

Campus Issues

From a nordic perspective
Torbjörn Wiberg, Umeå Universitet,
TF-EMC2 Marseille, 080204

Where are we going?

- An Identity Architecture (IdMgmt, PrivMgmt, AuthN, AuthR, and Attribute services) that
 - encourages trust from peers and service providers (basis for federation),
 - is supported by a Metadirectory (a Synchronisation Engine) and a Group Management tool
 - supports integration and process reengineering (self service and self reporting)

...Where are we going?

- Web fronted applications that
 - can be plugged in as components in Service Platforms
 - are designed to use information about identity, groups, roles and privileges provided in real time by the Identity Architecture for AuthR
 - support Virtual Organisations by being adapted to federated AuthN and AuthR

Why are we going there?

- possibilities to reduce the cost substantially
 - for management of “user accounts”
 - for deploying new services for the whole institution
- Only possible if you can resist the temptation to require a too fine control of the authority of the normal user - we dont do that in the physical world - Rolands key opens my door as well

! But these arguments hardly mention federations

- true!! the possibility to federate is not the dominating reason to introduce a fed.aai
- for ex the number of eduroam users are small
- But any group may have members from other countries
 - courses, boards, work groups, projects
- Why should we introduce applications that are not federation enabled
 - shared service centers - mail, CA, LMS, VOs

Vitual Organisations ...

- ... of main interest to campuses are small scale and often ad hoc
- They need to be supported by Virtual office services
- I expect my university of 37k students soon will have x0k virtual organisations requiring VO services
- LMSs --> VO-support platforms

We are almost there !!

- technologically that is
- but the small institutions need support, and we have a lot to do in packaging and documenting and supporting
- and most institutions have to improve the quality of their Identity, Privilege and Group management (in that order) and they need to design and deploy a repository for that information supported by a MetaDirectory

Identity Management

- Initial identification
- Procedure description - identities quickly but to whome, why, for how long
- Metadirectory - OM2, Student record connector, HR connector, LDAP connector, AD connector
- Enterprise repository - the amount of work needed is much more than anybody expects
- Management application - decentralised mgmt, reflecting the order of delegation

Quickly?

- A student that surfs in to our web site shall be so well serviced that she stays.
- A student shall get an account “immediately”
 - Increasing the loa is a later issue
- An employee shall get an account immediately
 - It has to be at the right loa
 - It can be prepared - after the employment decision

Authorisation

- Service or integrated in the app
- Service
 - SPOCP
- Integrated
 - Using enterprise information - Attribute Service, LDAP
 - Provisioned with enterprise information - OM2, Connector

Synchronisation through a meta-directory

- Integration support irrespective of the rest of the Identity Architecture
- Routing of synch data to subscribers
- OM2
- We need to develop best practice for when and how to include an application in a metadirectory structure