

Kva skal eg snakka om?

- Kva er FEIDE?
- BAS på kort og lang sikt
- Standardisering inn/ut for BAS
- Tenester i FEIDE
- Ny programvare for innlogging
 - ◆ SUN Java System Access Manager
 - ◆ Innlogging og føderasjonar (Liberty Alliance)
 - ◆ Sikkerhetsportal, eduGAIN og andre

FEIDE – Felles Elektronisk Identitet



Brukarar; alle med FEIDE-namn
im@uninett.no, bpd@uib.no



Vertsorganisasjonar; lærestaden
til brukaren

UiB, HiB, HiO



Tenester; system og applikasjonar
Frida, BIBSYS, SAP ESS, portalar

FEIDE - identitetsforvaltning for utdanning

Identitetsforvaltningen er samansett av:

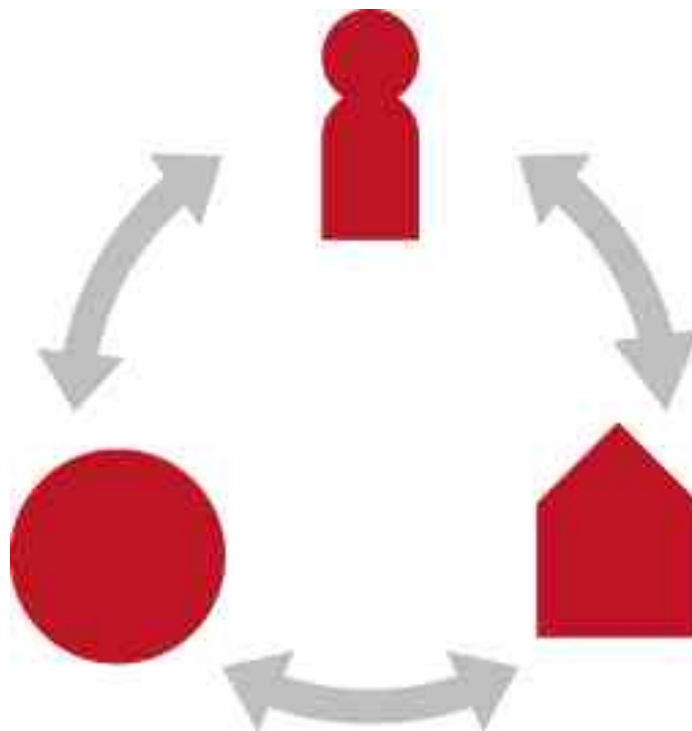
- Ein informasjonsmodell
 - ◆ Kva skal vi vita om personar
- Ei innloggingsteneste
- Ein tillitsstruktur og samarbeid mellom organisasjonar i utdanningssektoren og deira leverandørar av IT-baserte tenester
 - ◆ Formelle avtalar og kontraktar
 - ◆ Policy (t.d lokale IT-reglement)

FEIDEs informasjonsmodell

- Alle vertorganisasjoner lagar standardisert informasjon om sine brukarar tilgjengeleg for innloggingstenesta i FEIDE
- FEIDE henter informasjon i lokal LDAP
- Struktur og semantikk i katalogen basert på internasjonalt arbeid og standarder
 - ◆ norEduPerson
 - ◆ norEduOrg og eventuelt norEduOrgUnit
- Standardisert import/eksport til BAS
 - ◆ Starter formell standardisering i vår

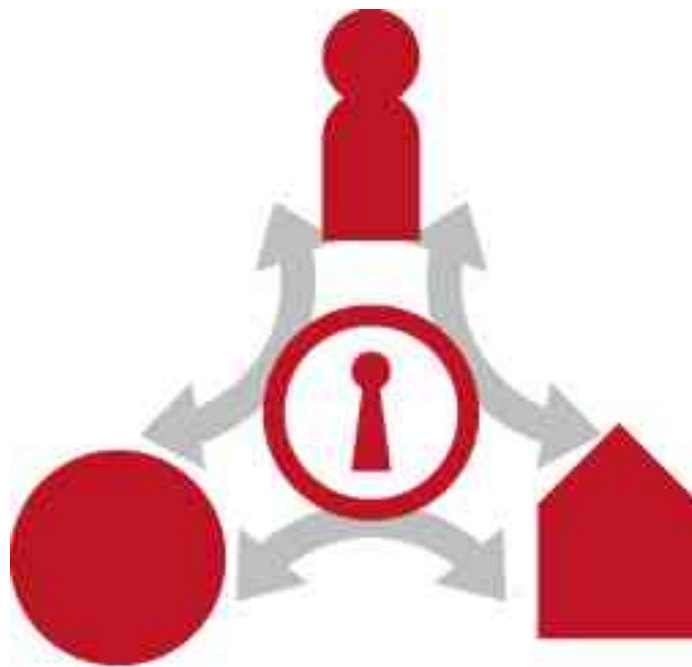


FEIDE – konseptet



- Brukarar, vertsorganisasjonar og tenester danner FEIDE infrastruktur – og dei må kommunisera med kvarandre

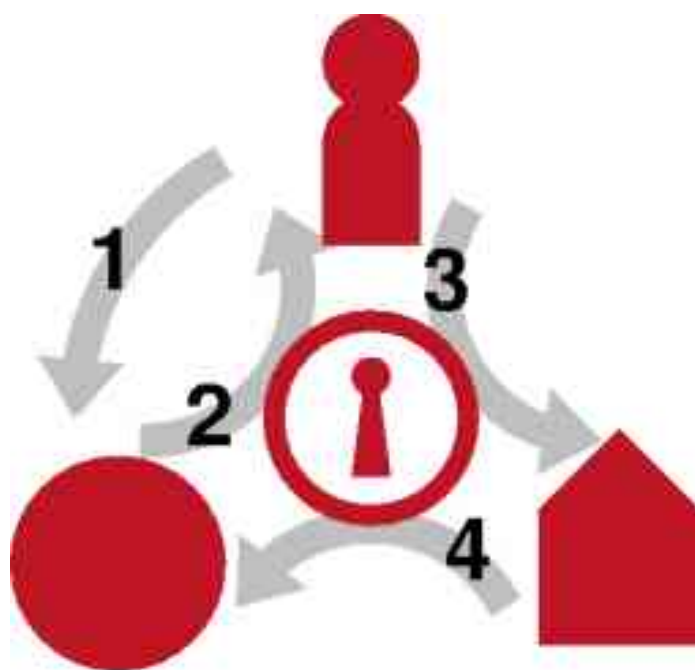
FEIDE bind saman datasystem



FEIDE sørger for:

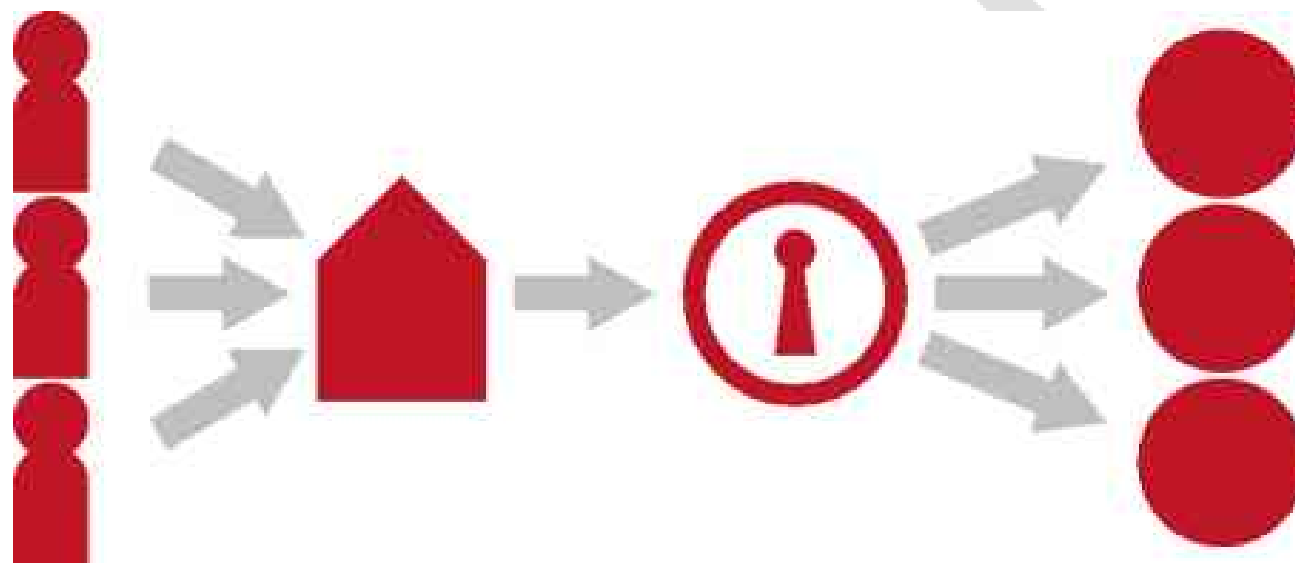
- autentisering
- informasjon til bruk i autorisasjon
- kontrollert dataflyt
- innsyn og personvern
- tryggleik
- tillit mellom alle parter

Slik virker innlogging med FEIDE



- 1) Bruker kontakter tjeneste
- 2) Tjenesten videresender bruker til FEIDEs innloggingstjeneste
- 3) Innloggingen viderefremidles til vertsorganisasjonen
- 4) Tjenesten får bekreftelse på innlogging og evt. ønsket datamengde

Fordeler for vertsorganisasjonar



- Kontroll, kvalitet og oversikt over informasjon om alle tilknytta personar
- Betre brukeradministrasjon som forenkler og automatiserer
- Felles innloggingsfunksjon for alle tjenester, egne og eksterne

Sebra er viktig komponent for FEIDE ved UiB

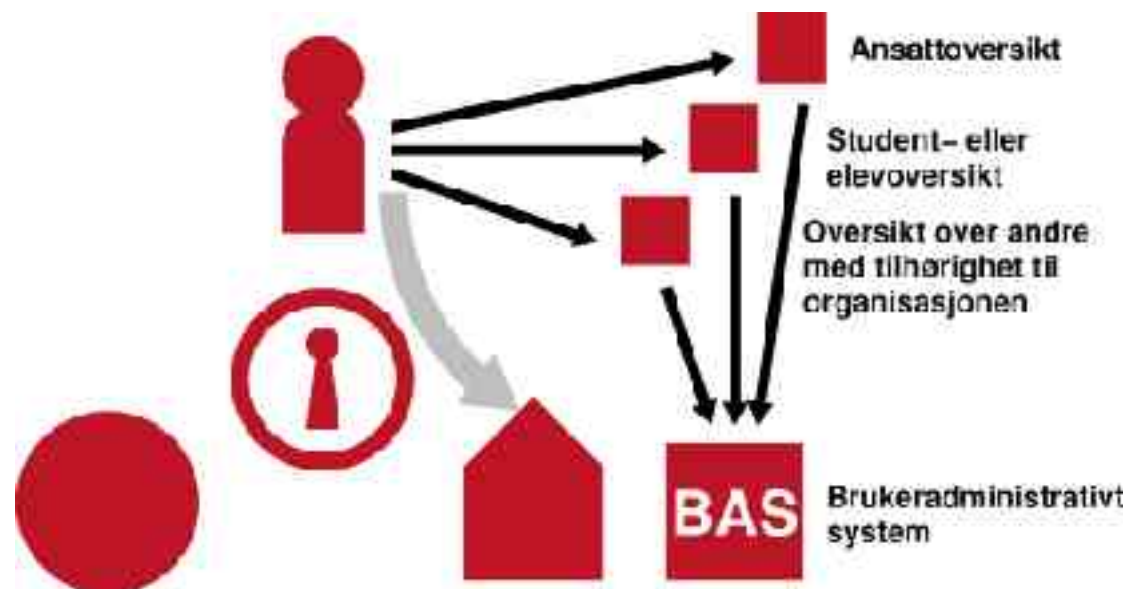
- Sebra er UiB sitt brukaradministrative system (BAS)
- Sebra har kontroll over alle brukarar
- Sebra sørger for at FEIDE-tre av informasjon blir lagt i LDAP
- Sebra har alltid oppdaterte data om alle UiB-brukarar
- Universiteta ønskjer å sjå saman på neste generasjons Sebra (ein sjiraff? ein antilope? utgreiing starter i år, operativ 2008)

BAS til kvardags «korleis ri ein sebra»

- Datakvalitet og rutiner for oppdatering
- Flytta arbeid frå IT-avdeling til riktig plass
 - ◆ Personalavdeling
 - ◆ Gjestehandtering (slik som UiB har gjort)
 - ◆ Studieavdeling og FS
- Kvalitetssikring, forretningslogikk i BAS
- Kva er viktigaste data å halda styr på?
- Sitat frå BAS-brukergruppe:
«Rensing, rydding og rutiner; det er BAS»



Brukeradministrasjon hos vertorganisasjonene



- Alle data hører hjemme i en datakilde
- BAS holder nødvendig oversikt og kontroll
- Kontrollert flyt av endringer, f.eks. når noen slutter
- BAS er en nødvendig lokal komponent

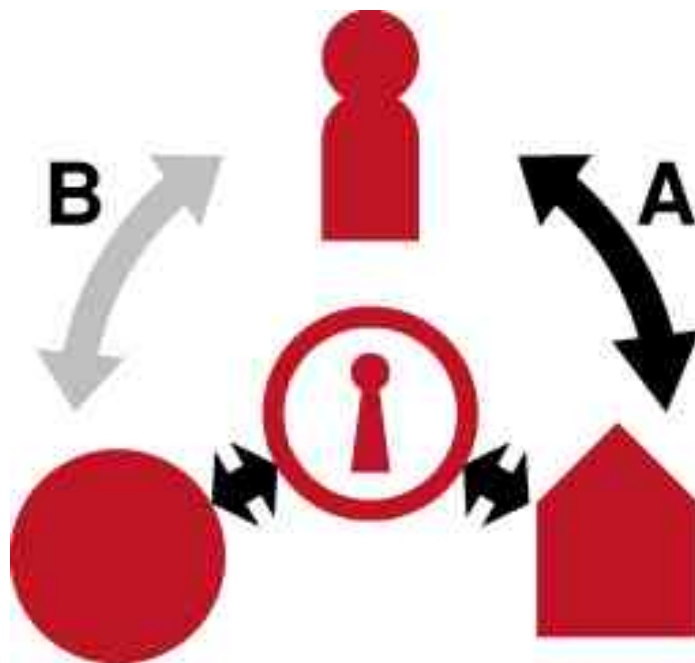
Standardisering

- Igangsetting av arbeid med standardisering
 - ◆ Arbeidsnamn: Elevidentifikasjonsstandard
 - ◆ Norsk Standard
 - ◆ Ope arbeidsgruppe
- Grensesnitt inn til og ut frå BAS
 - ◆ XML-format
 - ◆ Datadefinisjonar
- Innspel frå FEIDE med eksisterande batchløysingar og behov for event-drift
- Tidshorisont: 9-14 mnd frå oppstart

BAS med ulik horisont

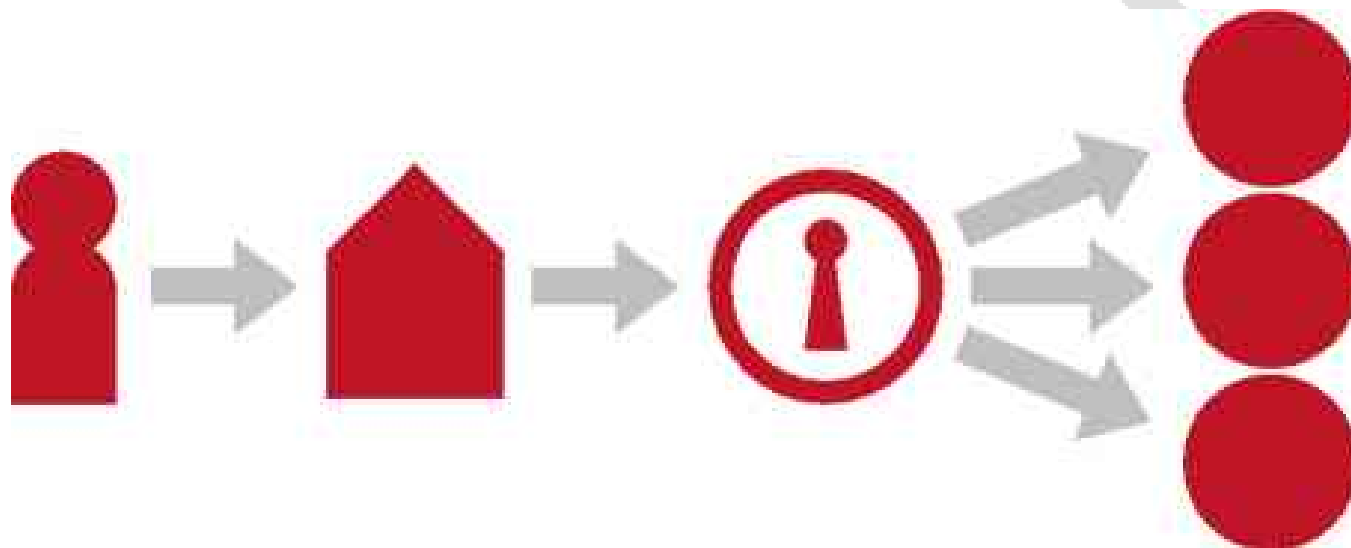
- Dagens løysingar vil leva ut 2008
- Kva skjer på sikt? 2008-2015
- Kravspesifikasjon er ønska av universiteta
 - ◆ integrasjon: FS, Frida/forskdok, Agresso, SAP HR, eBusiness Suite
- BAS-samarbeid om kravspesifikasjon mellom universitet og høgskular?
 - ◆ Vurdera tilgjengeleg system, vidareutvikling Cerebrum eller utvikling av nytt system
 - ◆ Heilskap i BAS, modulært oppbygd

FEIDE – en tillitsstruktur



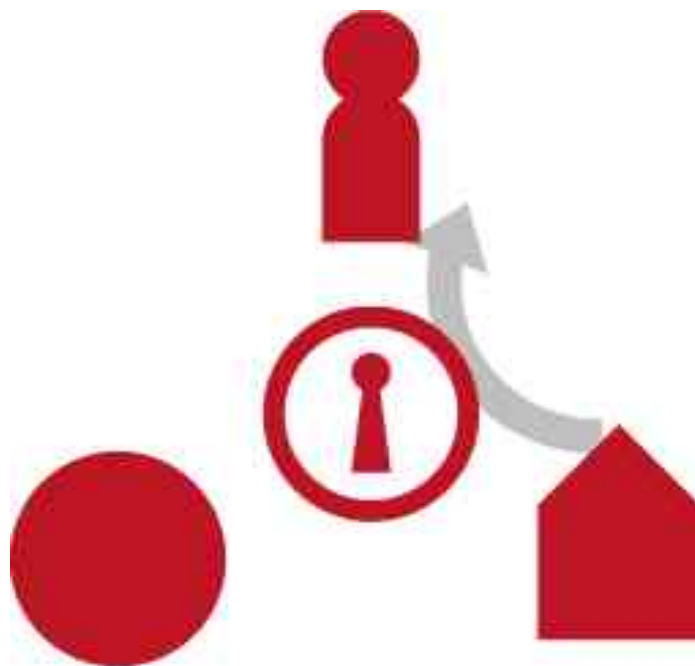
- FEIDE stiller krav og forplikter tjenesteleverandører og vertsorganisasjoner
- Formalisert i kontrakter og avtaler
- Tillit formidles mellom partene pga tillit til FEIDE

Fordeler for brukere



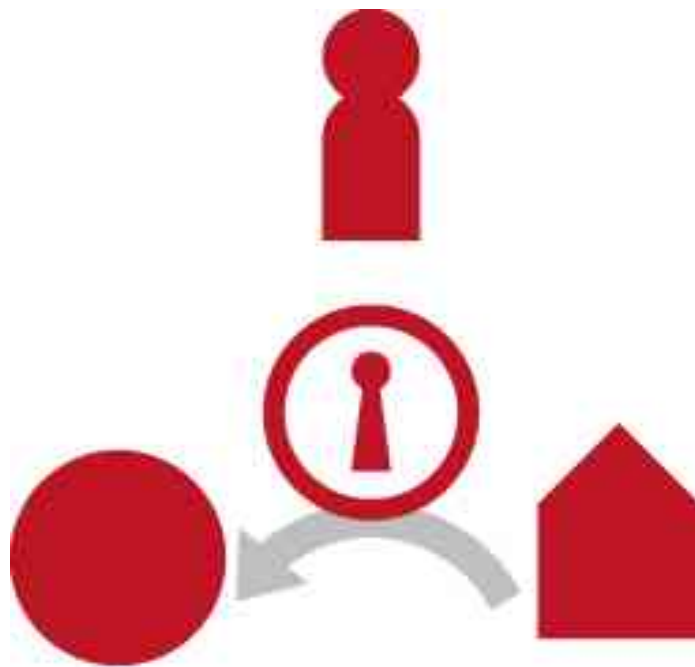
- Samme FEIDE-navn og passord virker for alle FEIDE-tjenester
- Ingen separat registrering i de enkelte tjenestene, FEIDE benytter kun data fra brukerens egen organisasjon

Brukerens rettigheter: innsyn i egne data



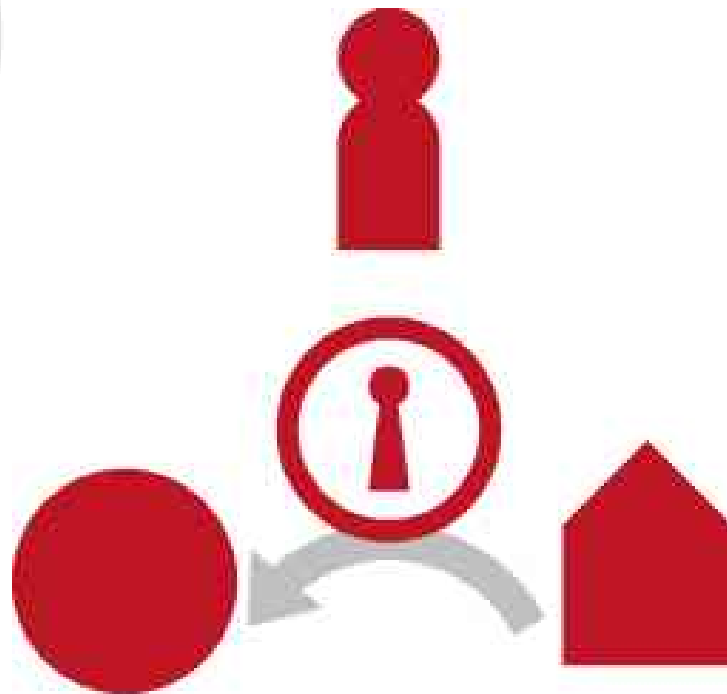
- FEIDE har egen innsynstjeneste
- Brukerne får se det egen organisasjon har lagret om dem

Brukerens rettigheter: samtykke til dataoverføring



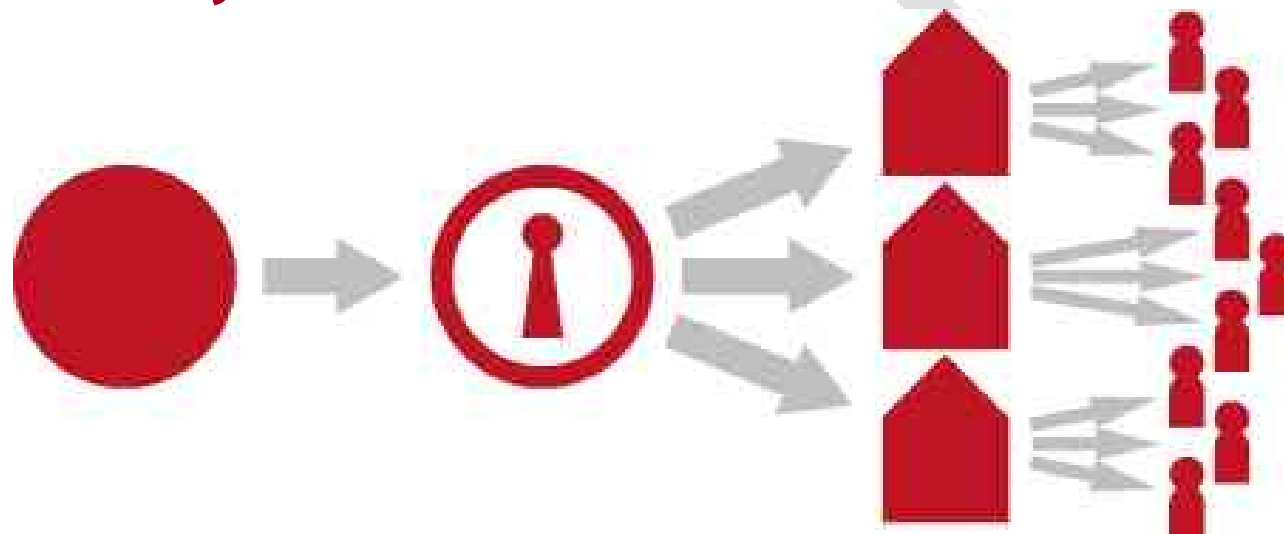
- Ved innlogging kan tjenesten be om data om brukeren
- På innloggingssiden blir brukeren informert om datamengden
- Brukeren gir samtykke

I FEIDE er alle data under lokal kontroll; ingen sentral database finnes



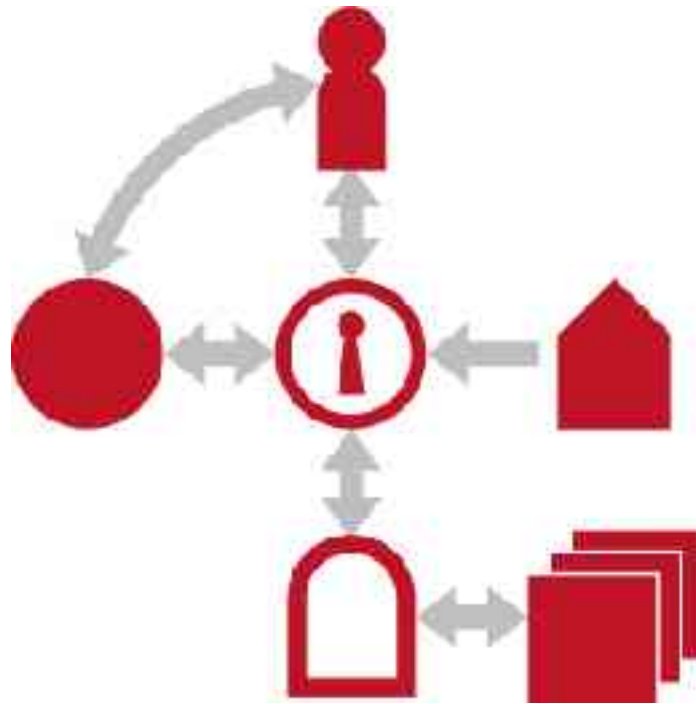
- FEIDEs innloggingstjeneste tar imot FEIDE-navn og passord på vegne av tjenestene
- Autentiseringen utføres i den enkeltes vertorganisasjon
- Informasjon om pålogget bruker kan gis til tjenestene, f.eks. navn og rolle
- Tjenestene behandler ikke passord

Fordeler for tjenester



- Tjenesten får potensielt tilgang til alle FEIDE-brukere
- FEIDE står for innloggingsfunksjonen og kan gi fra seg kvalitetssikrede data om påloggete brukere
- Tjenesten trenger ikke tenke på autentisering og vedlikehold av data (spesielt passord)

FEIDE og Sikkerhetsportalen



- Kryssfødererer med
 - ◆ Sikkerhetsportal
 - ◆ eduGAIN
 - ◆ andre føderasjonar
- Samtrafikk basert på opne standardar
- Operativ m/demo 20.06.2006

FEIDE handler om

- Identitetsforvaltning på campus
 - ◆ Ikkje (berre) for IT-avdelinga
 - ◆ Flytta ansvar dit det høyrer heime
 - ◆ Tilby gode teknisk løysingar
- Føderert identitetsforvaltning
 - ◆ Samarbeid er nøkkelord
 - ◆ Utdanningssektoren går saman om
 - ★ Tillit
 - ★ Policy
 - ★ Litt teknologi

Tenesteleverandører

- Mitt BIBSYS
- Frida
- Lokale portalar
- StudentWeb
- Elektronisk faktura
- Nasjonalbiblioteket
- Sympa epostliste
- Vortex skrivbar web
- Innsyn
- Tenester på veg:
 - ◆ ePhorte
 - ◆ ForskDok
 - ◆ Kvoter for tungregning
 - ◆ eLæring
 - ◆ SAP sjølvbetening
 - ◆ Oracle portal og andre portalar
 - ◆ Wiki

Tenesteintegrasjon

- Flytt innlogging ut av tenesta
 - ◆ Tjenesta får ikke tilgang til passordet
 - ◆ Krev ein modul eller eit filter i tenesta
 - ◆ Enkel web service-basert integrasjon
- Moria2: operativ fram til vår 2007
- SAML/ID-FF-basert: operativ sommar 2006
 - ◆ Sun Access Manager vald som programvare
 - ◆ Opne standardar basert på Liberty Alliance
 - ◆ Det er råd å laga integrasjon vha programvare frå mange ulike leverandørar

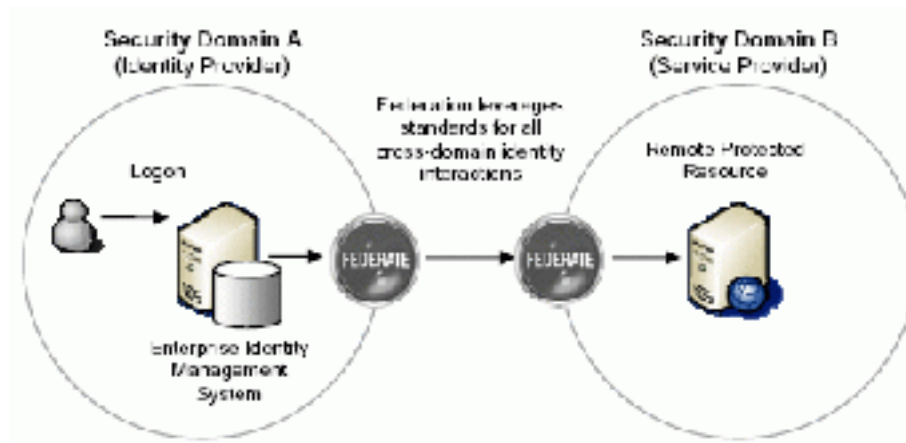
Kvar går Moria?

- FEIDE si innloggingsteneste blir styrka
- Enklare integrasjon pga standardisering
 - ◆ FEIDE har avventa SAML2.0
- Ryddigare identitetsforvaltning
 - ◆ Standardisering av grensesnitt
 - ◆ Diskusjon om eID
- Kryssføderering:
 - ◆ Sikkerhetsportalen
 - ◆ eduGAIN
 - ◆ nordisk samarbeid
 - ◆ norske identitetstenester?

Ny programvare for innlogging

- Strategisk avtale med Liberty Alliance-medlem
- Standardisering og utviding av funksjonalitet
- Operativ
 - ◆ Første fase: sikkerhetsportal 10.06.2006
 - ◆ Andre fase: SAML2.0/ID-FFI.2 juli? 2006
 - ◆ Tredje fase: Overflytting eksisterende tenester hausten 2006
 - ◆ Fjerde fase: WS-Federation? haust 2006

Føderert identitet



- Kopla saman lokal identitet med resten av verda
- Nøkling på unike fødererte identitetar
 - ◆ Støtte for ein ID per brukar per teneste
 - ◆ Støtte for å senda attributtar

Sun Java System Access Manager

- Liberty Alliance-støtte
 - ◆ Conformance testing utført
 - ◆ Integrerer mot programvare frå mange ulike leverandørar
- Avtalen dekkjer heile Identity Management Suite, meir enn berre innlogging
- Framdrift
 - ◆ Val av leverandør 10. mars 2006
 - ◆ Kunngjering går ut mandag
 - ◆ Testoppsett i gang, demo på UNINETT2006

Meir informasjon

- <http://www.feide.no/>
- Epost til FEIDE:
administrasjon@feide.no
- Epost til meg:
ingrid.melve@uninett.no