

From campus identity management to a federated solution

- Case: FEIDE
- Campus Identity Management
 - ◆ Authoritative Quality – the process
 - ◆ Operational technical solutions
- Federating

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

A solution for whom?



- Higher ed: 230000 person, 53 institutions
- (Lower ed: 780000)
- Total: 20% of population
- Tradition of sharing work
 - ◆ Dugnad
- Many shared services
 - ◆ Common software
 - ◆ Application Service Providers
 - ◆ Common interfaces

FEIDE – the players



End user
person with FEIDE-name



Home organization - IdP
university or school with end
user affiliation




Service Provider
Services and applications for
end users

FEIDE – identity management for education

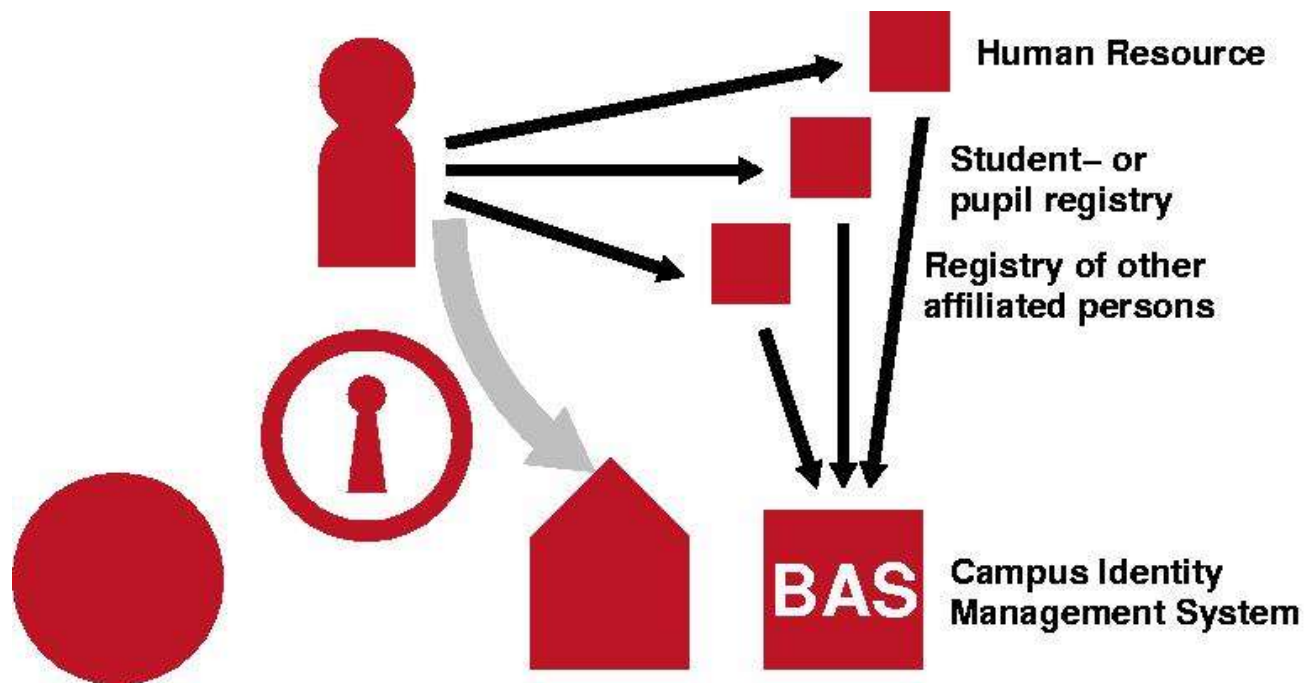
Identity management consists of:

- Information model
- Login service
- Chain of trust
- Policy issues
- Collaboration between educational institutions, service providers and vendors

FEIDE information model

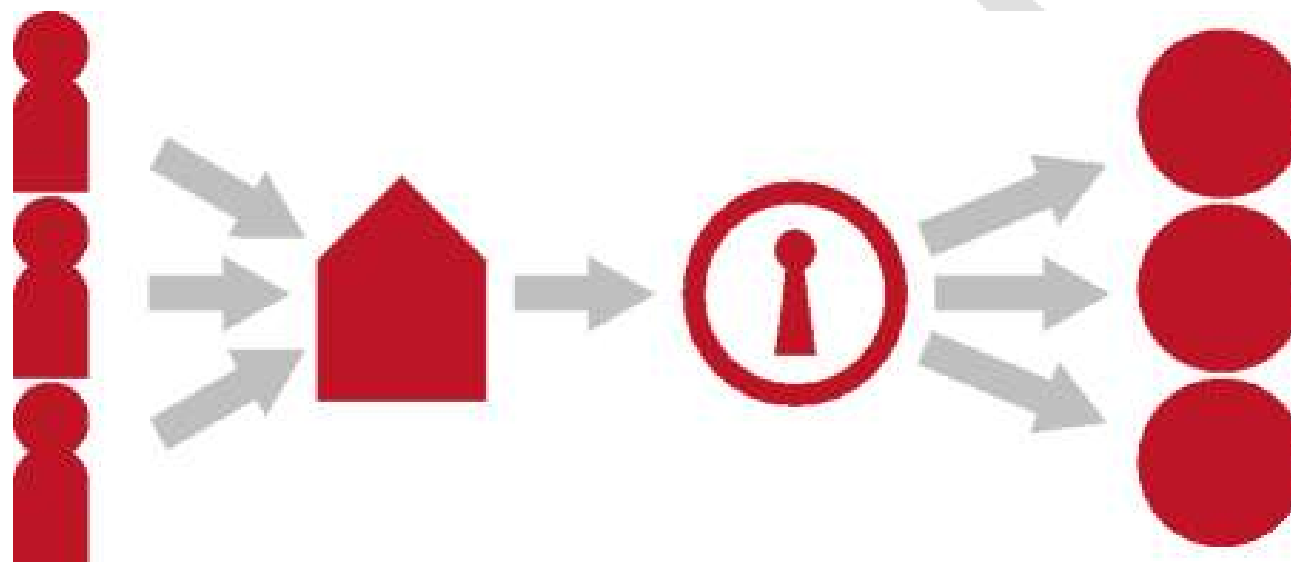
- Identity providers (=campus) 
- Authoritative data flows to LDAP-directory
- Information on standard format
 - ◆ eduPerson, eduOrg
 - ◆ norEduPerson, norEduOrg, norEduOrgUnit
- Standardized import/export
 - ◆ Provisioning
 - ◆ Service Provider integration
- Requirements for campus identity management

Campus Identity Management



- Authoritative data sources
- BAS (CIMS) is hub in information flow
- All updates and changes flows through BAS
- BAS is a necessary component

Campus Identity Provider benefits



- Authoritative quality and control of information flow for all affiliated users
- Enhanced user management simplifies and automates
- Federated login provides access to services

CleanIT, the **BAS/CIMS** process

- Identify key data
- Identify who is responsible for
 - ◆ Initial data
 - ◆ Data updates
 - ◆ Data removal
- Organizational process
 - ◆ Move data maintenance out of the IT department
 - ◆ Enable Human Resource and Student Management staff to do their jobs better

What is BAS? Campus IdM (User Management System)

- Campus Identity Management
- Routines and policy for data updates
- Data quality, well-defined requirements
- Quality assurance (identity)
- Not really an «application»
- Technical solutions:
 - ◆ Cerebrum
 - ◆ Novell
 - ◆ Stover's Microsoft-based
 - ◆ (In-house ad-hoc solutions)



Cerebrum

- Proof-of-concept
- Made for complex heterogenous environments
- Implementation
 - ◆ PostgreSQL db
 - ◆ API-set in python
 - ◆ Information import
 - ◆ Information export
 - ◆ Java client (XMLRPC)
- Open software
- <http://cerebrum.sf.net>
- Integrates with
 - ◆ FS, student registry
 - ◆ LSP, payroll system
 - ◆ ClassFronter
 - ◆ it's:learning
 - ◆ AD and NIS



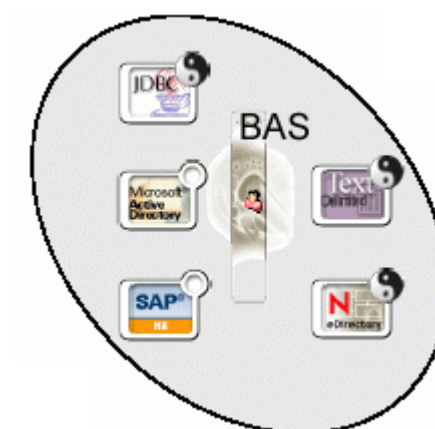


Cerebrum modules

- NIS
- AD
- Mail (Exim)
- Mail (IMAP)
- LDAP (FEIDE)
- FS (5.0) student registry
- LT payroll system
- FRIDA report system
- RADIUS (via LDAP, NIS, AD)
- Home disk (NIS)
- Admin client (BOFH)
- VLE (ClassFronter)
- MSTAS student registry
- SATS/IST school registry
- Print accounting (Via PRISS)
- Disk accounting
- Notes integration
- UA
- POLS payroll system
- AutoStud

Novell BAS solution

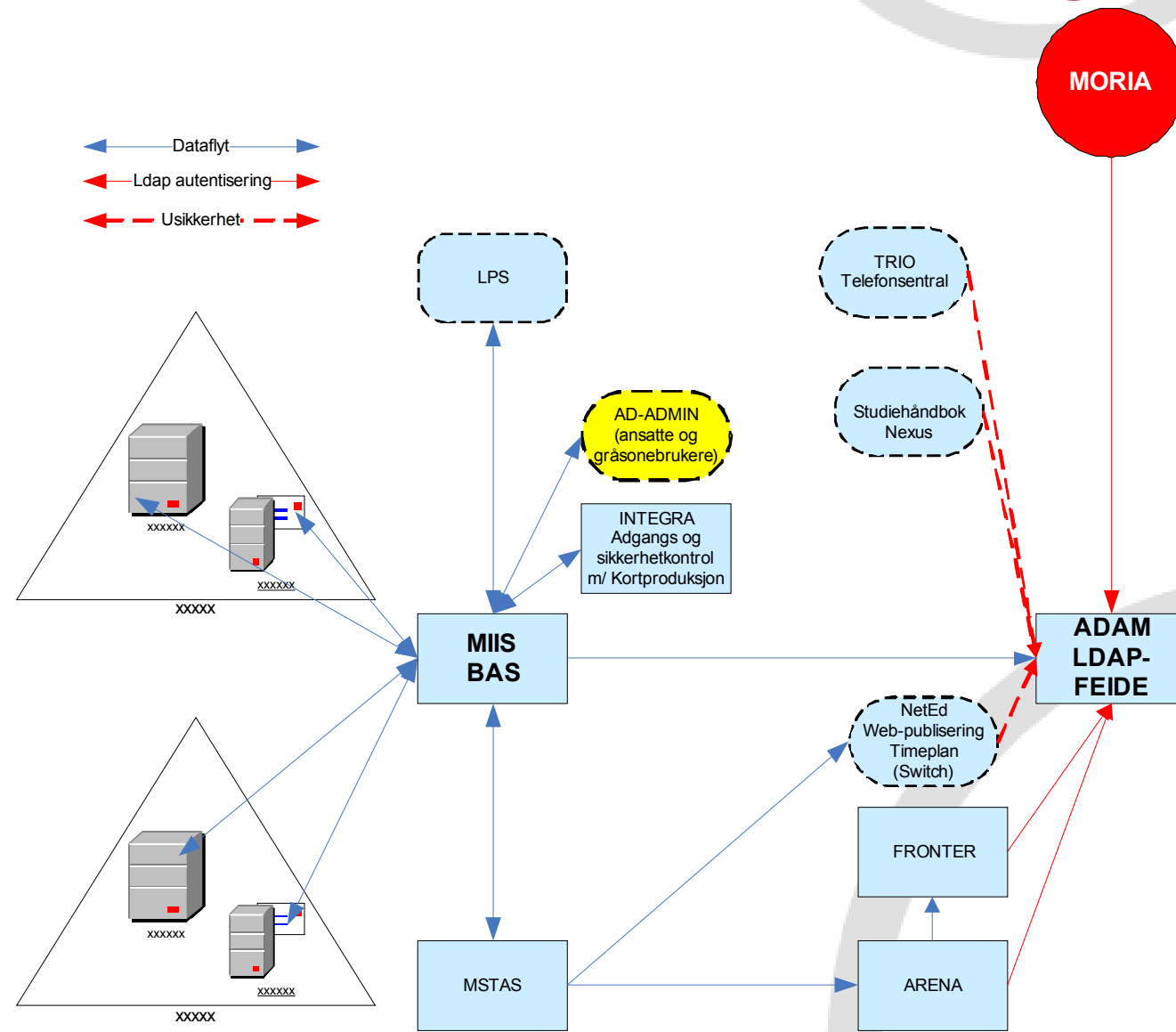
- Directory:
eDirectory 8.7.3
 - Data synchronization:
Identity Manager 2.0
 - Data management:
iManager 2.0.2
 - Cluster of 5 university colleges in user group
 - Future solution: Novell Access Manager
- Example: Sogn and Fjordane University College



Stover's Microsoft-based solution

- Active Directory (ADAM)
- Microsoft Identity Integration Server
- Integrates with
 - ◆ FS and MSTAS student registries
 - ◆ VLE: ClassFronter
 - ◆ PABX
- Cluster of 6 university colleges
 - ◆ User group
 - ◆ Community support

Example: Ålesund University College



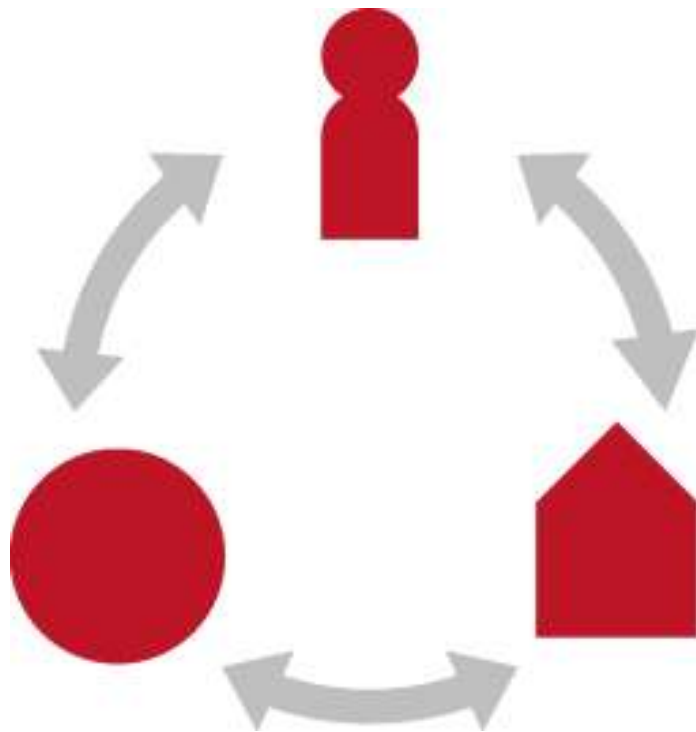
Campus Identity Management Systems

- Several systems are operational, pick one for your campus
- Integration with local systems decide which one to chose, dialogue with vendor
- Not cost-effective to have many
- Federating across different systems is relatively painless
 - ◆ Interfaces are important in bottom-up design
 - ◆ Collaboration, work with vendors

Future directions, campus IdM

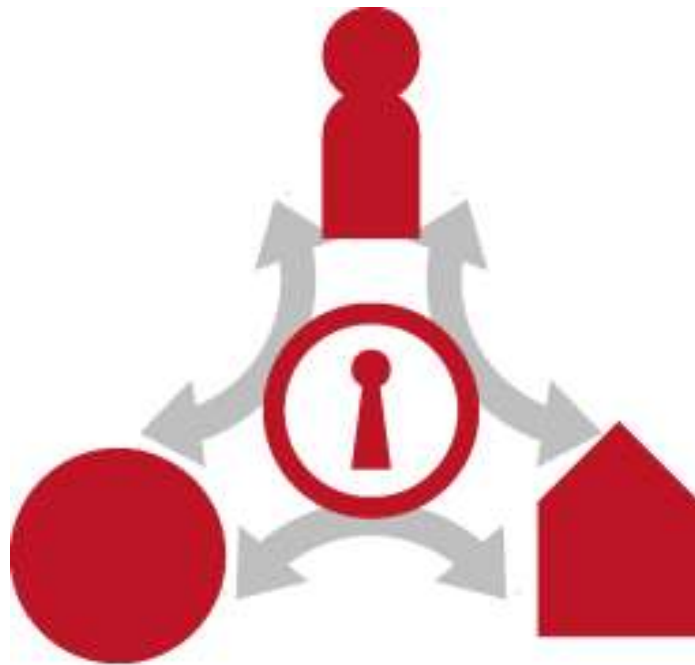
- Responsibility placed outside IT department
- Consolidating BAS for user management
 - ◆ Technical solutions
- Policy and regulations
 - ◆ Giving access to someone I do not control?
- Interfaces
 - ◆ XML definitions for import/export
 - ◆ LDAP based on eduPerson/noredu*
- Available software is improving

Why federate?



- Users and home organizations and service providers need to exchange information
- Trust establishment
- Information exchange
- Policy
- Technology

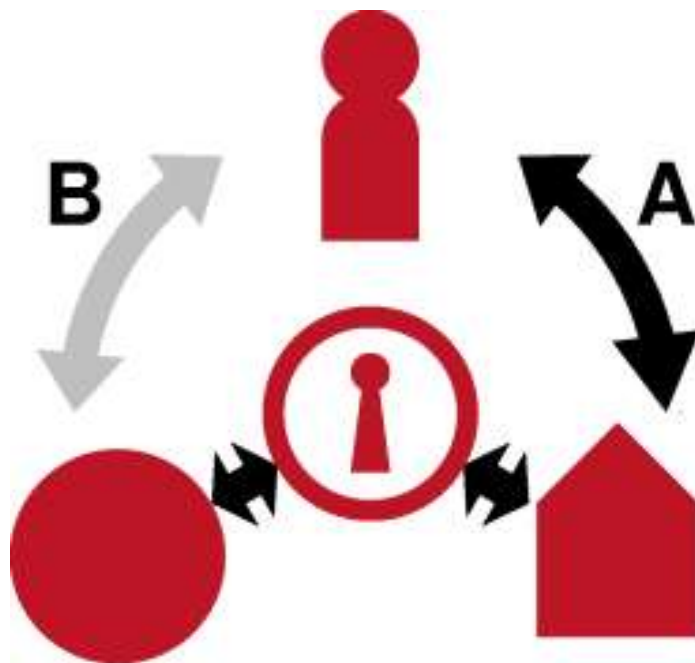
FEIDE federates education



Federations:

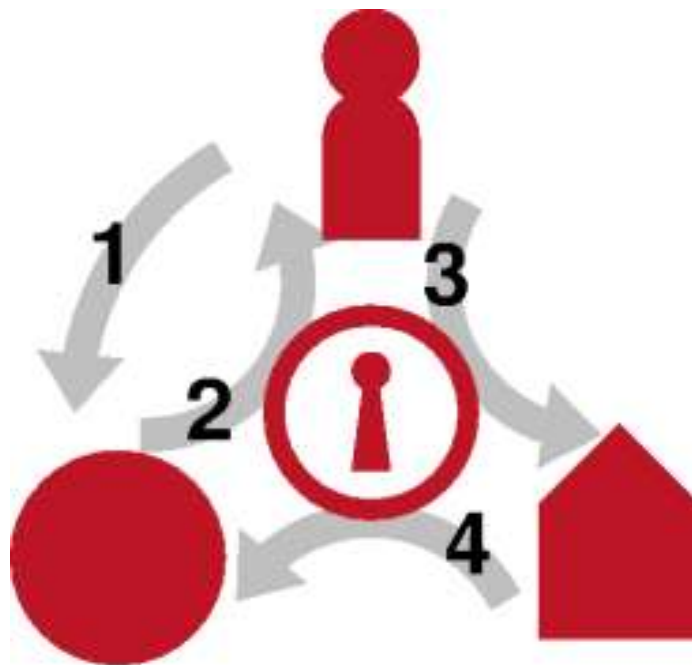
- authenticate
- enforce information flow policy
- privacy control
- security
- trust establishment

FEIDE – trust chain



- FEIDE regulates service providers and home organizations
- Formal contractual agreements
- Transitive trust from end user to service provider via identity provider

FEIDE login

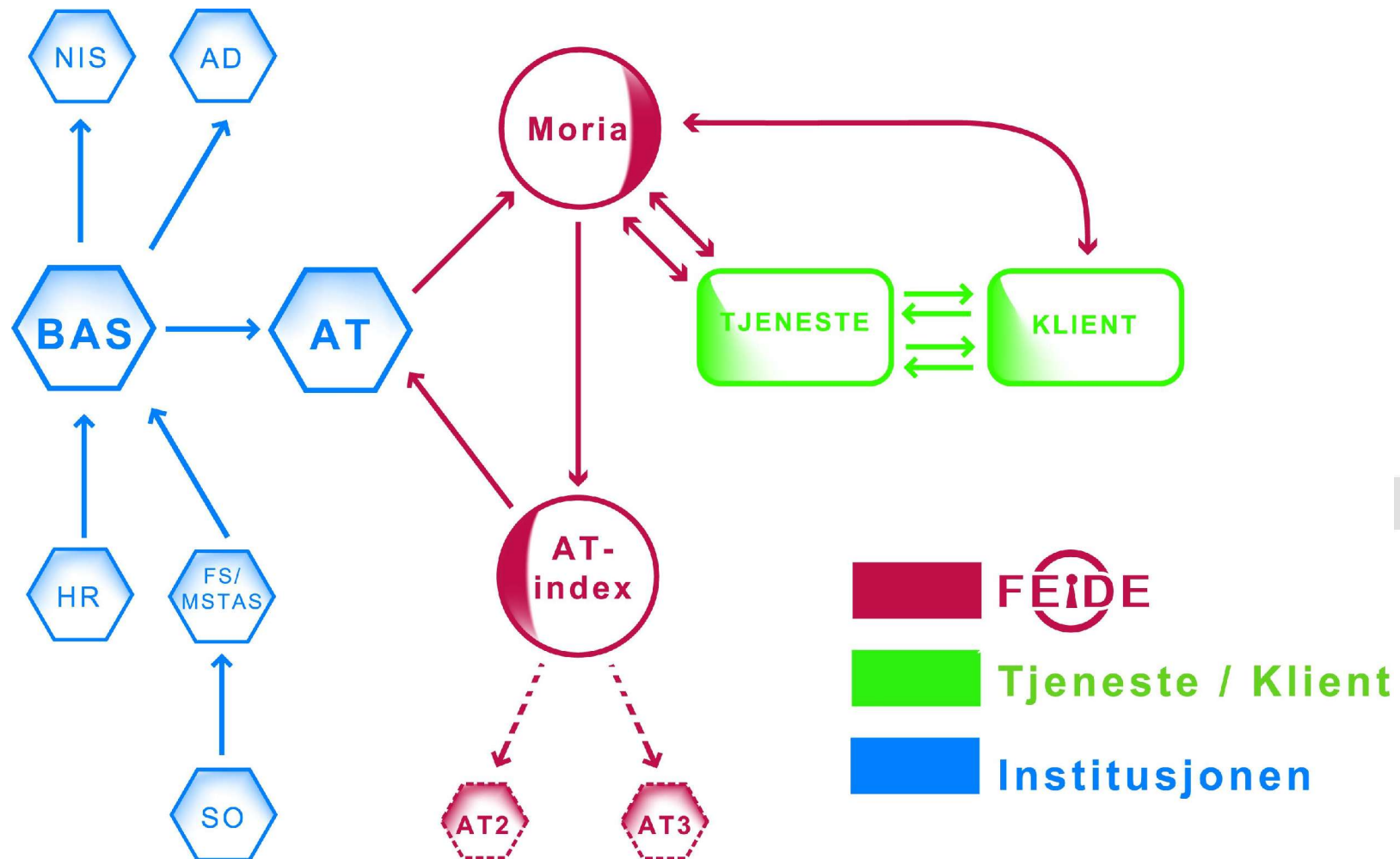


- 1) User tries to access service
- 2) Service transfer user to FEIDE login
- 3) Authentication is done at campus
- 4) Authentication is confirmed with the service, possibly with attribute release

FEIDE for Norwegian education

- Operational campus (start 2003)
 - ◆ Universities: 2003 - early 2006
 - ◆ University Colleges: 2004 - 2006
 - ◆ Lower education: phasing in from fall 2006
- Operational service providers
 - ◆ Shared services in higher ed: 2003 - 2006
 - ◆ Community web services in lower education: 2006 – 2007
 - ◆ Local university services: 2003 – 200X

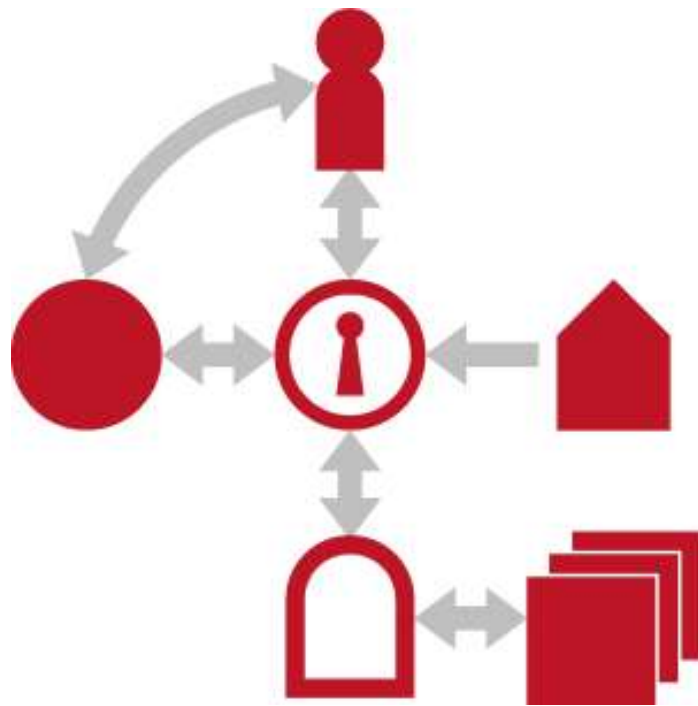
Federating FEIDE, first try



Federation software: Moria

- Open source, <http://moria.sf.net>
- Operational since 2003 (a year before Shib:)
- Technology
 - ◆ Centralized login solution (Web Service)
 - ◆ Distributed directory solution (LDAP)
 - ◆ Java
- FEIDE is adding support for SAML and Shibboleth, possibly in Moria

Federating FEIDE, next try



- Federating with
 - ◆ federations
 - ◆ portals
 - ◆ local login servers
- Standards
 - ◆ SAML 2.0
 - ◆ SAML 1.1
 - +extensions
 - ◆ ID-FF 1.2 ?

Future directions, federation

- Distributed federation (SAML, ID-FF)
- Cross-federating
 - ◆ eduGAIN
 - ◆ Government PKI-portal
 - ◆ Non-education federations
- Services for both higher and lower education
- Outreach program

Summary

- Campus identity management
 - ◆ Not an IT issue
 - ◆ Move responsibility to where it belongs
 - ◆ Provide technical solutions
- Federated identity management
 - ◆ Collaboration is the key
 - ◆ Community effort
 - ★ Trust
 - ★ Policy
 - ★ Some technology

More information

- <http://www.feide.no/index.en.html>
- Email for FEIDE:
 - ◆ administrasjon@feide.no
- Questions for Ingrid
 - ◆ ingrid.melve@uninett.no