# Infraservices – Core Middleware Enablers of eBusiness

2005-09-21

Torbjörn Wiberg
CIO, UmU

## Swedish Higher Education

- About 15 institutions with a "Faculty of…"
- About 20-25 other higher ed institutions
- Around 350-400k students
  - Around 50% in the 6 biggest universities
- Around 65k personnel

## Increased Self-Service and Electronic Workflow

- Two general trends can be observed:
  - there is an increase in Self-Service in our IT Applications
  - non-specialist users are active in electronic workflow
- These trends tend to make all our students and/or all our personnel (non-specialist) users of more and more of our systems
  - Managing some Directory Information
  - Tur och Retur (travel expenses)
  - Ladok på webb (student records)
  - Nya (national student admittance system)
  - Diariet (workflow for formal business)
  - Personal portals
  - eInvoices
  - Salary specifications
  - Reservation of Seminar rooms
- It is accelerating!

## Vision

- My vision is that the AAI shall provide a functionality that facilitates the following scenarios:
  - A student that visits another European campus shall, after being authenticated by his home authentication service be authorised to use basic services at the campus he visits
  - A student at another european campus shall after registering as a student on a course at our campus have the same authorisation to use learning mgmt system and portals
  - A group of researchers from european universities working on a common project shall, based on their home eID, be given authorisation to use collaboration resources at member universities
  - A newly appointed chairman of a department shall automatically be given authority to access information about her department in our business systems
- These are also the scenarios setting the ambition for the AAI parts of GN2, an FP6 project under negotiation with the commission

## How do we get commitment from Swedish HigherEd to go there?

- Provide Return of Investment material
  - Certificates, PKI, Smart Cards
  - Identity and Privilege Management
  - Externalising AA
- Offer education for management and technicians
- Work hard with coordination and harmonisation
  - Schemas: norEduPerson, norEduOrg, norEduCourse
  - fight the not-invented-here reactions
  - introduce a national roaming and initial logon service
- Suggest suitable Software
- Demonstrate of successful steps from early adopters
  - support and "use" early adopters as good examples
  - provide implementations/deployments to experiment with

## Federated Model for Authentication and Authorization

- I believe that eServices shall be based on a model where
  - Authentication shall be done by the home organisation
  - Authorizations may be given to members of virtual organisations belonging to a trusted Identity Federation
  - It should be possible to base the authorization decision on advice from the virtual orhganisation and/or the home organisation. (A resource may be allocated to a project but both the project manager and the user's home organisation may have an opinion on how the resource shall be allocated within the project)
- In order for this model to work
  - The concept of an identity and the corresponding assertion must harmonize over the federation and must be understood by the resource owner
  - The meaning and form of data or information services used for giving authority, must harmonize over the resource, virtual and home organisations
- This model is used in the Authentication and Authorization Infrastructure in GEANT2
- To succeed with eGov or other eBus we must make it possible to realize such a model

Electronic Identity

## We can not do it on our own

- National level
  - Codex-se – started as a group cooperating around uPortal
    - LiU, CTH, UmU, SU, UU, ÖU, KTH, (KI, LU)
  - Retreats – so far 7 workshops for initial experiments and piloting
    - CAS as an Authentication Service software for uPortal
    - implementation of Ladok på Webb service as a uPortal channel
    - SPOCP as Authorisation Service for Ladok på Webb
    - Development of initial logon protocol for Swedish HigherEd (Vision 11)
    - SU has developed cwaa – an implementation of the protocol
  - Thematic conferences - sofar 5(?) - on topics we want to know more about
  - Unitcf – platform to use for finding partners to work with in cooperative projects to develop software or other components of the infrastructure
    - SwUPKI, SPOCP, eID, norEdu..-schemas
  - OpenSource Software in the AAI and for general services (web, mail, portals, ...)
    - by using Open Source software we get access to code for adaptions
    - we can bring the result back into the OpenSource projects

Electronic Identity

## We can not do it on our own

- International level of harmonisation, coordination and project partnership
  - Gnomis
    - Nordic cooperation
    - Schema harmonisation
    - SPOCP
  - Terena task forces
    - TF-AACE (AA coordination in Europe)
    - TF-MOBILITY
  - FP6 projects – GN2
    - 4 year project
    - research network
    - AAI part: 2.8M€, 33 man years
    - Four areas
      - Roaming
      - Authentication and Authorization Infrastructure (AAI)
      - Single Sign-On (SSO)
      - Integration of advanced technologies (Nordunet)
  - Internet2's Middleware Initiative
    - Tae part in CAMPs (Campus Middleware Planning Workshops)

Electronic Identity

## The Components of an AAI

- An Enterprise Directory that supports the other components
  - Principals, Organisational Units and Resources
- An Identity Management System
- An Authentication Service with ...
- At least one Authentication Mechanism
  - User Name/Password
  - PKI Certificates
- A Privilege Management System
  - Information to base authority decisions on
  - Maintained by those with authority to delegate and appoint
- An Authorisation Service
  - Content Access Control and
  - General Authorisation
- (A Network Logon Service)