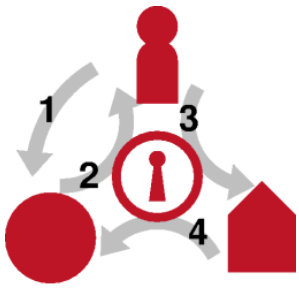
Identity collaboration and federation in Norwegian education

OECD workshop on Identity Management, Trondheim, 2006-05-08

Ingrid Melve, UNINETT Chief Technical Officer

Feide login (currently username/password)



- User tries to access service
- Service Provider redirects user to Feide login (Identity Provider)
- Authentication is done at campus
  - No big central user database
  - Distributed user management at school, university, college
- Authentication is confirmed with the service, possibly with attribute release (roles)
  - Informed consent for information release
- Single Sign On (SSO), and Single LogOut (SLO)

2

Feide federates education

Identity federations:

- Authenticate
- Trust establishment
- Enforce information flow policy
  - Attributes, roles
  - Privacy control
  - Enable sharing across organizations
- Standardize integration
  - Security
  - Well known integration path
  - Multi-vendor support
- Equal market access for service providers

3

UNINETT

Feide: trust and technology

Trust fabric:

- Contractual agreements
  - Feide signs contracts with all parties, contract hub
- Requirements for identity management
- Requirements for data protection and data flow
- Best practices and guidelines
- Support various service usage models

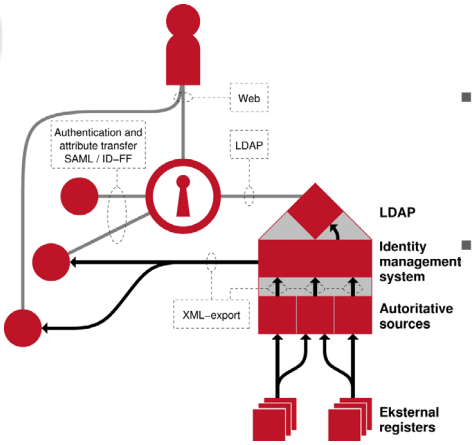
Technology:

- Goal: secure log-in and control sharing of personal information
- Implementation:
  - Moria2 in-house developed open source (2003-2007)
  - SAML2-based (2006-)
- Cross-federation
  - Demonstrated technology in 2006
  - MinSide portal (eID for government services)
  - Testing: eduGAIN, Shibboleth, openID, various SAML-based CoT

4

UNINETT

Requirements for campus identity management: analyze work flow



- Identify key data
  - Identify authoritative sources and external registry sources
- Identify who is reponsible for
  - Initial data
  - Data updates
  - Data removal
- Organizational process
  - Clean up work flow and procedures
  - Move data maintenance out of the IT department
  - Enable Human Resource and Student Management staff to do their jobs better

5

UNINETT

Why federated identity requirements?

- *Distributed nature of education and research. Resources exist at various network endpoints or are maintained by different institutions.*
- *Education and research require integration of resources on heterogeneous platforms or in legacy systems.*
- *Data needs to be made widely available beyond the core application that maintains and generates the data.*
- *Automation is needed for advanced services in higher education*
- *Policy varies between collaborators, and changes over time*
- *Norwegian universities and colleges have outsourced administrative systems and traditionally share many support structures*
- *Avoiding lock-in to particular vendors, levelling the playing field*
- *Research is collaboration: need software and collaborative working*

6

UNINETT

User benefits

7

- One username
- One password (or other credential)
- Access to webspace everywhere: learning support, library systems, administrative systems, project space for research
- Do not need to register information at each service, automatic updates from campus information
- Informed consent for personal data transfer
- Familiar log-in page may increase security

UNINETT

Campus Identity Provider benefits

8

- Authoritative quality for all affiliated users
- Control of information flow for all affiliated users
- Enhanced user management simplifies and automates business processes
- Federated login provides access to services
- One contract with Feide eliminates bi-lateral contracts with all service providers

UNINETT

Service Provider benefits

9

- Access for all Feide users
- No local administration of user database
- Feide handles login and gives high quality data about users
- One contract with Feide eliminates bi-lateral contracts with all identity providers
- Clear integration path, well-defined information flow

UNINETT

Feide goals

- Governance and standardization
  - Local dataflow clean-up
  - Overview and control of services
  - Common guidelines, requirements and best practice for identity management
- Identity management for education
  - Unity in identity management
  - Critical infrastructure: no login, no service
  - Federated approach, shared world
- Collaboration with educational institutions, service providers, vendors and standards organizations
- National level services comes first, support local and shared services

10

UNINETT

Business drivers for Feide

- Each institution benefits from
  - Local dataflow clean-up
  - Overview and control of services
  - Common guidelines, requirements and best practice for identity management
- Educational sector as Service Provider
  - Easy integration of non-local users
  - Data protection contracts and guidelines
- Services benefit from
  - Integrated user space (instant user db)
  - Data protection contracts and guidelines

- Rollout:
  - Universities (6): 2003 - 2006
  - University Colleges (37): 2004 – 2007
  - Lower education (4500): 2006–
- Operational service providers
  - Shared services: 2003–
  - Local university services: 2003–
  - Commercial service providers: 2006–
  - Public services (cross-federation): 2007–

11

UNINETT

Collaboration

- Strong involvement from schools, universities and colleges
  - User groups
  - Active participation in various project(s)
  - Close collaboration with service roll-out (SAP, NRK)
  - Operational Feide login service run by Oslo University
- Backing from Ministry of Education and Research
  - Financial support
  - Clear political support for integrating services
- Partnership with commercial technology partners for standards based software
- International cooperation: TF-EMC2/Terena, eduGAIN/EU 6th Framework, GNOMIS, Internet2, Liberty Alliance

12

UNINETT

More information

- http://feide.no/index.en.html
- Email for Feide:
  - administrasjon@feide.no
- Questions for Ingrid
  - ingrid.melve@uninett.no

13

Collaboration builds education

UNINETT