Use case: Federated Identity for Education (Feide)

Identity collaboration and federation in Norwegian education

Liberty Alliance workshop, Oslo, 2006-10-17

Ingrid Melve, UNINETT CTO
Overview

- Why work on federated identity in education?
- Feide
  - Higher education
  - Schools
- Liberty Alliance contributions to deployments
  - Service Provider integration
  - Privacy
- Current identity focused initiatives
- Future plans
  - Collaboration, research, development, deployment
Norwegian education

- 7 universities, 46 university colleges (210 842 persons)
- Extensive collaboration on electronic services in higher education
  - BIBSYS and other library services
  - FS and MSTAS student registry systems
  - Administrative systems: finance, HR, archive, invoice,
  - High performance computing, super-computers and grids
- Schools (865 000 persons, plus parents)
  - 454 upper secondary schools owned by 19 regions
  - Around 4500 schools owned by 430 municipalities
ICT trends: Usage in higher education

- All Norwegian universities and colleges are online since 1992
- Currently all students in higher education use e-learning
  - Tracking learning, tracking teaching
  - Personalization requires stronger central ICT systems
- Half of the students have laptops (growing number), and they grew up with PCs
- Web self service is increasingly deployed
- Traffic grows exponentially
UNINETT and Feide

- UNINETT is the Norwegian research network
- UNINETT is chartered to
  - Provide advanced network services among the world best
  - Support open standards and interoperability
  - Work in collaboration with education and research

- Feide organization
  - A central service (7 persons)
    - Login service, operated by Oslo University
    - Trust model
    - Information model
    - Project management
  - Deployment in higher education (3-1 persons)
  - Deployment for school owners (4-9 persons)
Collaboration

- Strong involvement from universities and colleges
  - User groups
  - Active participation in various project(s)
  - Close collaboration with SAP roll-out
  - Operational Feide service run by UiO

- Backing from Ministry of Education and Research
  - Financial support
  - Clear political support for integrating services
  - Identity management for schools scheduled for 2008

- Partnership with commercial technology partner (Sun) for open source Liberty-based software

- International participation: TF-EMC2/REFEDS, eduGAIN, GNOMIS, EuroCAMP, Internet2
Identity management for education

- Feide since 2000 (initially higher education)
  - Operational login service since 2003
  - Universities and university colleges: 2003 - 2006

- Schools and Feide
  - Participation decided by Ministry of Education early 2006
  - Identity management should be available by 2008 for all schools

- Strong campus identity management efforts
  - Universities and colleges develop and deploy IdM software
  - Organizational process: identify responsibilities and enforce routines for processing personal information
  - Supporting the Personal Data Act

- Operational service providers (current: 23)
Why federate?

- Users and home organizations and service providers need to exchange information
- Trust establishment
  - Feide-name and password
  - PKI and other credentials supported
- Policy with privacy support
- Technology:
  - easy service provider integration
  - Multi-vendor environment
  - Open standards
  - Clear integration path
Feide - Federated Electronic Identity for Norwegian Education

- Feide is a non-commercial identity management federation for people in education
- Feide is technology and platform agnostic
- Feide offers guidelines and policy for campus identity management
- Feide-names are valid for all education services, and may be used internally, for community services and with educational related services
Feide login

- User tries to access service
- Service transfer user to Feide login
- Authentication is done at campus
  - Local authentication point
  - Local control over information
- Authentication is confirmed with the service, possibly with attribute release
  - Attribute release controlled by user, governed by contract
Feide federates education

Federations:
- Establish trust
- Authenticate
- Do privacy control
- Enforce information flow policy
- Security
Business drivers for Feide

- End user: one username, one password
- Each educational institution benefits from
  - Local dataflow clean-up
  - Overview and control of services
  - Common guidelines, requirements and best practice for identity management
- University, college or school as Service Provider benefits
  - Easy integration of non-local users
  - Data protection contracts and guidelines
- Common shared services benefit from
  - Integrated user space
  - Data protection contracts and guidelines
Feide is glue in education
Ongoing work

- Feide operates with
  - One Identity Provider (central login service)
  - Many Authentication points (one at each educational institution)

- Attribute release is important
  - Feide-name valid only in organizational context
  - What school, affiliation, group, address, NIN, unit?
  - Provisioning: started PIFU standardization effort

- Cross-federations needed (imply IdP chaining)
  - National: MyID for public sector
  - Nordic: Kalmar Union for higher education and research
  - International: eduGAIN, InCommon?

- Service Oriented Architecture (implies ID-WSF)
  - Services talk on behalf of user to mediate content delivery
More information

- Information from Feide, including deployment status
  - http://www.feide.no/index.en.html
  - http://feide.no

- Email for Feide:
  - administrasjon@feide.no

- Questions for Ingrid
  - ingrid.melvet@uninett.no

Collaboration builds education
Campus Identity Provider benefits

- 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
Service Provider benefits

• 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
User benefits

- One username
- One password (or other credential)
- 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