


# NDB-Rammeverk


---

***Arbeidspakke 4: Autentisering og autorisering***  
**Sluttrapport**


 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato		27.12.2005
	Side		2
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Brygfeld	Godkjennes av: Styringsgruppen	Revisjon A

## Innhold

<b>1. Forord</b> .....	<b>2</b>
1.1 Oppsummering .....	2
<b>2. Generell informasjon</b> .....	<b>2</b>
2.1 Revisjonshistorikk .....	2
2.2 Dokumentets hensikt og omfang .....	2
2.3 Arbeidsgruppens sammensetning .....	2
<b>3. Introduksjon</b> .....	<b>2</b>
3.1 Hensikt .....	2
3.2 Omfang .....	2
3.3 Overordnet funksjonalitet .....	2
3.3.1 LDAP .....	2
3.3.2 Produkt implementering mot andre tjenester og produkter. ....	2
3.3.3 Identity Management (IdM) .....	2
<b>4. Design</b> .....	<b>2</b>
4.1 Løsningsdesign .....	2
4.1.1 Konfigurasjon av LDAP .....	2
4.1.2 Organizational Units (OU)- og Group Policy Objects (GPO)-struktur .....	2
4.1.3 Roller .....	2
4.1.4 Grupper .....	2
4.2 Kapasiteter/volum/skalering .....	2
4.2.1 Suksessfaktorer .....	2
4.3 SLA .....	2
4.4 Sikkerhet .....	2
4.4.1 Fysisk sikkerhet .....	2
4.4.2 Nettverkssikkerhet .....	2
4.4.3 Sårbarheter og konsekvenser .....	2
4.5 Kostelementer .....	2
<b>5. Grensesnittspesifikasjoner</b> .....	<b>2</b>
5.1.1 NDB .....	2
5.1.2 NTNU - FEIDE .....	2
5.1.3 Beskjed når brukere blir opprettet og slettet .....	2
5.2 Pålogging/autentisering/sertifikat /adgangskort .....	2
5.2.1 Sertifikat .....	2
5.2.2 Tilbakekallingslister .....	2
5.2.3 Sertifikat og tilbakekallingslister .....	2
5.3 Adgangskontroll .....	2
5.3.1 Synkronisering av informasjon .....	2
5.4 Beskjed når brukere blir opprettet og slettet .....	2
<b>6. Anbefalinger fra AP4</b> .....	<b>2</b>
6.1 Integrasjon med Feide .....	2
6.1.1 Innsamling av brukerinformasjon .....	2
6.1.2 Security komponenter .....	2
6.2 Identity and Access management hos NDB .....	2
6.2.1 Access management og Singel Sign On .....	2
6.2.2 Federated Identity Manager (FIM) .....	2
6.2.3 FIM Plug-ins .....	2
6.2.4 FIM og et eller annet AAA system .....	2
6.2.5 Forskjellige leverandører av FIM og andre 3rd party access management .....	2
6.2.6 Andre SAML kompatible løsninger .....	2

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato		27.12.2005
	Side		3
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Bryggfeld	Godkjennes av: Styringsgruppen	Revisjon A

6.3	Oversikt SAML og Liberty Alliance .....	2
6.3.1	Difrensatorer mellom SAML vs. Liberty Alliance og anbefalinger .....	2
6.3.2	Kort teknisk beskrivelse av SAML Assertions .....	2
6.3.3	Mulig bruk for SAML Tokens .....	2
<b>7.</b>	<b>Vedlegg .....</b>	<b>2</b>
<b>8.</b>	<b>Begreper .....</b>	<b>2</b>

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato		27.12.2005
	Side		4
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Brygfeld	Godkjennes av: Styringsgruppen	Revisjon A

## 1. Forord

Dette dokumentet er resultatet av arbeidet i den arbeidsgruppen som er satt ned for arbeidspakke 4, *Autentisering og Autorisering* i prosjektet *NDB-Rammeverk*.

Arbeidsgruppen har hatt som oppgave å utrede og komme med anbefaling i til løsning for Autentisering og Autorisering i NDB, og i dette dokumentet vil en finne denne anbefalingen i form av foreløpig beskrivelse av et systemdesign (PDR, Preliminary Design Review) som inngår i utviklingen og utredningen av NDB-Rammeverk.

Dette foreløpige designet har hatt til hensikt å få designet et system som ivaretar omforente krav mellom kundene, NDB, og andre aktuelle informasjons leverandører (andre bibliotek nasjonale og internasjonale) og systemavhengigheten mellom andre arbeidspakker.

Til slutt nevnes det at dokumentstrukturen vil revideres som underlag for utarbeidelse av endelig systemdesign (FDR, Final Design Review) på bakgrunn av de erfaringer som er gjort i prosjektet .

### 1.1 Oppsummering


Arbeidsgruppen for AP4 har sett på forskjellige prosesser inne Autentisering, Autorisasjon og brukerhåndtering for å kunne finne fram til alternative løsninger for NDB. En har sett på kjente metoder og mekanismer for de forskjellige fagområdene, samt sett på hvordan disse fagområdene utvikler seg med nye standarder. Basert på den utvikling vi ser innen disse områdene i dag, har en så sett på hvordan en skal kunne bygge en løsning som både ivaretar dagens behov i et samspill med de nåværende løsningene, og som er rustet for å håndtere framtidige behov og basert på fremtidige løsninger med de nye standardene.

En har valgt å forholde seg til internasjonale standardiseringsenheter innen fagmiljøene samtidig som en har innhentet produkt og informasjon fra forskjellige produsenter som anses som ledende innen de forskjellige fagmiljøene. En har således kommet frem til en foreløpig design som vil sikre NDB en stor grad av åpenhet, en leverandør-uavhengighet samtidig som en kan få integrert nye og teknologiløsninger som sikrer fremtidige investeringer og løsninger i NDBs rammeverk.

Vi har også sett på de forskjellige løsningene innen Autentisering, Autorisasjon og katalogtjenester som for tiden holder på å bli integrert hos offentlige og private virksomheter og organisasjoner. En ser for seg at en kan integreres med flere av disse, både eksisterende og fremtidige løsninger. En har sett spesielt på FEIDE, BankID og Norsk Tipping. Alle disse integrasjonene har til stor grad løsninger som lar seg integrere i den arkitekturen som en har sett på for NDB. Gruppen har sett spesielt på Feide-prosjektet, som enkelt kan la seg integrere inn i en løsning for NDB. En integrasjon med FEIDE, vil medføre at en enkelt kan tilby tjenester fra NDB til både universiteter, høyskoler og ungdoms-/barneskoler i hele Norge. Basert på tall fra FEIDE, vil dette kunne gi ca 1.500.000 brukere. En slik integrasjon vil kunne tilgjengeliggjøre NDB-informasjon til samtlige elever helt fra barneskolen og opp til universitetsnivå, basert på den enkeltes student / elev behov og interesser.

Arbeidsgruppen anser en fremtidsrettet Autentiserings-, Autorisasjons- og katalogtjeneste hos NDB som av de avgjørende suksessfaktorer i arbeidet med å etablere en løsning av nye tjenester og et fundament for fremtidige løsninger hos NDB. En ser for seg at NDB skal kunne koble seg opp mot de forskjellige tjenester og vil således bli et nav i tjenestehjulet for tilganger av NDB-tjenester avhengig av den enkelte personen eller kunde.

Arbeidsgruppen anser at en har fått gjennomført en god og gjennomgang av de teknologier og standarder som eksisterer i dagens marked. Dette, sammen med en gjennomgang av informasjon fra kjente internasjonale analyseselskap, har vært nyttig i den arkitekturen som en har kommet frem til. Dokumentet forøvrig inneholder en del tekniske vurderinger og aspekter som en vil ha med i en videre arbeidsdokument. Mye av dette kan også legges til grunn for å lage en kravspesifikasjon for NDB-prosjektets videre arbeid. Det er også beskrevet i slutten av dokumentet en anbefalt løsning for NDB i fremtiden.

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato		27.12.2005
	Side		5
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Brygfeld	Godkjennes av: Styringsgruppen	Revisjon A

## 2. Generell informasjon

### 2.1 Revisjonshistorikk

Versjon	Dato	Forfatter	Revisjon	Beskrivelse
0,1	16-8-04	KBM	0.1	
FA7	20-12-04	PsR		<ul style="list-style-type: none"> <li>• Dyttet inn i NDB-Rammeverk sin mal.</li> <li>• Generelt: fotnoter med forklaring til ord og uttrykk</li> <li>• Kap. 2.3 – Nytt kapittel</li> <li>• Kap. 3 – Tillegg</li> <li>• Kap. 4.1.2.1 – 4.1.2.3 – slettet</li> <li>• Kap. 8 Begreper – Nytt kapittel</li> </ul>
FA8	21-12-04	PsR		<ul style="list-style-type: none"> <li>• Kap. 1.1 . Nytt kapittel</li> <li>• Kap. 7 – Endret overskrift til <i>Vedlegg</i> og lagt inn liste over de tre vedleggene der</li> <li>• Kap. 2.4 – Nytt innhold: <i>Vedlegg</i> byttet ut med <i>Arb.gruppens sammensetning</i></li> </ul>
FA9	05-01-05	PsR		<ul style="list-style-type: none"> <li>• Nye figurer</li> <li>• Forklaring til begreper</li> </ul>
FA10	01-02.05	PsR		<ul style="list-style-type: none"> <li>• Mindre endring: feil i overskrift kap. 6.1</li> <li>• Slettet kap. 2.2.Rrevisorer</li> </ul>
A	27-12.2005	PsR		<ul style="list-style-type: none"> <li>• Versjonsnummer oppdatert til full versjon: A</li> </ul>

### 2.2 Dokumentets hensikt og omfang

Prosjektet NDB-Rammeverk har opprette en arbeidsgruppe for å håndtere arbeidspakke 4: Autentisering og autorisering.


Hensikten med dette dokumentet er å presentere resultatet av det arbeidet arbeidsgruppen har gjort i form av en anbefaling til løsning for håndtering av Autentisering og autorisering i NDB.

Dokumentet er delt i 8 hovedkapitler:

- **1: Forord**
- **2: Generell info**
- **3: Introduksjon**  
Overordnet beskrivelse av arbeidsgruppens arbeid og den anbefaling som er kommet ut av arbeidet.
- **4: Design**  
Beskriver av den anbefalte, overordnede design av løsningen,
- **5: Grensesnittspisikasjoner**  
Beskriver hvilke grensesnitt mellom ulike systemer som er nødvendig.
- **6: Anbefaling fra arbeidsgruppen**  
Beskriver hvordan arbeidsgruppen anbefaler at man går fram i det videre arbeidet for å implementere den løsningen vi mener er riktig.
- **7: Vedlegg**  
Vedlegg med Felt- og attributt-forklaring for Feide i tillegg til to rapporter fra Burton Group.
- **8: Begreper**

### 2.3 Arbeidsgruppens sammensetning

Arbeidsgruppen for AP4 har bestått av følgende personer:

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato	27.12.2005	
	Side	6	
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Brygfeld	Godkjennes av: Styringsgruppen	Revisjon A

- Svein Arne Brygfeld, Nasjonalbiblioteket  
Leder av arbeidsgruppen
- Kaare Bjørn Martinussen, Phalanx
- Jon Strømme, Feide
- Jan Erik Kofoed, Bibsys

I tillegg har prosjektleder Petter Rønningsen, Nasjonalbiblioteket, deltatt på alle møtene og fungert som sekretær for arbeidsgruppen.

### 3. Introduksjon

AP4 har som oppdrag å komme med en anbefaling innfor følgende områder:

- Minimumskrav til løsning for autentisering og autorisering
- Vurdere aktuelle katalogtjenester
- Vurdere Feide som løsningsmodell
- Anbefale løsning

En katalogtjeneste vil danne kjernen i en løsning for autentisering og autorisering som skal dekke de behov man vil ha i NDB.

Begrepet katalogtjenesten, som dekkes, er delt opp i to samvirkende elementer. Den består for det første av selve katalogen, for det andre av omkringliggende funksjonalitet for vedlikehold og synkronisering av data mellom forskjellige informasjonskilder i infrastrukturen. Katalogen alene omtales som ”katalogen”. Katalogen sammen med den omkringliggende funksjonaliteten omtales i dette dokumentet for katalogtjenesten.

Katalogtjenesten dekker infrastrukturens behov for lagring, konfigurering og deling av informasjon om ressurser i domenet og kontroll av tilgangen til disse. Katalogen lagrer alle data om brukere, aksess, autorisasjon og deres rettigheter satt opp i en RBAC<sup>1</sup> modell.

#### 3.1 Hensikt

Arbeidspakke – 4 inneholder aksess – autorisasjon og katalogtjenesten. En må definere domenestrukturen for det nye NDB, og integrere alle elementene i den nye infrastrukturen med de eksisterende og aktuelle miljøene fra FEIDE<sup>2</sup> og andre katalogtjenester som kan være aktuell for NDB.

Samtidig skal tjenesten sørge for at alle deler av den nye infrastrukturen samspillet i en effektiv helhet.

#### 3.2 Omfang

Katalogtjenesten dekker det nye NDB, og integrerer brukerdatatabasen med de tilsvarende entitetenes i de eksisterende systemene og løsningene som i dag finnes, eks FEIDE, Lånekort m flere.

#### 3.3 Overordnet funksjonalitet


Katalogen lagrer og tilgjengeliggjør aksessinformasjon om brukere og ressursene i domenet, og danner således grunnlaget for den totale tilgangskontrollen i nettet. Samtidig lagrer den tilknyttet informasjon om objektene, så den kan brukes som et oppslagsverk og søkedatabase for informasjon.

Katalogtjenesten som helhet sørger for opprettholdelse av identitetsinformasjon på tvers av datakilder i infrastrukturen.

Katalogtjenesten består av

<sup>1</sup> RBAC – Role Based Access Control

<sup>2</sup> FEIDE – Prosjekt som etablerer felles elektronisk identitet for brukere innenfor norsk utdanningssektor

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato		27.12.2005
	Side		7
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Bryggjeld	Godkjennes av: Styringsgruppen	Revisjon A

- En installasjon med konfigurering av LDAP<sup>3</sup>
- Nettverkstjenester
- LDAP, som brukes til synkronisering av identitetsdata på tvers av datakildene i infrastrukturen
- En webapplikasjon for søk i personell som også gir muligheter til kommunikasjon med personer som er søkt opp.
- Aksess-modul og -regler
- Autorisasjon av den enkelte bruker
- SSO – singel sign on til flere applikasjoner og tjenester i løsningen til NDB

Til sammen sørger disse komponentene for grunnlaget for kontrollen med brukeres tilgang til alle ressurser i infrastrukturen.

### 3.3.1 LDAP

LDAP (Lightweight Directory Access Protocol) er en åpen standard innen katalog. Den inneholder både en LDAP database og en sikkerhets-engine som autentiserer og autoriserer tilgangen til ressursene som er registrert i katalogen.

Informasjonsmodellen til objektene i LDAP er bestemt av et sett med skjemaer. Gjennom detaljeringsarbeidet under FDR<sup>4</sup> vil disse skjemaene tilpasses for å legge til rette for lagring av all den informasjonen delsystemene trenger om objektene i katalogen.


### 3.3.2 Produkt implementering mot andre tjenester og produkter.

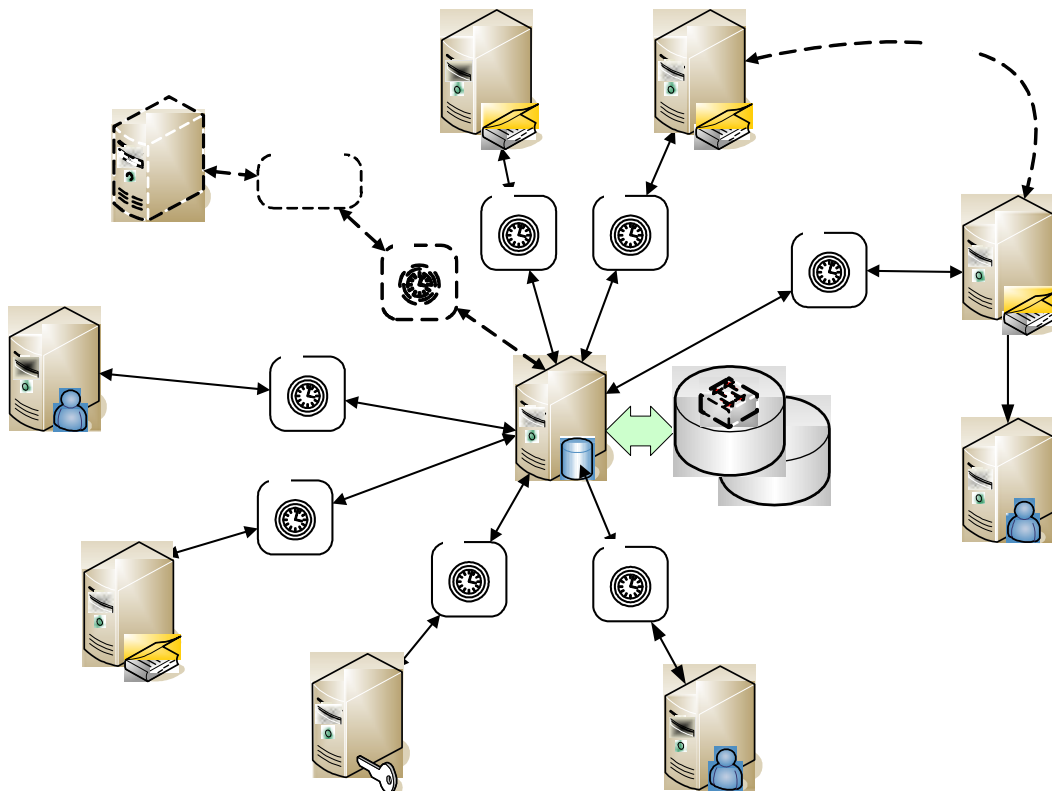
LDAP må være en regelbasert synkroniseringsmotor, for synkronisering av identitetsdata mellom heterogene datakilder.

I utgangspunktet må den gi en konfigurert svitsjematrise, hvor man kan sette opp regelsettet for flyten av informasjon mellom forskjellige tilkoblede systemene. Importen fra et system, og eksporten til andre, skjer på grunnlag av programmerte tidsintervaller. Det er ingen automatikk som umiddelbart sprer endringer mellom systemene.

<sup>3</sup> LDAP - Lightweight Directory Access Protocol. - Internett-protokoll som brukes til synkronisering av identitetsdata på tvers av datakildene i infrastrukturen

<sup>4</sup> FDR – Final Design Review – Detaljer design som utarbeides i det videre arbeidet.

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato		27.12.2005
	Side		8
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Bryggfeld	Godkjennes av: Styringsgruppen	Revisjon A



**Figur 1. Skisse av katalogtjenesten med enkelte systemene som må integrerer**

Intervall mellom kjøring av jobber må derfor tilpasses etter den takten man må kunne oppdage endringer.

Ved kjøring av en import gjennom en management agent (MA) vil endringene i datakilden forplante seg til LDAP's interne database. Når eksportjobber siden kjøres gjennom management agenter for andre datakilder, vil regelsettet eventuelt føre til at endringene sprer seg til disse datakildene.

### 3.3.3 Identity Management (IdM)

Denne løsningen vil være starten på en Identity Management løsning for NDB's kundeløsning. Løsningen vil bestå av følgende elementer:


- Synkronisering av brukerinformasjon
- Automatisk oppretting og sletting av brukere i katalogen
- Hente og oppdatere sertifikater/svartelister
- Informere systemer om at det er opprettet/slettet brukere i katalogen
- Tilretteleggelse for Single Sign-On
- Gi aksess til riktig tjenester avhengig av profil / rolle ( RBAC )
- Autorisasjon og verifisering av bruker

#### 3.3.3.1 Synkronisering av brukerinformasjon

Løsningen må synkronisere brukerinformasjon (fornavn, etternavn, telefonnummer og fakturerings-informasjon med mer) mellom forskjellige grensesnitt. Hvilke grensesnitt dette gjelder og hva som vil synkroniseres er beskrevet senere.

# Adgangskontroll

PRS

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato		27.12.2005
	Side		9
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Bryggfeld	Godkjennes av: Styringsgruppen	Revisjon A

### 3.3.3.2 Automatisk oppretting og sletting av brukere i katalogen

Brukere vil automatisk opprettes og slettes i katalogen når det opprettes eller slettes brukere i det systemet som er "master" for brukeridenter. Mest sannsynlig bli det systemet som bestemmer om en bruker eksisterer eller ikke. Automatisk oppretting og sletting av brukere vil kun skje i katalogen. I omkringliggende systemer vil brukere opprettes og slettes manuelt. Ikke alle brukere vil opprettes og slettes automatisk i katalogen. Dette vil medføre at en legger opp regler for *bruker-polecies* for tid for aktiv konto.

### 3.3.3.3 Hente og oppdatere sertifikater/svartelister

Løsningen må også hente *sertifikater*<sup>5</sup> fra en ekstern katalog og koble disse mot brukerne som ligger i katalogen. Fra den samme katalogen må det hentes svartelister som vil gjøres tilgjengelig i katalogen.

### 3.3.3.4 Informere omkringliggende systemer om at det er opprettet/slettet brukere i katalogen

Løsningen vil informere omkringliggende systemer om at det opprettes eller slettes brukere fra katalogen. Dette gjøres for at de som administrerer disse systemene skal få beskjed når de skal opprette eller slette brukere i sine systemer. Opprettingen/slettingen av brukere i omkringliggende systemer vil være en manuell prosess.

### 3.3.3.5 Tilrettelegging for Single Sign-On (SSO)

En helhetlig web-basert infrastruktur gir støtte for autentisering og autorisasjon av brukere på basis av brukeres identitet. Dette gir autorisert adgang til de fleste applikasjoner. En del systemer har derimot egne brukerdata og autorisasjonsmodeller. For å legge til rette for autentisering av brukerne mot disse uten interaksjon fra brukernes side, må det inn en *akkreditiv-database*<sup>6</sup> i katalogtjenesten. LDAP vil også gi applikasjoner mulighet for å lagre brukeres akkreditiver på kryptert form.

En fremtidig *IdM-løsning*<sup>7</sup> vil måtte synkronisere akkreditivene i baksystemene og i LDAP, slik at de settes likt og gir mulighet for Single Sign-On. Inicialt er det transparent å gi SSO-funksjonalitet til applikasjonen innenfor konteksten av NDB's tjenestebaserte arkitektur.

## 4. Design

### 4.1 Løsningsdesign

Designet av katalogtjenesten må beskrives i de følgende seksjoner. Detaljspesifisering av grensesnitt og objektflyt mellom datakildene vil fylles inn under arbeidet med FDR.


#### 4.1.1 Konfigurasjon av LDAP

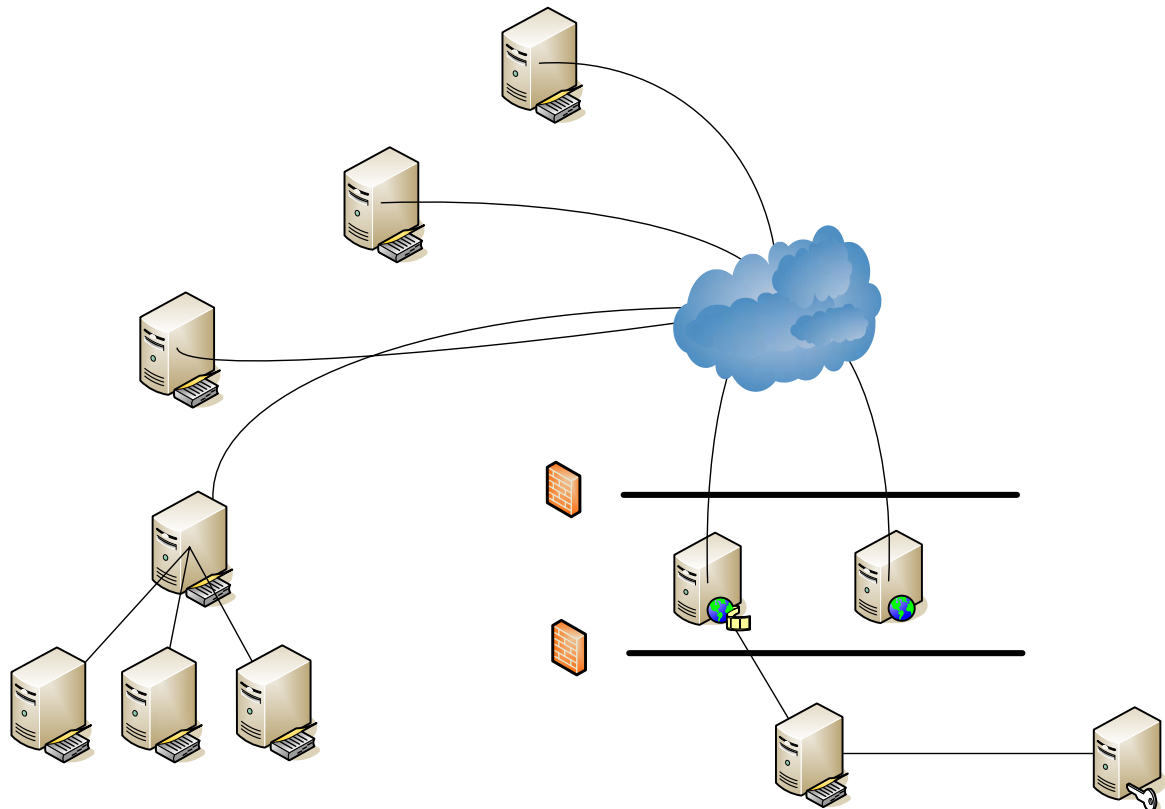
Katalogen realiseres som en LDAP katalog. Som populeres gjennom en system som vist under, og som baserer seg på data fra FEIDE og fra kunder som registrerer seg enten direkte eller via gjennom en avtale med NDB. Dette kan være både bedriftskunder og privatkunder.

<sup>5</sup> Sertifikat – Kortform av *elektronisk sertifikat* som enkelt sagt er legitimasjon i elektronisk form. Et elektronisk sertifikat benyttes særlig over åpne nett (som Internett) for å bevise at man er den man gir seg ut for å være.

<sup>6</sup> Akkreditiv-database – database som bl.a. inneholder brukernavn og passord til aktuelle brukere

<sup>7</sup> IdM-løsning – (Identity Management-løsning) Løsning som dekke nødvendig funksjonalitet for administrering og synkronisering av brukerinformasjon.

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>			Dato 27.12.2005
			Side 10
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Brygfeld	Godkjennes av: Styringsgruppen	Revisjon A



**Figur 2 : Sammenhengen mellom FEIDE – Bedrifter, høyskoler og privatkunder til NDB katalogen**

NDB opptrer i forhold til FEIDE som en FEIDE fellestjeneste<sup>8</sup> Hver gang en bruker fra utdanningssektoren autentiserer seg gjennom FEIDE for NDB, blir oppdaterte, kvalitetssikrede brukerdata overført til NDB. Det er brukerdata som fullt navn, hjemmeadresse, fødselsnummer (noe som faktisk endres for ganske mange personer i forbindelse med innvandring), telefon.

Brukerdataene er vedlikeholdt av brukerens utdanningsinstitusjon, og er de samme som institusjonen bruker i sin administrasjon av brukeren<sup>9</sup>.

NDBs internet-server kan velge å opptre som en FEIDE Single-Sign-On server, og dermed kunne integreres sømløst og uten ny innlogging i f.eks. studentportaler.

Høyskolen i Y

## 4.1.2 Organizational Units (OU)- og Group Policy Objects (GPO)-struktur

### 4.1.2.1 Administrasjonsmodell domain

I tillegg til roller for ”vanlige” brukere må det defineres administrative roller til de brukerne som skal drifte og administrere løsningen. En må også definere hvordan en skal utføre administrative oppgaver og om en skal bruke personlige administratorbrukere eller ikke.

#### 4.1.2.1.1 Administratorroller


### Bedrift XY

Oversikten nedenfor illustrerer hvilke administrative roller en vil få i katalogen.

- Kundesenter

<sup>8</sup> Se [www.feide.no](http://www.feide.no)

<sup>9</sup> For tilgjengelige attributter fra FEIDE se <http://www.feide.no/feide-prosjektet/dokumenter/feide-norperson-eduperson-13.pdf>

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato		27.12.2005
	Side		11
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Bryggfeld	Godkjennes av: Styringsgruppen	Revisjon A

- Bruker- og gruppeadministrasjon
- Domeneadministrasjon
- Diverse administratroroller

### Kundesenter

Et kundesenter som vil ha en brukerstøtte-funksjon skal ha følgende rettigheter:

- Resette passord
- Låse opp brukerkontoer
- Innmelding i grupper
- Endring av navn på brukere
- Endring av e-post adresser

#### 4.1.2.2 Bruker- og gruppeadministrasjon

Bruker- og gruppeadministrasjon skal ha følgende rettigheter:

- Opprette og vedlikeholde brukere
- Opprette og vedlikehold grupper (både ressursgrupper og rollegrupper)
- Disable og slette brukere

Siden en ønsker å gi tilgang til ressurser basert på roller er det viktig at ikke for mange er medlem av denne rollen. Det vil da fort flyte ut med hensyn på opprettelse av ressursgrupper og hvordan disse knyttes opp i mot rollegrupper. Alle som er medlem av denne rollen skal ha dyptgående kjennskap til hvordan en lager Roles (RBAC) & Rules er bygd opp med hensyn på ressursgrupper og rollegrupper og hvordan disse er nøstet sammen. Det er også veldig viktig å følge navnestandarden for grupper og fylle ut description-feltet for gruppen slik at andre vet hva gruppen gir tilgang til.

#### 4.1.2.3 Delegering av rettigheter

For å oppnå ønsket effekt med hensyn på rettigheter i LDAP må en delegere ansvar som beskrevet under.


Administrator	Ansvar
Bruker- og gruppeadministratorer	Rettighetene må delegeres fra OU-en <i>Brukere</i> og nedover og fra OU-en <i>Grupper</i> og nedover. Hvilke rettigheter de skal ha er beskrevet over
Brukerstøtte	Rettighetene må delegeres fra OU-en <i>kundetype</i> og nedover. Hvilke rettigheter de skal ha er beskrevet over
Diverse	Skal ikke ha rettigheter i katalogen, skal kun ha administrative rettigheter til systemene de skal administrere
Domeneadministratorer	Trenger ikke å delegerere rettigheter. Har allerede alle rettigheter i domenet
System	Skal ikke ha rettigheter i LDAP

#### 4.1.2.4 Personlige administratorbrukere

Ansatte med administrative oppgaver vil ha flere brukere. De vil ha en ”vanlig” bruker som de bruker til dagligdagse oppgaver som å lese e-post og skrive i Word, samt en (eller flere) administrative brukere.

En kan løse dette på en av to måter:

1. Bruke en (eller flere) administratorbrukere for hver rolle, for eksempel Adm\_UNI ( universitet ) , Adm\_Domain og lignende. Passordene til disse brukerne blir oppgitt kun til de personene som trenger tilgang. ”Alle” skal ikke kunne bruke disse brukerne. Det er vanskelig å administrere passord på disse brukerne på grunn av at mange personer bruker den samme brukeren og dermed har behov for å bruke passordet.
2. Bruker personlige administratorbrukere. Det betyr at hver bruker får sin personlige administratorbruker som tildeles aktuelle administratroroller, for eksempel Adm\_Gunnar.

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato		27.12.2005
	Side		12
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Bryggfeld	Godkjennes av: Styringsgruppen	Revisjon A

Vi anbefaler å bruke alternativ 2, personlige administratorbrukere, på grunn av logging. En vet da hvilken person som har gjort hva på hvilken server til hvilket tidspunkt. Katalogen vil bruke standard loggemekanismer i *LDAP eventlog*<sup>10</sup>.

### 4.1.3 Roller

Det er ønskelig å ta i bruk roller for å styre tilgangen til ressurser i katalogen. En vil på den måten forenkle og effektivisere administrasjonen av brukere som igjen fører til økt sikkerhet og lønnsomhet. I katalogen vil bruk av rollegrupper implementeres ved at man oppretter egne ressursgrupper (sikkerhetsgrupper) for hver enkelt ressurs. Dette kan for eksempel være NTNU studenter (NTNU-grupper), filområder (filområdegrupper), applikasjoner (applikasjonsgrupper), distribusjonslister og lignende. I tillegg vil det opprettes rollegrupper (sikkerhetsgrupper) som knyttes sammen med ressursgruppene. Brukerne vil meldes inn i rollegruppene. Rollene vedlikeholdes manuelt ved at grupper opprettes og knyttes sammen i katalogen.

For å få implementert en slik løsning trengs følgende:

1. Rollegruppene må defineres (Elever & typer, Bedrifter osv) Disse vil også være ihht. de forskjellige tjenestene som skal lanseres.
2. Det må defineres hva de forskjellige rollene skal ha tilgang til (applikasjoner, betalingsformer, osv).
3. De ansatte og partnerne må knyttes opp i mot roller.

### 4.1.4 Grupper

I kataloger har man forskjellige typer grupper, sikkerhetsgrupper og distribusjonsgrupper. Disse kan være lokale, globale eller universale. Grupper kan enkelt gis nytt navn hvis det er ønskelig. Sikkerhetsgrupper vil brukes aktivt i katalogen for å styre tilgangen til ressurser og tjenester. Objekter kan samles i grupper på tvers av trestrukturen, og tilgangsrettigheter kan gis til disse gruppene. Gruppene vil også knyttes sammen for å forenkle styringen av tilgangsrettigheter.

#### 4.1.4.1 Navnstandard på grupper

For å få enklere drift og bedre oversikt er det viktig å opprette en navnstandard på gruppene som opprettes i katalogen. En slik navnstandard bør si noe om følgende:

- Hvilken type gruppe det er (Lokal, Global, Universal)
- Hvilken type ressurs det er (Elever ( type ), fagområder ?, distribusjonsliste, filområde, rolle)
- Navn på ressurs (navn på applikasjon, skriver, filområde, distribusjonsliste, rolle)
- Lokasjon på ressurs (hvor skriveren står, hvor filområde ligger)
- Prøv og begrens gruppenavnet til 20 (maks 30) tegn

I tillegg er det viktig å fylle ut description-feltet til gruppene. Her skal en beskrive hva denne gruppen brukes til. Dette feltet kan maks inneholde 256 tegn.


## 4.2 Kapasiteter/volum/skalering

Løsningen vil være basert på Unix og må designes for å kunne håndtere 1 500 000 – 2 000 000 brukere og implementert i et helt redundant miljø.

### 4.2.1 Suksessfaktorer

- Katalogtjenesten vil være en suksess dersom den lar infrastrukturen operere med oppdatert bruker- og ressursinformasjon med høy tilgjengelighet.
- Administrasjonskostnaden skal bli vesentlig redusert med automatisert flyt av identitetsdata mellom komponentene, samtidig som tiden fra en ansatt registreres til bruker er opprettet og dataene spredd i alle berørte systemer skal forkortes vesentlig.

<sup>10</sup> Organizational Units – Dette er en oppdeling av grupper og enheter i katalog strukturen, vil bli spesifisert i den videre utredningen

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato		27.12.2005
	Side		13
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Brygfeld	Godkjennes av: Styringsgruppen	Revisjon A

Begge disse faktorene er avhengige av i hvilken grad katalogtjenesten integreres med...:

- Informasjon fra kunden om roller, tilganger og brukere. Kunden må stille med ressurser til dette arbeidet i løpet av FDR perioden.
- God opplæring av driftspersonell
- Gode og klare grensesnittspesifikasjoner
- Strømformet prosess for opprettelse/vedlikehold av brukere, ressurser og tilganger

## 4.3 SLA

Service Level Agreement innen de enkelte områdene bør etableres.

Spesifikt for:

- LDAP - Måleparameter: **Oppetid**
- Nettverkstjenester - Måleparameter: **Oppetid**
- Søkeapplikasjon - Måleparameter: **Responstid/søketid**

## 4.4 Sikkerhet

Det bør etableres et regime for pålagte lover og regler i henhold til sikkerhets policies og harmoniseres med NDBs andre sikkerhetspolicies.

### 4.4.1 Fysisk sikkerhet

Alle servere plasseres i avlåste serverrom. For å få fysisk tilgang til serverne må man ha spesiell godkjenning.

### 4.4.2 Nettverkssikkerhet

Serverne vil plasseres i forskjellige nettverkssoner slik at de kan beskyttes mest mulig mot angrep. Mellom hver nettverkssone er det en brannmur som styrer tilgangen til sonen. De forskjellige sonene er:

1. Sikker sone
2. Intern sone (inkl service nettverk)
3. Åpen sone


Katalogserverne til rotomene vil stå i sikker sone som er den sikreste sonen. Ingen ordinære brukere skal logge seg på dette domenet, det er derfor sikret mest mulig ved å være plassert i sikker sone. Katalogserverne til child-domenet vil stå både i sikker og intern sone. For dette domenet er det nødvendig å ha domenekontrollere i begge sonene pga. at det vil være tjenester i både sikker sone og intern sone som har behov for å kommunisere med disse domenekontrollerne. I intern sone vil det i tillegg være brukere som har behov for å kommunisere med disse domenekontrollerne.

Det vil plasseres to servere i åpen sone som tilbyr nettverkstjenester til PC-er og lignende i denne sonen. Hvis en ikke tilbyr disse tjenestene i åpen sone vil utstyr måtte aksessere disse tjenestene fra intern sone. All denne trafikken ville gått via FW (brannmur) mellom intern og åpen sone som er uønskelig.

### 4.4.3 Sårbarheter og konsekvenser

#### 4.4.3.1 Sårbarheter

Sårbarhet	Sannsynlighet
Systemkræsje på databasen til katalogen	Liten
Systemkræsje på aksessmodulen	Liten
Systemkræsje på autorisering delen	Liten
Systemkræsje på RBAC delen	Liten

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato		27.12.2005
	Side		14
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Brygfeld	Godkjennes av: Styringsgruppen	Revisjon A

Systemkræsje på databsen til	Liten
Utilgjengelige nettverkstjenester (DHCP, DNS)	Liten
Utilgjengelig søkeapplikasjon	Liten

#### 4.4.3.2 Konsekvenser

Hvis katalogen skulle bli utilgjengelig vil dette få store konsekvenser. Brukere vil ikke få logget på og får dermed ikke tilgang til tjenester og ressurser i nettverket. Dette kan også få kritiske konsekvenser for meldingstjeneren som er avhengig av informasjon fra katalogen.

Hvis katalogservere skulle bli utilgjengelig kan det få følgende konsekvenser:

- brukerinformasjonen i de forskjellige grensesnittene blir ikke oppdatert
- nye bruker kommer ikke inn i katalogen
- systemet får ikke beskjed om at bruker er blitt opprettet/slettet i katalogen
- brukerne får ikke sertifikater
- sertifikater og svartelister blir ikke oppdatert

Hvis Hvite Sider-applikasjonen<sup>11</sup> ikke er tilgjengelig fører det til at brukerne ikke kan søke på informasjon i katalogen.

## 4.5 Kostelementer

Kostelementene i Katalogtjenesten er

- Servere
- Lisenser på programvare
- Vedlikeholds- og supportavtaler
- Konsulenttid

## 5. Grensesnittspesifikasjoner

### 5.1.1 NDB

Grensesnitt	Funksjon
Integrasjon mellom eksisterende og ny katalog	Opprettes trust mellom katalogene for å gi tilgang til ressurser på tvers av dem.
Migrering av brukere	Brukere vil bli migrert fra eksisterende katalog til ny katalog.


### 5.1.2 NTNU - FEIDE

Grensesnitt	Funksjon
Synkronisering av informasjon	Det vil synkroniseres brukerinformasjon mellom LDAP katalogen og FEIDE - kataloger.

### 5.1.3 Beskjed når brukere blir opprettet og slettet

Når en bruker blir opprettet eller slettet i katalogen må en ha en løsning som gir systemet beskjed slik at de får opprettet eller slettet brukeren i sitt system. De enkelte kunde (Skole, bedrift osv.) må så kjøre en manuell prosedyre for opprettelse eller sletting av denne brukeren.

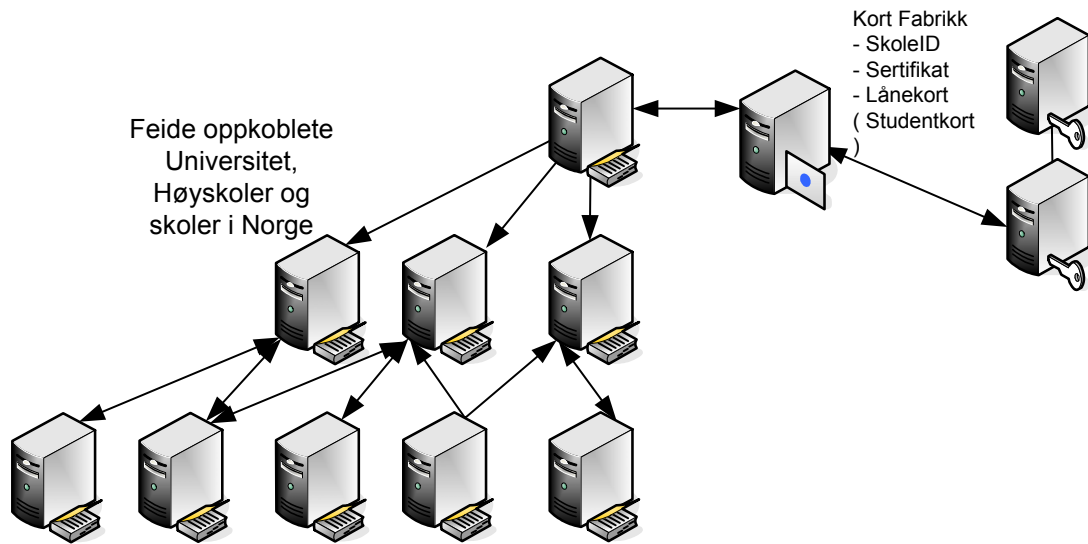
<sup>11</sup> Hvite Sider-applikasjonen – applikasjon som gir tilgang til informasjon om brukere på lik linje med en tradisjonell telefonkatalog gir på sine hvite sider.

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato		27.12.2005
	Side		15
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Bryggfeld	Godkjennes av: Styringsgruppen	Revisjon A

## 5.2 Pålogging/autentisering/sertifikat /adgangskort

### 5.2.1 Sertifikat

Brukersertifikatene skal publiseres i katalogen. Løsningen kan / vil lese ut denne informasjonen fra katalogen til CA<sup>12</sup>en og skrive denne informasjonen inn i katalogen. Løsningen er skissert under.



Figur FEIDE

### 5.2.2 Tilbakekallingslister

Tilbakekallingslistene<sup>13</sup> skal publiseres i katalogen. Kortfabrikken vil lese ut denne informasjonen fra katalogen til CA og skrive denne informasjonen inn i katalogen. Løsningen er skissert over. I Figur - FEIDE

### 5.2.3 Sertifikat og tilbakekallingslister

Sertifikat og tilbakekallingslister skal være tilgjengelig for klient ved pålogging fra ulike soner, noe som vil bli tilfredsstillt ved at katalogen vil bli replikert<sup>14</sup> mellom de forskjellige sonene.

## 5.3 Adgangskontroll

Aksess metoden, er lagt opp til at det genereres en session cookie fra en browser. En må kunne integrere forskjellige kataloger og databaser hvor en har brukerinformasjon.


### 5.3.1 Synkronisering av informasjon

FEIDE er basert på oversending av oppdatert personinformasjon ved hver innlogging, og har et forbud mot annen tilgjengeliggjøring av informasjon gjennom FEIDE (f.eks. overføring av utdrag av hele registre for flere personer fra en eller flere utdanningsinstitusjoner).

<sup>12</sup> CA – Certificate Authority – den instans som er ansvarlig for utstedning av elektroniske sertifikater.

<sup>13</sup> Tilbakekallingslister – liste over sertifikater som skal kalles tilbake fordi de ikke lenger er gyldige fordi tilgang er tatt fra brukeren av en eller annen årsak.

<sup>14</sup> Replikere – kopiere og ajourholde data fra en datakilde til en annen.

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato		27.12.2005
	Side		16
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Brygfeld	Godkjennes av: Styringsgruppen	Revisjon A

Synkronisering med FEIDE må derfor skje dynamisk ved hver pålogging. Den personinformasjonen som oversendes er den samme som brukes internt i undervisningsinstitusjonen som har gitt brukeren et FEIDE-navn, og institusjonen har en kontraktfestet plikt til å bare gi ut informasjon der den kan gå god for datakvaliteten, inkludert at informasjonen er oppdatert til enhver tid.

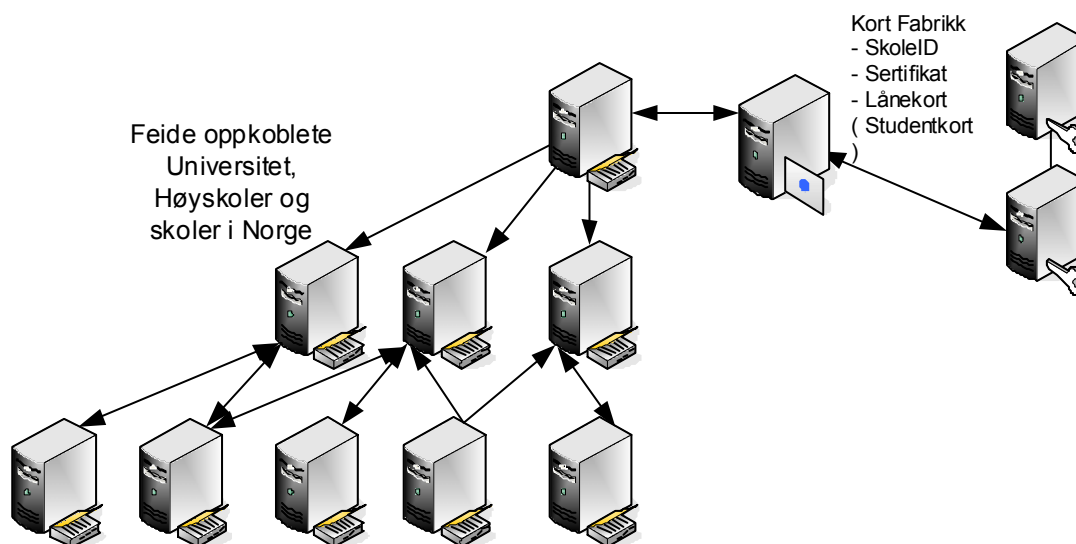
Den delen av NDBs tjeneste som foretar innlogging av brukere, må derfor oppdatere NDB-Bib-LDAP (se figur XX s. 9) med brukerdata ved hver innlogging, så den oppdaterte informasjonen blir tilgjengelig for NDBs banksystemer.

Merk at NDB kan velge å lagre brukernavn (FEIDE-navn) som attributt<sup>15</sup> i LDAP-katalogen, og dermed kunne beholde brukerprofilen automatisk selv ved skifte av fødselsnummer. Slike skifter forekommer ganske ofte, særlig i forbindelse med innvandring, hvor personen tildeles et permanent fødselsnummer som er forskjellig fra det midlertidige fødselsnummeret vedkommende har fått som f.eks. student eller flyktning.

## 5.4 Beskjed når brukere blir opprettet og slettet

Når en bruker blir opprettet eller slettet i katalogen må en ha en løsning som gir adgangskontrollsystemet beskjed slik at de får opprettet eller slettet brukeren i sitt system. Dette kan for eksempel løses ved at man skriver inn informasjon i en tabell i adgangskontrollsystemet som sier at en bruker er opprettet eller slettet i katalogen. De må så kjøre en manuell prosedyre for opprettelse eller sletting av denne brukeren.

Forslag til løsning er skissert under.




**Figur 2**

I figuren over, vil kortfabrikken håndtere sertifikater og aksess prosessen ved bruke av en verifiserings tjeneste.

## 6. Anbefalinger fra AP4.

Arbeidsgruppen har sett på de forskjellige løsningene som en har diskutert, og som er sammenfattet tidligere i dokumentet. En ønsker samtidig å kunne integrere løsningen inn mot FEIDE og de brukergruppene som er definert der, samtidig som en ser at FEIDE kan få en nasjonal utberedelse innen skolene. Dette samt den utviklingen innen aksess, autentisering og Federated identiteter og nettverk, har arbeidsgruppen konkludert med følgende.

<sup>15</sup> For tilgjengelige attributter fra FEIDE se <http://www.feide.no/feide-prosjektet/dokumenter/feide-norperson-eduperson-13.pdf>

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato		27.12.2005
	Side		17
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Bryggfeld	Godkjennes av: Styringsgruppen	Revisjon A

## 6.1 Integrasjon med Feide

En inngår avtale med Feide prosjektet for implementering av Feide brukere inn ot NDB, for å kunne tilby NDB tjenester opp mot universitet, høyskoler og skoler som Feide i dag har avtaler med. Integrasjon med FEIDE

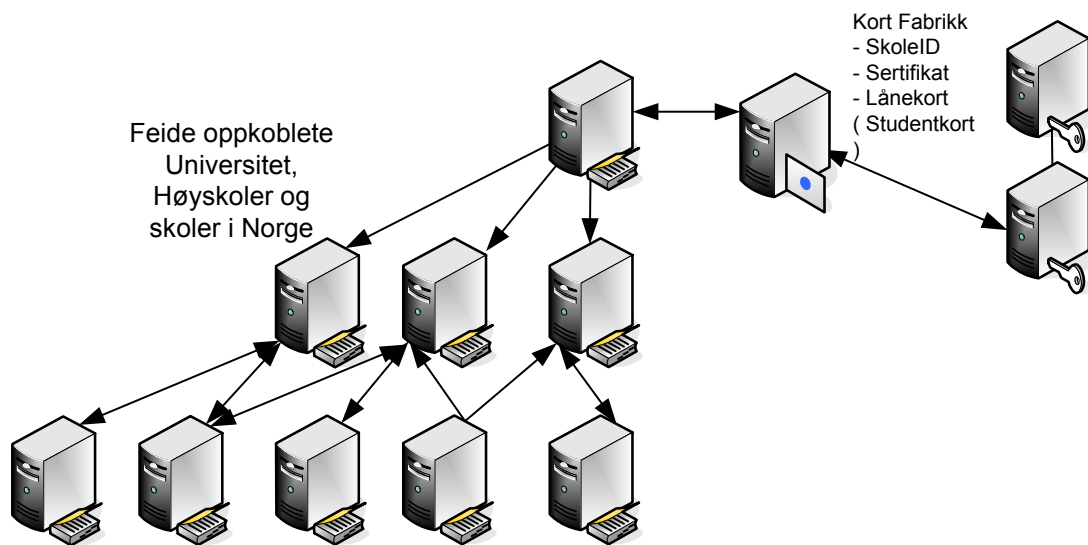
### 6.1.1 Innsamling av brukerinformasjon

En ser at en synkronisering av brukere fra FEIDE, vil kunne gi både NDB og FEIDE en god felles plattform for utvikling av felles tjenester. Det som kreves, er at en får lagt opp en fornuftig synkronisering og oppdatering av brukerkontoer og at en enes om hvilke data som skal overføres til NDB. Siden en også skal kunne foreta betalings tjenester, vil dette også innbefatte personlige data og personell opplysninger.

I en implementering av FEIDE i skolene, ser for seg at en vil ha Administratorer/registratorer på de forskjellige skoler/universiteter som legger inn brukerdata inn i systemet og at disse er ansvarlig for å vedlikeholde disse. Dette kan gjøres med en Web-front end, eller en lokal klient på den enkelte skole. Disse dataene lagres lokalt, og replikeres (kanskje gjennom flere steg/ og etter oppsatte tider.) til sentral FEIDE-database eller en LDAP brukerdatabase sentralt. Denne databasen vil være en sentral katalog for alle elever. FEIDE blir således et sentralisert register, som en også kan bruke til å utstede sertifikater, Bib kort, Studentkort osv.

Produksjon av sertifikat/smart card kan distribueres til lokale enheter / skoler for å sikre riktigheten av sertifikatene og sikre utlevering av sertifikatene (valideres).

En vil da personalisere et smart-kort for bruker, generere nøkkel-par, og forespørre et sertifikat fra en CA. "Best practice" anbefaler at bruker sertifikatet er utstedt av en sub CA. Ved å ha et CA-hierarki muliggjør en endringer i trust relasjoner og senere opprettelser av ytterligere CA mye enklere, med kun minimal ekstraarbeid.




Figur – FEIDE & CA - sertifikater

### 6.1.2 Security komponenter

CA programvare kan bli brukt til å implementere Root og sub CA(er), og en bør også påse at en kan supportere uendelig antall nivåer og hierarkier, en kraftig web basert administrasjon, API'er og høy sikkerhet gjennom EAL4+ sertifisering og støtte for maskinvarebasert sikkerhets moduler (HSM).

En kan også etablere en *Validation Server* som er en *OCSP* responder som muliggjør andre medlemmer av PKI'en (for eksempel NDB eller andre nasjonale biblioteker) denne kan validere sertifikater i real tid med et minimum av overhead.

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato		27.12.2005
	Side		18
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Brygfeld	Godkjennes av: Styringsgruppen	Revisjon A

## 6.2 Identity and Access management hos NDB

Generell funksjonalitet til en portal vil være web-front-end for tilgang til alt innhold hos NDB.

Innlogging til NDB Portalen.

Når en bruker aksesserer portalen, vil følgende steg bli fulgt:

- Brukeren må autentisere ved å benytte hans/hennes sertifikat.
- Portalen med agent vil sammen med en mellomvare server systemer vil validere sertifikatet.
- Agenten vil sammen med AAA serveren sjekke rettighetene til den autentiserte brukeren, og bestemme om brukeren har tilgang til den forespurte ressurs.
- Brukeren får en sessions cookie og får tilgang til ressurser eller blir nektet tilgang.

Den beste teknologien rundt portalen for en integrasjon av teknologien vil være en løsning basert på J2EE, men det kan være alternativer til dette om en ikke har spesielle krav til skalering og ytelse.

”Federation” til andre nasjonale bibliotek

- Brukeren har allerede en gyldig sesjon med NDB
- Brukerne klikker på en link i NDB portalen
- Linken initierer en identitetsutveksling via FIM
- FIM ”federerer” brukeren til den forespurte utenlandske bibliotek.
- FIM kan samarbeide med den utenlandske SAML implementasjonen for å utveksle brukerprofilinformasjon. Denne informasjonen kan også inneholde løsningsspesifikk informasjon.

### 6.2.1 Access management og Singel Sign On

Flere leverandører av mellomvare har designet løsninger for høy tilgjengelighet, høy ytelse, fleksibilitet og enkel administrasjon av brukermasser. Løsningen kan enkelt skaleres opp til mange millioner brukere. Alle mellomvarekomponenter kan konfigureres til å ha flere replika for å sikre høy tilgjengelighet og høy ytelse, dette gjelder alle som har løsninger som går på Unix / Linux.

Tilgangsrettigheter for brukere/grupper kan defineres statisk (for eksempel spesifikke brukergrupper og enkelte applikasjoner de kan benytte) eller dynamisk (for eksempel kan bruker tillates aksess til en applikasjon hvis en spesiell profil (universitet eller annet) hvor en har en spesifikk rolle.

### 6.2.2 Federated Identity Manager (FIM)

*FIM*<sup>16</sup> er basert på *SAML*<sup>17</sup> 1.0 og *SAML* 1.1 og de fleste leverandører er bygget opp på denne standarden. Liberty Alliance’s ID-FF 1.2 support vil være tilgjengelig i slutten av 2004. *FIM* kan integreres i eksisterende *autentiserings- og autoriserings-metoder samt alle andre kjente metoder for dette formålet*.

### 6.2.3 FIM Plug-ins


Mange selskaper har laget FIM-løsninger som også kan benyttes som stand alone løsninger. Ved slik bruk er det mulig for en FIM-løsning å bli integrert med andre Aksess, Autentisering Authorisasjon-løsninger som baserer seg på Web access management løsninger. Dette oppnås ved å tilpasse FIM-løsningene med en *ticket plug-ins*<sup>18</sup>.

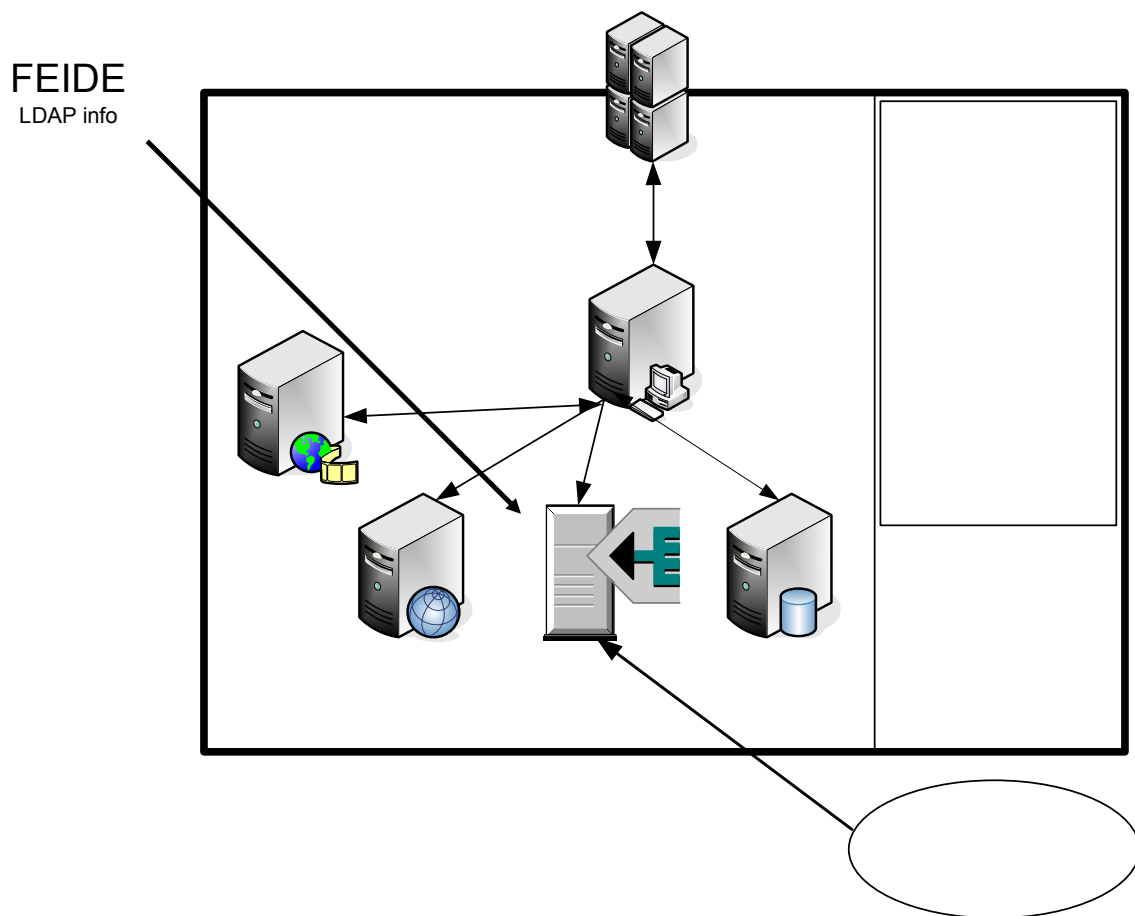
Under en identitetsutveksling (WEB SSO SAML profile) er det mulig å sende bruker profil informasjon til en partner (relying party). Oversendelsen av brukerprofilen kan enten bli gjort ved AAA-løsnings-integrasjon eller ved å benytte attributt plug-in-grensesnitt. Brukere kan ha mange forskjellige ID’er hos den utstedende part og hos relying part. I stedet for å bruke standard 1:1 mapping, er det mulig å skrive navn-mapping plug-ins til for eksempel jsmith til john.smith osv. En vil kunne unngå mye av dette, ved en fellesregistrering av brukerne i henholdsvis FEIDE og i NDB basen.

<sup>16</sup> FIM – Federated Identity Manager Er en måte en bygger og utveksler identiteter på mellom partnere , på en sikker metode

<sup>17</sup> SAML – Security Assertion Markup Language er en XML-baser rammeverk for Web services som muliggjør utveksling av authentication og authorization information mellom foretnings partnere.

<sup>18</sup> Ticket plug-ins – En plugg in for Fim løsningen , brukes for å få utført den ønskede servisen hos motparten

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>			Dato 27.12.2005
			Side 19
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Bryggfeld	Godkjennes av: Styringsgruppen	Revisjon A



Opsjoner for deltagende biblioteker

### 6.2.4 FIM og et eller annet AAA system

Deltagende "Relying Parties" (andre bibliotek) kan bruke lignende oppsett til det NDB har, for å benytte "federated identity" på samme måte.


### 6.2.5 Forskjellige leverandører av FIM og andre 3rd party access management

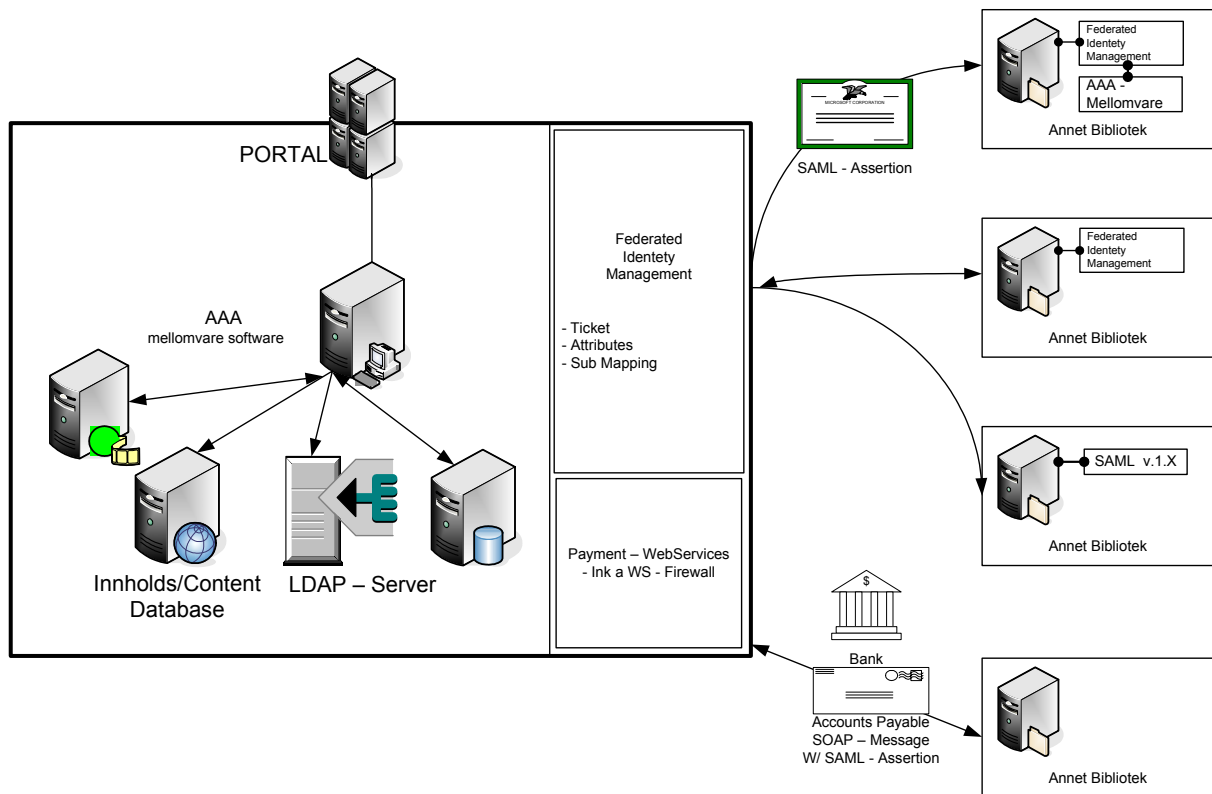
FIM kan bli brukt som SAML front-end også for web access management løsninger som allerede er implementert hos de forskjellige utenlandske biblioteker. Dette kan gjøres ved å benytte tilpassede "ticket plugins" til FIM på deres løsning.

### 6.2.6 Andre SAML kompatible løsninger

Det er også mulig å benytte SAML 1.1 eller 1.2 kompatible løsninger for de andre partnere i et internasjonalt samarbeid, dermed får en en løsning som kan integreres og implementeres for alle typer av samarbeidsformer.

Ved bruk av SAML og FIM-løsninger, vil en kunne ha en fremtidsrettet løsning, og som samtidig er rettet mot åpne standarder, dette gir NDB en stor grad av fleksibilitet og stor sikkerhet for fremtidige implementeringer, og oppbygging av tjenester og samarbeid mellom andre biblioteker. Under er vist hvordan dette kan bygges:

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato	27.12.2005
	Side	20
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Brygfeld	Godkjennes av: Styringsgruppen
		Revisjon A



## 6.3 Oversikt SAML og Liberty Alliance

### 6.3.1 Difrensiatorer mellom SAML vs. Liberty Alliance og anbefalinger

*SAML* er portal-sentrisk. Med dette menes at for å få Singel Sign On må brukeren alltid gå igjennom en sentral portal (NDB Portal) hvis han ønsker å gå til et annet domene (for eksempel et bibliotek i utlandet).

*Liberty Alliance* bygger på *SAML*. Det gjør det mulig for brukerne å gå direkte til hver deltagende service provider (bibliotek) og eventuelt bli redigert til NDB for å autentisere. Ved siden av denne egenskapen, støtter også LA global logout og andre utvidede funksjoner.

For NDB vil en ren SAML-løsning kunne være nok – i hvert fall i en startfase. Når brukerne uansett vil aksessere NDB-portalen, vil begrensningene i SAML ikke være så negative som det kan virke. Det virker også mer sannsynlig at utenlandske bibliotek vil være SAML-enabled enn LA-enabled.


Uansett, det er mulig å ha et oppsett hos NDB som supporterer SAML i starten, og som oppgraderes til LA hvis det er ønskelig.

### 6.3.2 Kort teknisk beskrivelse av SAML Assertions

Det er tre mulige SAML assertions:

- Autentisering assertion
- Atributt assertion
- Autorisasjon assertion

**Autentiserings assertion** inneholder brukerID, type autentisering, signatur(er) og andre data (for eksempel assertion og relying party IDer). Autentiserings assertions er brukt til å muliggjøre SSO mellom assertion og relying parties.

 <b>NB</b> <b>NDB-Rammeverk, Rapport for AP4 – Autentisering og Autorisering</b>	Dato		27.12.2005
	Side		21
Ansvarlig: Kaare Bjørn Martinussen, Phalanx	Gransket av: Svein Arne Brygfeld	Godkjennes av: Styringsgruppen	Revisjon A

**Attributt assertion** inneholder brukerprofil informasjon som er sendt fra asserting party til relying party. Som autentisering assertion kan den (og bør) være digitalt signert.

**Autorisasjons assertion** inneholder den biten som bestemmer om brukeren kan få tilgang til en spesiell ressurs hos relying party. Dette sees på som en eksotisk bruk av SAML fordi det ikke sees på som normalt at relying party "outsourcer" autorisasjonsbeslutninger til en utenlands (eller andre) asserting party.

FIM supporterer autentisering og attributt assertion og de sammenfallende SAML protokollene.

Note: Det er noen ganger misforståelse mellom SAML tokens og SAML protokoll. SAML tokens er XML meldinger som inneholder assertions. SAML-protokollen beskriver hvordan SAML tokens er forespurt og sent mellom asserting og relying parties.

### 6.3.3 Mulig bruk for SAML Tokens

SAML kan ikke bare bli brukt til å gi brukere singel sign on, men også for utvide brukerens sesjon utover det rene web-miljøet. Ofte kan SAML autentisering brukes som en del av SOAP meldinger. Disse SOAP meldinger kan valideres og får bare lov til å bli gjennomført hvis de inneholder SAML token fra en tiltrodd asserting party. Web service brannmurer som Vordel, Westbridge og Data Power tilbyr denne funksjonaliteten.

## 7. Vedlegg

Følgende vedlegg finnes til denne rapporten:

- Vedlegg 1: Kravtabeller, felt- og attributtbeskrivelse for Feide
- Vedlegg 2: *User Authorization - How should an organization manage and control access to applications and online information resources?*  
Rapport (Statement of problem) fra Burton Group
- Vedlegg 3: *Roles and Access Management: Seeking a Balance Between Roles and Rules*  
Rapport (Research overview) fra Burton Group

## 8. Begreper

Begrep	Forklaring
Federert identety	En felles identitet mellom partnere
IdM	Identity Management
LDAP	Lightweight Directory Access Protocol
Liberty Alliance	Er en allianse mellom mange av de største produsentene i verden for å sikre en felles måte å kommunisere på, i tett samarbeid med SAML
RBAC	Rolle Basert Access Control - NIST standard
Relying Parties	Er en transaksjon som foregår mellom 2 partnere
SAML	Secure Assertion Markup Language
Sertifikat	Et sertifikat for å identifisere seg
Ticket Plug In	En plugg in for Fim løsningen , brukes for å få utført den ønskede servisen hos motparten
Validation Server	Validering server sjekker og gjør en bekreftelse på at en er den en utgir seg for å være (validerer sertifikatet)