

Uninytt nr. 4 2004

Innhold

- [Nettforskning på dagsordenen](#)
- [LOBSTER](#)
- [UNINETT Sigma AS er født](#)
- [Teite ting om tryggleik](#)
- [Nytt om innkjøpsavtaler](#)
- [UNINETTs betalingsmodell for 2005](#)
- [Vårens vakreste eventyr](#)
- [Høgskolen i Agder fornøyd med FEIDE](#)
- [Bygde grunnmur med FEIDE i verktøykassen](#)
- [Med andre briller: USIT – FEIDE – Cerberum – HIA](#)
- [FEIDE setter nye mål](#)
- [Stor oppslutning om sikkerhetsseminar](#)
- [Redaktørhjørnet](#)

uninytt@uninett.no

2005-06-27

Nettforskning på dagsordenen

Norsk nettforskningsseminar ble arrangert i Trondheim 21.–22. oktober 2004. De forskjellige miljøene som driver med nettforskning i Norge hadde funnet ut at det var på tide å komme sammen og fortelle hverandre hva de holder på med. UNINETT var hovedarrangør.



Til tross for relativt kort varsel samlet arrangementet 56 deltakere. Flest deltakere kom fra de fire institusjonene som hadde gått sammen om arrangementet: Senteret for kvantifiserbar tjenstekvalitet ved NTNU (Q2S), Simulasenteret i Oslo, Institutt for telematikk ved NTNU og UNINETT. Videre kom det deltakere fra flere høyskoler og fra industrien.



Høydepunktet for de fleste var nok det innbudte foredraget fra internettveteranen Yngvar Lundh (bildet), som trakk opp utviklingslinjene fra han knyttet Kjeller-miljøet til Arpa-nettet i 1973 og frem til våre dager. Arpanettet var forløperen til Internett, og Kjeller var første tilknyttede punkt utenfor USA.

Foredraget finnes på: http://uninett.no/nettforskning/nfs2004/2_lundh_internet_history.pdf

Det er allerede klart at det blir nytt nettforskningsseminar. Simulasenteret i Oslo blir arrangør, og foreløpig dato er satt til 27.–28. oktober 2005.

Jon Kåre Hellan

jon.kare.hellan@uninett.no



Programmet bød på 20 faglige foredrag fra forskjellige områder, i hovedsak fra

- ruting
- svermintelligens
- distribuerte systemer
- nettverk

Blant aktuelle anvendelsesområder kan nevnes

- kortdistansenett som forbinder komponenter i en datamaskin eller et cluster
- mulimultimedia (tale, video)

- tilgangskontroll
- måling og overvåking

- optiske nett

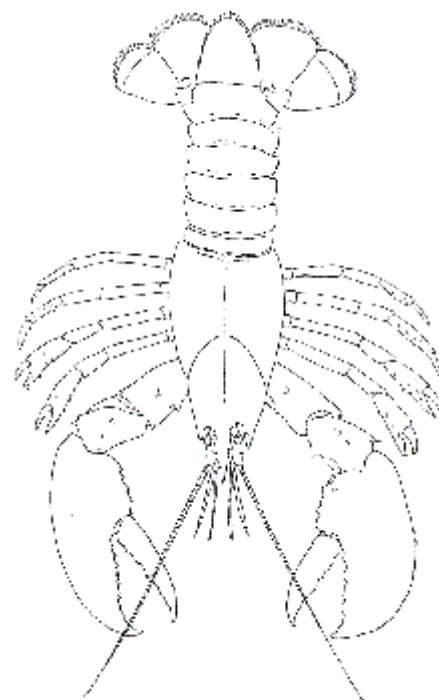
Presentasjonsmaterialet er lagt ut på
<http://uninett.no/nettforskning/nfs2004/>

uninytt@uninett.no

2005-06-29

LOBSTER

UNINETT har siden 1. april 2002 vært involvert i EU prosjektet SCAMPI, som har utviklet maskin- og programvare for passiv overvåking av høyhastighetsnettverk. Dette prosjektet nærmer seg nå slutten, og et oppfølgingsprosjekt kalt LOBSTER har allerede startet. LOBSTER er et EU-prosjekt hvor både nye og gamle partnere fra SCAMPI deltar.



Hovedmålene for prosjektet er:

- Opprette en avansert infrastruktur for passive målinger i Europa. Basert på resultatene og erfaringene fra SCAMPI, skal det utplasseres måleprober hos ISP'er og akademiske nett rundt omkring i Europa. Disse vil kunne snakke med hverandre og utveksle måledata.
- Samordne interessegrupper for avanserte passive mlinger. Infrastrukturen vil involvere mange forskjellige grupper, både kommersielle og akademiske. Prosjektet vil snakke med de forskjellige gruppene for å prøve å komme fram til felles krav for en infrastruktur og for en plan om hvordan den best kan brukes og vedlikeholdes.
- Implementere mekanismer for sikkerhet og anonymisering. Passiv overvåking kan gjøre sensitive data lett tilgjengelig. I prosjektet vil det derfor bli lagt stor vekt på sikkerhet og anonymisering. Mekanismer som tillater brukerdefinerte nivåer med sikkerhet og anonymisering vil bli utviklet. Dette vil gjøre det lettere å utveksle data på tvers av landegrenser.
- Implementere applikasjoner som utnytter infrastrukturen.

Eksempler på noen applikasjoner som vil bli vurdert implementert er:

* Nøyaktig identifisering av applikasjoner som bruker dynamiske porter. Mange applikasjoner, for eksempel P2P, bruker dynamiske porter for overføring av data, noe som gjør det vanskelig å bestemme at trafikken tilhører akkurat denne applikasjonen. Med passiv overvåking er det mulig å se inn i kontrollpakker som blir brukt for å sette opp de dynamiske portene og på den måten identifisere trafikken.

* Detektere spredning av nye ormer. Spredning av nye ormer på Internett kan være et

stort problem. I januar 2003 ble Sapphireormen sluppet løs, og i løpet av 30 minutter hadde ormen infisert over 70 000 PC'er rundt omkring i verden. Ved å bruke LOBSTER-infrastrukturen kan man se på data fra mange måleprober for å detektere unormal trafikk, slik at man blir varslet når nye ormer blir sluppet løs.

* Europeisk måletjeneste. Nettverksstatistikk på en europeisk skala kan samles inn og presenteres. Dette kan gi nyttig informasjon for problemer med ende-til-ende-ytelse, forskjellige typer forskning og for planlegging av nettverksutbygging. Offisiell start av prosjektet var 1. oktober 2004, og det skal avsluttes 31. desember 2006. Hele prosjektet har en ramme på 183 månedsverk, hvor UNINETT bidrar med 10. UNINETT er ikke involvert i selve utviklingen av måleprobene, men skal lede arbeid med uttesting og utplassering i siste fase av prosjektet.

Arne Øslebø
arne.oslebo@uninett.no



uninytt@uninett.no

2005-06-29

Uninett Sigma er født

29. oktober 2004 inngikk Norges forskningsråd og UNINETT avtale om framtidig ansvar for operativ drift og utvikling av norsk tungregning. Dagens prosjektaktivitet videreføres med en tidsramme på 10 år, og skal ledes av et nytt datterselskap i UNINETT-konsernet. Dermed sikres en stabil utvikling av infrastrukturen for avansert vitenskapelig beregningsarbeid i Norge.

Siden 2000 har norsk tungregning vært organisert i prosjektet NOTUR under ledelse av NTNU. Prosjektet har vært drevet i samarbeid med de øvrige universitetene, Meteorologisk institutt, Statoil, SINTEF og andre aktører og vært finansiert av Forskningsrådet og deltakerinstitusjonene.

Langsiktig investeringsplan

En av fordelene med å etablere det nye selskapet under UNINETT, er at vi kan se nettverk og maskin- og lagringsressurser i sammenheng. Dette er særlig viktig framover siden datastrømmene blir større både når det gjelder beregning og lagring. Det vil også bli mulig å legge en langsiktig investeringsplan som kan utnytte infrastrukturen på en bedre måte, både med hensyn til utstyr og kompetanse.

Av flere kandidater ble UNINETT valgt fordi selskapet har lang erfaring som driftsorganisasjon. I tillegg forventes det synergi på flere områder av den samordningen som skjer.

Tungregningsaktiviteten støtter UNINETTs engasjement som norsk grid-kordinator. En felles organisering vil dessuten gi mulighet for en mer

koordinert utbygging av forskningsnettets framover slik at kapasitetsbehovene innenfor tungregningsmiljøene til enhver tid er dekket.



Muligheter for samordning

– Et knippe nasjonale infrastrukturtiltak – nett, tungregnerressurser, elektronisk identitet og grid – er nå samlet i UNINETT-konsernet. Dette gir gode muligheter for samordning. I internasjonal sammenheng er dette ganske enestående, kommenterer administrerende direktør i UNINETT, Petter Kongshaug.

Fra Forskningsrådets side understrekes det at den nye organisasjonsmodellen i stor grad følger opp anbefalingene til en internasjonal komité ledet av professor Risto Nieminen ved Helsinki-universitetet, en modell som har vært til høring i berørte miljøer. Ved å etablere et offentlig finansiert verktøy for tungregning, vil satsingen kunne få både økt synlighet og et mer varig preg.

–UNINETT pekte seg ut som vertsinstitusjon på bakgrunn av selskapets erfaring med leveranse av ITinfrastruktur til kunder innen høyere utdanning, sin kompetanse innen høyhastighetsnett og posisjonering som aktør innen GRID infrastruktur. Disse elementene forventes å være sentrale for videreutviklingen av en nasjonal infrastruktur for tungregning, sier rådgiver Gudmund Høst i Forskningsrådet.

Arbeidet videre

Arbeidet med oppstart av det nye selskapet er i full gang i UNINETT-organisasjonen. Selskapet ble offisielt stiftet på UNINETTs styremøte 2. desember 2004 med oppstart 1. januar 2005. Selskapets styre består av Lars-

Anders Breivik, Meteorologisk Institutt, Pinar Heggernes, UiB, Randi Holmestad, NTNU, Petter Kongshaug, UNINETT og Kenneth Ruud, UiTø. Varamedlemmer til styret er Mats Carlsson, UiO og Morten Hjorth-Jensen, UiO. Styret ble utnevnt av selskapets generalforsamling (UNINETTs styre) etter innstilling fra Forskningsrådet.

Arbeidet med nye partneravtaler er i gang. Intensjonsavtaler skal etter planen bli skrevet før nyttår, mens endelige avtaler først vil være klare tidlig til neste år. Kravspesifikasjonen til prosjektet, som har vært ute til høring i de berørte miljøer, er snart klar. En formell søknad vil deretter bli sendt til Norges forskningsråd, som utarbeider prosjektavtale og setter økonomiske rammer for en 5-årsperiode framover.

Administrative tjenester som økonomi, sekretærfunksjon og informasjon vil bli leiet av UNINETT AS inntil man kjenner arbeidsoppgavene og behovet for ansatte i det nye selskapet bedre.



Bjørn Hafskjold
bjorn.hafskjold@uninett.no



uninytt@uninett.no

2005-06-29

Teite ting om tryggleik

Har du følelsen av at datamaskinen din har blitt tregere enn den var da den var ny? Opplever du til stadighet uforklarlige systemkrasj og at enkelte programmer virker ustabile eller ikke lenger virker slik som de gjorde tidligere?

Da er det mulig at maskinen din har fått installert såkalt spionprogramvare eller spyware som det kalles på nynorsk. Fenomenet har vært kjent en tid, men det er først i løpet av det siste året at dette har fått et omfang som minner om en gryende sikkerhetstrussel. Ennå er det i første rekke Windows-systemer som er hjemsoekt, men også andre plattformer har potensial til å kunne bli vertskap for slike parasitter.

Spyware er en fellesbetegnelse for teknologi som innhenter informasjon om en person eller organisasjon sine surfevaner, og som deretter sender dette tilbake til slemminger som har interesse av å vite slikt. Denne aktiviteten foregår som regel uten at brukeren av maskinen har kjennskap til det, og formålet er som regel å kartlegge brukerens interesser og vaner, for deretter å kunne produsere og sende tilbake tilpasset reklame om dette og hint.

I den senere tid har man dessverre også avdekket at denne typen programvare kan drive med mer ondsinnet spaning, som for eksempel snoking i brukerens private filer, kontonummer, kredittkortinformasjon og nettbank for å nevne noen muligheter.

Spionprogramvare er typisk programvare som kan følge med på kjøpet når du laster ned gratis programvare fra nettet. En del populære gratis fildelingsprogrammer er blant annet kjent for å inneholde spionprogramvare.

Hva kan man så gjøre for å unngå dette problemet?

Det beste er selvsagt å hindre at denne typen programvare blir installert i utgangspunktet. Ved å være litt kritisk ved installasjon av ny programvare, og spesielt ved installasjon av gratis programvare, så kommer man et godt stykke på vei. Mange programmer som inneholder spyware forteller faktisk om dette i de vilkårene du vanligvis må akseptere før det hele lar seg installere. Men det er jo ikke alltid at man tar seg tid til å lese det med liten skrift.

Hvis først uhellet er ute, så finnes det heldigvis hjelp å få. Leverandørene av antivirusprogramvare har vært bemerkelsesverdig passive på dette området, men ironisk nok har et par gratisprogrammer :) gjort seg bemerket.

Disse er:

- Ad-aware
- Spybot Search && destroy

Programmene ligner mye på de antivirussystemene de fleste av oss har installert. Maskinen gjennomsoekes for kjente mønstre, eventuelle funn blir varslet og brukeren får anledning til å

rydde opp.

Mønsterfilene kan og bør oppdateres jevnlig for å fange opp nye problemer. Spybot Search && destroy gir deg også muligheten til å vaksinere systemet mot nye forekomster av lure programsnutter som står klar for å tappe maskinen din for informasjon. Det finnes sikkert etter hvert også andre programsystemer som gjør tilsvarende jobb, og det er rimelig å forlange at antivirussekskapene etter hvert også tar tak i dette.



uninytt@uninett.no

2005-06-29



Nytt om innkjøpsavtaler

Innkjøpsavtalene som UNINETT FAS tilbyr er forhandlet frem med basis i kundemassen og ut fra ønsker og behov hos våre abonnenter. Disse avtalene skal gi bedre priser enn det hver enkelt kan oppnå på egen hånd.

Vi har i dag 77 abonnenter, deriblant 25 høgskoler, samtlige 6 vitenskapelige høgskoler og begge kunsthøgskolene. I tillegg er en rekke ikke-kommersielle forsknings- og utdanningsinstitusjoner i Norge abonnenter.

Tjenesten finansieres av en abonnementsavgift fra de UNINETT-medlemmer som ønsker å benytte seg av tilbudet. I 2004 ble følgende prismodell benyttet:

Antall ansatte	Pris pr.år
Under 100	Kr 4 000
101-500	Kr 13 500
Over 500	Kr 20 000

Eksisterende programvareavtaler i dag:
● CA Arcserve

- NSD
- Cad Quality AS
- Nyno
- Citrix
- Opera
- Corel
- Oracle
- Fronter
- Panda Antivirus
- F-Secure
- SPSS
- Macromedia
- Symantec
- Microsoft
- Veritas Backup Exec
- Novell

Ved kjøp av maskinvare, samarbeider UNINETT FAS både med Bravida, Ementor og Evolve.

Nyheter

I 2004 startet vi arbeidet med en grundig gjennomgang av alle eksisterende avtaler. I denne prosessen har vi valgt å sette i gang anbudsrunder for å forsikre oss at vi har de absolutt beste tilbudene på ønsket programvare.

Dette arbeidet vil bli prioritert også i 2005.

Vi ønsker å minne om at UNINETT FAS i slutten av 2003 inngikk en ny avtale med Oracle, en Campus-avtale for Oracle Database Enterprise Edition. Avtalen gjelder for et endelig antall ikke-kommersielle UNINETT-institusjoner under kategorien "høgere utdanning".

Les om avtalen på

<http://www.uninett.no/innkjop/programvare/oracle-campus.html>.

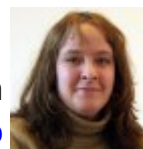
Kontaktpunkt

Informasjon om tjenesten finnes på

<http://www.uninett.no/innkjop/>.

Jeg ønsker til slutt å benytte anledningen til å ønske alle en god jul.

Marion Andreassen
marion.andreassen@uninett.no



uninytt@uninett.no

2005-06-27

Uninets betalingsmodell for 2005

UNINETTs prismodell omfatter forskningsinstitusjoner, bibliotek, museer, private utdanningsinstitusjoner, grunnskoler og videregående skoler. Den gjelder ikke universitetene, de offentlige regionale høgskolene, kunsthøgskolene eller de vitenskapelige høgskolene.

UNINETTs priser baserer seg på estimert kapasitetsuttak per kunde. Statistisk trafikkanalyse, som foretas for å finne flaskehals i nettet slik at effekten av linjeoppgraderinger blir størst mulig, gir også en indikasjon på hva den administrative kapasiteten bør settes til.

Hva inkluderer tjenesteavgiften?

UNINETT driver et utdannings- og forskningsnett som opererer med overkapasitet for å unngå flaskehals. Dette vil brukere særlig merke på trafikk til utlandet (Europa og USA), hvor UNINETT har tilgang til forskningsnettforbindelser som har gigabitkapasitet.

I tillegg kan UNINETT tilby innkjøpsavtaler, hvor kundene kan spare betydelige beløp på kjøp av maskinvare, programvarelisenser, leie av samband med mer.

Betalingsmodellen for 2005

UNINETTs kunder kobler seg til et UNINETT tilknytningspunkt i form av to ulike tilknytningstyper:

I) Lokalisering nær UNINETTs tilknytningspunkt. Kunden har en kort, intern fiberforbindelse eller leier/graver egen fiber som gir kunden tilknytning med svært høy kapasitet 100 Mbps.

II) Kunden leier et digitalt samband, normalt 2 Mbps, fram til UNINETTs tilknytningspunkt.

Kundegruppe I og II betaler i dag en tilknytningsavgift til UNINETT basert på estimert kapasitetsuttak, målt ved 95. persentil av deres maksimale kapasitetsuttak. Man får med andre ord eliminert ekstreme utslag på trafikkmålinger, som kan skyldes traøkkstormer eller andre forhold. Samtidig oppnår man et noenlunde rettførdig bilde av institusjonens kapasitetsuttak.

Mens institusjoner i kundegruppe I og II kan ha samme gjennomsnittlige kapasitetsuttak, vil de kunne oppleve ulik tjenestekvalitet som følge av den store øyeblikkskapasiteten som er tilgjengelig for institusjoner i gruppe I. Dette gir kunden en merverdi som vi nå prøver å illustrere i betalingsmodellen.

Forslag til ny betalingsmodell er som følger:

Kundegruppe I: Betaling basert på estimert kapasitetsuttak (administrativ kapasitet). Tillegg for tilgjengelig øyeblikkskapasitet

Kundegruppe II: Betaling basert på estimert kapasitetsuttak (administrativ kapasitet). Les

mer om hva du får som kunde hos UNINETT på

<http://www.uninett.no/produkt/beskrivelse.html>.

Administrativ kapasitet	Pris før	Pris nå	Endring	Tillegg for høykapasitetstilknytning
9 kbit/s	8 800	8 500	-3,41 %	850
19 kbit/s	17 600	17 000	-3,41%	1 700
64 kbit/s	29 600	29 000	-2,03 %	2 900
128 kbit/s	41 600	41 600	-3,85 %	4 000
256 kbit/s	50 000	47 500	-5,00 %	4 750
512 kbit/s	67 000	64 000	-4,48 %	6 400
1 Mbit/s	79 800	77 000	-3,51 %	7 700
2 Mbit/s	99 800	95 000	-4,81 %	9 500
3 Mbit/s	127 200	121 000	-4,87 %	12 100
4 Mbit/s	166 800	159 000	-4,68 %	15 900
5 Mbit/s	180 600	172 000	-4,76 %	17 200
10 Mbit/s	340 600	324 000	-4,87 %	
34 Mbit/s	554 000	526 000	-5,05 %	
155 Mbit/s	699 800	665 000	-4,97 %	

Lars Skogan
lars.skogan@uninett.no



uninytt@uninett.no

2005-06-27

Vårens vakreste eventyr

Mange har fattet interesse for NORDUnet-konferansen på Svalbard til våren. Vi har allerede 150 påmeldinger, så her gjelder det å være rask for den som har tenkt seg av sted.

Den 22. NORDUnet-konferansen går av stabelen under tittelen "Extending the frontiers of networking", noe som både avspeiler at fiberkabelen til Svalbard har utvidet grensene for Internett, og at den faglige ambisjonen er å strekke kjente grenser innenfor netteknologi.

Bredt faglig program

Programmet dekker et stort spekter av tema, blant annet:



- nettinfrastruktur
- GRID
- trådløse nettverk og mobiltet
- ende-til-ende-ytelse
- mellomvare
- passive målinger

Det vil gå rundt 35 foredrag i løpet av konferansen. Noen vil gi en generell oversikt over utviklingen innen en del av temaene, som for eksempel trådløs teknologi, mobilitet og GRID, og gi god mulighet for dem som ønsker å lære om nye ting eller holde seg oppdatert innenfor det aktuelle temaet.

Nye og gamle internasjonale prosjekter, som SCAMPI, LOBSTER, GEANT2, GLIF og Bere, blir presentert, med oversikt over resultater og framtidige planer.

Det vil også være en del mer praktisk orienterte foredrag, som hvordan bruke PKI i praksis, hvordan få god ende-til-ende-ytelse, hvordan bruke videokonferanse på en effektiv måte innenfor høyere utdanning, og hvordan nå fram til sluttbrukeren.

Under konferansen vil det være noen plenumsforedrag, men det meste vil gå i to parallelle sesjoner. I plenum vil det være mulig å få en oppdatering om NORDUnet, høre om planene EUkommisjonen har om en e-Infrastruktur, få en oversikt over akademiske nettverk i Asia, og få presentert det nye europeiske GEANT2-prosjektet.

Mange av foredragsholderene kommer selvfølgelig fra de nordiske landene, men det vil også være en del fra andre land i Europa og fra USA, og noen er til og med langveisfarende fra Australia og New Zealand.

Eksotiske omgivelser

Svalbard i april betyr lyse og gnistrende omgivelser. Midnattsola er et faktum først noen dager

etter konferansen, men med et fullstendig snødekt landskap vil vi likevel få oppleve det fantastiske lyset nesten døgnet rundt.

Mange ønsker å benytte anledningen til å forlenge oppholdet, enten sammen med en ledsager eller på egen hånd. På grunn av kapasitetsbegrensninger, spesielt når det gjelder flyseter til og fra Svalbard, har vi sett oss nødt til å tilby opplegg for ledsagere i helgene før og etter konferansen, men ikke i de dagene selve konferansen pågår. Et større antall hotellrom og flyseter er reservert for hele perioden. Begge deler er tilgjengelig gjennom registreringssystemet til konferansen. I skrivende stund er det fortsatt en del å velge i, men både hotellrom og flyseter går raskt unna.

Utendørsaktiviteter

Vi har sørget for et bredt tilbud av utendørsaktiviteter, både under konferansen og i dagene før og etter. I tillegg til turer med snøscooter og hundeslede, er det mulighet for gruvebesøk og isgrotting. Dessuten får alle deltakere en guidet busstur i og rundt Longyearbyen som en del av konferansepakken.

I god NORDUnet-tradisjon arrangerer vi en mottakelse med middag kvelden før den offisielle konferanseåpningen. Denne gangen skjer dette i form av en utendørs polaraften i Adventdalen Æ med værguder som vi håper står oss bi. Et arrangement på Svalbard krever is også i magen.

Velkommen til et fullspekket faglig program i spektakulære omgivelser på Svalbard i april.

For program og påmelding, se:

www.nordunet2005.no

Arne Øslebø

arne.oslebo@uninett.no



Elisabeth Farstad

elisabeth.farstad@uninett.no



uninytt@uninett.no

2005-06-27

Høgskolen i Agder fornøyd med FEIDE

Høgskolen i Agder (HiA) bestemte seg i 2002 for å skaffe et



Lars Nesland, Egil Eik, Gunnar Norlie og Embret Nettet har sammen med mange andre lagt ned stor innsats for å innføre FEIDE ved Høgskolen i Agder.

brukeradministrativt system (BAS). Behovet for å holde orden på over 800 ansatte, 8000 studenter og deres roller krevde en automatisk administrasjon. For HiA ble løsningen å velge FEIDE med Cerebrum som BAS.

Prosjektleder for FEIDE ved HiA, Lars Nesland, har hatt hovedansvaret for den utfordrende oppgaven det var å gå fra halv- til helautomatisk vedlikeholdte systemer.

–Vi hadde ingen enhetlig brukeradministrasjon da vi startet med prosjektet, autorative systemer som FS og personalsystemet hadde jo en automatikk knyttet til seg, men de ble vedlikeholdt manuelt. Da vi innførte FEIDE fikk vi et annet krav til presisjon og enhetlig registrering i de autoritative systemene. Vi erfarte virkelig at ting som er forståelig på skjermen for et menneske, ikke er godt nok for en maskin, sier Nesland.

For at FEIDE-løsningene skulle kunne fungere var de avhengige av at alle roller var konsistente slik at data kunne sendes mellom de ulike programmene. HiA ble etablert i 1994 etter en sammenslåing av seks høgskoler i Kristiansand, Grimstad og Arendal, og var i forbindelse med dette nødt til å gjøre store oppryddinger i brukerbasen. Lars Nesland forklarer at de derfor trodde de hadde god orden på brukerne sine, men de erfarte at det er like langt fra nitti til hundre prosent orden, som fra null til nitti.

Valg av BAS

HiA hadde ikke noe BAS fra før, kun loggfiler med historikk. Når avgjørelsen for å ta i bruk et BAS var tatt, var det viktig at alle plattformene som allerede var i bruk kunne implementeres. Det operative arbeidet startet først i 2003, og valget av BAS stod mellom en Novell-løsning og Cerebrum fra UsIT.

IT-sjef Egil Eik forteller at valget av Cerebrum slettes ikke var enkelt. –Vi led virkelig valgets kval fordi vi allerede hadde operativsystem fra Novell da vi fikk tilbud om Cerebrum, som ennå ikke var ferdig utviklet. Det var et dilemma for oss fordi vi syntes at vårt Novellprodukt fungerte godt, og vi viste at Novell kunne tilby løsninger som vi kunne bruke. Når vi til slutt endte opp med Cerebrum, var det mye på grunn av USITs kompetanse og erfaring med Cerebrum, pluss at de tilbød en ferdig integrasjon mot FS, sier Eik.

Felles passord til alle systemer

For administrasjonen og it-avdelingen har innføringen av nytt BAS og FEIDE-løsninger vært en tidkrevende prosess. Alle studenter skulle få ett brukernavn og ett passord som de skulle kunne bruke i alle systemer knyttet til høgskolen. Studenter som allerede var lagt inn i FS fikk tildelt nytt passord ved semesterstart, og det var stort sett disse som opplevde startvansker i høst. Nye studenter ble importert inn i FS fra Samordna opptak, og fikk automatisk tilgang til sine rom i Classfronter. Ved å gi studentene tilgang til sine systemer så tidlig som mulig, ønsket HiA å oppnå at studentene følte et eierskap til studieplassen sin slik at de ikke ville omprioritere før studiestart.

Sikkerhet neste oppgave

For Høgskolen i Agder har brukeradministrasjon vært det viktigste gjennom hele prosessen. Løsninger på sikkerhetsproblematikk og autentisering er fremdeles i støpeskjeen. Egil Eik peker på at det er behov for et felles IT-reglement for hele UH-sektoren for at FEIDE



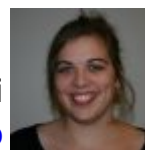
skal kunne fungere på tvers av høgskolene. – Dette med elektroniske identiteter gir store muligheter for flyt av personinformasjon, men for at dette skal fungere trenger vi en felles bruk av regler. I tillegg må vi være enige om hvilken sertifikat-teknologi vil skal bruke for de høye sikkerhetsnivåene. Så lenge dette ikke er avklart for hele sektoren, sitter vi litt på gjerdet og venter.

Fornøyd pilotskole

HiA har tradisjonelt valgt å være pilot ved innføring av nye løsninger, og er fornøyd med innføringen av både Cerebrum og FEIDE. Arbeidet i forkant har vært tidkrevende, men i dag blir nye brukere tatt inn i FS automatisk, og dette har ført til store besparelser.

For de høgskolene som lurer på om de skal sette i gang, anbefaler HiA at de først rydder opp i rutinene sine. – Innføring av FEIDE-løsninger er åtti prosent rutiner og tjue prosent teknologi, sier Nesland.

Karoline Ski
karoline.ski@uninett.no



uninytt@uninett.no

2005-06-29

Bygde grunnmur med FEIDE i verktøykassen

Ved Høgskolen i Agder startet de med en ambisjon om å bruke informasjonssystemer mye mer i kommunikasjonen mellom studenter og ansatte. Både lærere og studenter skulle kunne finne relevant informasjon om fag, oppmelding eller lønn via web-baserte løsninger. For å kunne gjennomføre noe slikt var det grunnleggende med sikkerhet i bunn.



Høgskoledirektør Tor A. Agedal ved HiA er fornøyd med innføringen av FEIDE

En slik sikkerhet kunne FEIDE tilby, i følge høgskoledirektøren, Tor Agedal. –Å bygge opp et brukeradministrativt system slik som vi ønsket det, er som å bygge et hus. Det er viktig å ha en grunnmur i bunn som er solid, og det er der FEIDE kommer inn. FEIDE ga oss det vi hadde behov for: sikker identifisering og gjenbruk av identifiseringen i de ulike systemene.

Hva var det viktigste for dere gjennom prosessen?

–Vår drivkraft for å sette i gang dette prosjektet har vært forenklet brukeradministrasjon. For å få et BAS til å fungere, var vi avhengige av å ha god kvalitet og sikkerhet på våre informasjonssystemer, både de som går mot studentene og de som går ut mot omverdenen.

Har det blitt slik dere ønsket dere?

–Selve prosessen var utfordrende, spesielt for it-tjenesten som hadde en stor jobb med rydde i data og oppdatere omliggende løsninger. Det har absolutt blitt lettere å navigere mellom de systemene vi har tilgang til, så sluttbrukerne synes nok det har blitt enklere. Det er nok allikevel administrasjonen som har merket mest, i og med at deres rutiner har blitt endret og arbeidet har blitt mer oversiktlig.

Har andre høgskoler vært interessert i deres erfaringer?

– Høgskolene er jo i utgangspunktet enige om å forsøke å ha et mest mulig homogent opplegg for dataløsninger, og vi har hatt flere som har vært nysgjerrige på det vi har gjort. For sektoren er det jo en fordel å ha felles administrative systemer for å oppnå stordriftsfordeler når det gjelder innkjøp og drift. Og i forhold til dette ligger det jo en FEIDE

problematikk. Det er en fordel å ha en felles grunnmur, og så kan FEIDE være verktøykassen vi bruker for å få det til å henge sammen.

Hvordan tror du behovet for sentral støtte vil være i fremtiden?

–Med FEIDE i bunn kan støttefunksjonen ligge hvor som helst. En høgskole som er god på en applikasjon kan være ressurs på den og så videre. Så lenge høgskolene er under statsforvaltningen, er det en fornuftig idé å dele på ressursene på denne måten. Det handler om å få mest mulig ut av de midlene vi har og ikke sitte på hver vår tue, men dra lasset sammen. Så får vi heller konkurrere om å ha det beste læringsmiljøet.

Hvilke planer har dere videre?

–Nå har vi innført FEIDE og det ligger i bunn, så vi vil vel jobbe mot andre institusjoner for å kunne samkjøre autentisering. I tillegg skal vi utvikle våre egne datasystemer med tanke på de mulighetene FEIDE gir.

Har du til slutt noen råd for de som lurer på om de skal innføre FEIDE-løsninger?

–Det er viktig at ledelsen ser at de ulike systemene som benyttes må ha krav til integrasjon slik at administrasjonen kan bli håndtert effektivt. Jeg ser FEIDE eller tilsvarende løsninger som en forutsetning for sikker og robust drift, samt administrasjon av brukere. Fordelen med FEIDE er at det ikke er en kommersiell aktør som ikke ser sektoren under ett.

uninytt@uninett.no

Karoline Ski
karoline.ski@uninett.no



2005-06-27

Med andre briller: USIT–FEIDE– Cerberum–HiA



Av Isabel
Barroso
Gómez

prosjektmedarbeider FEIDE

USIT har i løpet av det siste året arbeidet sammen med Høgskolen i Agder (HiA) for å få opp en FEIDE-løsning for høgskolen. Innføringen av Cerberum ved HiA har vært et vellykket prosjekt, og et eksempel på godt samarbeid mellom flere institusjoner.

Valg av BAS

Før institusjoner kan FEIDE sertifiseres, må de ha et brukeradministrasjonssystem (BAS) i bunnen for å ha kontroll på person- og brukerdataene sine. Etter å ha vurdert ulike løsninger, valgte HiA å ta i bruk Cerberum, et BAS som er utviklet ved USIT. Cerberum er et Open Source-produkt som er GPL-lisensiert.



Isabel Barroso Gómez er prosjektleder for Cerberum i UH-sektoren og i FEIDE

Prosessen

USIT tok høsten 2003 kontakt med HiA for å tilby en løsning som tilfredsstillte de krav som FEIDE har satt til et BAS. HiA har mange av de samme systemene som UiO, og det lå til rette for at Cerberum ville fungere godt her også.

Cerberum består av en kjerne med mange moduler. Disse modulene er laget for at Cerberum skal kunne utveksle data med systemer som inneholder person- og brukerinformasjon, enten Cerberum skal importere informasjonen eller eksportere den. Første del av prosjektet besto i å kartlegge hvilke systemer som skulle interagere med Cerberum, og dermed avdekke hvilke moduler det var nødvendig å ta med i løsningen. Det ble også kartlagt hvilke moduler som ikke eksisterte per i dag. For Novell eDir og SAP gikk vi sammen med HiA for å innhente informasjon om systemene.

HiA var pilotdeltaker på OPAL-prosjektet sin SAP løsning. Det ble etter hvert sannsynlig at flere andre høgskoler skulle over på SAP, og vi tok derfor kontakt med FEIDE for å lage en kravspesifikasjon som tok høyde for dette behovet.

Nå som alle modulene er tilpasset, har Høgskolen i Agder koblet sin FEIDE-løsning til Moria, FEIDEs sentrale autentiseringstjeneste. Det blir en ny spennende fase for FEIDE ved HiA.

uninytt@uninett.no

2005-06-29

FEIDE setter nye mål



I 2005 går FEIDE over fra prosjekt til permanent drift, og prosjektleder Jon Strømme kan fortelle om en interessant prosjektperiode hvor FEIDE har levert gode resultater. Det beste resultatet er, ifølge Strømme, en felles forståelse og et felles ordforråd i hele sektoren.

I løpet av prosjektperioden har FEIDE fått på plass et system med over 100 000 brukere og tjenester som kan håndtere disse brukerne.

Over all forventning

FEIDE har ved prosjektets slutt gått langt forbi de målene som ble satt. –Målet var å innføre FEIDEnavn bare i UH sektoren, men i dag er vi i en posisjon hvor vi har teknisk kapasitet til å dekke hele Norges befolkning dersom det skulle være aktuelt, forteller Strømme.

Ivrige brukere

–I starten av prosjektet var mange forventningsfulle og spente på hva FEIDE var. Store og små høgskoler hadde ulike forventninger til hva vi kunne tilby, og i hvilken hastighet vi kunne rulle ut, sier Strømme. Noen av de små var utålmodige og kunne ikke skjønne hvorfor vi ikke kunne levere automatisk brukerkontogenerering

med en gang, det var jo bare snakk om noen script. Slik kan det fortone seg for små skoler med få brukere, men det er jo snakk om å organisere alle persondata i hele institusjonen på én måte – samkjørt og harmonisk. For store institusjoner er det snakk om år med arbeid, og for hele sektoren vil det også ta år før alt er ordnet på en ensartet måte.

Lett å selge FEIDE

Universitets- og høgskolesektoren har vært et egnet sted å innføre FEIDE, fordi institusjonene har egne it-avdelinger og håndterer sin administrative databehandling selv. Forutsetningen for arbeidet med FEIDE var institusjoner som hadde denne graden av egenkontroll og egenutvikling.

Ifølge prosjektleder Strømme er det i dag lett å selge FEIDE. Det gjøres mye arbeid lokalt med problemstillingene fra FEIDE, og skolene vil gjerne være med på det store samarbeidet for å sikre at løsningene blir kompatible i hele sektoren. Men kompatibelt skal ikke være det samme som monopol, og Strømme er spesielt fornøyd med at systemene som bærer det aller meste av FEIDE er kommersielle. –Det er kommersielle leverandører som leverer mange av de lokale FEIDESystemene, men også disse er i konkurranse med åpne programvarer.

Viktig med felles forståelse

FEIDE har mange tekniske utfordringer siden driftsopplegget for den sentrale tjenesten må være like stabilt som det underliggende nettet. Jon Strømme mener at den store utfordringen for FEIDE fremover er å skape felles forståelse. –Vi har en utfordring i å skape felles forståelse både innad og mellom institusjonene. Derfor er det viktig at vi fortsetter å fortelle om FEIDE gjennom å reise rundt eller skrive artikler, men vi er over den kritiske fasen.

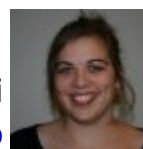
–Det er mange prosjekter i departementer og etater som jobber med sikker identifikasjon. Jeg tror FEIDEs viktigste bidrag er at vi har vist at det er mulig til en veldig moderat kostnad å etablere et teknologinøytralt rammeverk hvor man kan ta opp mange autentiseringsmekanismer etter hvert.

Høy sikkerhet blir viktig fremover

For FEIDE har det vært en avveining når det gjelder hvilken type autentiseringsmekanismer som skulle tilbys i startfasen. Valget falt på brukernavn og passord og satsing på de tjenestene som trengte denne typen sikkerhet. Utrulling av identiteter på lavt sikkerhetsnivå har vist seg å være et godt valg, FEIDE har i dag over 100 000 brukere fordelt på åtte høgskoler og universiteter.

–Vi forlot PKI som et hovedspor i 2002, men nå er det naturlig å gå videre fra brukernavn og passord og igjen se på hvordan vi kan håndtere høysikkerhetsoppgaver som vi ikke kan betjene i FEIDE per i dag. Vi har en sterk og generell single-sign-on-løsning klar, og vi har et system hvor tjenestene kan få persondata, ikke bare autentisert hvem dette er. Dette er løsninger som vi kan gjøre oss nytte av i hele samfunnet, ikke bare UH-sektoren avslutter Jon Strømme.

Karoline Ski
karoline.ski@uninett.no



uninytt@uninett.no

2005-06-27

Stor oppslutning om sikkerhetsseminar



10. og 11. november arrangerte UNINETT et sikkerhetsseminar for universitets- og høgskolesektoren. Intensjonen var å beskrive status for sikkerhetsarbeidet innen sektoren og presentere aktuelle løsninger på forskjellige områder.

Seminalet var beregnet på IT-personale og sikkerhetsansvarlige ved universiteter og høyskoler. Interessen var så stor at arrangøren ble nødt til å begrense antall deltakere til fra hver institusjon.

Tilsammen 56 deltakere fra de fleste universiteter og høyskoler var påmeldt. Til glede for alle som ikke fikk plass, ble seminaret streamet. I tillegg bidro 15 personer fra UNINETT med presentasjoner og teknisk gjennomføring.

Sikkerhet og brukervennlighet

Petter Kongshaug og Lars Oftedal (UiO) innledet seminaret, og de la begge vekt på avveiningen mellom sikkerhet, brukervennlighet og utgifter til sikringstiltak. De tok også for seg hvordan den økende avhengighet av IT og nett øker kostnadene ved sikkerhetshendelser, samtidig som strenge sikringstiltak oppleves negativt av brukerne og minsker nytten av IT-systemene.

Tettere samarbeid, for eksempel prosjekter av type grid, stiller økede krav til samordning av sikkerhetspolicyer. Alf Hansen (UNINETT FAS) presenterte TROST-prosjektet, som har tatt frem et forslag til generisk sikkerhetspolicy for UH-sektoren.

Sesjonen ble avsluttet med presentasjoner av UNINETT CERT og UNINETTs driftssenter, med demo av "driftsportalen" hvor institusjonene kan få oppdatert driftsinformasjon og kan oppdatere informasjon om seg selv med selvbetjening.

Deling av erfaringer

Andre sesjon var viet "beste praksis ved institusjonene". Foredragsholdere fra UiO (Øyvind

Waal) og NTNU (Knut Helge Windheim, Daniel Sandvold) presenterte sine løsninger for blant annet oppdatering av programvare, antivirus, antispam, sårbarhetsovervåkning, logging og håndtering av sikkerhetshendelser. Peder Seband (HiVolda) presenterte praktisk bruk av NAV, et verktøy som har gjort livet enklere for mange administratorer.

Roger Aas (HSH) og Ketil Forselv (HiN) fortalte om sikkerhetshendelser på studentboliger og policy for håndtering av denslags. Disse temaene ble fulgt opp med en plenumsdiskusjon hvor det blant annet kom fram at det er behov for dialog med samskipnadene om hvem som er ansvarlig for nettilgang til studenthybler, og hva som skjer når tilgangen blir misbrukt.

Nye verktøy

Ansatte fra UNINETT tok for seg Çnettsentriske metoderÈ og presenterte blant annet NAV, som er et verktøy som blir brukt av mange i UH-sektoren, VPN-løsninger og gode grunner til ikke å forlite seg på brannmurer.

Jardar Leira fortalte om beste praksis for trådløse nettverk, og la vekt på at det etter mange år med sikkerhetshull, nå er blitt mulig å få et trådløstnett med noenlunde sikkerhet.

Antispam-løsninger som "dike" og "spamassassin", samt forskjellige typer lokale sikkerhetsagenter og overvåkningsprogrammer ble også presentert. Som siste foredragsholder fortalte Olaf Schjelderup om GigaCampusprosjektet, med vekt på sikkerhetsperspektivene.

Seminaret ble avsluttet med en paneldebatt med Lars Oftedal, Olaf Schjelderup, Rune Sydskjør, Per Arne Enstad og Vidar Faltinsen. Noen av sakene som ble diskutert var:

- Behovet for å øke forståelsen for IT-sikkerhet i ledelsen ved den enkelte institusjon, som å sørge for at sikkerhetspolicy er forankret i ledelsen.
- Etablering av et fast "sikkerhetsforum" med tilrodde deltakere for UH-sektoren, hvor man trygt kan utveksle informasjon.
- Håndtering av sikkerhetshendelser på studentbyene.
- Behov for informasjon om og opplæring i sikkerhetsverktøy, spesielt NAV. Det ble uttrykt ønske om en NAV-workshop for versjon 3.0 med fokus på konfigurasjon og bruk av verktøyet. Det var stor enighet om at seminaret hadde vært svært nyttig, og mange kommenterte at det var på tide at UNINETT holdt et slik seminar.

Presentasjonene er tilgjengelig fra

<http://www.uninett.no/arrangement/sikkerhets-seminar-2004/presentasjoner.html>

Øyvind Eilertsen
oyvind.eilertsen@uninett.no



uninytt@uninett.no

2005-06-27

Redaktørhjørnet

Enda et år er gått, og det siste Uninytt for 2004 er et faktum.

Redaksjonen ønsker å takke for alle bidrag til utgivelsen og alle kommentarer til det som har stått på trykk.

Vi minner om at abonnement er gratis. Send en e-post til uninytt@uninett.no for bestilling av flere eksemplarer av papiirutgaven.

Så ønsker vi alle en riktig god jul og et flott, godt nytt år i 2005!



uninytt@uninett.no

Grete Duna
grete.duna@uninett.no



2005-06-27