National Identity Management for the Education Sector

AFSecurity Seminar @ UniK

2009-01-22

Anders Lund

<anders.lund@uninett.no>

Feide

- Feide is a system for identity management within the national education sector.
- This talk presents the concepts and technologies used in Feide, as well as the possibilities and advantages that Feide offers

Feide concepts [1]

- Users have one username and password
- Users access web-services via a central log-in service
- Services are given what they need to know about the user
- Services are not given the users password, only information about the user

Feide concepts [2]

- Feide have formal agreements with the schools before they are connected
- The home organizations (schools) are responsible for the data about the users (correct and up-to-date)
- Home organizations decide themselves what services their users should be able to access via the central log-in service

Feide concepts [3]

- Data about the users in a standardized format
- Feide handles the connection of new services to the central log-in service
- Home organizations are only connected once

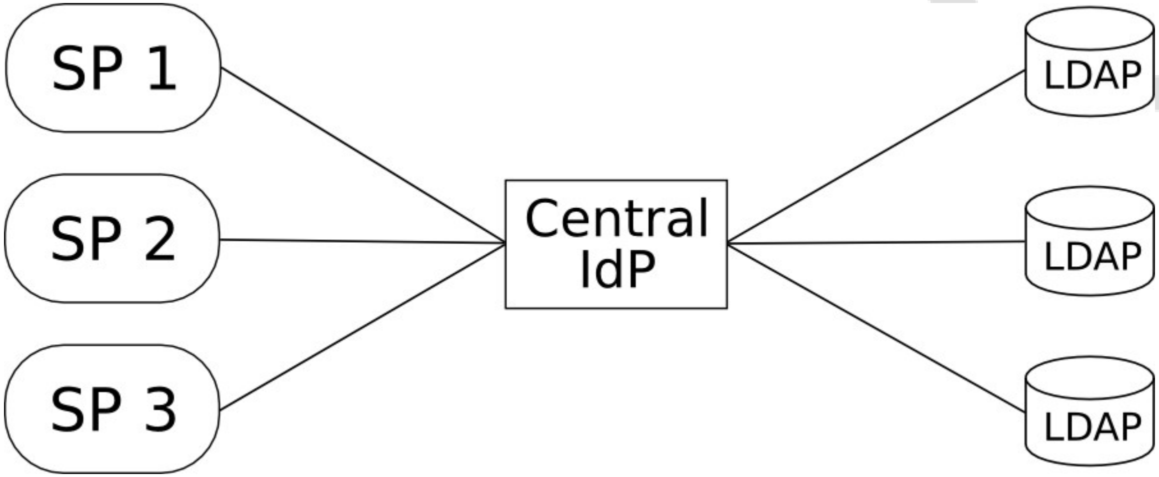
Some numbers

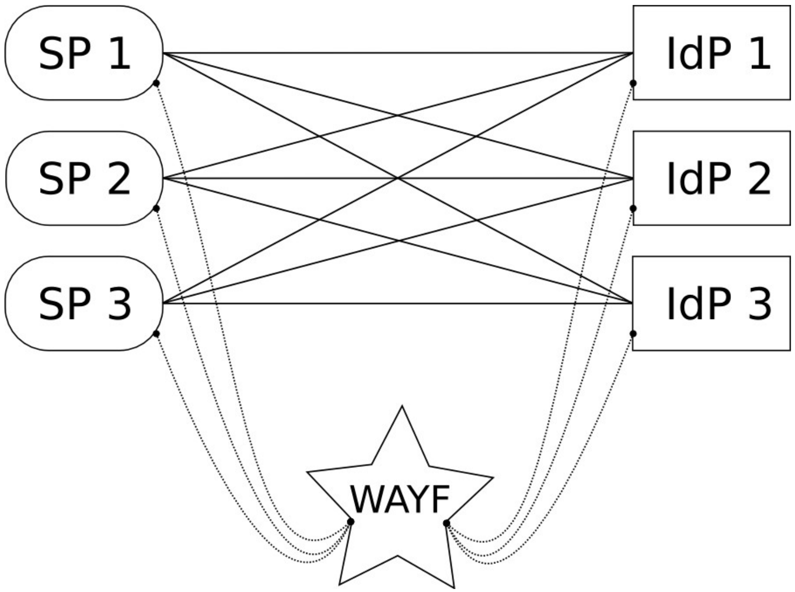
- More than 80% of the users in higher education (employees and students)
- 7 (of 19) county councils (upper secondary schools)
- 1 out of 430 muncipalities... (primary schools)
- More than 2.500.00 logins in 2008

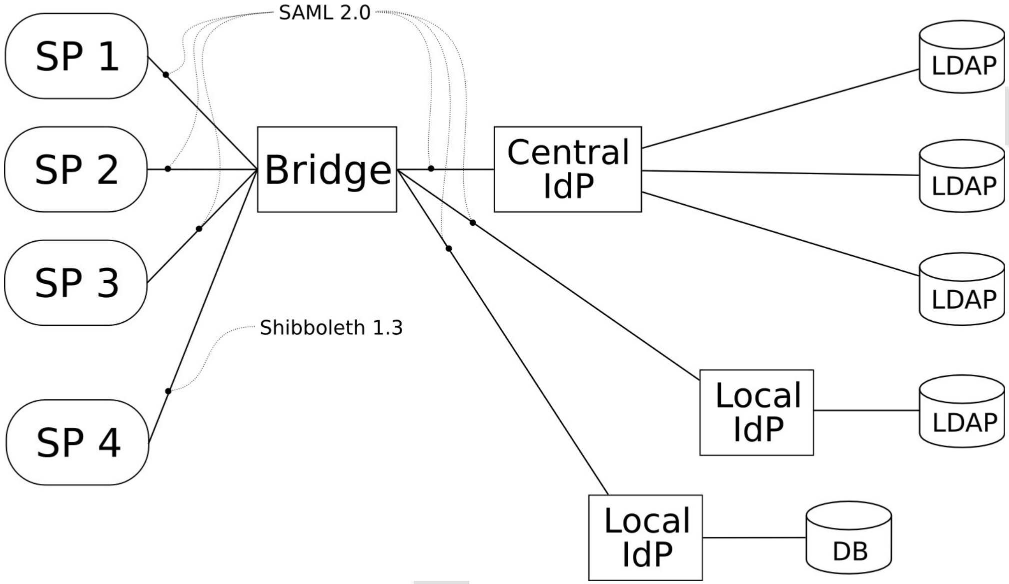
Todays solution

- Based on SAML 2.0
- Backend authenticate users by using LDAP
- One central identity provider (IdP) where service providers (SPs) are connected
- Single Sign On when going between services
- Single Log Out when logging out from a service

Architecture(s)







Issues we are working on [1]

- New look & feel
- Migrating to new software (opensource, developed in-house)
- Showing what is actually going on when doing Single Log Out in a more user friendly way
- Looking into possible changes in architecture (hybrid instead of central)

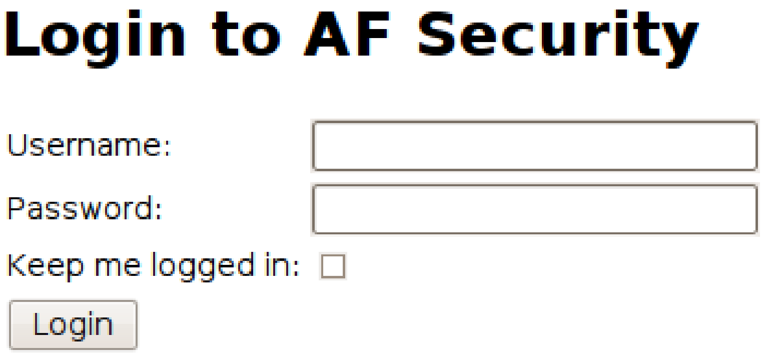
Issues we are working on [2]

- 2-factor (or somthing else) authentication to give higher level of assurance – level 3 according to governmental policies
- WebServices and delegation (WS-Trust, ID-WSF, OAuth, etc.)
- Getting more Service Providers and home organizations connected
- and more...

Demo ?

Play with this?

- simpleSAMLphp is opensource
  - http://code.google.com/p/simplesamlphp/
  - Can act as SP or IdP, or both
- Perhaps set up internally to replace pages like this:



Login to AF Security

Username:

Password:

Keep me logged in: □

Contact

- Feide web-pages:
  - http://www.feide.no/
  - http://rnd.feide.no/
- administrasjon@feide.no
- Anders Lund <anders.lund@uninett.no>