 20)
- Better control of who is a user with what rights in our systems
- Cheap to build and deploy simple enterprise applications

... if you can formulate your
business rules!

- ☞ What defines an active student?
- ☞ How is an organisational unit established?
- ☞ What authority has a guest professor, or a professor on sabbatical?
- ☞ What happens when you no longer have an employment contract?
- ☞ ...

Electronic Identity

We are reengineering our business processes



- ☞ IT support for a process invariably results in a "need" to use the AAI
- ☞ Cheap to adapt a system to use the webiso
 - ☞ 28-40 hours
- ☞ Expectation to add system specific information to the enterprise repository
 - ☞ discuss how enterprise data can be used
- ☞ Expectation to be in the meta directory

Electronic Identity

We are in the middle of all this!



☞ I am not here alone

☞ Magnus Andersson, Magnus Söderlund, and Roland Hedberg are also here

☞ We are trying to agree on a component based national Meta Directory reference model

☞ There is no rational reason why we shall use different approaches

☞ Pål Axelsson, Roland Hedberg are also here

☞ See swami.se

Electronic Identity MetaDirectory Architecture

