

Norwegian middleware (mostly Feide)

GNOMIS 25.09.2006

Ingrid Melve, FEIDE manager and UNINETT CTO

Overview

- Feide organization
- Campus IdM for higher education
- IdM for schools
- Login service (Sun AM/FM)
 - ◆ Government security portal
 - ◆ Open source, vendor support
 - ◆ SAML
- Information model: norEdu + provisioning
- Contracts and trust model
- Deployed services



Feide organization 2006

- 7 man years (4 women, 4 men) for central Feide
- 6-8 man years for Feide in schools, 1,5 for Feide on campus in higher education
- Steering committee with 5 members
 - ◆ Appointed by Uninett board
- Advisory concil appointed by KD (Ministry of Education)
- Formal meetings with Abelia and IKT-Norge (vendors)
- User groups: technology and/or region-based



Campus status

Organization	Deployment status			FEIDE
	Students	Employees	Other	
NTNU				
Universitetet i Bergen				
Universitetet i Oslo				
Universitetet i Stavanger				2007
Universitetet i Tromsø				2007
UMB				2007
Høgskolen i Agder				
Høgskolen i Akershus				2007
Høgskolen i Bergen				
Høgskolen i Bodø				2007
Høgskolen i Buskerud				
Høgskolen i Finnmark				
Høgskolen i Gjøvik				2007
Høgskolen i Harstad				
Høgskolen i Hedmark				
Høgskolen i Lillehammer				
Høgskolen i Molde				
Høgskolen i Narvik				
Høgskolen i Nesna				
Høgskolen i Nord-Trøndelag				2007
Høgskolen i Oslo				
Høgskolen i Sogn og Fjordane				2007
Høgskolen Stord/Haugesund				2007
Høgskolen i Sør-Trøndelag				
Høgskolen i Telemark				2007
Høgskolen i Tromsø				2007
Høgskolen i Vestfold				2007
Høgskolen i Volda				
Høgskolen i Østfold				2007
Høgskolen i Ålesund				
Samisk Høgskole				
Norges Handelshøgskole				2007
Norges Musikkhøgskole				



Campus IdM for higher education

- The great cleanup process is mostly finished
- Change of HR system ahead (SAP coming) implies changes for employees
- Daily IdM routines are getting better, still work to do on
 - ◆ Interfaces from student registries
 - ◆ Integration BAS/CIdMS with applications
 - ◆ «Others» categori (10-30% of users)
 - ◆ Security, risk assessments, documentation, privacy, policy



IdM for schools

- Political decision february 2006: all schools should have federated IdM available by 2008
- Pilots started 2005, first operational 2006
- Regional support for secondary schools (Vgs), 8 regions operational by fall 2007
- Special support team: Uninett ABC
- Share
 - ◆ Login service
 - ◆ Trust model
 - ◆ Information model (mostly)

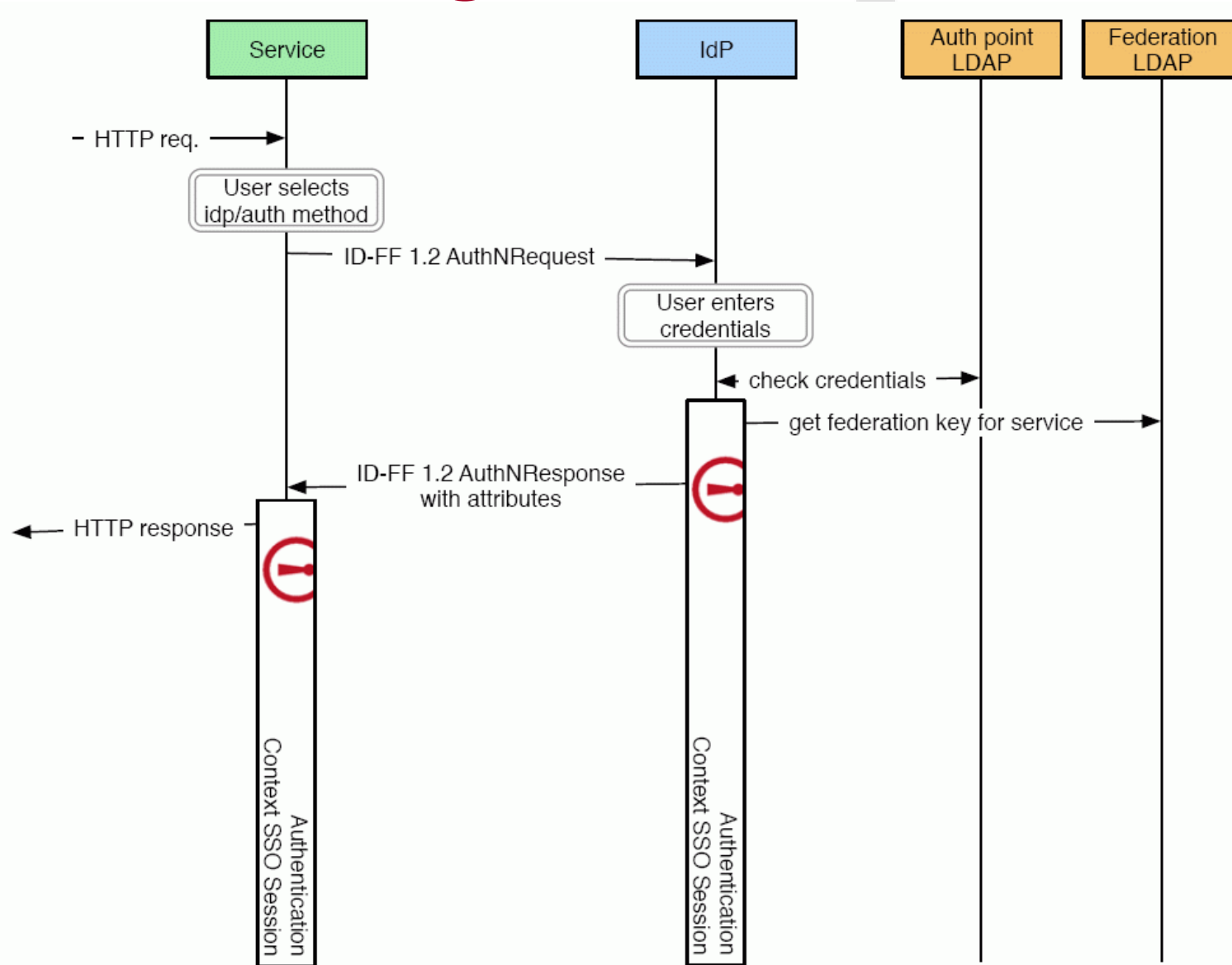


Login service (Sun AM/FM)

- Collaboration with Sun
 - ◆ Access Manager, demo 20.06, pre-prod 18.9, operational medio November
 - ◆ Federation Manager, ready? package
- Open source, vendor support
- Underlying standards
 - ◆ ID-FFI.2 + homegrown attribute support + multi-LDAP
 - ◆ SAML2.0 + homegrown multi-LDAP



MoriaAM, new login



Login: Liberty Alliance and SAML

- More effort on gathering LA-compliant Norwegian players
 - ◆ Workshop October 17, start user group
- Plan to support multi-vendor environment
 - ◆ First test: Shibboleth (worked OK)
 - ◆ Next test: NAM from Novell (TBD)
- Want to deploy services in collaboration with other players, most importantly MyID

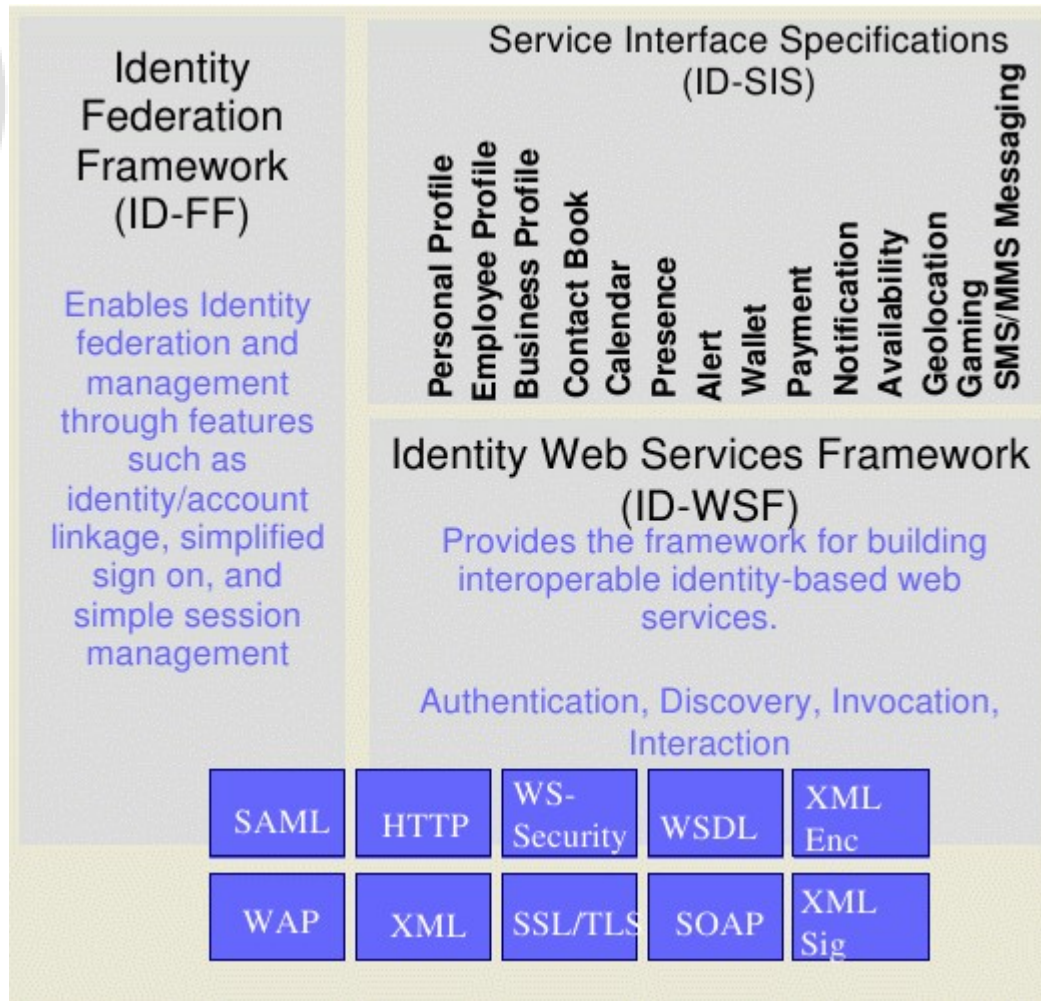


Liberty Alliance

- ID-FF (Federation Framework)
 - ◆ Single sign-on and single log off
 - ◆ Supports sessions and federated identities
 - ◆ Based on HTTP, XML, SAML
 - ◆ Communication for user, login and service
- ID-WSF (Web Service Framework)
 - ◆ Communication between service (on behalf of user)
- ID-SIS (Service Interface Specifications)



Liberty Alliance rammeverk



■ Operational

◆ ID-FF

- ★ Replace Moria2 WSDL
- ★ SSO and SLO

■ Investigate

◆ ID-WSF

- ★ Personal Profile
- ★ Employee Profile

◆ Maybe ID-SIS



Components

- IdP (Identity Provider)
 - ◆ Moria, with multiple AP
 - ◆ I Feide: Ein IdP og fleire SP danner føderasjon
- AP (Authentication Point)
 - ◆ ID-bank, local LDAP
- SP (Service Provider)
 - ◆ service/applicaiton
 - ◆ May contact multiple IdPs, implies membership in multiple federations
- Web client (end user)



Federated identity

- Each service provider has one key per user
 - ◆ One-time or permanent key
 - ◆ Service may change key
 - ◆ User may change key (without changing identity)
- Identity Provider (IdP) knows all keys within federation
- «To federate» is for two parties to agree on a key for a user



Login: Crossfederations

- Government security portal support implemented, PKI portal cancelled due to financial/commercial issues
- Interim solution 2007: MyID based on SAML2.0 (SunAM)
- MyID will act as IdP for Feide, Feide as SP for MyID
- EduGAIN
 - ◆ Demonstrated first login with Switch
- Nordic work
 - ◆ Watch Mikael's demo
 - ◆ Integration of Shibboleth and Sun software (AM/FM)



Information model: attribute definitions

- Final draft of norEdu* 1.4 with modifications
- Feide usage notes added to all relevant attributes in norEdu* 1.4
- norEdu definitions are part of Feide contract
- Work started on school requirements
 - ◆ Parents (legal guardians), pupils, teachers
 - ◆ Organizational structure
 - ◆ Advise on Feide usage
 - ◆ Data inspectorate (started with age 15+)



Information model: standard for provisioning

- Starting work on Norwegian standard for CIdMS-related provisioning 10.10.2006
- Several components exist:
 - ◆ IMS Enterprise Services, multiple use cases
 - ◆ ESU for describing course related XML
 - ◆ ABC enterprise (CIdMS) from student registry
 - ◆ Specific XML solution
- Aim to have XML description by mid-2007



Contracts and trust model

- Revamped contract text based on operational experiences
 - ◆ Rewritten everything
- Added hooks for cross-federation
- Tried to align with HAKA and Swich-AAI
 - ◆ Different architecture
 - ◆ Differences due to politics and culture
- Minor adjustments in trust model due to SSO



Deployed services (new 2006)

- University colleges (SP: Trofast): ePhorte (casework/archive)
- Higher ed (SP: Inmeta): Student software license (in test)
- UiO: Elections
- NTNU: Course subscriptions, DNS update requests
- Uninett: Sympa, wiki, portal
- Feide: Customer portal

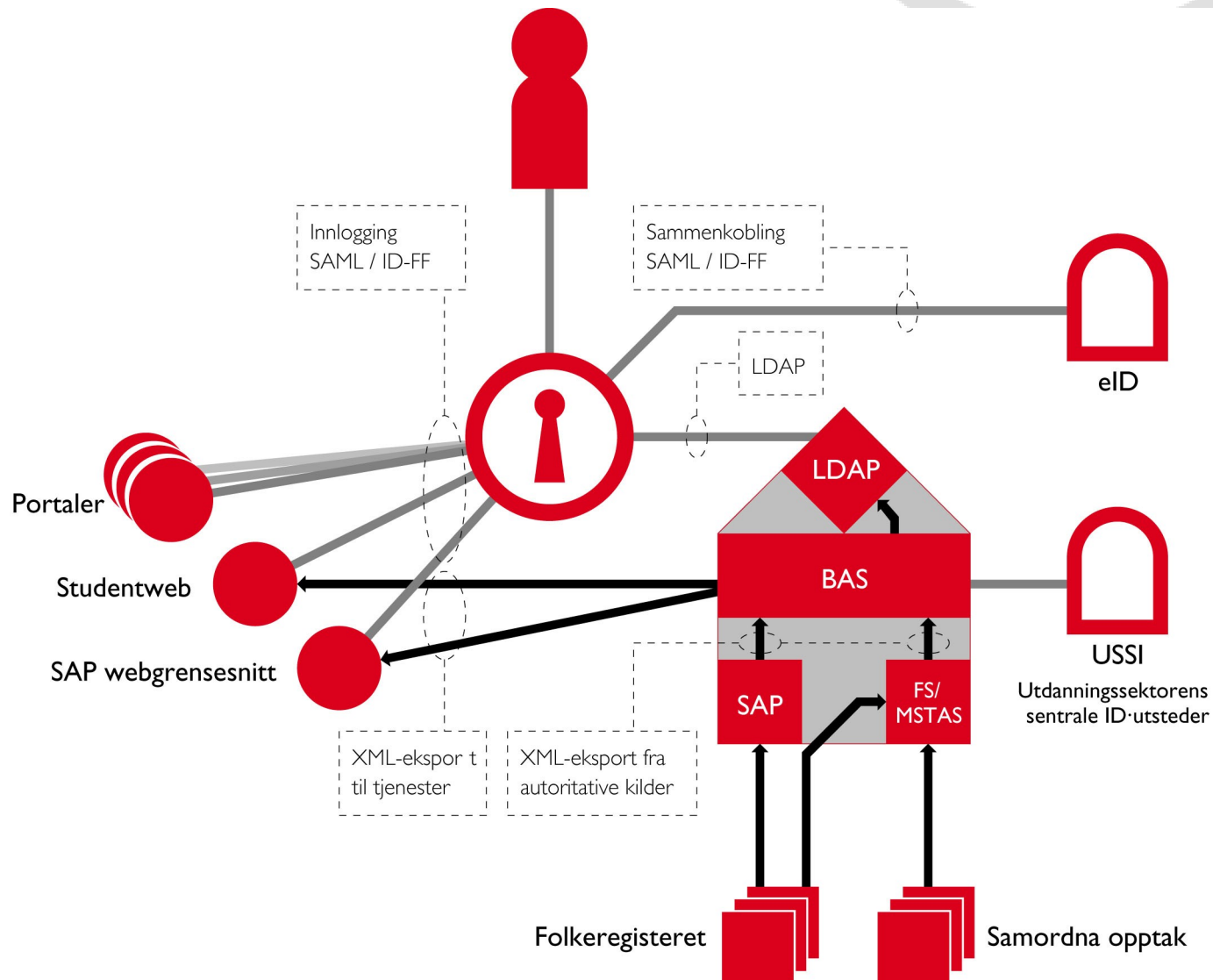


Service Providers (2003-2005)

- Mitt BIBSYS
- Frida
- Local portals
- StudentWeb
- Vortex webdav
- Innsyn (who am I)
- SAP testing (SAP HR/EP)
- Lasso
- Infodesign course
- FAS-portal serveroversikt
- National library research services
- Electronic invoice
- E-learning: BrainBank



Future work



Contact us

- www.feide.no
- Technology discussions
 - ◆ aktive@feide.no
- Talk to Anders and Ingrid
- Email administrasjon@feide.no
- Email for Ingrid
 - ◆ ingrid.melve@uninett.no

