Nordic middleware identity federation

NORDUnet Conference 27.9.2006

Mikael Linden

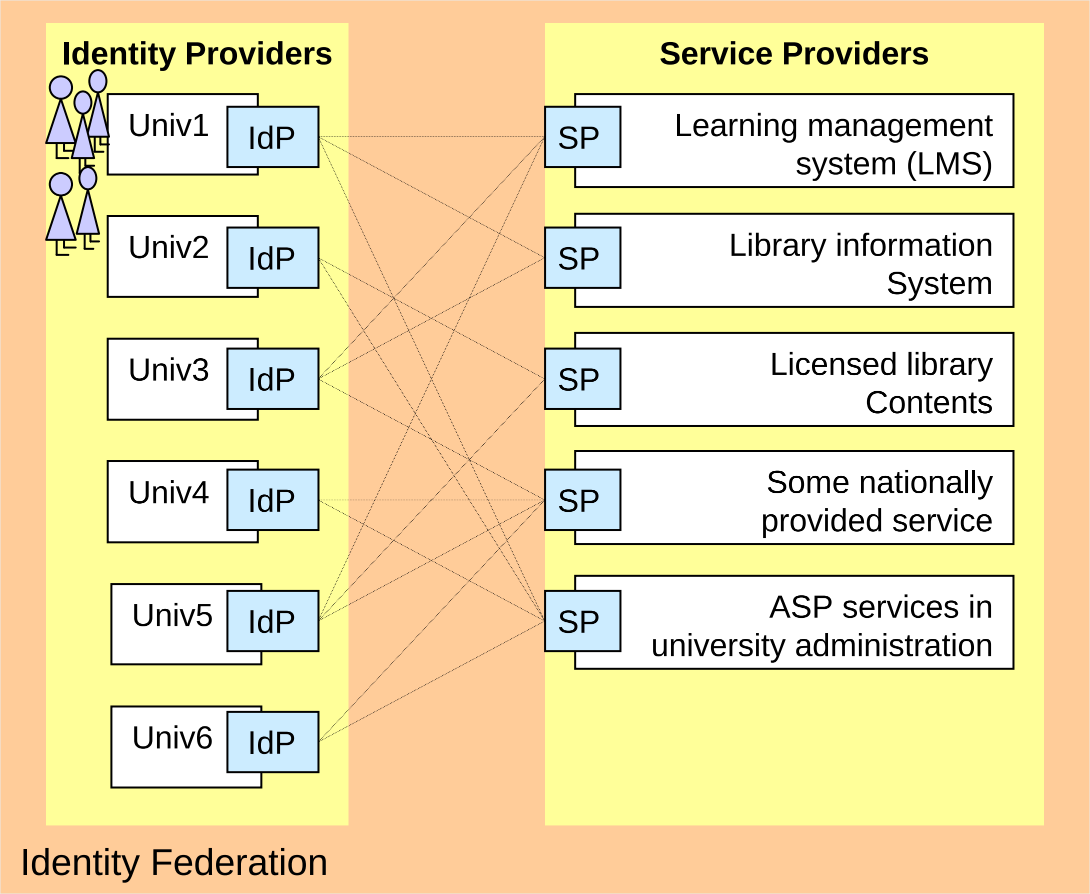
mikael.linden@csc.fi

CSC, the Finnish IT Center for Science

Outline

- Basics of an identity federation
- Current identity federations in Higher education in the Nordic countries
- Nordic confederation: Kalmar union in digital identity?
- DEMO: cross-federational login to a supercomputer
- Nordic confederation technical sketch
- Tough part: the policy
- What is the next step?

What is an identity federation?



Identity Providers
Univ1
IdP
Univ2
IdP
Univ3
IdP
Univ4
IdP
Univ5
IdP
Univ6
IdP
Service Providers
SP
Learning management system (LMS)
SP
Library information System
SP
Licensed library Contents
SP
Some nationally provided service
SP
ASP services in university administration
Identity Federation

- User’s **home institution** (Identity Provider, IdP) **maintains user’s identity** and attributes (name, contact info, role, major etc)
- **Home institution authenticates** the user (e.g. by password)
- **Home institution releases attributes** to the Service Provider (on user consent)
- Based on **the attributes, service provider decides what kind of service** the user will get

Currently identity federations in higher education are national

Haka (Finland):	**Operational (Shibboleth)**
FEIDE (Norway):	**Operational (Moria, Liberty/Sun)**
DK-AAI (Denmark):	**Piloting (Shibboleth)**
SWAMID (Sweden):	**Piloting (Shibboleth)**

Kalmar Union in digital identity?

- **Do we need 4 national federations? Could we have just one Nordic (con)federation?**
  - A federation of federations
- **Is 1+1+1+1>4?**

- **Are there services that would benefit from easy authentication and authorisation between the Nordic countries?**

DEMO: Cross-federational login to a supercomputer

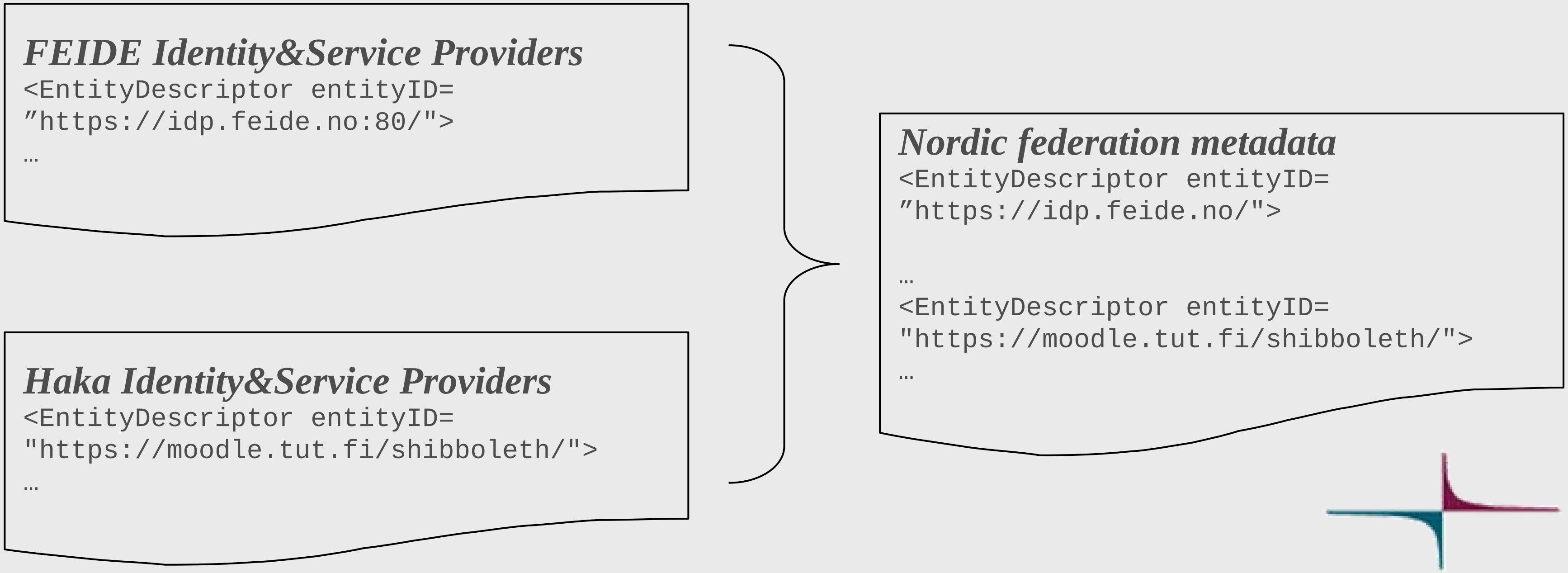
- **”Scientist’s Interface” (Service Provider)**
  - CSC’s supercomputers
  - available for federated access in Finland since 3/2006
  - Shibboleth

1. **DEMO1: Federated log-in to Scientist’s Interface from the Norwegian FEIDE federation**
   - FEIDE login server (Sun Access Manager) adjusted to talk Shibboleth

2. **DEMO2: Federated log-in to Scientist’s Interface from the Danish DK-AAI pilot federation**
   - Shibboleth

Nordic confederation technical sketch 1/2

- **No protocol gateways, make IdP&SP talk directly to each other**
  - unlike eduGAIN of GN2/JRA5, where there is the Bridging Element
- **Just aggregate the metadata from the four federations**
  - technically speaking, IdPs and SPs would see just one federation



FEIDE Identity&Service Providers

```
<EntityDescriptor entityID=
”https://idp.feide.no:80/">
…
```

Haka Identity&Service Providers

```
<EntityDescriptor entityID=
"https://moodle.tut.fi/shibboleth/">
…
```

Nordic federation metadata

```
<EntityDescriptor entityID=
”https://idp.feide.no/">


…
<EntityDescriptor entityID=
"https://moodle.tut.fi/shibboleth/">
…
```

Nordic confederation technical sketch 2/2

- **Schema for attribute syntax and semantics**
  - All Nordic federations based on eduPerson schema
  - Schac covers some of the rest (e.g. SSN)
- **PKI for server certificates**
  - Haka: certs provided by TeliaSonera and VeriSign
  - UNI·C: certs provided by GlobalSign
  - SWAMID: certs by SwUPKI
  - FEIDE: certs by VeriSign and Globalsign

  ⇒ perhaps we could accept each other's CAs
- **the WAYF (Where Are You From server)**
  - each federation would have a national WAYF, with the flags of other countries 🇫🇮 🇳🇴 🇸🇪 🇩🇰 linked to the corresponding WAYF

Tough part: the federation policy

- **There should not be extensive gaps in our federations' policies**
  - requirements for joining IdP's & SPs
  - obligations of the federation operator
  - Mechanisms and practices for data protection
  - liability and indemnification…
- **Are there gaps, then?**
  - FEIDE (Norway) and Haka (Finland): policies mostly similar, for example requirement for up-to-date user data in the enterprise directory of the IdP
  - DK-AAI (Denmark) and SWAMI (Sweden) have the policies still under preparation

How many steps we want to take?

Third step: have it in production, and start to look for and promote it to **cross-national services**

Second step: adjust the policies and **run it in a production** environment

Make a **technical demo** to convince people that it is technically workable

DONE

CSC