


Electronic Identity

Status - AA Middleware Sweden




TF-EMC2, 3-4 november 2004

Torbjörn Wiberg
CIO, UmU

031216 T Wiberg, UmU 1

Electronic Identity

Trends and drivers




- More and more of our systems are critical for our business
- We get more and more small enterprise wide system
- "Every" student and "every" personnel is a user in "every" system
 - travel expenses, meeting room reservation, calendar, personal portal
- eBusiness is an every day reality in the private life for students, and they expect it to be the same at the university - high degree of eReadyness
 - bank, movie tickets, airline tickets -
 - apply for courses, sign up for tests, support for work in groups, look at results from tests, look at course schedules etc

031216 T Wiberg, UmU 2

Electronic Identity

Relevant Campus IT-strategies




- Centralise to increase efficiency and quality
 - ROI for central user administration after externalising authN, authZ at UmU shows that we will decrease our cost with 80%/year (from 1"€ to 0"2€)
 - <http://www.umu.se/it/personal/tvw/pub/> soon
 - provide services between universities
 - Certificate Service Provider
 - Operation of Student Administration
- Implement the Information society on UmU
 - paper, processes, work flow etc
- Cooperate in an organised manner with peers
- Use, contribute to and develop Open Source software

031216 T Wiberg, UmU 3

Electronic Identity

Relevant Campus IT Strategies




- Internal Information shall spread through personal portals
 - uPortal
 - calendar, webmail, collaboration tools, file storage
 - planning tools
 - services
- Electronic identities shall be introduced and used
 - ONE electronic identity
 - for resource objects and persons

031216 T Wiberg, UmU 4

Electronic Identity

How do I work with these strategies? For ex




- Introduce electronic identities that can be used in various systems (ONE eID)
 - Make sure they harmonise/interoperate
 - ... within Sverige, Norden, Europa, Nordamerika
- Cooperate around Infrservice software, harmonisaation, deployment and adaption of applications

031216 T Wiberg, UmU 5

Electronic Identity

Sunet has a contract with UmU



- ... to promote the introduction of a harmonised Infrservice-infrastructure in Swedish higher education institutions (från 040401)
 - preferably harmonising with Norden, Europe and USA as well
 - there are some scenarios we are striving for
- Our contract with Sunet will be increased from 2005

031216 T Wiberg, UmU 6

Electronic Identity

Scenarios to Support



- It shall be possible for
 - an employee from UmU visiting Oslo University to be given access to local resources (network, library ...) after being authenticated at home.
 - a student from Oslo University taking a course at UmU to, after registering on the course, automatically be given access to library data bases and be authorised to work in Ping-Pong, our LMS
 - the members of a cooperative project (between UmU and several other universities) to be authorised to work in our project support software
 - a newly appointed Prefekt to automatically be authorised to use our business systems in any way our delegation decision implies

031216

T Wiberg, UmU

7

Prerequisites for successful cooperation



- I mean that, in order to succeed, you shall only engage in projects where
 - the partners shall be prepared to contribute with money
 - you shall not expect to get the money back
 - the resulting software shall be freely available within our community
- I have run two projects according to this model
 - SwUPKI - a PKI club, open for Swedish higher education (the operation of the PMA and the PolicyCA is paid for as a member fee)
 - SPOCP - development of a policy based authorisation server

031216

T Wiberg, UmU

8

Model for work with the Sunet contract



- Work in projects to realise scenarios
- Set up a strategic alliance, between universities that commit to cooperate long term according to this model. Commitments:
 - Be part of the Steering Committee for the task
 - Contribute financially to the projects
 - Provide development and maintenance personnel for the projects
- Develop architecture and principal solutions using a group of experts

031216

T Wiberg, UmU

9

Model for work with the Sunet contract ...



- Offer other higher ed institutions to be partners in the projects or early adopters
 - with deployment support from the project
- Arrange conferences where experts, developers and deployers take part
- Create sustainable structures for maintenance of developed systems and adapters

031216

T Wiberg, UmU

10

Electronic Identity

Right now - what happens



- Web site - rudimentary
 - <http://www.umu.se/it/projupp/infratj/>
- Directory Day at Stockholms universitet 25 nov
 - One strategic and one technical track
 - <http://www.umu.se/it/projupp/infratj/konf>
- Working group to suggest undisputable set of roles - finished this Tuesday - to be used for "simple" authorisation between universities
 - Result - triplets for internal and external use
 - A lot of work left to do

031216

T Wiberg, UmU

11

Electronic Identity

Roles -> triplets



- User types:
 - anonymous, browsers, report (controllers) users, self-service users, scrutinizers, decision makers, update users
- Organisational scope
- System, area
 - Finance,
- Our idea is to map positions and roles to these triplets
- Admission officer
 - -(update, UmU, NyA)
 - -(update, UmU, LANT)
 - ...

031216

T Wiberg, UmU

12

Externalisation of Infraservice Functionality



- I prefer the **application perspective on Infraservices** (before a network perspective):
- The idea of Infraservices (Middleware) is to identify common functionality in applications and to explore the possibilities opened through an externalisation of these functions
 - Directory Services
 - Authentication Service
 - Authorisation Service
 - Discovery Services
 - Agents/Proxies
 - ...

031216

T Wiberg, UmU

13

Components of a Supporting Infrastructure



- Issuing of electronic identities - only for servers - x00/yr
- PKI - SwUPKI has been up since 2001 - 8 members
- Enterprise Directory - strong harmonisation efforts - 3 univ
- Mechanisms of authentication - A few - CAS seems to be the common choice
- Federated network authentication service - cwaa - 6? universities
- Shibboleth - Stockholm universitet's library - we need to do some work to integrate it with the other services
- Authorisation Service - SPOCP - 3 universities are in the process of deploying it

031216

T Wiberg, UmU

14

Electronic Identity Harmonisation Arenas



- Unitcf - the swedish universities' CIO/CTO network
 - Codex - swedish code exchange cooperation network
 - Swedish government - Electronic Identities
 - Gnomis - nordic middleware coordination network
 - Terena - network of national research networks
 - Eunis - network of campus IT ...
 - Internet2 - US project
 - NMI - NSF Middleware Initiative
- For each problem we are preparing to solve we have to decide what arenas we shall strive to harmonise with

031216

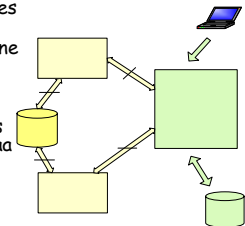
T Wiberg, UmU

15

Current Swedish Infraservice Harmonisation Situation



- Cooperating servers in distributed systems often have server certificates from **SwUPKI**
- **Directory** harmonisation has been done in Codex and Gnomis
- There are many different Authentication Services
- **Net-logon** - Protocol and service has just been implemented in Codex - cwaa
- **Authorisation** - SPOCP is being deployed
- **Identity Certificates** - a new national procurement just done



031216

T Wiberg, UmU

16

SwUPKI - The Swedish PKI for Higher Education



- One common CP, separate CPSs
- It is a club - www.swupki.su.se
 - started in february 2001
 - 7 members dec 2003
 - cwaa - Codex Netlogon protocol - requires server certificates
- Stockholm University is Policy Management Authority
 - Accepts new members
 - Carries out inspections
 - May decide to cross certify with other
- Umeå University is Policy CA
 - Issues certificates to the member CAs
- Preparations are made to organise issuance of identity and or secondary certificates
 - probably two hierarchies - one with identity certificates

031216

T Wiberg, UmU

17

Electronic Identity Harmonisation of Directories



- Work on Harmonisation of directories has been done in Codex
- The instruction is to strive for harmony on the Scandinavian arena
 - norEduPerson - done
 - norEduOrg - done
 - norEduCourse - not done.

031216

T Wiberg, UmU

18

Swedish Authentication Harmonisation?



- We need to decide who to trust
 - for network and basic service access
 - for single signon
- Many different approaches and mechanisms
- Harmonise
 - levels of strength
 - Message formats
 - Build Federations
- How does it scale
 - nationally
 - internationally
- Codex has specified a protocol for a Netlogon Service
 - It is currently being evaluated
 - It allows different authentication mechanisms at the home authentication service
 - Each university decides who to trust

031216

T Wiberg, UmU

19

Authorisation is not only Access Control!



- It is easy to mistake Authorisation for just Access Control
- We mean that authorisation at least can be "the right for a Subject to perform an Action on a Resource, an object belonging to some application space"

031216

T Wiberg, UmU

20

Electronic Identity SPOCP - Where do we stand?



- We have still not found any serious flaws in the approach (the NPspace way of expressing things)
 - the policy language can't express what is forbidden, only what is permitted
- We need to understand better the process of developing a policy
- We have some tools for policy management but need more
 - There are commands that modify the policy but we need powerful tools
 - We need tools for browsing the authority space
 - We do not yet have software that supports policy management for those who dont know the policy language

031216

T Wiberg, UmU

21

Electronic Identity SPOCP - Where do we stand? 2



- SPOCP plays a central role in our development of personal portals
 - the portal channels need to support external authn/authz
- We require that new applications can take advantage of authn/authz services
 - often the first time they have heard this requirement
 - mail distribution list manager
 - meeting/classroom reservation system

031216

T Wiberg, UmU

22

Identity Certificates in Swedish Higher Education



- A couple of large universities are seriously considering to provide identity certificates for their students
 - citizens certificates or SwUPKI certificates
 - decision during 2004 probably
 - 25-30% of the swedish student population
 - for signing eMail and for authentication

031216

T Wiberg, UmU

23

Electronic Identity Infraservices (AA Middleware)



Torbjörn Wiberg
CIO, UmU

031216

T Wiberg, UmU

24