nyhetsbulletin

Uninytt 2

2007

.NO I RØDT, HVITT OG BLÅTT

INNKJØPSAVTALER

NORSTORE

UNINETT

HK Reklamebyrå - Trykk: Tapir Uttrykk

INNHOLD UNINYTT 2–2007

Postadresse
UNINETT, NO-7465 Trondheim

Besøksadresse
Abels gate 5 – Teknobyen

UNINETT	73 55 79 00 (faks: 73 55 79 01)	info@uninett.no
Driftssenteret	73 55 79 60 (døgnvakt)	drift@uninett.no
Norid kundesenter	73 55 10 00 (faks: 73 55 79 99)	info@norid.no

TRÅDLØS, SØMLØS, GRENSELØS

4.–6. desember arrangeres årets UNINETT-konferanse. På tradisjonelt vis er det en av våre egne institusjoner i universitets- og høgskolesektoren som er vertskap, denne gangen NTNU i Trondheim.

Årets konferanse tar for seg den pågående utbyggingen av neste generasjon av forskningsnettet – hybridnettet. Økt kapasitet og anledningen til å kunne tilby enkeltforskere samme kapasitet som hele det øvrige forskningsnettet, er stikkord. Dette vil føre til at en rekke nye forskningsanvendelser innen bl.a. fysikk, kjemi, klima, havforskning, vil se dagens lys.

I regi av GigaCampus-programmet presenteres en rekke interessante prosjekter innen fysisk infrastruktur, sikkerhet, trådløse nett, nettovervåking, mm. Av mer administrativ karakter er det gjennomført en rekke avtaleforhandlinger vedrørende telefoni, utstyr og programvare. Gjennom GigaCampus-programmet er det et tett samarbeid mellom UNINETTs medarbeidere og fagpersoner i UH-sektoren som hele sektoren drar nytte av.

Feide programmet går videre med ny innloggingsteknologi og et jevnt økende antall nye tjenester som gjøres tilgjengelig via Feide autentisering. Målet om å gjøre Feide operativ for hele utdanningssektoren er blitt svært realistisk.

UNINETT har de senere år overtatt ansvaret for nasjonal koordinering av tungregning og det siste året også grid og spesielle lagringsressurser for naturvitenskaplig forskning. UNINETT er dermed i ferd med å bevege seg fra å være en nettleverandør til å bli en leverandør av e-infrastruktur for forskning og høyere utdanning. Vi tror dette er en utvikling som vil være interessant for en rekke nye institusjoner og ikke bare universitetene.

UNINETT, med sine brukerinstitusjoner, har hele tiden en utfordring med å få de "riktige" IT-tjenestene ut til brukerne. Vi tror IT har et stort uprøvd potensiale, og at faglig ansatte ved våre institusjoner har et stort og udekket behov for mer avansert brukerstøtte. UNINETT vil i tiden framover søke å skape arenaer for økt oppmerksomhet mot brukerstøtte slik at våre institusjoners primærvirksomhet får ut dette potensialet innen sin forskning og utdanning. IT-kompetanse og annen fagkompetanse bør kombineres på andre og mer omfattende måter enn tidligere.

Dersom UNINETT-konferansen fører til at deltakerne reiser hjem med økt innsikt og motivasjon har vi lyktes. Etter et nytt "dugnadsår" blant kolleger ute i sektoren og ansatte i UNINETT føler vi oss trygge på at det vil skje.

15. UNINETT-konferanse
Det er 14 år siden vi startet med UNINETT-konferansen. Da ved Høgskolen i Telemark i Bø. Vår primære målgruppe har hele perioden vært IT-ledere og annet IT-personell ved UNINETTs institusjoner. Antallet deltakere har variert mellom 150 og 350, med toppnotering i Oslo i 1994 (arrangert av Høgskolen i Østfold).

Konferansene har vært en møteplass hvor man har utvekslet kompetanse og erfaringer, og samtidig utviklet et sosialt fellesskap. Vi i UNINETT føler oss priviligerte som har fått ta del i dette meget gode fellesskapet gjennom så mange år.

Petter Kongshaug
petter.kongshaug@uninett.no

BANEBRYTENDE BØLGELENGDER I FORSKNINGSNETTET

UNINETT bygger i disse dager neste generasjons Internett. I tillegg til det tradisjonelle forskningsnettet, etablerer UNINETT et såkalt hybridnett mellom breddeuniversitetene i Norge, med mulighet for videre lambda-forbindelse til Europa og resten av verden. Det nye nettet vil åpne for helt nye bruksområder og plassere Norge helt i front på nettteknologiområdet.

Det som skjer av utbygging på nettsiden er en aldri så liten revolusjon i UNINETTs transportnett. Ikke bare blir kjernenettet oppgradert fra 2.5Gbit/s til 10 Gbit/s, men dette bæres av et helt nytt optisk nettverk som kan tilby direkte og dedikerte forbindelser på kryss og tvers mellom forsknings- og undervisningsmiljø. Samtidig som det byr på muligheter norske forsknings- og undervisningsmiljø ikke har hatt tidligere.

Det hybride nettverket tilbyr tradisjonelt forskningsnett basert på et delt IP-nett, men i tillegg kan det settes opp dedikerte optiske kanaler, på f.eks. 1, 2.5, 10 og i fremtiden 40 Gbit/s, mellom ulike noder både nasjonal og internasjonalt.
Sistnevnte forteller at den nye nettverksmodellen er et satsingsområde for mange forskningsnett rundt om i verden.

Grenseløst nettverk
Det er nye behov innen forsknings- og undervisnings-miljøene som har drevet fram behovet for den nye nettverksmodellen. På grunn av disse behovene stilles det i dag større krav til nettets kapasitet og kvalitet. Eksempler på slike behov er sammenkobling av store distribuerte lagringssystemer, tungregneanlegg, overføring av høyoppløselig og høykvalitets video og lyd, radio-astronomi og eVLBI. Et konkret eksempel på et slikt behov er en høykvalitets videooverføring som skal settes opp mellom St. Olavs hospital og Korea i høst og vinter.

UNINETTs hybridnett møter resten av verden på to separate steder i Oslo, hvor tilkobling til internasjonale forbindelser blir mulig gjennom NORDUnets optiske nett.

At Norge har et slikt nettverk nasjonalt, er en forutsetning for å kunne delta og bidra på den internasjonale arenaen. Et typisk eksempel på hvordan prosjekter nyttiggjør seg maskinressurser på tvers av landegrensene er den nye partikkelakselleratoren i CERN som leverer enorme datamengder for lagring og prosessering på universiteter over hele Europa. Nettopp over de dedikerte optiske kanalene som hybridnettet i de ulike landene tilbyr. Et slikt nettverk har en stor kostnad, men er samtidig nødvendig for at Norge skal henge med i front på forsknings- og undervisningsområdet.

Fleksibelt nettverk
Prinsippet for dette nye hybridnettet kalles bølgelengde-multipleksing. Det vil si at flere uavhengige optiske signaler kan transporteres over en og samme fiber. Ved at de ulike kanalene har ulik bølgelengde, eller "farge" på laserlyset, kan forskjellige prosjekter benytte forskjellige bølgelengder innenfor samme fiber.

Dette betyr også at flere av de stedene der fiberkabelen passerer vil kunne nyte godt av hybridnettfunksjonaliteten, bl.a. Narvik, Harstad, Bodø, Mo i Rana, Lillehammer og Hamar. For øvrige steder i Norge, der UNINETT leverer gigabitkapasitet, kan også tilsvarende forbindelser leveres, men da basert på oppgradering av forbindelsene, slik vi har gjort tidligere i forhold til BaneTele-avtalen.

Utbyggingstakt
Gjennom opsjoner i UNINETTs avtale med BaneTele startet vi høsten 2005 dialogen om mulig oppgradering av UNINETTs nett, basert på det fibernettet som BaneTele disponerer. Sommeren 2006 startet anbudsprosessen på optisk transmisjonsutstyr, og et stykke ut i 2007 ble Siemens valgt som leverandør basert på pris og teknisk funksjonalitet.

Hybridnett

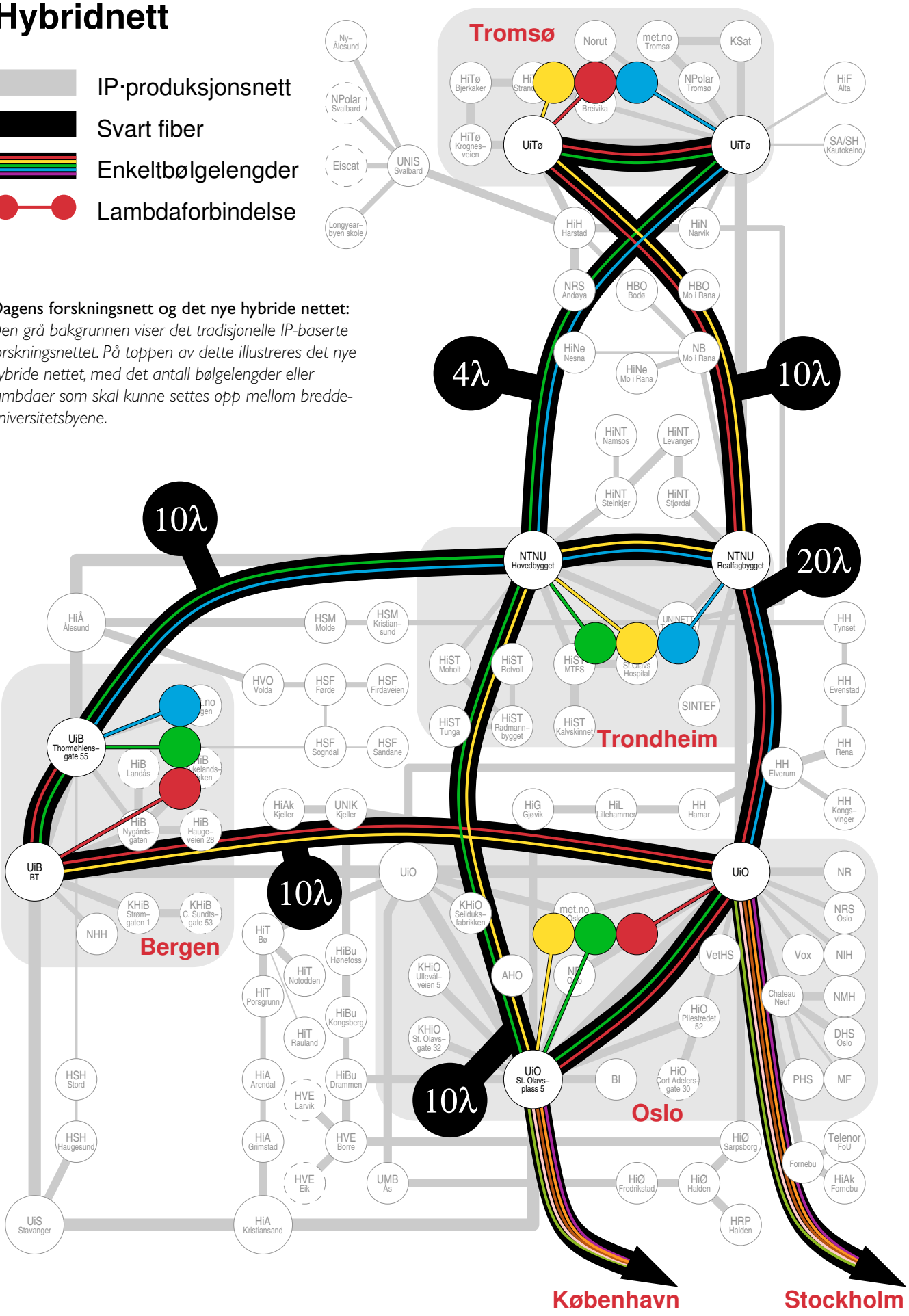
IP-produksjonsnett

Svart fiber

Enkeltbølgelengder

Lambdaforbindelse

Dagens forskningsnett og det nye hybride nettet:
Den grå bakgrunnen viser det tradisjonelle IP-baserte forskningsnettet. På toppen av dette illustreres det nye hybride nettet, med det antall bølgelengder eller lambdaer som skal kunne settes opp mellom bredde-universitetsbyene.



Realiseringen av nettet startet høsten 2007, og den første langdistanse 10 Gbit/s forbindelse ble etablert mellom Trondheim og Tromsø over den nye Kysttele-kabelen som snor seg oppover langs nordlandskysten. Installasjonen av det optiske utstyret langs fiber-strekkene foretas av BaneTele, noe som vil være en klar fordel med hensyn på det videre drifts-samarbeidet.

Pr. november 2007 er det første anlegget mellom Oslo og Trondheim klart, og like etter i løypa ligger anlegget som skal bære hybridnettet mellom Oslo - Bergen. Øvrige strekk og redundans på alle strekkene tas fortløpende utover i 2008.

I tillegg til det optiske transmisjonsutstyret, skiftes også mange av UNINETTs kjernerutere ut. Både Cisco og Juniper leverer rutere som skal kunne bære de økte trafikkmengdene i IP-produksjonsnettet. Det nye hybridnettet vil også kunne by på feiltoleranse gjennom redundante forbindelser. Innsats både for å sikre separate fibertraséer, og system- og strømdiversitet har vært nødvendig for å sikre kommunikasjonen.

UNINETT oppfordrer medlemmene til å ta kontakt med oss for å diskutere muligheter der det er prosjekter som kan tenkes å ha nytte av hybridnettkapasitet.

Olaf Schjelderup
olaf.schjelderup@uninett.no

GIGACAMPUS INNKJØPS-AVTALER OMSETTER FOR 300 MILLIONER

En statusgjennomgang viser at avtalene som UNINETT forvalter gjennom GigaCampus-programmet samlet vil ha en omsetning på nærmere 300 millioner kroner i 2007. – Dette viser at det er en stor avtaleportefølje under GigaCampus, og at totale besparelser for sektoren må være betydelige, sier Lars Skogan.

En av aktivitetene i GigaCampus-programmet har vært å koordinere felles anskaffelsesprosesser og inngåelse av store, felles rammeavtaler på produkter og tjenester innen IKT og nett. – Vi mener vi har oppnådd gode betingelser i avtalene våre. Og omsetning på 300 mill sier ikke bare at vi forvalter en stor mengde avtaler, men også at besparelsene for UH-sektoren samlet sett må være betydelige, sier ansvarlig for innkjøpsaktiviteten, økonomisjef Lars Skogan.

Stordriftsfordeler

UNINETT har i dag 25 innkjøpsavtaler, fordelt på ni avtaleområder. Intensjonen har vært å spare kostnader for sektoren, både ved å oppnå gode betingelser fordi man samlet representerer et stort volum og ved at virksomhetene sparer ressurser på å kjøre tidkrevende prosesser selv.

– En god anbudsprosess er ressurskrevende. Det tar minimum 5-8 måneder å gjennomføre, og involverer ofte mange personer. Da er det bedre at noen få gjør en stor jobb for mange, enn at mange virksomheter skal kjøre hver sine prosesser. Ser man stort på det, vil besparelser kunne bety at mer penger kan brukes på å drive forskning og utdanning i stedet, sier Skogan.

UNINETTs rolle er i stor grad å koordinere gjennomføringen av anbudsprosessene. Fordelene for sektoren er ikke bare volumfordelene eller at man får redusert arbeidskostnaden. Denne måten å gjøre det på medfører også at man får utnyttet kompetansen i sektoren, generell økning i samhandlingen og samarbeidet mellom virksomhetene, og ikke minst at følgekostnadene kan reduseres på bl.a. standardisering og logistikk.

Avtaleansvarlig Lars Skogan forvalter avtaler med omsetning på 300 millioner kroner i 2007. Her med storkundeansvarlig i NetCom, Sven O. Storløs.

Forvaltning av avtalene etter at de er inngått er også en viktig oppgave. Dette innebærer kontinuerlig kontakt med brukere i sektoren og ulike leverandører for å avklare bl.a. uklarheter, hjelpe til med tilrettelegging og sørge for endringer. Det gjennomføres statusmøter med leverandørene en til to ganger per år hvor faste tema er gjennomgang av tilslutning og omsetning, betingelser, bestillingssystemer og service og support. Dette arbeidet er svært viktig for å sikre at avtalene forblir gode over tid.

Fakta
Eksisterende avtaleområder via UNINETT:
Mobiltelefoni
PC, MAC og servere
Nettverksutstyr
Fastelefoni
Vedlikehold av telefonsentraler
Lagringsutstyr
Maskin- og programvare
Programvare fra Microsoft
ADSL

Nyttig informasjon om avtalene og status på ny prosesser:
http://forskningsnett.uninett.no/innkjop/

Kontaktpunkt: innkjop@uninett.no

God oppslutning om avtalene

UNINETT har i underkant av 200 institusjoner innen forskning og utdanning som kunder. Så langt er det totalt 122 av disse som bruker en eller flere av de inngåtte avtalene. Denne oppslutningen er vi svært godt fornøyd med.

UNINETT har en koordineringsfunksjon i innkjøpsarbeidet. For hver runde settes det ned nye arbeidsgrupper bestående av personer fra UNINETT og representanter fra kundegruppen. Det er nært samarbeid med UH-rådets innkjøpsutvalg. UNINETT fungerer som sekretariat for prosessene og koordinerer prosessene fra idé til ferdig skrevne avtaler.

Grethe Steen
grethe.steen@uninett.no

PROSJEKTSTATUS I UNINETT FAS

Hos UNINETT FAS har mye av aktiviteten i høst vært orientert rundt anskaffelse av nye systemer, og vi nærmer oss nå sluttforhandlinger for både prosjektstyringsverktøy og felles bestillingssystem.

Prosjektstyringsverktøy
Forhandlingsrundene med leverandørene er avsluttet og kontraktsforhandling med valgt leverandør gjenstår. Beslutningen om hvilket system som blir valgt blir tatt i desember, og på nyåret er vi klare til å starte pilotinnføringen hos to institusjoner. Det vil bli gjennomført en ny bindende påmeldingsrunde første kvartal 2008 for å avdekke hvor mange institusjoner som ønsker å innføre prosjektstyrings-verktøy.

Mer informasjon finner du på:
http://www.uninett.no/trofast/psv/index.html

Felles bestillingssystem
UNINETT FAS er i ferd med å gjennomføre en gjenåpning av konkurranse på de rammeavtalene som E-handels-sekretariatet har inngått på bestillingssystem. Status er at vi gjennomfører avklaringer med de leverandørene som har valgt å gi tilbud. Vi planlegger å være ferdig med disse avklaringene, og ha skrevet kontrakt med en leverandør innen utløpet av desember. Når en leverandør og et system er på plass, vil vi starte arbeidet sammen med pilotinstitusjonene HiL og HiO med oppsett, testing og integrering av løsningen, slik at den fungerer godt sammen med vår øvrige systemportefølje. Dette arbeidet vil gå frem til 1. april. Fra 1. april og tre måneder frem vil vi gjennomføre akseptansetester, dvs tilnærmet normal drift, på en begrenset del av virksomheten til pilotene. Etter sommeren/høsten 2008 vil bestillingssystemet være klart for utrulling til øvrige virksomheter. Nå som vi begynner å nærme oss et konkret system og leverandør vil vi sende ut et månedlig nyhetsbrev med status på hva som har skjedd den siste måneden og hva som skjer fremover. Dette slik at de som er interessert i å følge utviklingen skal få enkel og oppdatert tilgang. Vi skal også holde en kort presentasjon av bestillingssystemprosjektet på UNINETT-konferansen, og vi håper å se mange av dere der!

For mer informasjon gå inn på: http://www.uninett.no/trofast/innkjop/index.html

KGV – Konkurransegjennomføringsverktøy
I samarbeid med UHRs Innkjøpsutvalg vil UNINETT FAS gå ut med en påmelding til alle universiteter og høgskoler, hvor vi oppfordrer til å bli med i vår prosess for gjenåpning av konkurranse på konkurransegjennomføringsverktøy (KGV). Som for bestillingssystemet har E-handelssekretariatet under Fornyings- og Administrasjonsdepartementet inngått to rammeavtaler for offentlig sektor på KGV. For å kunne ta i bruk disse, må det gjennomføres en minikonkurranse, hvor man inviterer begge leverandørene til å konkurrere om UH-sektorens gunst. Det at din institusjon melder seg på en slik felles prosess i regi av UNINETT FAS medfører at dere får rett til å bruke det valgte systemet. Dere plikter ikke til å ta det i bruk. Det eneste vi forventer er at dere er med og dekker kostnadene til fellesprosjektet, og høster gleden av et felles system. KGV skal være et verktøy som skal bidra i gjennomføring av anskaffelsesprosedyrer i offentlig sektor. KGV vil i hovedsak være et verktøy for innkjøpere og sikre at vi som innkjøpere følger lov om offentlige anskaffelser og dokumenterer våre vurderinger og skjønn der det er nødvendig. Vi skal også holde en kort presentasjon av KGV-prosjektet på UNINETT-konferansen, og vi håper å se mange av dere der!

For mer informasjon gå inn på http://www.uninett.no/trofast/innkjop/index.html

Bjørn Kopperud
bjorn.kopperud@uninett.no

Bjørn-Are Lyngstad
bjorn-are.lyngstad@uninett.no

INTERNASJONALT FoU-ARBEID

Et forskningsnett skal tilby avanserte tjenester til sine kunder. Og for å ha tjenestene klare når kundene trenger dem, må vi ligge i forkant av utviklingen. Mye av arbeidet vi gjør er resultat av satsinger over flere år sammen med internasjonale samarbeidspartnere. Vi jobber sammen med andre forskningsnett i TERENA, men også direkte i EU-prosjekter sammen med forskningsinstitutter, universiteter og industri.

GÈANT2

Nettet som binder sammen forskningsmiljøene i Europa fornyes stadig, og den generasjonen som nå blir rullet ut heter GÈANT2. Dette er et hybridnett som tilbyr både bølgelengder og IP. Hensynet til forskningsaktivitet omkring den nye partikkelakseleratoren LHC hos CERN i Genève står sentralt. I Norge deltar Universitetene i Oslo og Bergen med å regne på deler av den enorme datastrømmen som skapes.

UNINETT har sterk deltagelse omkring måling og overvåking. Vi er med og utvikler perfSONAR, en samling webtjenester og programvare som på en kontrollert måte skal gjøre måledata og målepunkter tilgjengelig for andre forskningsnett og for sluttbrukere. På den måten kan forskerne som jobber i en global samarbeidskontekst få et ende-til-ende bilde av kvaliteten på nettet.

En annen viktig delaktivitet er Edugain som er neste generasjon autentiseringssystem som kobler sammen domener gjennom føderering, og gjør Feide internasjonalt.

Eduroam bygges av arbeidsgruppen TF-mobility i TERENA og er i praksis en føderasjon for nett-aksess.

RING - NESTE GENERASJON RUTING

Man har de siste årene kommet frem til at måten dagens ruting blir gjort på i Internett ikke skalerer på sikt. IP versjon 6 gir mange flere adresser, men ruting foregår omtrent som før, det er derfor ikke nok å gå over til IPv6. Spesielt innenfor IETF (Internet Engineering Task Force) og relaterte miljøer, jobbes det nå aktivt med å se på løsninger. I dag brukes IP-adresser både for å identifisere en maskin (en maskin på Internett har typisk en fast adresse som identifiserer den), og for å lokalisere maskinen, dvs. for å rute datapakker frem til den. Mange mener løsningen på problemet er å skille identitets- og lokasjonsegenskapene. Det jobbes med løsinger på mange hold. Noen kommer med konkrete løsninger som må vurderes, mens andre driver med mer teoretisk forskning.

RiNG er et EU-prosjekt som i hovedsak sprer informasjon om utfordringer og løsninger for neste generasjons ruting, og forsøker å få til bedre kommunikasjon mellom de forskjellige miljøene som jobber med dette, mellom både forskere og de som driver de forskjellige delene av Internett.

LOBSTER - MÅLEINFRASTRUKTUR FOR PASSIVE MÅLINGER

LOBSTER var et EU-prosjekt som startet i januar 2005 og ble avsluttet i juni 2007. Hovedmålet var å lage en passiv måleinfrastruktur i Europa og utvikle nye passive måleapplikasjoner som kunne utnytte denne infrastrukturen. UNINETT benytter seg av denne teknologien til målepålene som har blitt plassert ut i stamnettet og hos institusjoner. En av applikasjonene som har blitt utviklet er utvidet flytanalyse (ex. netflow). Denne applikasjonen bruker IPFIX-standarden til å generere flytrapporter med ekstra attributter slik at det er mulig å si noe om kvaliteten på trafikken som overføres på nettet. Andre applikasjoner er Nemu som kan detektere polymorfiske virus og Appmon som kan gjenkjenne trafikk som bruker dynamiske porter, som for eksempel P2P trafikk.

Olav Kvittem
olav.kvittem@uninett.no

NORSTORE

– infrastruktur for dataforvaring, arkivering og lagring av vitenskapelige data

Bakgrunn

E-vitenskap muliggjør nye former for samarbeidende forskning, på tvers av ulike disipliner ved hjelp av økt deling av instrumenter og beregningsressurser, og lettere tilgang til samlinger av forskningsdata og informasjon. Deling av vitenskapelige data gir en kunnskapsbase som danner nye muligheter og horisonter for forskning og oppdagelser. E-vitenskap entrer nå en fase hvor det kreves mer avanserte nivå av dataforvaring, dvs. strategier, policy og praksis angående dannelse, forvaltning og langtidsbevaring av data. Data blir ikke kun lagret og arkivert lenger, men er utsatt for revidering og utvidelse etter hvert som det blir nødvendig. Datalagre med aktiv og kontinuerlig bruk av datasett er nå blitt en realitet. Dette med verktøy som assisterer lokalisering, gjenbruk og presentasjon av data.

e-vitenskap er avhengig av tilgjengelighet til moderne informasjonsteknologiske verktøy. Disse verktøyene utvikler seg raskt og fleksibiliteten i bruken av disse verktøyene setter selve dataene de produserer og omdanner i risiko. Digital vitenskapelig informasjons overlevelse er avhengig av et hierarki av konstant utviklende teknologi, dvs. maskinvare, lagringsmedier, operativsystemer, applikasjons software og mellomvarer. Den er også avhengig av taus kunnskap som eksisterer utenfor dataene. En infrastruktur for digitale data må være i stand til effektivt å håndtere ulike typer av data fra flere ulike opprinnelser og de ulike måter dataene samles, lagres, gjenopprettes og manipuleres på. Alle disse aspekter reiser seriøse og komplekse utfordringer for aktiv bevaring av data. Mye gjenstår på alle nivå for å sørge for at data som dannes forblir tilgjengelige og valide for framtidige forskere.

Behovet for lagringsressurser og nye måter å bevare og publisere data på melder seg fra flere områder i naturvitenskap som klimaforskning, biovitenskap, kjemi, fysikk, materialvitenskap, strømningsteknikk og medisin. Også datamengdene som må håndteres øker raskt. Et kjent eksempel er Large Hadron Collider ved CERN som begynner med å produsere relevante datasett i 2008. Norge deltar i det internasjonale samarbeidet for analyse og lagring av disse dataene og det forventes at omtrent 1.5 petabyte (1 500 terrabyte) skal lagres i Norge før slutten av 2010. Også klimaforskere i Norge ser behov for å lagre flere hundre terrabyte data hvert år som kommer fra observasjoner, sensorer eller simuleringer på datamaskiner. Det oppstår dermed et spørsmål om hvordan man på en kostnadseffektiv og kvalitativ måte skal kunne ta hånd om det økende behovet for datalagring for ulike fagfelt.

Med dette som bakgrunn har eVITA programmet i Forskningsrådet opprettet et nytt prosjekt – NorStore – som skal dekke behovene for datalagring og datahåndtering fra flere felt i naturvitenskap og e-vitenskap. UNINETT Sigma har det koordinerende og administrative ansvaret for prosjektet som gjennomføres i samarbeid med UNINETT morselskapet og de fire universitetene UiO, UiB, UiT og NTNU. Prosjektet omfatter utvikling og etablering av en effektiv og stabil infrastruktur for lagring av vitenskapelige data med tilsvarende drift- og støttetjenester.

Mål

Det overordnede mål for NorStore prosjektet er å etablere og vedlikeholde en nasjonalt koordinert infrastruktur for forvaring, arkivering og lagring av digitale data fra ulike vitenskaper og opprinnelser. Infrastrukturen skal gi lett og trygg tilgang til datasett som finnes på distribuerte lagringsressurser i Norge eller utlandet. Prosjektet vil betjene storskala lagringsressurser og tilby brukerstøtte til forskere og forskergrupper som har behov for lagringskapasitet og dataforvaringstjenester. Prosjektet vil også fremme et sett av standardtjenester og beste praksis som retter seg mot forbedret gjenbruk av vitenskapelige data, øke antallet av multidisiplinære forskningssamfunn og øke muligheten til nye vitenskapelige funn på tvers av ulike disipliner.

Det nye tungregneanlegget "stallo" som ble installert ved Universitetet i Tromsø i november.

Foto: Thilo Bubek

Infrastrukturen må være bærekraftig, kostnadseffektiv og tillate effektiv utnyttelse av tilgjengelige ressurser, tjenester og kompetanse, og den skal være attraktiv for en vid rekke av vitenskapelige disipliner. Infrastrukturen vil være en integrert del av den nasjonale e-infrastrukturen som inkluderer tungregneanlegg, høyhastighetsnettverk og vitenskapelige instrumenter.

Oppgaver

Det vil ligge en rekke aktiviteter i prosjektet for å forsøke å nå de satte mål. Disse omfatter blant annet

- koordinering av investeringer i infrastrukturen
- drift av ressurser, verktøy og tjenester i infrastrukturen
- gi ekspertråd til og assistanse til brukere
- sørge for kostnadseffektiv og høy utnyttelse av infrastrukturen
- analyse av nåværende og framtidige brukerbehov
- vedlikehold av kjernetjenester og -verktøy
- koordinering og administrasjon av tilgang til infrastrukturen
- bidra til en nasjonal policy og beste praksis for infrastruktur for data
- øke oppmerksomheten omkring viktigheten av dataforvaring til alle interessenter

Oppgavene i 2007 inkluderer definisjonen av prosjektets organisasjonsform og etablering av den initiale infrastrukturen med få store lagringsressurser. De første forskergruppene får tilgang til infrastrukturen tidlig i 2008. Infrastrukturen oppgraderes skrittvis og hvert år skal det tilføyes kapasitet og nye tjenester etter brukerbehov.

Aktiv lagring og bevaring av data reiser mange ikke-teknologiske problemstillinger, eks. spørsmål angående sikkerhet, konfidensialitet, eierskap, forsikret opphavsrett, autentisering, integritet og kvaliteten på primærdata og assosierte metadata. I dagens digitale miljøer er det ingen selvfølge å ha lit til data som har blitt videreformidlet. Tilliten til dataene kan forsterkes ved eksistens av kvalifiserte domenespesialister og datasentre som bevarer og håndterer dataene.

Prosjektet skal aktivt engasjere seg i samarbeid med parter som har lignende mål, interesser og behov. Det vil også etableres nasjonalt og internasjonalt samarbeid med organisasjoner som har interesse for infrastruktur for vitenskapelige data og behov for standardisering og interoperabilitet av tjenester. Sluttbrukere av den nasjonale infrastrukturen vil inkludere prosjekter og programmer finansiert av Norges forskningsråd og Kunnskapsdepartementet.

Fordeler
Det er mange fordeler ved å samarbeide om infrastruktur for digitale databaser og datalagre. Koordinering av investeringer, drift og brukerstøtte og koordinert bruk av infrastrukturen muliggjør kostnadseffektiv utnyttelse av infrastrukturen. De totale kostnadene for investering og drift av få datalagre som deles mellom ulike organisasjoner og fagområder er lavere enn for flere datalagre vedlikeholdt av de enkelte institusjonene. Delte datasamlinger kan tilrettelegge for kostnadseffektiv innovasjon i teknologi, unngå unødvendig duplisering av data og dermed faren for inkonsekvent informasjon mellom institusjoner. Delte datalagre muliggjør lettere datadeling uavhengig av organisasjon eller land.

Mer informasjon:
Hjemmeside NorStore prosjektet: http://www.norstore.no
Hjemmeside UNINETT Sigma: http://sigma.uninett.no

BETYDELIG MER REGNEKAPASITET FOR NORSKE FORSKERE

Mellom august 2007 og mars 2008 øker det totale antall prosessorkjerner innen det nasjonale tungregneprosjektet Notur med en faktor på nesten ti.

Dette som et resultat av tre investeringer i regneressurser som ble avgjort rett før sommeren i år. I august ble beregningsklyngen titan ved Universitetet i Oslo utvidet med 224 noder fra SUN og totalt 448 to-kjerne prosessorer. Disse vil erstattes med fire-kjerne prosessorer (AMD Opteron "Barcelona") innen utgangen av året. Sammen med oppgraderingen av den eksisterende del av klyngen, vil totalt 2432 prosessorkjerner tilføyes.

Universitetet i Tromsø installerte en ny HP klynge tidlig i november som inneholder 704 noder med totalt 5632 prosessorkjerner (Intel "Woodcrest").

Universitetet i Bergen vil installere en ny Cray XT4 tidlig 2008 med 1388 noder og totalt 5552 prosessorkjerner (AMD Opteron "Budapest").

Mer informasjon om ressursene og hvordan man kan søke tilgang finnes på hjemmesiden for Notur-prosjektet: www.notur.no.

Eva Haugen
eva.haugen@uninett.no

FLERE GODE ARGUMENTER FOR FEIDE

God økonomi og hensyn til personvernlovgivningen er to av grunnene en skoleeier har for å sørge for god identitetsforvaltning og innføring av Feide – Kunnskapsdepartementets valgte løsning for sikker identifisering i utdanningssektoren. Når NDLA lanserer en fagwiki med Feide-pålogging, blir også muligheten for deltakelse, egenproduksjon og web-læring gode argumenter for å innføre Feide.

Innføringen av digital kompetanse som den femte basisferdighet har resultert i et sterkere fokus på IKT i undervisningen. En vellykket integrering av grunnleggende digitale ferdigheter i de nye læreplanene forutsetter tilgang til gode digitale læringsressurser og kunnskapskilder.

Både kommersielle og offentlige tjenestetilbydere arbeider med å utvide mengden av tjenester som er Feide-klare, og antall tilgjengelig tjenester er økende.

En av disse er Nasjonal digital læringsarena (NDLA), et fellesinitiativ fra fylkeskommunene som skal tilby fritt tilgjengelige læremiddel for alle fag i den videregående opplæringen. I første omgang, det vil si til skoleåret 2007-2008, skal det gjennom prosjektet tilbys digitale læremidler som dekker læreplanene i helse og sosialfag, norsk og naturfag på videregående trinn 1 (VG1).

– Feide en sentral brikke

I løpet av det neste halve året planlegger NDLA lansering av en egen fagwiki, der lærere og elever selv skal bidra til å utvikle innholdet. Wikien baseres på kjent teknologi, og bruker Feide for sikker pålogging.

– Vi har tro på at deltakelse og egenproduksjon er med på å fremme læring, og gjennom en fagwiki der brukerne selv bidrar med kunnskap ønsker vi å skape et eierforhold til innholdet, sier Øivind Høines, prosjektleder i NDLA.

For å kunne redigere innholdet på wikien må man ha brukernavn og passord fra Feide. Høines sier Feide er en sentral brikke i NDLAs arbeid for deling av innhold.

www.ndla.no

– Vi trenger å vite hvem folk er, om det er en lærer, en fagperson eller en elev som logger på tjenesten. Feide gir brukerne rettigheter etter hvilken rolle de har.

Høines poengterer at utfordringen for NDLA er å legge til rette for god pedagogisk bruk og sørge for at tjenesten blir best mulig implementert i skolen, og at dette er en problemstilling som handler om digital dannelse og digital kompetanse.

Flere tjenester underveis

Innholdet som gjøres tilgjengelig gjennom NDLA er tilgjengelig for alle, men bare brukere med Feide-navn kan redigere innholdet.

– Vi mener det er uheldig for læringen om man hindrer tilgang til innhold, og man bør se på Feide som noe annet enn en nøkkel som låser innhold inne. For vår del bruker vi Feide til å koble brukere til innholdet. Det spesielle er at alle med tilgang til Internett også har tilgang til dette innholdet.

NDLA er nå inne i en konseptfase der de ser på flere alternative tjenester. Felles for alle er at de skal være tilgjengelige via Feide-pålogging.

– Vi jobber for eksempel med å utvikle en "min elevside" og "min lærerside" som brukerne kan tilpasse etter egne interesser og fag. Dette blir et blogg-lignende verktøy der elever og lærere hver for seg eller i fellesskap kan publisere faglig innhold. Dette verktøyet gir elevene kontroll over egenprodusert materiale, og lar dem også ta det med seg videre etter endt skolegang, avslutter Høines.

Øivind Høines, prosjektleder NDLA.

Nasjonal digital læringsarena (NDLA) er et fellesinitiativ fra fylkeskommunene som skal tilby fritt tilgjengelige læremiddel for alle fag i den videregående opplæringen. Kunnskapsdepartementet har i 2007 gitt 15 millioner kroner til de 18 fylkeskommunene som har gått sammen om prosjektet. NDLA skal bidra til å øke mangfoldet av digitale læremiddel til bruk for elever og lærere i den videregående skolen.

Øyvind Vikan
oyvind.vikan@uninett.no

BRUK AV 802.1X I TRÅDLØSE NETTVERK

Bakgrunn
Den 24. juni 2004 ble den etterlengtede IEEE 802.11i ferdig. Dette var en standard som skulle gi trådløse nettverk den sikkerheten den trengte etter at det i 2001 ble offentlig kjent hvor dårlig WEP egentlig var. Det skulle altså gå tre år før vi fikk en standard som adresserte sikkerhetsproblemet. I mellomtiden ble det benyttet løsninger som ikke alltid var like vellykket. Her kan det nevnes rullerende WEP-nøkler, VPN og web-portaler alt etter hva det var man ønsket å sikre. IEEE høstet mye kritikk for WEP i 802.11-standarden selv om den strengt tatt aldri hadde lovet at WEP skulle være en god løsning.

Markedet var svært utålmodig men IEEE hadde ikke råd til å gjøre noen feil og måtte bruke den tiden som var nødvendig. Wi-Fi Alliance er en interesseorganisasjon som bl.a. står bak "Wi-Fi" sertifisering av 802.11-produkter. Medlemmene består i stor grad av produsenter av 802.11-produkter og de så at kundene ikke var fornøyd med å måtte vente på 802.11i. Da 802.11i fikk status som Draft 3.0 lanserte Wi-Fi Alliance "Wi-Fi Protected Access", bedre kjent som WPA. De første produktene som støttet dette ble sertifisert i april 2003. Etter hvert kom den ferdige 802.11i og Wi-Fi Alliance fulgte opp med WPA2 i september 2004.

WPA og WPA2 kom begge i to varianter, Pre-Shared Key (PSK) og Enterprise. Forskjellen er at med PSK så bruker man en fast krypteringsnøkkel på 64 hexadesimale tegn, mens man i Enterprise bruker 802.1X som autentiserings-mekanisme. Å taste inn 64 hexadesimale tegn er noe de færreste har lyst til å prøve seg på, derfor ble det også laget en algoritme hvor man ut i fra en pass-frase (passphrase) genererer de nødvendige 64 tegnene.

I WPA fikk vi krypteringen "Temporal Key Integrity Protocol", TKIP som lik WEP bruker en RC4 som er en symmetrisk chiffrering (kryptering). I motsetning til WEP får hver pakke sin egen nøkkel og blir dermed unikt kryptert. Metoden blir ansett som rimelig sikker i den forstand at det er kjente svakheter ved den, men det er ingen som hevder å ha kunnet utnytte det i praksis. En annen stor fordel med metoden er at den benytter seg av RC4. Det var innebygd støtte for RC4 i hardware på de fleste trådløskort som var på markedet. Gamle kort med støtte for 128-bits WEP kunne med firmware oppgraderes til også å støtte TKIP og dermed også WPA.

WPA2 bruker den beste krypteringen som er tilgjengelig i 802.11i, CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) som er basert på CCM av Advanced Encryption Standard (AES). Forenklet blir det sagt at WPA2 bruker AES. Denne krypteringen går for å være svært sikker og er et anbefalt valg. Eldre trådløse nettverksklienter støtter ikke dette, men nyere kort og da spesielt i Enterprise-markedet, har støtte for AES.

I de fleste Enterprise-klasse basestasjoner er det mulig å tilby både WPA og WPA2 samtidig, slik at klienten kan velge etter egen preferanse.

PSK variantene er neppe aktuelle å bruke hos de fleste institusjoner, men er mer en variant for hjemmemarkedet som sjelden er i stand til å sette opp autentisering med 802.1X. Enterprise med sin 802.1X baserte autentisering er til gjengjeld svært attraktivt å bruke.

IEEE 802.1X for trådløse nettverk
802.1X er en standard for portbasert aksesskontroll. Det vil si at klienten først må gjennomføre en vellykket autentisering før porten blir åpnet og lag 2 trafikk kan passere.

Tabellen under viser forskjellen på de forskjellige WPA-versjonene.

Type	Autentisering	Kryptering
WPA-PSK	Pass-frase (64 tegn hex)	TKIP
WPA2-PSK	Pass-frase (64 tegn hex)	CCMP (AES)
WPA-Enterprise	802.1X	TKIP
WPA2-Enterprise	802.1X	CCMP (AES)

Standarden kom i juni 2001 og var før 802.11i mest kjent brukt i switcher hvor man har en fysisk port å forholde seg til. I en trådløs blir denne porten en assosiering mellom en basestasjon og en gitt klient.

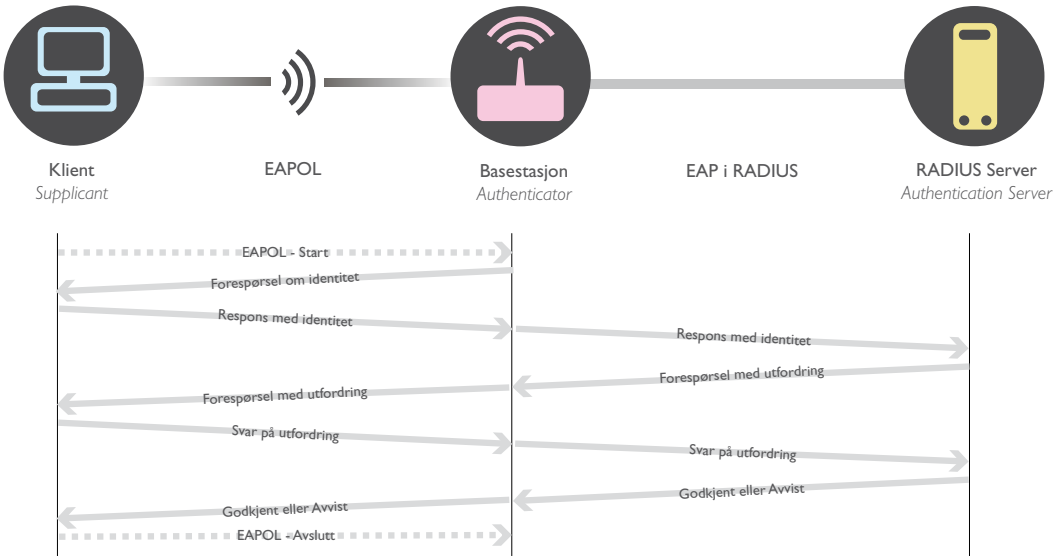
En RADIUS server er en nødvendig del av autentisering med 802.1X. Med det får en institusjon muligheten til å knytte autentisering av sine trådløse brukere opp mot eksisterende brukerdatabaser og med det forenkle bruker-administrasjonen. I tillegg får man en god oversikt over hvem som bruker trådløsnettet når og man kan identifisere hvilken IP-adresse brukeren har disponert.

Selve autentiseringsmekanismen gir oss også muligheten til å få en svært nødvendig funksjon for autentisering mot trådløse nettverk, nemlig gjensidig autentisering. I motsetning til en kablet tilkobling kan man med trådløst i utgangspunktet ikke være helt sikker på at den basestasjonen man prøver å koble seg til virkelig er det den gir seg ut for. En falsk basestasjon kan være svært farlig og en gullgruve for en som driver med phishing og sniffing.

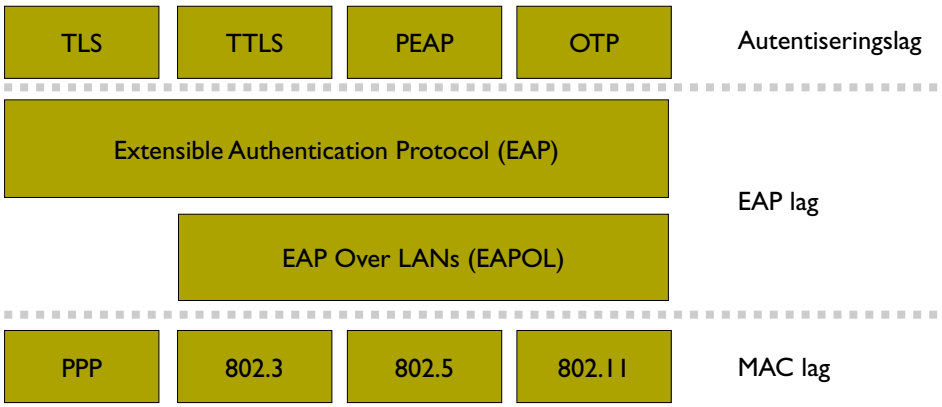
Hvordan IEEE 802.1X fungerer

IEEE 802.1X gjør bruk av tre parter i en autentiseringsprosess: Supplicant (klienten), Authenticator (AP) og Authentication Server (RADIUS). Kommunikasjonen mellom disse går via en protokoll med forkortelsen EAP (Extensible Authentication Protocol). Mellom Supplicant og Authenticator går EAP direkte på lag 2 (EAPOL - EAP over LAN) mens det mellom Authenticator og Authentication Server går over TCP/IP som en del av RADIUS-protokollen.

Autentiseringsprosessen initieres av enten Supplicant eller Authenticator i det klienten prøver å assosiere seg mot basestasjonen. Det er flere måter å gjøre det på, men ved gjensidig autentisering så vil Authentication Server først sende sitt sertifikat til Supplicant via Authenticator. Dersom Supplicant godtar denne, så vil den så følge opp med å oppgi sitt brukernavn/passord eller sertifikat, avhengig av hvilken metode som brukes. Dersom Authentication Server godtar dette svaret så vil den sende beskjed til Authenticator om dette som så vil åpne en trådløs "port" for Supplicant. Denne virtuelle porten er en sikret, trådløs tilknytning mellom Supplicant og Authenticator slik at klienten får fri tilgang til nettverket bak basestasjonen.



Figuren viser gangen i EAP-prosessen. Den initielle prosessen hvor RADIUS serveren først sender sin offentlige nøkkel er ikke tatt med i denne figuren, men vil foregå før klienten blir spurt som sin identitet. EAP er konstruert for at man skal kunne benytte seg av en valgfri autentiseringsmekanisme.



Det finnes mange muligheter, men det er få av dem som gir den gjensidige autentiseringen vi trenger på trådløse nettverk. Disse er TLS (Transport Layered Security), TTLS (Tunneled TLS) og PEAP (Protected EAP). Felles for alle er at Authentication Server må ha et serversertifikat. TLS benytter seg av klientsertifikat for alle brukere mens TTLS og PEAP, som er veldig like, benytter seg av brukernavn og passord. TTLS og PEAP bør da bruke MS-CHAPv2 for å pakke inn dette før det sendes til Authentication Server. Det er ingenting i veien for å tilby flere autentiserings-mekanismer samtidig. De fleste som kjører 802.1X for trådløse nettverk gir gjerne klienten valget mellom TLS, PEAP og TTLS.

EAP type	Metode RADIUS/Klient	Krever
EAP-TLS	Sertifikat/Sertifikat	PKI
EAP-PEAP	Sertifikat/MS-CHAPv2	Brukerdatabase
EAP-TTLS	Sertifikat/MS-CHAPv2	Brukerdatabase

Tabellen viser en oversikt over anbefalte EAP typer og autentiseringsmetode.

Sertifikater

Autentiseringsprosessen med TLS, PEAP og TTLS krever alle bruk av sertifikater. Et minimum er et serversertifikat til RADIUS serveren. Disse kan man enten kjøpe eller generere selv. Dersom man kjøper et sertifikat så er det gjerne fra en "Certificate Authority" (CA) som allerede ligger i registeret til operativsystemet klienten kjører på. Det er mange slike CA tilgjengelig.

UNINETT er medlem i TERENA's SCS-prosjekt (Server Certificate Service), og kan levere serversertifikater til sikring av tjenester. Sertifikatene er utsted av GlobalSign, en CA lokalisert i Belgia og som er en del av Cybertrust-gruppen. GlobalSign CA ligger allerede i de aller fleste operativsystemer.

Se http://forskningsnett.uninett.no/scs/ for mer informasjon om hvordan å bestille sertifikat fra UNINETT.

For å få den høyeste grad av sikkerhet er det beste å generere sine egne sertifikat med sin egen CA. Dette krever at man installerer det offentlige sertifikatet til alle klientene. Da har man full kontroll på de utstedte server-sertifikat slik at det ikke vil være mulig for noen å skaffe seg et annet serversertifkat og så bruke det til å utgi seg for å være en gyldig RADIUS server. Det er dessverre enkelte klienter (som Windows XP) som ikke har mulighet for å sjekke sertifikatets "Common Name" (CN) for å se om det stemmer med hva det skal være. Da holder det at sertifikatet er utstedt fra samme CA for at det skal bli godkjent av klienten.

Hvorvidt bruken av kjøpte sertifikat utgjør noen praktisk risiko kan diskuteres. Så lenge man bruker MS-CHAPv2 inne i PEAP/TTLS så bør det i seg selv være sikret rimelig bra mot en falsk RADIUS server. Ved en ren TLS-løsning vil ikke brukernavn og passord kunne komme på avveie. Om en falsk basestasjon og RADIUS gir godkjent autentisering så kan brukeren bli utsatt for senere phishing og sniffing av trafikken. Selv om dette er teknisk mulig så må man vurdere denne risikoen opp mot ressurskostnaden med å distribu-ere egen CA til alle klienter. Å etablere en full Public Key Infrastructure (PKI), dvs. å ha sertifikater til alle brukere, vil for de fleste være svært ressurskrevende.

Oppsummering

UNINETT anbefaler at man bruker WPA2-Enterprise i trådløse nettverk. For å støtte flest mulig klienter er det forståelig at man i påvente av bedre WPA2-Enterprise støtte i klientene, også støtter WPA-Enterprise i sitt nettverk.

EAP-metodene som anbefales brukt er TLS, PEAP med MS-CHAPv2 og/eller TTLS med MS-CHAPv2.

Sertifikater til RADIUS kan man enten kjøpe eller generere selv.

Vi viser også til UFS 112 for mer informasjon om omkring dette emnet.

Jardar Leira
jardar.leira@uninett.no

Innlegg i gjestespalten *På den annen side* i Adresseavisen 14.07.2007
Av Elisabeth Farstad, UNINETT Norid AS

.NO I RØDT, HVITT OG BLÅTT

Husker du tida før Internett? Den gangen brev gikk i frankert konvolutt som A- eller B-post, og e-post var noe vi såvidt hadde hørt om.

Tro det eller ei, men slik var det for bare ti år siden. Med en så kort historie i ryggen, er det ikke så merkelig at mange stusser når jeg forteller at jeg jobber i Norid og forklarer at Norid driver .no-domenet. Og legger jeg til at det faktisk er slik at norsk Internett stopper uten Norid, er samtalen som oftest i gang. For selv om nesten hele befolkningen har tilgang til Internett og mange er på nettet store deler av døgnet, er det få som tenker over at et internasjonalt adressesystem er helt nødvendig for at jeg skal kunne bestille hotellrom til ferien eller finne igjen gamle kjente på Facebook.

Adressesystemet for Internett kan sammenlignes med NO foran postnummer og N på norske biler. Alle internettadresser som ender på .no sorterer under det norske toppdomenet. De ivrigste innenfor internett- og domenebransjen her i landet har et like varmt forhold til .no som til det norske flagget, som begge gir signal om tilknytning til Norge. Om det kan være så mye å skryte av? Det er i hvert fall slik at norske virksomheter satser på et domenenavn under .no når de skal markedsføre seg fordi de forbinder .no med kvalitet. I en fersk internasjonal kartlegging av sikkerhet ved bruk av websider, fikk .no nesten topplassering blant verdens 256 nasjonale toppdomener.

.no kom til Norge i 1983. Internett i den formen vi kjenner det i dag, var fortsatt under utvikling, og et felles adressesystem var en av flere forutsetninger for at verdensomspennende nettverk av datamaskiner skulle kunne fungere. Opplegget med landkoder ble laget av en dataentusiast i California, og det var en like entusiastisk privatperson i Norge som overtok stafettpinnen og delte ut de første internettadressene her i landet.

Mot slutten av 80-tallet fantes det fortsatt bare en håndfull .no-domener. Noen så likevel at dette kunne få stor betydning og ikke kunne drives videre på hobbybasis. Men hvem var i stand til å ta et slikt ansvar på den tida? Oppdraget gikk til UNINETT, som allerede drev et datanett for universitetene og hadde forutsetninger for å påta seg jobben.

Når vi vet hvordan det gikk, kan vi vel si at det var en klok og framtidsrettet beslutning å legge et slikt ansvar til et teknisk kompetent miljø med et klart samfunnsoppdrag. Med nettleseren ble Internett etter hvert allemannseie, og kurven for domeneregistreringer gikk dramatisk i været. I 1997, for ti år siden, var det 6 000 domener under .no. I dag er tallet oppe i nesten 330 000, og kurven stiger fortsatt bratt. På verdensbasis passerte vi i fjor ufattelige 100 millioner domener, noe som avspeiler den betydningen Internett har for store deler av verdens befolkning.

Internett er i sitt vesen globalt, og en rekke forhold, både tekniske og politiske, må

Elisabeth Farstad
elisabeth.farstad@uninett.no

avklares av internasjonale organer. Tema knyttet til styring av Internett har vært på FNs dagsorden de siste årene, og en rekke viktige spørsmål knyttet til forankring, mandat og beslutningsprosesser er under arbeid. Norske myndigheter bidrar aktivt i dette arbeidet, og alle med interesse for disse spørsmålene kan faktisk delta.

Samtidig må de nasjonale toppdomenene styres ut fra lokale interesser i det enkelte land. For Norges del er toppdomenet blitt en svært viktig del av infrastrukturen, noe som selvsagt stiller meget strenge krav både til et overordnet rammeverk og til den faktiske driften. En robust teknisk infrastruktur må ligge i bunnen, men det er også avgjørende at vi har et regelverk for tildeling og bruk som er tilpasset behovene i det norske samfunnet og som utvikles etter hvert som disse endrer seg.

Som min nabo kommenterte over hekken: – Og jeg som har trodd at et domenenavn bare var en internettadresse.

TEITE TING OM TRYGGLEIK

KLASSISK GRESK: TROJANARAR

Utanfor Troja gøymde angriparane seg i ein stor trehest som trojanarane trilla inn i byen. Då mørket kom, gjekk slemmingane inni hesten til angrep frå innsida. Dagens trojanarar er ikkje dummingane som trilla inn hesten, men små program som gøymer seg slik at du ikkje ser kva du laster ned. Etter at mørket fell, går slemmingprogrammet til aksjon og tar over maskina di. Slik kan også du bli ein del av organisert kriminalitet

ORGANISERT KRIMINALITET

Verda er skummel. Og det viser seg også på Internett. No er det stadig oftare at organiserte kriminelle prøver seg på å overta store mengder PCar for å bruka til å bryta seg inn eller å sabotera. Ikkje berre organiserer dei folk, men det er også ein PC mafia av saboterte maskiner som dei bruker til å overfalla uskuldige offer.

Dei farlege angrepa på Internett i dag er i stor grad organisert kriminalitet, der dei er ute etter pengar. Dette gjer at informasjon som kan leia dei vidare til pengar, slik som bankkontonummer eller kredittkortinformasjon, er av stor interesse. Nettverk med stor bandbreidde, slik som UNINETT, er også av interesse, då det gjev høve til å gjera mange angrep samtidig.

DET DU VEIT, HAR DU IKKJE VONDT AV

Målepålane som er sett ut i nettet gjev deg informasjon om trafikken hos deg, og fram til eit anna målepunkt. Dette kan hjelpa deg med å finna kva som er problemet mellom deg og dei andre (viss problemet ligg i nettverket). https://drift.uninett.no/kart/malepale/norden.html

Oversikt over programvare som er installert er ofte lurt å ha. Sjølv om det har blitt litt mindre virus, betyr ikkje det at nettet er ein helsebringande plass å setja ein PC.

Då kan det vera lurt å vita kvar eg har lagt backupdata. Data har ikkje vondt av å eksistera fleire stader, så lenge dei berre blir oppdatert ein plass.

RETURADRESSE

UNINETT

NO-7465 TRONDHEIM

DISTRIBUERT AV POSTEN NORGE

NORGE P.P.

Uninytt utgis av UNINETT
Ansvarlig redaktør: Petter Kongshaug

uninytt@uninett.no
7465 Trondheim
73 55 79 00

Abonnement er gratis
Elektronisk utgave finnes på
http://www.uninett.no/uninytt/