UNINyTT
Nyhetsbulletin
Nr 1 1996

Utvikling av tenester i nett

Tenestene på Internett er inne i ei rivande utvikling. Det er viktig å styra denne utviklinga slik at norske brukarar innan forsking og utdanning får tilgang på dei beste tenestene, og slik at desse tenestene blir tilpassa dei behov brukarane har.

Internasjonalt samarbeid

Etablering av standardar for nett-tenester skjer internasjonalt, dersom brukarane i UNINETT skal få gode nok tenester må ein inn og påverka standardiseringsarbeidet.

Eit døme på gode løysingar er MIME for e-post, som gjer at brukarar ikkje har problem med øæå eller vedlegg. Neste steg i prosessen er å sørga for at tenestene blir tatt i bruk og at tenleg programvare er lett tilgjengeleg.

Hovudsatsingsområde

Tryggleik og multimedia informasjonstenester er hovudsatsingsområde for UNINETT framover. I tillegg vil eksisterande tenester og infrastruktur bli vidareutvikla.

UNINETT har valt eit europeisk samarbeid innan tryggleiksteneste (sjå eigen artikkel) og webutvikling (sjå artikkel) for å kunna sikra at tenester som blir utvikla på desse to områda blir tilpassa brukarane i Norge.

Utbygging og utvikling av ein internasjonal breibandsinfrastruktur er sentral for bruken av multimedia informasjonstenester. Gjennom NORDUnet deltar UNINETT i fleire initiativ på dette området. Det nordiske samarbeidet i NORDUnet har sikra ein god internasjonal infrastruktur for norske akademiske brukarar.

Gjennomføring av prosjekt

UNINETT er open for prosjektframlegg frå sine medlemsinstitusjonar og andre som har framlegg til utviklingsarbeid som gagnar brukarane i UNINETT.

Prosjekt i UNINETT blir utført av det norske forskings- og utviklingsmiljøet, spesielt speler nettkompetanse ved universiteta ein stor rolle.

Små prosjekt kan løysa store problem, ei rekkje mindre prosjekt blir gjennomført for å løysa konkrete problem med nett-teknologi eller tenester i nettet.

Innhald

I dette nummeret av UNINyTT finn du ei drøfting av betalingsmodellen, litt informasjon om Kompakt-satsinga i høgskulesektoren og informasjon om dei europeiske forskingsprosjekta der UNINETT deltar i 1996

Utgiver av UNINyTT er
UNINETTs sekretariat
Postboks 6883 Elgeseter
7002 Trondheim
Redaktør: Ingrid Melve
Telefon: 73 59 29 80
Epost: uninytt@uninett.no

En betalingsmodells hverdag

Bjørnar Pedersen, UNINETT

UNINETT har fra 01.01.96 en betalingsmodell for sine tjenester. Artikkelen skisserer noen av erfaringene som er gjort, og temaer som har vært diskutert. Dette for å vise hva som diskuteres og gi noen signaler om utviklingen.

Informasjon

En viktig erfaring vi har gjort er at det må legges økte ressurser i arbeidet med informasjon ut til våre medlemmer. Litt for mange har gitt uttrykk for at de har mottatt utilstrekkelig informasjon om innføringen av ny betalingsmodell for UNINETT. Dette gjelder både med hensyn til prisfastsetting og bakgrunn for dette, og hva de enkelte av UNINETTs tjenester innebærer og inkluderer. UNINETT arbeider nå med å forbedre den informasjonen som allerede finnes, og vil i større grad informere om og spesifisere de tjenester som er tilgjengelige.

KUF-UH institusjoner

Det ble tidlig i prosessen presisert at det ville bli et skille mellom KUF-UH institusjoner (institusjoner som hører inn under universitets- og høgskolesektoren i Kirke-, Utdannings- og -Forskningsdepartementet) og øvrige medlems-institusjoner. Denne delingen har gitt rom for to feiltolkninger. Den ene er hva som er KUF-UH og den andre at disse institusjonene ville få sterkt reduserte priser, eller gratis tilknytning.

KUF har gitt UNINETT ei liste over institusjoner de tar budsjettansvar for. Listen består hovedsaklig av de statlige høgskolene og universitetene, samt ytterligere noen få institusjoner av samme art. Disse institusjonene er det UNINETT benevner som KUF-UH. Flere av våre øvrige medlemsinstitusjoner har tilknytning til departementet, men dette medfører **ikke** en kategorisering i denne gruppen.

KUF-UH institusjonene er ikke kategorisert for seg fordi disse skal ha rimeligere vilkår i UNINETT enn andre institusjoner, men fordi departementet ønsket å ta et budsjettansvar for disse. Prisene for KUF-UH institusjonene er forskjellige fra den generelle prismatrisen.

Antall ansatte

Ulikt de kommersielle nettoperatørene, har UNINETT valgt å bruke en variabel i sin prismodell som heter *antall ansatte*. Bruken av en slik variabel har ført med seg en del interessant diskusjon. Det ene er bruken av denne variabelen i forhold til det å benytte *antall brukere*. Det andre er diskusjonen rundt inndelingsnivåene som benyttes.

Foreløpig vil vi holde fast ved bruken av *antall ansatte* som variabel i prismodellen. UNINETT ønsker at våre medlemsinstitusjoner skal gi så mange som mulig av sine ansatte og studenter tilgang til bruk av nettet. UNINETT er ikke tilstede kun som en nettleverandør på helt kommersielle vilkår, men har også ansvar for den alminnelige utbredelsen og tilgangen til de tjenester som finnes i nettet. Dette gjør vi, blant annet, ved å opprettholde en prismodell som gjør det "økonomisk lønnsomt" (regnet i kroner pr. hode) å gi flest mulig ved institusjonen tilgang.

Et annet område det har vært noen tilbakespill på er inndelingskategoriene for antall ansatte, og mønsteret på reaksjonene har vært tydelige. Mindre institusjoner mener at det er for lite inndelt i grupper, større institusjoner at det er for mange inndelinger. Begge leire har gode argumenter for sin syn, og valget blir om man skal velge å se på prisen som en kostnad for hele organisasjonen under ett der organisasjonen har en gitt kapasitet, eller om man legger vekt på prisen pr. hode i en organisasjon for en gitt kapasitet. Heller ikke her føler vi at det er grunnlag for å endre betalingsmodellen nå.

Direkte eller indirekte tilknytning

Det var i en initieringsfase viktig for UNINETT å konstruere en prismodell som var oversiktlig og enkelt gjennomførbar. Dette er gjort blant annet ved å unngå for mange unntak fra hovedreglene.

For institusjoner med indirekte tilknytning via oppringt til en annen institusjon medførte dette at avgiften ville være den samme som for en direkte tilknytning. Dette har konsekvenser som ikke er ønskelige sett fra et samfunnsøkonomisk og regionalpolitisk ståsted. Høgskoler som ønsker å være et kompetansesenter i sitt nærmiljø på bruk av nettjenster i skolesektoren, vil ikke kunne koble opp skoler mot seg, fordi dette krever tilknytningskostnader som kommer i tillegg til det som betales inn mot UNINETT. Resultatet er at en slik løsning blir for dyr for de aktuelle skolene. Dette er en lite optimal løsning, høgskolene har en naturlig misjon i sitt nærmiljø som den lokale kompetanseinstitusjon.

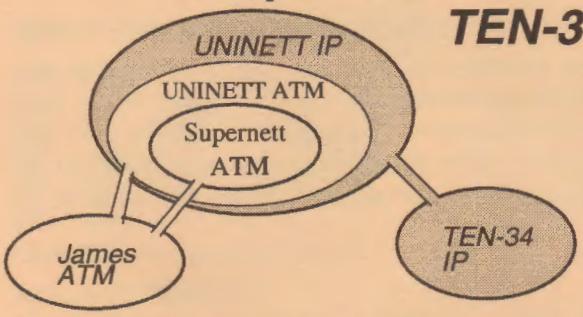
En beslektet diskusjon er hvordan en skal håndtere flere institusjoner som har knyttet seg til UNINETT med ei felles linje. Praksis i dag er at hver institusjon blir vurdert for seg ut fra tilgjengelig kapasitet. Den kritikken som har kommet mot dette er av grunnleggende art for prismodellen. Det er viktig å se på om dette kan håndteres på en bedre måte, og om vi kan få en endring i dette prinsippet til å passe inn i helheten. Dette er et felt hvor vi ennå ikke kan gi noen signaler om hva som vil skje.

Veien videre

En rekke elementer i dagens prismodell er under vurdering og blir diskutert. UNINETT har hele tiden gitt uttrykk for at dagens modell neppe er helt vanntett, men vi tror heller ikke at vannet fosser inn skroget. De store endringer vil neppe bli iverksatt før 1997-prisene skal fastsettes, slik at 1996 nok vil bli å forløpe etter dagens modell.

Vi er takknemlige for tilbakespill på de valg vi tar i den grad man mener at det finnes argumenter vi ikke har tatt godt nok hensyn til.

Europeisk akademisk bredbåndssamarbeid TEN-34 og JAMES



Petter Kongshaug, UNINETT.

I forbindelse med oppstartingen av EUs 4. rammeprogram høsten 1995 forelå det to forslag til bredbånds forskningsinfrastruktur i Europa nemlig TEN-34 og JAMES. Begge vil tilby minimum 34 Mbit/s til bruk for blant annet Telematics for Applications programmet, men det forventes videre utbygging til 155 Mbit/s i programperioden.

Bak JAMES står et antall teleoperatører: France Telecom, Austrian Telecom, Belgacom, BT, DT, Finnet, OTE, Portugal Telecom, P&T Luxembourg, PTT NL, Swiss Telecom, Telecom Eireann, Telecom Finland, Telecom Italia, Tele Danmark, Telefonica, Telenor og Telia. Deres fokus er utprøving og evaluering av ATM-baserte bredbåndstjenester i samarbeid med brukere ved de nasjonale forskningsnettene (som UNINETT i Norge). JAMES er i praksis en videreføring av den europeiske ATM-piloten som har vært operativ mesteparten av fjoråret og som ble brukt av bl.a. UNINETT, Universitetet i Oslo og Norsk Regnesentral. Kontrakt mellom EU og teleoperatørene er fremdeles ikke undertegnet.

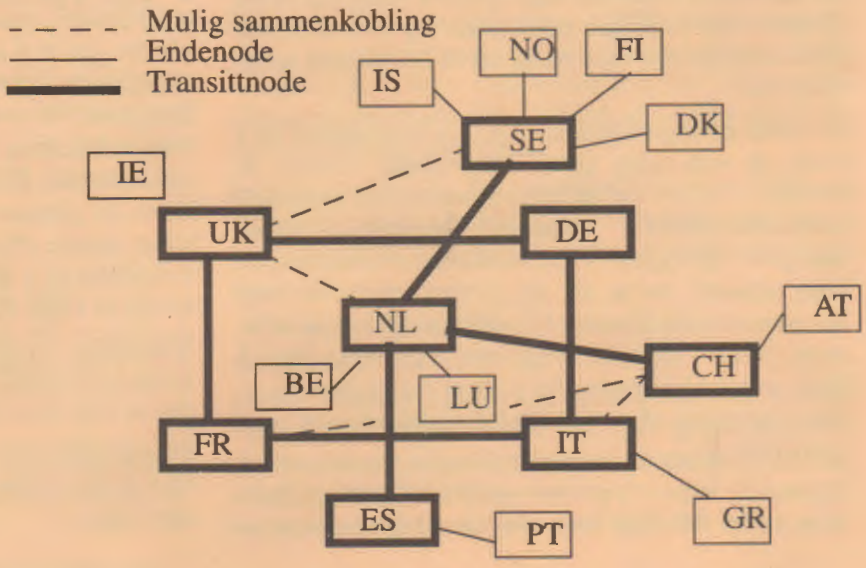
TEN-34 er et konsortium av nasjonale forskningsnett (DFN i Tyskland, INFI i Italia, UKERNA i England, Switch i Sveits, GSRT i Hellas, SURFnet i Nederland, FCCN i Portugal, ACOnet i Østerrike, SRP-HT i Luxemburg, NORDUnet (som representerer DEnet, FUNET, SUNET og UNINETT i norden),CICYT i Spania og RENATER i Frankrike) og endel teleoperatører som assosierte medlemmer (British Telecom, Deutsche Telecom, Telecom Italia og Unisource Carrier Services). Dette konsortiet er opptatt av å få etablert en driftsstabil Internett tjeneste med 34 Mbit/s så raskt som mulig, for så å gå videre med eksperimentelle tjenester opp til 155 Mbit/s basert på et ATM bærernett. Det er derfor foreslått at 2. fase i TEN-34 benytter den infrastruktur som JAMES skal etablere, og det er tatt høyde for dette i kontraktstekstene. UNINETT er med i TEN-34 som en av partnerne, men vi har overlatt til NORDUnet å ivareta våre og de andre nordiske forskningsnettenes interesser. En avtale er signert mellom EU og konsortiet, men med mulighet for å trekke seg ut under prosjektets definisjonsfase som løper fram til ca. 1. mai i år.

EU har satt av 30 MECU, tilsvarende ca 240 Mkr, over en toårsperiode hvorav 25 MECU går til TEN-34 og 5 MECU til JAMES. EU vil finansiere inntil 50 % av linjeinfrastrukturen første året, 30 % det neste, for så å trekke seg helt ut det tredje året.

Skissen over viser skjematisk hvordan brukere tilknyttet Supernett/UNINETT vil kunne dra nytte av henholdsvis TEN-34 og JAMES infrastrukturene. Fra UNINETTs IP-tjeneste kan man kommunisere direkte til TEN-34. Til JAMES kan man enten kommunisere direkte fra Supernett ATM eller fra de ATM-svitsjer UNINETT har utplassert ved universitetene som et skall rundt Supernett. Figuren under viser den foreslåtte topologien for TEN-34.

Det gjenstår fremdeles uavklarte spørsmål som prismodell, steder for sammenkobling av de involverte teleoperatører, samt forbindelser til USA, men det er berettiget håp om at nettet vil være oppe og kjøre innen utgangen av 1996. Uavhengig av dette vil NORDUnet oppgradere den internordiske kapasiteten til 34 Mbit/s og utvide sin USA-kapasitet til det samme til sommeren.

Med TEN-34 og JAMES på plass vil forholdene ligge til rette for forskning både på selve nettet og på anvendelser som bruker nettet. UNINETT vil delta aktivt i forsøks- og eksperimentvirksomheten forbundet med ATM sannsynligvis i et samarbeid med Telenor. UNINETT deltar også i anvendelsesorienterte prosjekter (DESIRE og ICE-TEL) og vi håper at også øvrige forskningsmiljøer i Norge skal bli i stand til å gjøre det samme over den infrastruktur som nå begynner å komme på plass. For mer informasjon om anvendelsesorienterte prosjekter under Telematikkprogrammet se *http://www.scimitar.terena.nl/scimitar/*



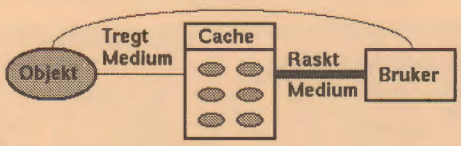
Caching av World Wide Web

Lars Slettjord, Universitetet i Tromsø

"The Information Superhigway" er et begrep de fleste av oss kjenner, men som ikke ligner så mye på den kjerreveien som møter oss i vår elektroniske hverdag. Når en skal hente ned informasjon via web holder ikke pek&klikk metoden. Som oftest må en bruke pek, klikk og vent metoden. Caching er en metode som kan brukes for å bedre situasjonen. Bruk av web-cache tjenere kan fjerne 20-50 prosent av web-trafikken på nettet, og gi brukeren mye raskere respons. Jeg skal i denne artikkelen gi en del tips om hvordan både du og din nettleverandør kan ta i bruk caching.

Hva er caching

Caching er en kjent og velprøvd teknikk som brukes for å øke ytelsen til alt fra CPU-er til World Wide Web. Prinsippet er enkelt. Når du henter et objekt gjennom et tregt medium, så lagrer du det i et cache slik at det er tilgjengelig fra et raskere medium. Neste gang du trenger objektet hentes det fra cachet, og du sparer dermed mye tid.



Dersom du bruker Netscape Navigator som din web-klient, så har du allerede tatt i bruk en form for caching. Alle dokumenter du henter med Netscape blir lagret i et cache på harddisken din. Dersom du prøver å hente et dokument som allerede ligger i dette cachet (og det ikke er for gammelt) vil du slippe å gå ut på nettet. Du får isteden dokumentet fra din lokale disk, noe som går mye raskere og sparer nettet for trafikk. Men dette cachet er lite, og det er kun du som drar nytte av det.

Caching av World Wide Web

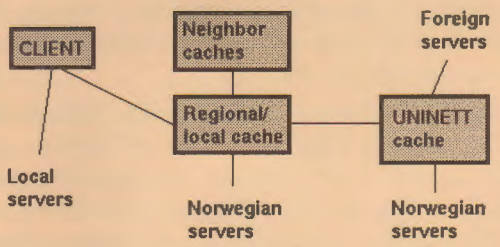
For at også andre skal dra nytte av at du har lastet ned et dokument kan du velge å bruke en web-cache tjener i tillegg til caching til lokal disk. Nettverket mellom deg og din web-cache tjener bør være kjappest mulig slik at det går fort å spørre den etter dokumenter. Og for å få utnyttet web-cache tjeneren best mulig må så mange som mulig bruke den.

De fleste av dagens web-klienter kan konfigureres til å bruke en web-cache tjener. Dokumentet *Caching av WWW <URL:http://www.service.uit.no/uninett/caching.html>* beskriver hvordan denne konfigureringen gjøres for de mest brukte web-klientene. Legg spesielt merke til `no_proxy` direktivet som bestemmer hvilke domener klienten ikke skal gå via web-cache tjeneren for å nå. Det er som regel ingen vits i å bruke web-cache tjeneren for å hente dokumenter fra en lokal web-tjener, så sett inn ditt lokale domenenavn her.

UNINETT driver en nasjonal web-cache tjeneste som er tilgjengelig fra port *81* på ***www-cache.uninett.no***. Foreløpig er det ikke lagt noen som helst begrensninger på tjenesten, den er tilgjengelig for alle. Men meningen er at hver organisasjon skal drive sin egen web-cache tjener, og så skal den bruke UNINETTs nasjonale web-cache tjener som "foreldre" når noe skal hentes fra utlandet.

Et nasjonalt nettverk av web-cache tjenere

UNINETT ønsker å være pådriver for å få opp et nasjonalt nettverk av samarbeidende web-cache tjenere. Derfor har vi satt i gang et web-cache prosjekt som blant annet får midler fra EU sitt 4.rammeprogram (Desire prosjektet). Vi ønsker nå å komme i kontakt med UNINETT medlemmer som har mulighet og ønske om å kjøre en egen web-cache tjener. Web-cache prosjektet vil da hjelpe til med å få i gang en web-cache tjener, og koordinere disse tjenerne slik at de samarbeider best mulig.



Programvaren som skal brukes er Harvest cached *<URL:http://excalibur.usc.edu/>*, og den er kun tilgjengelig for Unix plattformer. Det er mulig å bruke annen programvare, men Harvest cached har unike muligheter når det gjelder å samarbeide med andre cache-tjenere av samme type. Det er mulig å definere nabotjenere og foreldretjenere. Når en klient spør en harvest web-cache tjener etter et dokument kontaktes først alle nabotjenere (+ foreldretjenerne). Hvis de ikke har dokumentet vil tjeneren hente det gjennom en av foreldretjenerne. Andre web-cache tjenere (Netsite Proxy, CERNhttpd, ...) mangler muligheten til å definere nabotjenere, og kan derfor bare brukes til å lage strengt hierarkiske strukturer.

Web-cache prosjektet vil komme med en web-cache pakke for SAMSON maskiner, samt en oppskrift på hvordan en Harvest web-cache tjener installeres og drives.

Dersom dette høres interessant ut for din organisasjon bør du kontakte *webmaster@uninett.no* slik at vi kan hjelpe deg i gang.

Desire - europeisk webutvikling

Desire står for Development of a European Service for Information on Research and Education, og er eit forskingsprogram i EUs 4. rammeprogram. UNINETT webcachingsaktivitet inngår som ein del av prosjektet.

Målet med Desire er å sørga for tenlege webløysingar for europeiske brukarar innan forsking og utdanning.

Aktivitetar innan Desire:

1. Indeksering og katalogisering

   Å finna fram til informasjon på web er eit stort problem, prosjektet ser både på automatisk indeksering og emnesortering i fagleg tunge emnekatalogar

2. Caching

   Ved bruk av caching får ein betre respons og reduserer trafikken på linja, dette gjev betre webtenester for brukarane

3. Tryggleik

   Dersom informasjon skal vera tilgjengeleg for spesielle grupper, men ikkje for alle, må ein leggja inn tryggleiksfunsjonar. Informasjon bak brannmurar er eit av emna for prosjektet

4. Informasjonsverktøy

   Ei vurdering av verktøy som er tilgjengeleg for informasjonsleverandørar for vedelikehald av informasjon som er lagt ut på web.

5. Tenestekvalitet

   System for overvaking og kontroll av webtenarar, skal betre kvaliteten på webtenesta ved å leggja til retta for standard metodar i overvaking og drift.

6. Opplæring

   Opplæring i bruk av dei tenestene som blir utvikla, dokumentasjon av tenestene

Desire har 22 deltakarar frå 9 land og har eit budsjett på 2. KECU, eller 17,6 millionar norske kroner. EU bidrar med halvparten av dette, mens deltakarane sjølv bidrar med halvparten av kostnadane. Prosjektet starta 1. januar 1996 og går fram til 1. april 1998.

Veronica og gopher lagt ned

Gopher-tenesta til UNINETT blir lagt ned 1. april, som ei følge av dette blir også veronica (som er ei søketeneste for gopher-informasjon) lagt ned frå same dato.

Gopher blir lagt ned fordi bruken av tenesta har gått sterkt ned, og web har same (og betre) funksjonalitet

KOMPAKT 1995 og 1996

KOMPAKT-II aktivitetene for 1995 er gjennomført etter planen. Arbeid av større eller mindre omfang er gjennomført på følgende høgskoler:

Høgskolen i Gjøvik
Høgskolen Stord/Haugesund
Høgskolen i Hedmark
Høgskolen i Østfold
Høgskolen i Agder
Høgskolen i Sogn og Fjordane
Høgskolen i Buskerud
Høgskolen i Molde
Høgskolen i Finnmark og Samisk
Høgskolen i Stavanger

Siden arbeidsbelastningen i KOMPAKT har vært svært høg og arbeidet i stor grad berører øvrige aktiviteter i sekretariatet, vil vi for 1996 omorganisere prosjektet. Flere personer vil bli trukket inn i arbeidet og støttefunksjonene blir tilpasset den nye infrastrukturen ved høgskolene.

UNINETT styre har vært et kontrollorgan for KOMPAKT noe det fortsatt vil være, men i tillegg vil det bli opprettet et prosjektråd. Prosjektrådet skal sikre best mulig brukermedvirkning i prosjektet og blir kalt inn til møter to ganger årlig der status og planer blir presentert. Rådet skal bestå av 4 representanter oppnevnt av Høgskolerådet, 1 representant fra KUF samt representanter fra prosjektgruppen i UNINETT. Høgskolerådet har oppnevnt :

IT-leder Lars Nesland, Høgskolen i Agder
IT-leder Knut Jakobsen, Høgskolen i Finnmark
IT-leder Espen Drougge, Høgskolen i Gjøvik
IT-leder Anne Irene Krogsether, Høgskolen i Vestfold

Prosjektgruppen består av:

Prosjektleder:	Roald Torbergsen
Prosjektsekretær:	Anne Lise Ellevset
Ansv. for rutere:	Olaf Schjelderup
Driftsmodell:	Alf Hansen
Software:	Hans Terje Bakke

De største Kompakt-prosjektene i 1996 vil være høgskolene i universitetsbyene. Ved Høgskolen i Bergen (HiB) etableres det nå felles fiber-infrastruktur for UiB og HiB. Så snart kontraktsarbeidet er fullført vil en starte opp arbeidet med de andre høgskolene.

Endelig prosjektplan for KOMPAKT-arbeidet i 1996 vil bli utsendt til IT-lederne ved høgskolene så snart den er godkjent. Skulle det være spørsmål til prosjektet så kan det sendes til:

kompakt@uninett.no

som består av alle prosjektdeltakerne.

I tillegg arbeides det med å få etablert administrative servere ved hver høgskole, disse skal kjøre de administrative systemene for høgskolen. Dette er et separat prosjekt som vi vil komme tilbake til senere.

Sikkerhetsarbeid i UNINETT i et europeisk samarbeid

Alf Hansen, UNINETT sikkerhetsansvarlig

Sikkerhet og Internett er et aktuelt tema. Mye av ansvaret for hvordan brukerne oppfatter sikkerhetsnivået, er tillagt tjenesteyterne, dvs. UNINETT for våre medlemmer. Det er viktig for UNINETT at vi utnytter ressursene i sikkerhetsarbeidet effektivt, at vi får løsninger som følger relevante internasjonale standarder, og at våre medlemmer derved opplever et "sikkerhetsnett" som dekker såvel lokale som internasjonale forhold.

UNINETT har orientert seg inn mot relevante europeiske sikkerhetsaktiviteter innen EUs 4. rammeprogram. ICE-TEL (Interworking Public Key Certification Infrastructure for Europe) som vi har vært med å planlegge, og som vi nå er deltakere i, er et prosjekt innen rammeprogrammet med 15 deltakerinstitusjoner fra 11 europeiske land.

Vårt engasjement i ICE-TEL henger nøye sammen med våre interne aktiviteter rundt UNINETT CERT (Computer Emergency Response Team) og UNISA (UNINETT sertifiseringsautoritet). Ved å delta i ICE-TEL sikrer vi at de løsningene vi kommer fram til for våre medlemmer blir utarbeidet i et europeisk fellesskap, og derved utvider fokus fra lokale spesialløsninger til internasjonale fellesløsninger. Samtidig får vi tilført ekstra ressurser fra EU til prosjektet i tillegg til den egenandel vi selv bidrar med.

ICE-TEL

http://www.darmstadt.gmd.de/TKT/security/ice/

Målet med ICE-TEL er å tilby løsninger på sikkerhetsproblemer i Internett for den akademiske og den industrielle sektor. Dette skal vi gjøre ved å tilby sikre tjenester der brukere må være **sertifisert**, dvs. man skal kunne stole på at de elektroniske nøkler som anvendes til kryptering og signering av elektroniske meldinger faktisk tilhører brukeren.

Prosjektet vil:

- Tilpasse og utplassere nødvendige verktøy for drift av sikkerhetsinfrastrukturen og støtte til brukerne av infrastrukturen på PC, UNIX, Mac
- Tilpasse og utplassere verktøy som tillater å integrere nøkkelbaserte sikkerhetstjenester med forskjellige tjenester som benytter sikkerhetsinfrastrukturen
- Tilpasse og utplassere sikkerhetstjenester som umiddelbart tillater bruk av infrastrukturen uten videre integrering med brukertjenestene
- Støtte integreringen av sikkerhetstjenester i brukertjenester og utføre tester (på europeisk basis)

Nytten og brukbarheten av de verktøy som utplasseres, skal testes i tre forskjellige sammenhenger:

1. Sikker formidling av dokumenter i Torino-regionen i Italia. Dette er et stor-skala eksperiment som fokuserer på vanlig samfunnsmessig nytte.
2. Sikker kommunikasjon mellom CERT-er og andre distribuerte nettverks-støttegrupper. Denne aktiviteten koordineres av UNINETT og vår CERT benyttes som en prøvebruker av sikkerhetstjenestene.

   Tjenesten skal benyttes til å formidle informasjon av konfidensiell art mellom europeiske CERT-team i forbindelse med informasjonsutveksling om internasjonale sikkerhetshendelser.
3. Drift av en sikker elektronisk katalogtjeneste for et stort engelsk forskningsselskap. Dette går ut på å bygge opp en sikker X.500(93) DSA med tilhørende DUA bibliotek.

   I tillegg skal man definere en overordnet arkitektur for den offentlige nøkkel-infrastrukturen, og spesifisere relevante verktøy, applikasjoner og tjenester innenfor denne arkitekturen (stikkord: "trust models" og sikkerhets-policy).

Deltagerne (deriblant UNINETT) skal gjøre sin del av jobben med å tilby **Sertifiserings-autoriteter** innen sitt område, og gi støtte til organisasjoner som benytter seg av disse tjenestene. I UNINETT gjøres dette allerede av UNINETT sertifiseringsautoritet, UNISA (se nedenfor).

ICE-TEL prosjektet startet i desember 1995 og varer i 2 år. EU bidrar med 1.7 millioner ECU (ca. 13.6 millioner norske kroner) i prosjektperioden. Deltakerorganisasjonene bidrar tilsammen med omkring tilsvarende beløp slik at totalbudsjettet for ICE-TEL blir ca 27.2 millioner norske kroner.

UNINETT sertifiseringsautoritet, UNISA

http://www.uninett.no/pca/

Sikker utveksling av informasjon kan basere seg på forskjellige krypteringsteknikker. Man kan kryptere meldinger/filer slik at innholdet er uleselig for uvedkommende, og man kan signere et utdrag av en melding (eller fil) for å sikre seg mot at innholdet blir endret under transport, samt for å garantere identiteten til avsender.

Et problem melder seg hvis man skal kryptere en melding, og sende denne til en person man ikke kjenner. For å få gjort dette trenger en denne personens offentlige krypteringsnøkkel, som en trolig kan finne i en nøkkel-database. Hvis denne personen har registrert sin nøkkel i nøkkeldatabasen, vil en finne den der, men hvordan kan en være sikker på at den virkelig tilhører korrekt person?

Problemet med distribusjon av krypteringsnøkler løses ved å la autoriteter som "alle" stoler på (tiltrodd tredjepart) gå god for bindingen mellom en brukers identitet og denne brukerens offentlige krypteringsnøkkel. Dette gjøres ved at autoriteten utsteder et såkalt offentlig-nøkkel sertifikat. Disse autoritetene må fysisk validere brukeres identitet, de må derfor være lokalisert rundt i de forskjel-

lige brukeres organisasjoner. Dette gjør at man har behov for et "hierarki" av autoriteter. Autoriteten på toppen (roten) stoler alle på. Denne autoriteten utsteder sertifikater for andre autoriteter, som igjen kan utstede sertifikater for brukere eller andre autoriteter.

UNINETT sertifiseringsautoritet, UNISA, er UNINETTs sertifiseringsautoritet i ICE-TEL. UNISA er betegnelsen på tjenesten UNINETT tilbyr for sikker utveksling av offentlige krypteringsnøkler. Nøkler utveksles i form av sertifikater. Disse sertifikatene er signert av eierens sertifiseringsautoritet.

Tjenesten tilbyr også programvare for kryptering/signering av meldinger eller filer.

UNISA følger PEM (Privacy Enhanced Mail, RFC 1421-1424) standarden. Nøkkelsertifikater er basert på X.509. UNINETTs X.500 tjeneste skal brukes for distribusjon av sertifikater. For brukere som ikke har aksess til X.500 er det utviklet en epostsvarertjeneste. Sertifikater kan også hentes via WWW.

Når de øvrige ICE-TEL deltakeren har etablert sine sertifiseringsautoriteter i henhold til den "trust model" som skal defineres for ICE-TEL, vil vi ha en europeisk infrastruktur som sikrer at autoriteter som "alle" stoler på går god for bindingen mellom en brukers identitet og denne brukerens offentlige krypteringsnøkkel. UNINETT medlemsorganisasjoner vil allerede fra starten av tilhøre denne europeiske infrastrukturen.

UNINETT CERT

http://www.uninett.no/info/cert/home.html

Dette er UNINETTs "Computer Emergency Response Team" som står til rådighet for våre medlemmer. UNINETT CERT behandler all informasjon på en fortrolig måte, og har til tider behov for informasjonsutveksling med tilsvarende team i andre land.

Gjennom ICE-TEL vil det etableres en infrastruktur som skal benyttes til sikker kommunikasjon mellom CERTer i Europa. UNISA vil som en del av ICE-TEL infrastrukturen administrere offentlige nøkler som UNINETT CERT kan benytte for sikker (kryptert/signert) kommunikasjon, både mot enkelt-brukere innen UNINETT og mot de øvrige CERTer som benytter samme teknologi og infrastruktur.

Denne teknologien vil selvsagt ikke være den eneste som vil være i bruk hos alle av UNINETT CERT sine kontaktpunkter. Derfor må UNINETT CERT også håndtere PGP teknologi, se

http://www.uit.no/cc/tjenester/PGP/

UNINETT CERT er i ferd med å bygge opp sitt interne sikre lokalnett bak en brannmur-bastion. Ved å gjøre dette i fellesskap med miljøer som har tilsvarende problemstillinger, utnytter vi ressursene bedre samtidig som vi får etablert gode tekniske løsninger. UNINETT har nylig inngått et samarbeid med regionsykehusene i Trondheim og Tromsø samt Kompetansenter for IT i Helsevesenet (KITH) i Trondheim for å bygge opp felles brannmurløsninger som kan oppfylle de krav som også må settes for helsevesnet.

Gjennom ICE-TEL prosjektet og samarbeidet med partnerne fra sykehussektoren, vil UNINETT få erfaring i anvendelser og drift av sikre kommunikasjonsløsninger over åpne nett, og vi vil benytte denne bl. a. til å bidra i den formelle prosessen som er nødvendig for å etablere godkjente sikre tilknytninger mot Internett.

Omlegging av infrastruktur, KOMPAKT

Olaf.Schjelderup@uninett.no

Som en vesentlig del av KOMPAKT-aktiviteten har nå en rekke høgskoler nå fått implementert ny nettstruktur. Dette har for flere bl.a. omfattet:

1. Økt linjekapasitet fra knutepunkt mot UNINETTs ryggradsnett, men for flere høgskoler også økt linjekapasitet på internlinjene mellom studiestedene. Flere høgskoler kjører nå både telefon- og datatrafikk samtidig på de digitale internsambandene.

2. Nye og kraftigere rutere er kommet til i knutepunktene. I tilfeller der høgskolen består av flere **større** studiesteder har tilsvarende kraftige rutere også blitt utplassert der. Andre, mindre og mer perifere studiesteder, har i vinter nå blitt tilknyttet nettet.

Det forventes at den nye nettstrukturen er rimelig på plass innen første halvår 1996. Imidlertid har flere høgskoler flytteaktiviteter i inneværende og/eller neste år, og omleggingen av nettet tilpasser seg dette. For disse er det da introdusert en planlagt forsinkelse på delaktiviteter som tilpasning til flytteaktiviteten, og for å unngå dobbeltarbeid.

Som de fleste er kjent med, har KOMPAKT-aktivitene også lagt grunnlag for langt høyere nett-sikkerhet. Primært tenkes det her på beskyttelse av administrative systemer og data, og intern kablingsstruktur på høgskolen utgjør fundamentet for å få dette til. Man har derfor etablert fysisk adskilte nettsegment for f.eks. studenter og adminstrasjon/ansatte. Den første sikkerhetsmessige gevinst dette gir er at tilfeldig såkalt pakkesniffing vanskeliggjøres. Typiske konsekvenser av pakkesniffing er at uvedkommende på nettsegmentet kan snappe opp passord m.m. som kringskastes på ethernet-kabelen.

Videre må man regulere hvilken trafikk som skal kunne slippe inn på de nettsegmenter som skal beskyttes. For å gjøre dette introduseres streng pakkefiltrering i ruterne, slik at bare epost- og navnetjenertrafikk kan initieres utenfra og inn til disse nettsegmentet. Merk bruken av ordet "initiere" - personene på de beskyttede nettsegmentene ønsker jo likevel å kunne nyttegjøre seg Internett-tjenester og derfor tillater pakkefiltrene i ruterne at disse personene kan **initiere** trafikk fra innsiden og ut mot omverdenen. Med pakkefiltrene stopper man altså trafikk som initieres fra utsiden og inn, med unntak for epost, navnetjenester

og evt. driftssentra som har driftsansvar for systemer på innsiden. I tilfeller der f.eks. administrasjonen er geografisk adskilt på flere studiesteder, vil man etablere full IP-transparens mellom disse segmentene.

Erfaringen så langt har vist det hensiktsmessig at man foretar etablering av ny infrastruktur og trafikkregulering som to adskilte aktiviteter, da begge er nokså omfattende. Forut for etableringen av trafikkreguleringen må det gjøres en del behovsanalyser for ulike nett-tjenester på de enkelte nettsegmenter, med påfølgende omorganisering av dem ved høgskolen. En del grunnprinsipper kan legges for dette arbeider:

1. Høgskolens epost- og navnetjeneste bør ligge på et beskyttet nett, iallfall for administrasjonens epost, og gjerne på det studiestedet der knutepunktet befinner seg.
2. Offentlig tilgjengelige tjenester, f.eks. WWW-tjenere, plasseres på et av nettsegmentene med minst trafikkregulering, typisk studentnett.
3. Programvaretjenere må på ingen måte brokoble nettsegmenter med ulik sikkerhetsklasse. Dette er ofte maskiner som også kan utføre ruting og dermed gjøre trafikkreguleringen foretatt i ruterne verdiløs. Dersom høgskolen er avhengig av en felles programvaretjener bør denne ikke legges på sikrede nettsegment, da disse kan tjene som springbrett for videre uønsket aktivitet på beskyttede nettsegment. Ideelt sett bør det finnes en programvaretjener for hver sikkerhetsklasse, altså minimum to pr. høgskole. Dersom det ikke lar seg gjøre på kort sikt, bør programvaretjeneren legges på nettsegmentet med lavest sikkerhetsklasse som interimsløsning, men en skal da være oppmerksom på større muligheter for at uvedkommede kan plassere virus etc. som kan true sikkerheten på det segmentet som henter programmer fra tjeneren.
4. Vær oppmerksom på at X-Windows og RPC-baserte tjenester som NFS og NIS, ikke bør kjøres mellom ulike sikkerhetsklasser uten at en i stor grad åpner for uønsket trafikk inn mot de beskyttede nettsegmentene. Dette har sin årsak i at autentiseringen er meget svak for type X-Windows trafikk og at mange RPC-baserte tjenester ikke benytter veldefinerte UDP portnumre.

Etterhvert som ny infrastruktur er på plass vil KOMPAKT-prosjektet for alvor kjøre sikkerhetsaktivitetene mot hver høgskole. Spørsmål o.l. i den forbindelse kan rettes til artikkelforfatteren.

UNINETT årsmelding 1995 på web

Årsmelding for UNINETT er lagt ut på web

http://www.uninett.no/info/uninett/1995/

Meldinga inneheld også ein komplett oversikt over dei utviklingsprosjekta som blei gjennomførte i 1995, til saman 38 prosjekt av ulikt omfang. Meir informasjon om kvart enkelt prosjekt er tilgjengeleg gjennom webutgåva av årsmeldinga.

Papirutgåva av årsmeldinga vil bli tilsendt alle medlemsinstitusjonar i UNINETT.

UNINETT hadde 1.1.1996 463 medlemsinstitusjonar tilknytta nettet. UNINETT har fått 239 nye medlemsinstitusjonar i løpet av 1995. Talet på tilknytta maskiner registrert i DNS i UNINETT har gått opp frå omlag 40.000 til omlag 65.000

Det har skjedd ei svært omfattande oppgradering av linjenettet, utanlandslinja er oppgradert til 8 Mbps (og vil i 1996 bli oppgradert til 34 Mbps) og stamnettet er oppgradert tilsvarande. Supernett er lagt over til ATM-teknologi.

UNINETT'96

Konferansen UNINETT'96 finn stad på Lillehammer 14. - 16. oktober 1996. Høgskolen i Lillehammer står som arrangør i samarbeid med UNINETT.

Konferansen vil bli retta mot teknisk driftspersonale ved UNINETT medlemsinstitusjonar. Program blir sendt ut før sommarferien, dette er ei påminning om å setja av tidsrommet 14. - 16. oktober.

Tredjeparts trafikk

Formidling av tredjeparts trafikk er ikkje tillatt i UNINETT. Unntak gjeld for UNINETT medlem etter avtale med UNINETT i kvart enkelt tilfelle.

Typisk unntak er der fleire institusjonar deler ei linje inn mot UNINETT, eller der ein institusjon gjev ein annan institusjon tilgang til Internett via oppringt til den første institusjonen. Alle slike tilfelle skal avtalast med UNINETT. Formidling av tredjeparts trafikk der tredjepart ikkje er medlem i UNINETT er ikkje tillatt.