Electronic Identity

Infraservices – Core Middleware Status in Swedish Higher Education

Trefpunkt Karlshamn – 2005-04-20

Torbjörn Wiberg
CIO, UmU

Electronic Identity

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

Electronic Identity

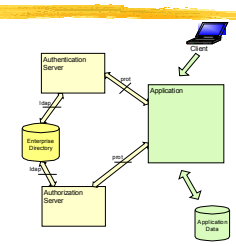
Increased Self-Service and Electronic Workflow

- 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 trend tends to make all our students and/or all our personnel (non-specialist) users of more and more of our systems. At UmU right now
  - 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!

Electronic Identity

Model Application

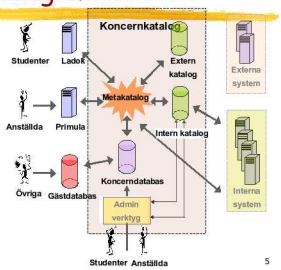
- Authentication and Authorisation is external to the application
- Service Oriented Architecture
- This is the application view
- There is also an
  - Identity management view
  - Privilege management view



Electronic Identity

The Identity Management View

- Centralised Accounts
- Synchronisation of identity information
- Internal and External Access to Identity Information



Electronic Identity

The Components of an AAI

- An Enterprise Directory (with a metadirectory) that supports the other components
  - Principals, Organisational Units and Resources
- An Identity Management System
  - Management of a datum
- 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)

Electronic Identity

Vi måste samarbeta!

- Samma problem hos alla
- Det är först när lösningarna harmonierar vi kan realisera scenarierna
  - Kataloginnehåll
    - hur representeras en identitet
    - hur ser man att en individ tillhör personalen
- Mycket genomgripande förändringar
  - Centralisering
  - Svår teknik
  - Anpassning av applikationerna

Electronic Identity

Vi måste samarbeta! ....

- Nationellt, i Norden, Europa med USA
  - 24h-myndigheten
  - Gnomis
  - GEANT
  - Internet2s middleware initiative
  - Vi har i Sverige och Norge har en stark ställning internationellt
    - SPOCP är tillsammans med ett engelskt auktorisationssystem de som övervägs
    - Internet2 deltar i mötena i europa

Electronic Identity

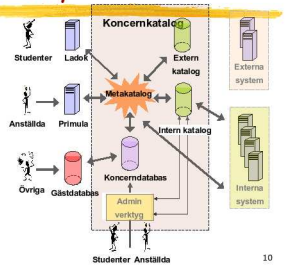
The Swedish Cooperation model

- It is a complicated field – we need a sustainable model
- Inner circle of experts that design and recommend an Infraservice Infrastructure Architecture.
- Cooperate within an alliance of higher ed institutions who is focused on deploying an Infraser... whose members
  - is the steering group
  - takes part in projects to reach the common goals
  - provides the alliance with development and deployment personnel
  - contributes to the maintenance of the components of the infrastructure
- Organise the work in projects with partners from the alliance and other higher ed institutions
  - the partners shall be prepared to contribute financially to the projects they participate in
  - results shall be available to higher ed (even internationally -> project documents in english)
- Invite "early adopters" who get support with deployment

Electronic Identity

The components of ONE Enterprise Directory

- Enterprise Information Repository
- Internal and External Access Directories
- Metadirectory
  - Synchronisation tool
- ID & Privilege Management Systems
- Philosophy: Offer directory supported services rather than allowing export of directory content



Electronic Identity

Enterprise Directory

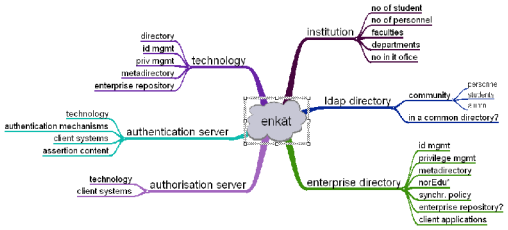
- More than a telephone book or an e-mail directory!
- Every person affiliated with the organisation shall be in the directory
  - Present the list to the dean and say: This is my personnel!
- Attributes of relevance for authorisation shall be registered
  - The maintenance shall reflect the delegation of responsibility
  - If for ex authority follows with being a chairman, the assignment of that attribute shall be done by those who appointed her
- A metadirectory synchronises data
- All information in the directory must not be available through an anonymous LDAP-request
  - Question: What attributes shall on what grounds be made available to what application (privacy issue, and organisational security issues)

Electronic Identity

Directories - Status

- Most higher ed institutions have some kind of directory
- Not many are enterprise directories (with a metadirectory and part of an AAI) though
  - 7? SU, ÖU, LU, LiU, UmU, UU?
  - Several deployment projects – KI, UU, UmU
  - Broader projects often
    - One user account per person
    - ID and Privilege Mgmt
- Schema harmonisation
  - Most are said to use norEdu...

Electronic Identity
Statusenkät planeras



Electronic Identity
Authentication Services - Status

- Homegrown, CAS, and Pubcookie (and Kerberos) are used
  - CAS dominates >5 and increases
  - I recommend that A-Select is tested as well as CAS

Electronic Identity
Authentication mechanisms - Status

- Username Password is the only one used
- PKI-based is planned as a pilot this year
  - Uppsala
  - Stockholm – initial signon to get a Kerberos ticket

Electronic Identity
SwUPKI - Status

- Club – around 7 members
- No person certificates yet
- SwUPKI2 is discussed
  - Self service based
  - More than one root (for different strengths)
- Certificate factory for certificates stored on Smart Cards to reasonable prices -3.5 €/yr

Electronic Identity
Authorisation

- **Authentication** – establishes identity to a certain strength
- **Authorisation** – controls what you may do
  - Policy Control, Access Control
  - Once authenticated, depending on the strength of the authentication and other information you will (not) be authorised to do …
- Authorisation – can be realised as a middleware service
  - Requires a high quality Enterprise directory to be really valuable
  - Can be implemented as a Server or an application Plug-in
- **Note!** - What from a simple application is considered authentication, is from an enterprise perspective an authorisation to use that application!

Electronic Identity
Authorisation Service - Status

- Shiboleth – will probably be used for authorisation with content providers
- Spocp
  - Stockholm univ largest users
  - Deployed in UmU but not widely used yet
  - Used in Directory deployment at KI and UmU
  - Used for message routing in UDS
- Other
  - Uppsala - AKKA

Electronic Identity

Network Logon – Status

- Wireless network logon
  - Several use web logon
    - requires access to the network – security risk?
    - Radius
  - 802.1x
  - CWAA –
    - Codex -> SU (Love Hörn...
    - It doesnt scale
- Eduroam
  - A european hierarchically structured interorganisational network logon pilot
  - .1x
  - We are not a member yet, but have started preparations and are waiting for some policy issues to be resolved
  - There are security issues as well

Electronic Identity

Development Projects

- Spocp
  - Authorisation service and Policy Engine
  - working with policy writing tools
  - redoing the documentation
- UDS
  - Roland Hedberg
  - Universal Data Dispenser
  - Meta Directory tool
- GEANT2 jra5
  - AAI, Roaming, Single Signon, Future Technologies

Electronic Identity

Interinstitutional AAIs

- Model for an AAI between organisations
  - Device: Authenticate at home and Authorise at the Resource institution
  - Need a trust fabric – Build an Identity Federation!
    - Federation Document
      - Who gets a user account
      - Harmonised identity information
      - Requirements of ID & Priv Mgmt procedures
      - Minimum Authentication strength
  - Implement Federation Services for AuthN and AuthZ

Electronic Identity

Infraservices – Core Middleware Status in Swedish Higher Education

Trefpunkt Karlshamn – 2005-04-20

Torbjörn Wiberg
CIO, UmU