Mellomvare:

Den neste frontlinjen i utbyggingen av IT-tjenestene

Sist oppdatert 29. november 2000, bness@usit.uio.no

Innledning

Dette notatet argumenterer for at UNINETT må ta et nytt skritt i retning av å integrere UH-sektoren i Norge i en felles IT-omgivelse. Gjennom UNINETT er det bygd opp en fysisk infrastruktur som omfatter hele UH-sektoren og som gjør at institusjonene kan kommunisere med hverandre og med omverdenen. Det er flere forhold som gjør det nødvendig å ta noen skritt i retning av å gjøre nettbaserte tjenester, systemer og ressurser tilgjengelig innenfor kontrollerbare rammer med identifiserbare brukere og prosesser:

- Den statlige utdanningspolitikken har samarbeid og arbeidsdeling som en uttalt målsetting, en målsetting som kommer til å bli tydeligere gjennom behandlingen av Mjøs-utvalgets innstilling
- Fellesadministrative systemer
- Trøkket i retning av nettbasert læring og utvikling av digitale læringsomgivelser og digitale læringsressurser
- Deling av forskningsdata og forskningsressurser, blant annet illustrert gjennom tungregnesatsingen, vil i økende grad være en forutsetning for å drive avansert forskning i landet

I tillegg kommer ressurssituasjonen ved institusjonene som tilsier satsing på kosteffektive fellesløsninger.

Notatet er primært en beskrivelse av en gruppe fenomener kalt mellomvare. Mellomvare er det konkrete uttrykket for at nettet er kommet mellom brukeren og tjenestene, ressursene og systemene brukeren benytter seg av. Dette innebærer at en del funksjoner må flyttes ut av de lokale maskinene og bli nettbaserte for å ivareta tilgjengelighet, sikkerhet og en del andre forhold. En kritisk faktor her er en felles brukeridentifikasjon med tilhørende støttesystemer og tjenester for UH-sektoren. Bak notatet ligger et ønske om å få organisert et prosjekt for å realisere dette. Notatet er hverken en prosjektplan eller et prosjektdirektiv. Hensikten er kun å lage en litt overordnet beskrivelse av området, en beskrivelse som kanskje kan tjene som motivasjon og kanskje også som en klargjøring av bredden i dette arbeidet.

Et mellomvareprosjekt vil falle pent inn i en tradisjon for samarbeid i UH-sektoren i Norge om nasjonale løsninger der det er rasjonelt, kosteffektivt og nødvendig. UNINETT, BIBSYS og FS kan, med sine gode og kanskje ikke like gode sider tjene som eksemplarisk praksis.

Et aspekt som henger nøye sammen med mellomvaren, men som ikke er behandlet i dette notatet er sikkerhetsarbeid. En vellykket gjennomføring er avhengig av og vil inkludere veldefinerte sikkerhetskrav og en velfungerende sikkerhetstjeneste, noe som ikke er behandlet i dette notatet.

Mellomvaren plassert

Alt var mye enklere i 'gamle dager', også når det gjelder datamaskiner. Før Internet ble stort hadde brukerne én datamaskin å forholde seg til:

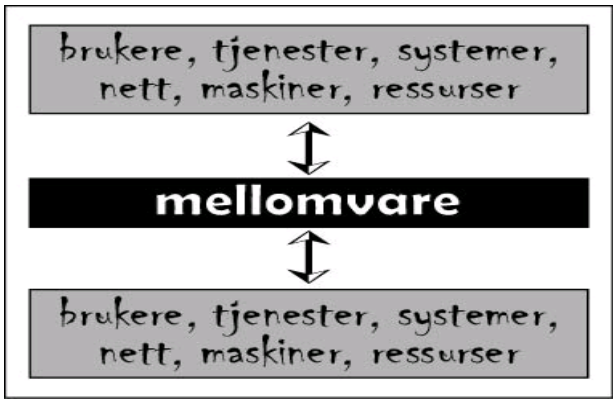
- På denne datamaskinen var brukeren *identifiert* ved hjelp av et brukernavn
- I innloggingen ble brukeren *autentisert* overfor systemet ved at passordet bekreftet identiteten til brukeren
- Via privilegier knyttet til gruppemedlemsskap og lignende ble brukeren *autorisert* til å starte programmer, bruke ressurser på datasystemet
- Filbeskyttelsen og andre mekanismer tjente som *adgangskontroll* til tjenester og ressurser på systemet
- Ulike mekanismer sørget for at bruken av maskinressurser (prosessor, disk, I/O med mer) ble *avregnet* som grunnlag for enten tildeling av maskintid eller betaling for bruk av systemene
- Via enkle kommandoer kunne brukeren liste opp *kataloger* med oversikt over brukere, ressurser,

programmer, dokumenter og annet på systemet
- Og så videre ...

Med andre ord, – databehandlingen skjedde innenfor *et kontrollert miljø med enkelt identifiserbare brukere, tjenester og ressurser*. Dette varte ikke lenge. Vi fikk systemer med egen autentisering og autorisering som medførte at brukerne hadde flere brukernavn og passord på samme maskin. Vi fikk PC-ene som ikke hadde noe begrep om brukere i det hele tatt. Og vi fikk Internet og Web som flyttet tjenestene ut av maskinene og gjorde dem distribuert og nettbasert.

Brukerne forholder seg med andre ord ikke lenger til én maskin, svært ofte har brukeren tilgang til mange maskiner, – på jobb, hjemme, bærbart utstyr, publikumsmaskiner ('internet-kaféer' og lignende). Ofte trenger ikke brukerne å logge seg inn på disse maskinene, og om de må oppgi brukernavn og passord, så garanterer dette sjelden brukerens identitet med noen grad av sikkerhet og er et dårlig grunnlag for å autentisere brukeren. I sin virksomhet benytter brukeren tjenester og systemer som de ikke aner noe om lokaliseringen av og som kan befinne seg på et helt annet sted på kloden og under kontroll av organisasjoner og foretak som brukeren ikke har noe forhold til. Internet er i sin karakter grunnleggende ukontrollerbar og det å skaffe seg oversikt over ressurser og tjenester er en velkjent utfordring.

Samtidig utvikles det i Internet forretningsmodeller og virksomheter som forutsetter varierende grad av – nettopp – kontrollerbare omgivelser og identifiserbare brukere, tjenester og ressurser, men i dette tilfelle er det snakk om nettbaserte og ikke maskinbaserte brukere, tjenester og ressurser. I tillegg kommer behovet for å skape sikrest mulige omgivelser for transaksjoner, enten det er penger eller andre kreditiver som utveksles. Begrensningene ved å bruke den tradisjonelle maskinbaserte modellen til å løse disse oppgavene i Internet er åpenbare. Søkingen etter andre modeller har ført til løsninger og mekanismer som flytter prosesser knyttet til identifikasjon, autentisering, autorisasjon, adgangskontroll, katalogisering og lignende ut av lokale systemer og samler dem i et eget lag mellom nettet og maskinvaren på den ene siden og brukere, programmer og tjenester på den andre, et lag som i de samme sammenhenger kalles **mellomvare** ('middleware'):



Mellomvaren er i utgangspunktet en broket samling av funksjoner og oppgaver. Ikke alle er enige om hva den faktisk omfatter og definisjonene av begrepet varierer sterkt i de sammenhengende de opptrer. De aller fleste ender opp med at mellomvaren er *samlingen av de verktøy og mekanismer som gjør at programmer, systemer og brukere kan få tilgang til og benytte nettbaserte tjenester og ressurser* (i humoristiske ordelag ofte uttrykt som *«the intersection of the stuff that network engineers don't want to do, with the stuff that application developers don't want to do»*). I desember 1998 ble det arrangert et arbeidsseminar som blant annet diskuterte egenskapene ved mellomvare i bred mening av begrepet, – jf RFC2768: «Network Policy and Services: A Report of a Workshop on Middleware». Dette arbeidsseminaret konkluderte med enighet om behovet for og eksistensen av mellomvare, men [1] at det ikke er mulig å definere noen klare grenselinjer mot laget over og laget under i figuren, [2] at det ikke er mulig å sortere ut noen kjerne av mellomvarefunksjoner som alle applikasjoner benytter og [3] at figuren kun er et mentalt bilde og ikke en presis plassering av mellomvaren.

Mellomvare er med andre ord en kontekstavhengig størrelse, hva som er sentrale mellomvarefunksjoner i en sammenheng, kan godt være helt irrelevant i en annen sammenheng. Et par eksempler:

- En mekanisme som sørger for at tidsstyrte applikasjoner (eksempelvis audio-/videosystemer) kan reservere båndbredde, kategoriseres i mange sammenhenger som mellomvare
- En søkemotor som kartlegger og finner ressurser i nettet oppfattes også av mange som en mellomvare

To generelle forhold knyttet til mellomvare kan det allikevel sies å være gjennomgående enighet om:

- Mellomvare blir en kritisk komponent i organisasjoners og foretaks IT-omgivelser
- Mellomvare blir en kritisk komponent når IT-tjenester og ressurser skal samvirke og være tilgjengelig for brukere på tvers av organisasjoner og foretak

Det siste aspektet er spesielt viktig for forskning og høyere utdanning. Det er påtrengende i tungregnesammenheng der ressurser både skal samvirke og deles på tvers av institusjoner. Det vil bli særdeles påtrengende når aktiviteter i et nasjonalt læringsnett skal utvikles, integreres og brukes i ulike læringskontekster. Utdannings- og forskningssektorens utallige læresteder, institusjoner, organisasjoner og foretak og desentrale struktur er en sentral forklaring på dette. Et av de sentrale mellomvareaktivitetene er nettopp knyttet til mellomvarebehovene innen forskning og høyere utdanning, – mellomvareaktiviteten i Internet2, – jf http://middleware.internet2.edu/, spesielt MACE – Middleware Architecture Committee for Education som er et samarbeid mellom Internet2 og EduCause. Et nasjonalt læringsnett vil kunne hente mye av grunnlaget for å implementere mellomvareløsninger kanskje spesielt her, men også i andre fora der mellomvare vies oppmerksomhet:

- NPACI – NSF Partnerships for Advanced Computational Infrastructures
- The Grid Forum
- NGI – Next Generation Internet
- W3C – World-Wide Web Consortium
- Terena
- Med flere

Også innenfor standardiseringsaktiviteter på læringsområdet er dette et felt som vies oppmerksomhet, – IEEE Learning Technology Task Force (LTTF) , IMS Global Learning Consortium og AICC Sharable Courseware Object Reference Model (SCORM).

Innenfor norsk forskning og høyere utdanning er det allerede gode tradisjoner for mellomvaretype-løsninger, – systemer som er tatt ut fra en lokal kontekst og løst på et nasjonalt nivå. FS (Felles studentsystem), SO (Samordnet opptak), Vitnemålsdatabase, Godkjenningsdatabase, Doktorgradsdatabase er eksempler på hvordan dette er gjort på studieadministrativ side, BIBSYS sine bibliotekskataloger et eksempel på at dette er gjort på bibliotekssiden. Sist, men langt fra minst, – UNINETT er et lysende eksempel på at det kan være mulig også å implementere mellomvareløsninger innenfor norsk forskning og høyere utdanning. Motivasjonen for slike felles grep kan oppsummeres i følgende punkter:

- Sikre rasjonelle og kosteffektive fellesløsninger for sektoren som helhet
- Implementere nasjonale standarder, sikre likebehandling og sikre et felles nivå av tjenestekvalitet og -tilgjengelighet
- Legge grunnlag for samvirke og samarbeid innen sektoren
- Redusere administrativ overhead og sørge for at enhetene kan konsentrere mest mulig av ressursene om primærvirksomheten, – forskning, utdanning og formidling

I et nasjonalt læringsnett vil motivasjonen for mellomvareløsninger gå langs akkurat de samme linjene.

Kritiske mellomvarefunksjoner

Innenfor et nasjonalt læringsnett vil det være en kjerne av mellomvarefunksjoner som må være på plass for å oppnå ønsket funksjonalitet:

- Identifikasjon
- Autentisering
- Autorisering og adgangskontroll
- PKI, kryptering og sertifikater
- Katalog

I tillegg kommer en del støttefunksjoner i form av systemer med autoritativ informasjon, felles regler, prosedyrer og rutiner for blant annet å sikre datakvalitet og bygge sikkerhet rundt løsningene.

Den første oppgaven vil være **identifikasjon** av aktørene, det vil si tilordne aktørene et entydig navn ('distinkt identifikator'). Aktør kan her være en bruker, en ressurs, en tjeneste, en gruppe, en organisasjon eller whatever. Tidligere var brukernavnet den sentrale identifikasjonen. Etter hvert har vi fått mange brukernavn, vi har en eller flere epostadresser, vi har fødselsnummer og vi har andre mer

spesielle identifikatorer. Disse identifikatorene utstedes av forskjellige instanser og det er ofte tilfeldige koplinger mellom dem og det er varierende rettigheter og plikter knyttet til dem. I et nasjonalt læringsnett vil en entydig identifikasjon av aktørene, enten de er personer, ressurser, tjenester eller noe annet, være av vesentlig betydning.

Den andre oppgaven er **autentisering** som innebærer å bekrefte eller garantere at aktøreren som presenterer en identifikasjon overfor et system eller en tjeneste virkelig er den ID-en ble utstedt til. For en person kan denne bekreftelsen eller garantien bygge på noe en *vet* (for eksempel et passord), noe en *har* (for eksempel et smartkort eller et digitalt sertifikat) eller noe en *er* (for eksempel formidlet av foto, fingeravtrykk eller lignende). Hva slags autentisering som velges er avhengig av kravene til sikkerhet og kontrollerbarhet. Det er allment kjent at ukrypterte passord i nett ikke garanterer noe som helst. Krypterte passord i nett hjelper noe, sertifikater hjelper enda mer. Når det gjelder sertifikater og smartkort kommer sikkerheten og troverdigheten til utsteder inn som et sentralt element. Biometrisk autentisering (fingeravtrykk, retinascan, stemmegjenkjenning og lignende) er på trappene.

Autentisering er en nøkkelfaktor i en nettverksbasert omgivelse som et nasjonalt læringsnett innebærer. Det er av avgjørende betydning at autentisering en felles, samordnet funksjon, at den er tilgjengelig for enhver tjeneste, ressurs eller anvendelse som trenger det og at den er effektiv.

Den tredje oppgaven – **autorisering** – innebærer å gi tillatelse til å sette i gang prosesser, gi adgang til å rekvirere tjenester og ressurser og fordele plikter og rettigheter til autentiserte aktører. Autoriseringen er avhengig av sikker autentisering, men i motsetning til denne er autorisering en lokal oppgave. Beslutning om å gi tillatelse til noe som helst tilligger den instans som eier eller tilbyr dette 'noe som helst'. Autorisering vil bli en stor utfordring etter hvert som samarbeidsbaserte applikasjoner ('gruppevare') der arbeids- og dokumentflyt er et sentralt aspekt. Dette gjelder blant annet såkalte LMS-er[6] ('Learning Management Systems'). Et godt eksempel er utfordringer knyttet til hvem som får lese og endre hva i en gruppekalender. Systemer for autorisering innebærer gjerne en gjenskaping i datasystemet av en organisasjons struktur og distribusjon av plikter og rettigheter til organisasjonsledd og personer.

Autoriseringen er avhengig av at systemene som leverer informasjonen (for eksempel katalogen, – jf nedenfor) ikke bare har et begrep om objekter (brukere), men også har et gruppebegret og er i stand til å gruppere objektene i meningsfulle objektklasser (grupper), gjerne også hierarkisk organiserte grupper og tilordne brukere og grupper roller. Autorisering vil i stor grad skje på gruppe- og rollebasis og i liten grad på individuell basis.

Den fjerde oppgaven – **PKI, kryptering og sertifikater** – er den delen som skal sørge for at disse og en rekke andre prosesser kan utføres innenfor så sikre omgivelser som mulig. PKI står for 'Public Key Infrastructure' og er en infrastruktur som støtter kryptering av (utveksling av) informasjon. PKI-er bygger på et system der alle aktører har to krypteringsnøkler, en offentlig og en privat nøkkel og begge nøklene kan brukes til både å kryptere og dekryptere. Digitale signaturer er en av flere anvendelser av dette og kan tjene som eksempel på hvordan en PKI fungerer:

- Utgangspunktet er to parter (Tom og Jerry) som ønsker å utveksle informasjon som ingen annen part skal kunne ha innsyn i
- Når Tom skal sende en hemmelig melding til Jerry, så krypterer Tom først meldingen med Jerrys offentlige nøkkel for å sørge for at det bare er Jerry som kan dekryptere og lese meldingen, deretter krypterer Tom meldingen med sin private nøkkel
- Når Jerry mottar meldingen, så dekrypterer han først meldingen med Toms offentlige nøkkel og får derved bekreftet at meldingen faktisk er fra Tom, og deretter dekrypterer han meldingen med sin private nøkkel

Kombinert med ulike funksjoner for å beregne sjekksummer med utgangspunkt i innholdet i meldingen ('hash'-funksjoner) gir dette systemet bekreftelse (i alle fall i teorien) på at avsender og mottaker er identifisert og at ingen har hatt innsyn i eller endret meldingen underveis.

Et sertifikat er en kopling mellom en offentlig nøkkel og en identitet. Sertifikatet er utstedt og signert av en tredjepart som partene i utgangspunktet stoler på, – en sertifiseringsautoritet. I en PKI er det et hierarki av slike tredjeparter, der autoriteter på høyere nivåer garanterer for identiteten til autoriteter på lavere nivåer. Resultatet er et komplekst system som blant annet har den egenskapen at sertifikater kan benyttes på tvers av autoritetene. I Norge er det etablert tre offentlige sertifiseringsautoriteter, – Posten SDS, Strålfors og Telenor Bedrift Zebrasign og disse har inngått avtale om kryssertifisering slik at sertifikater signert av den ene godkjennes av de andre. Bankene kommer sikkert med sin egen sertifiseringsautoritet. Til forskjell fra de tre andre vil bankene allerede i utgangspunktet ha tung anvendelse av sertifikatene i egen virksomhet.

PKI, krypering og sertifikater er et komplekst område som har en enkel målsetting, – ved hjelp av kryptering og sertifikater ønsker en å bygge omgivelser for sikrest mulig kommunikasjon mellom identifiserbare parter.

Den femte oppgaven – **katalogtjenestene** – er det som skal holde orden på alle objektene og egenskapene (attributtene) ved objektene i disse og andre prosesser på datasystemene og i nettverket. Katalogene inneholder informasjon om brukere, organisasjoner, grupper, prosesser, ressurser, programmer og whatever aktører og objekter på et datasystem eller i et nettverk og gjør informasjonen tilgjengelig for brukere, prosesser, tjenester, systemer og whatever som er avhengig av informasjonen for å løse sine oppgaver. Kataloger fungerer på samme måte i IT-omgivelsene som i den 'virkelige' verden. Er de ikke oppdatert, har dårlig datakvalitet, inkonsistente data eller er ufullstendige, er de mer eller mindre ubrukelige for oss, de gir ikke opplysningene som er nødvendig for å løse en oppgave. Med andre ord, – gode kataloger er en nødvendig forutsetning for å realisere målene med de andre mellomvareoppgavene.

Katalogtjenestene ('directory services') som det her er snakk om, er noe langt mer enn IT-verdenens svar på telefonkatalogenes hvite, rosa og gule sider. Ved siden av å gjøre opplysninger om objekter tilgjengelig for oss, gjør katalogtjenestene også nettbaserte tjenester og systemer tilgjengelig for oss og forenkler lokaliseringen av nettbaserte ressurser. I en nettbasert verden er de med andre ord en forutsetning for at vi som brukere skal kunne manøvrere i en nettbasert verden av tjenester og systemer og de er en forutsetning for at disse nettbaserte tjenestene og systemene skal kunne fungere og være tilgjengelig for oss. De er *også* en forutsetning for at system- og nettadministratorer skal kunne administrere, drive og vedlikeholde nettbaserte systemer, tjenester og ressurser. *Og* de er en forutsetning for at prosesser skal kunne samvirke og utveksle informasjon. Hvis det er noe som fortjener omtale som limet som holder nettbaserte brukeromgivelser sammen, så er det katalogtjenestene.

I utgangspunktet var katalogene enkle lister basert på data lagret i flate filer. Etter hvert som datasystemene vokste i størrelse, utstrekning og kompleksitet, vokste katalogene ut av disse lokale system- og maskinomgivelsene og utviklet seg til spesialiserte tjenester med global rekkevidde enten bokstavelig eller innenfor et domene eller gjenstandsområde. I disse katalogene er objektene de lagrer informasjon om og egenskapene (attributtene) ved disse definert i et skjema. Dette skjemaet beskrives oftere og oftere i XML. Interaksjonen med katalogen skjer på samme måte oftere og oftere med LDAP. Katalogene bygges vanligvis ofte opp i en trestruktur som gjør det mulig å bygge distribuerte kataloger, noe som gjør at systemet skalerer fra lokale til globale anvendelser. Navnetjenesten i Internet (DNS – Domain Name Service) er et godt eksempel på en slik trestrukturert distribuert katalog, og som leverer varene både lokalt og globalt.

For brukerne er det et par mekanismer som er av vesentlig betydning. Den ene er at disse katalogene implementerer en datalagring som er optimalisert for lesing, det går og skal gå lynraskt å lese fra katalogen. Det andre er at de implementerer effektive søkemekanismer som gjøre det enkelt å lokalisere og få tilgang til informasjon om objektene.

Støttefunksjoner og annet

Mellomvareløsningene er avhengig av autoritativ informasjon for å fungere etter hensikten. Denne kan enten ligge i og oppdateres direkte i katalogene eller den kan hentes annet steds fra. I den grad informasjonen allerede finnes i autoritative systemer som det er mulig å kommunisere med, skal den naturligvis hentes derfra for å unngå dobbeltregistrering (etter prinsippet 'en kilde – utallige anvendelser'). Innenfor høyere utdanning inneholder Felles studentsystem (FS) – i prinsippet i alle fall – oppdatert informasjon om både studenter og studietilbud. I tillegg har alle institusjonene et lønns- og personalsystem som – i prinsippet – inneholder informasjon om alle ansatte. Begge systemer vil – i prinsippet – ha innebygget en organisasjonsstruktur i form av stedkoder eller en annen konstruksjon som identifiserer organisasjonsenhetene.

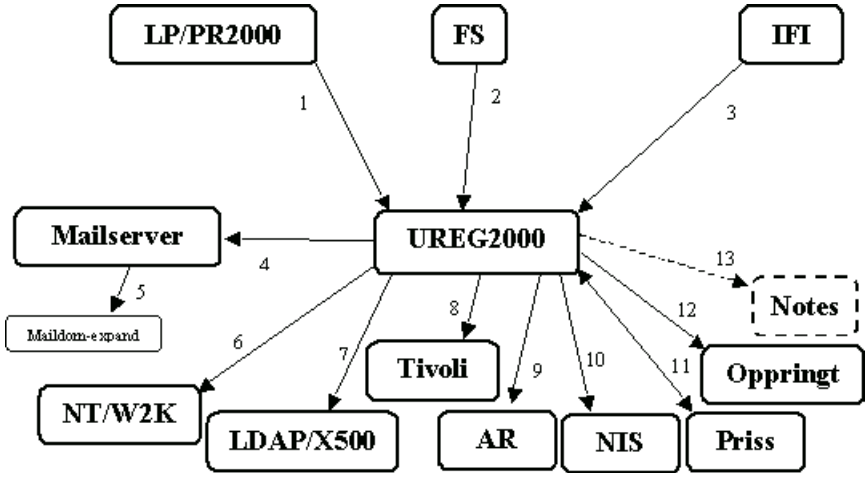
Disse systemene (og andre systemer) kan gi mellomvareløsningene autoritativ informasjon. 'I prinsippet' understreker at dette ikke nødvendigvis er tilfelle i praksis. Erfaringsvis er datakvaliteten i disse systemene sterkt varierende. Årsakene til dette er mange og knyttet til at organisasjonene bruker systemene på forskjellig måte og at rutinene for oppdatering og vedlikehold av informasjonen er tilfeldige eller fullstendig fraværende. For at systemene skal levere autoritativ informasjon må det implementeres prosedyrer, rutiner og praksis som sikrer ønskelig datakvalitet og det må etableres mekanismer som kan verifisere dette.

En annen forutsetning for en mellomvare som fungerer etter hensikten er noen felles regler for

organisasjonene i form at et minste felles multiplum når det gjelder IT-reglement. Dette må minimum inneholde klare bestemmelser om hvilke rettigheter og plikter ulike grupper av brukere har, hva som er akseptabel praksis og hvilke sanksjonsordninger som kan settes i verk ved brudd på reglementet.

Et eksempel: UREG2000 ved Universitetet i Oslo

Et effektivt system for brukeradministrasjon er en forutsetning for å gi brukerne enkel tilgang til nettbaserte tjenester. Det er også en forutsetning for effektiv administrasjon og drift av tjenestene. Ved USIT, Universitetet i Oslo har vi utviklet og tatt i bruk et eget system, – UREG2000, til dette formålet. Målsettingen med UREG2000 er størst mulig grad av automatisering av brukeradministrasjonen. En forutsetning for dette er at brukeradministrasjonen kan bygge på autoritative kilder når brukere etableres, gis rettigheter og tilordnes gruppemedlemsskap. En skisse av systemet kan se omtrent slik ut:



UREG2000 har tre autoritative kilder. Opplysninger om studentbrukere hentes fra FS – Felles studentsystem. Opplysninger om ansattebrukere hentes fra Lønns- og personalsystemet (som nå heter LT og ikke LP/PR2000). I stedet for IFI skal det stå BOFH2 som er programmet som brukes til å legge inn bruker som det ikke finnes opplysninger om i de autoritative systemene. I tillegg brukes BOFH2 til andre brukeradministrative oppgaver. Stedkodene er den mekanismen som binder dette sammen gjennom å tilordne brukere til organisasjonsenheter.

UREG2000 leverer brukerinformasjon til systemer og tjenester som har behov for det (postsystemet, Active Directory, katalogen, NIS og en del andre ting, i tillegg arbeides det for tiden med en løsning som gjør det mulig å levere brukerinformasjon til Domino Directory).

Kjernen i UREG2000 er en Oracle-database med et 60-talls tabeller. Rundt denne er det en rekke småprogrogrammer som henter data fra de autoritative systemene og og leverer data fra UREG2000 til systemene som har behov for dem. Hele denne pakka er lagd slik at det er forholdsvis enkelt å flytte den, for eksempel til en annen database. Et sentral begrep i systemet er gruppebegrepet. Via gruppebegrepet er det mulig å organisere brukere i grupper og tildele dem rettigheter og ressurser. Foreløpig kjenner UREG2000 til tre grupper, – filgrupper, nettgrupper og IT-grupper. Filgruppen bestemmer hvilke filer og filområder brukeren har tilgang til, mens nettgruppen blant annet bestemmer hvilke maskiner vedkommende kan logge seg inn på. IT-gruppen brukes til å tildele lokale IT-ansvarlige og andre rettigheter til å administrere (en delmengde) brukere i systemet. Arbeid er på gang for å implementere et mer genetisk gruppebegrep der blant annet grupper kan være medlem av grupper og der grupper kan bestå av både brukere, maskiner og domener. Gruppebegrepet er (naturligvis) helt avhengig av et fungerende system for stedkoder.

UREG2000 har gitt Universitetet i Oslo besparelser, nye funksjonalitet og langt mer stabile, bedre fungerende og enkelt tilgjengelige IT-tjenester. Den største og mest umiddelbare besparelsen ligger i selve systemet. Ved å ha en felles brukerdatabase spares betydelig arbeid som ellers ville gått med til å vedlikeholde et større antall lokale brukerdatabaser. Ved å bygge brukere basert på autoritative kilder spares mye arbeid ved at man slipper dobbelt- og trippelregistrering av samme opplysninger.

UREG2000 innebærer også store fordeler ved at systemet muliggjør desentralisering av brukeradministrasjonen. I systemet kan lokale IT-ansvarlige vedlikeholde informasjon om sine brukere, noe som gjør at informasjonen kan oppdateres raskt. Med over 40.000 brukere ville sentralt vedlikehold

være bortimot umulig, i beste fall sterkt tidkrevende. En felles brukerdatabase sikrer også at brukerinformasjonen i de ulike systemene er konsistent og har den nødvendige datakvalitet.

I dette systemet er det også muligheter for å lage nye tjenester og funksjonalitet. En ting som står høyt på dagsorden er en kopling mellom brukere og lokal IT-ansvarlig. Dette vil gi mulighet for at brukerhenvendelser kan rutes direkte til riktig lokal IT enten henvendelsen skjer via en IT-vakt (helpdesk) eller til et IT-basert feilmeldingssystem.

Det er et betydelig arbeid knyttet til å etablere et system som UREG2000. En vesentlig (antakeligvis den største) del av arbeidet er knyttet til organisasjon og til å sikre kvalitet og konsistens i de autoritative systemene. Et stort arbeid er lagt ned i å utforme et felles stedkodesystem for de autoritative systemene og som UREG2000 kan bruke. Et annet stort arbeid er knyttet til datakvaliteten i de autoritative systemene. På dette området må det legges ned mye arbeid i regler, rutiner og prosedyrer for innlegging og vedlikehold av data i disse systemene.