Er ruting og tenestekvalitet i IP-nett sikkert?

Eli Winjum

Forsvarets forskningsinstitutt/Norwegian Defence Research Establishment (FFI)

19. februar 2007

FFI-rapport 2006/03914

869

ISBN 978-82-464-1139-2

Emneord

Sikkerhet

Informasjonssikkerhet

Kommunikasjonssikkerhet

Ruting

Tjenestekvalitet

IP-nett

Godkjend av

Torunn Øvreås	Prosjektleiar
Vidar S. Andersen	Avdelingssjef

Samandrag

Det framtidige kommunikasjonsnettet for det nettverksbaserte Forsvaret skal understøtta operasjonar med dynamisk organisering, høg mobilitet og einingar frå fleire nasjonar. Slike scenarium krev saumlaus kommunikasjon mellom sluttbrukarar, noko som i sin tur krev at kommunikasjonsnetta er interoperable og at dei grunnleggjande nett-tenestene er gjennomgåande. Denne rapporten dokumenterer eit studie der formålet har vore å undersøkja om dei sivile sikkerhetsstandardane for IP-nett/Internett er eigna til å sikra nett-tenestene ruting og tenestekvalitet. Studiet har teke utgangspunkt i eit kommunikasjonsnett basert på *Internet Protocol* (IP) versjon 6.

Rapporten ser det framtidige kommunikasjonsnettet som eit distribuert informasjonssystem og diskuterer kva konfidensialitet, integritet og tilgjenge vil seia for informasjonen som ligg til grunn for ruting og tenestekvalitet. Rapporten syner at her trengs ein særeigen sikkerhetspolicy.

Rapporten tek særleg føre seg dei to viktigaste sikkerhetskomponentane utvikla av *Internet Engineering Task Force* (IETF): Sikkerhetsarkitekturen for IP (IPSec) og den offentlege nøkkel-infrastrukturen PKIX. Rapporten syner at desse komponentane *slik dei er spesifisert i dag*, ikkje er tilstrekkelege for å sikra nett-tenestene ruting og tenestekvalitet. Årsakene til dette er at:

- Sjølv om IETF utfører eit omfattande arbeid for å sikra nett-tenestene i framtidige IP-nett, har sikkerhetsstandardar og spesifikasjonar veikskapar og manglar. På mange sentrale felt er dei enno uklare og uferdige. Ein veikskap i høve til militære krav er at standard protokollar for ruting og tenestekvalitet ikkje er utforma for å støtta *konfidensialitetskrav*. På den andre sida støttar dei *integritetskrav*, men manglar eksplisitt støtte for *fleirnivå* sikkerhetsmodellar for nettinformasjon. Både IPSec og PKIX vil medføra store skaleringsproblem i nett med låg kapasitet. Det bør gjerast grundige analysar før ein eventuelt går inn for å nytta IPSec og PKIX for å sikra protokollane for ruting og tenestekvalitet dei mobile delane av NbF målnett
- IPSec tilbyr sikkerhetstenester på nettlaget. Dette medfører mellom anna at ein ikkje utan vidare kan sikra informasjonen som vert utveksla i samband med dei ulike mekanismane for tenestekvalitet
- Sikkerhetskomponentane dekkar berre informasjonsutvekslinga mellom nodane i nettet. Sikring av prosessering og lagring i nodane vert ikkje omtalt, heller ikkje sikkerhetsproblematikk knytt til overgangen mellom to ulike rutingprotokollar eller mellom fastnett og ad hoc-nett.

At dei sentrale sikkerhetsspesifikasjonane ikkje strekk til for ruting og tenestekvalitet, vil sjølvsagt ikkje seia at det er umogleg å sikra slike tenester i IP-nett;- heller ikkje at det er umogleg å få til sikre og fleksible løysingar med utgangspunkt i desse spesifikasjonane. Om ein ynskjer å bruka sivile standardar, bør ein arbeida innanfor standardiseringsorgana for å gjera standardane best mogleg. Eit alternativ er å utvikla eigne løysingar på grunnlag av dei sivile standardane. I så fall bør slike løysingar vera kompatible med dei sivile standardane for å ivareta krav om interoperabilitet og dynamikk i alle delar av det framtidige kommunikasjonsnettet.

English summary

Future communication networks for network centric warfare should support operations characterized by dynamic organization and high mobility. Units from several countries may take part. Such scenarios demand seamless communications between end users. Hence, interoperable communication networks are required. Network services like routing, quality of service (QoS) and security should be consistent and compatible throughout the network. This report documents a study which aimed at investigating to which extent civil security standards and specifications for IP networks are suited to secure routing and QoS in an IP version 6 environment.

A communications network may be viewed as a distributed information system, and the report discusses requirements on confidentiality, integrity and availability, and the impacts on information underlying services like routing and QoS. The report states the need of a specific security policy to regulate this type of information.

The report concentrates on two main security components developed within the *Internet Engineering Task Force* (IETF): *Security Architecture for the Internet Protocol* (IPSec) and the *Internet X509 Public Key Infrastructure* (PKIX). The report states that current specifications do not provide sufficient security to routing and QoS in military IP networks. Also, if utilized to protect routing and QoS, the security services as such do not provide the needed scalability and flexibility. This, however, does not mean that it is impossible to protect routing and QoS in IP networks or that it is impossible to develop adequate security services on top of civil standards and specifications. If utilization of pure civil standards is desired, participation in IETF working groups should be considered. If development of solutions on top of civil standard is desired, such solutions should be in compliance with the civil standards to support the required interoperability and a flexible and dynamic network organization.

Innhald

1 Innleiing

1.1 Bakgrunn og formål

Det framtidige kommunikasjonsnettet for Nettverksbasert Forsvar (NbF) er skildra i [5]. For å integrera ulike transmisjonsteknologiar best mogleg, vert *Internet Protocol* (IP) tilrådd som gjennomgåande teknologi, og [79] skildrar komponentar som vil vera sentrale i den nye nettarkitekturen. Ein etappevis overgang til eit framtidig kommunikasjonsnett for NATO er foreslått i [84]. Alle desse rapportane legg vekt på at det framtidige kommunikasjonsnettet skal understøtta operasjonar med dynamisk organisering, høg mobilitet og einingar frå fleire nasjonar. Slike scenarium krev saumlaus kommunikasjon mellom sluttbrukarar, noko som i sin tur krev at kommunikasjonsnetta er interoperable og at dei grunnleggjande nett-tenestene er gjennomgåande. Grunnleggjande nett-tenester inkluderer konnektivitet, ruting, tenestekvalitet og sikkerhet. For å utføra slike funksjonar, må nodane utveksla, prosessera og lagra nettinformasjon. Mangelfull sikring av nett-tenestene kan bremsa utviklinga fram mot interoperable kommunikasjonsnett.

Kommunikasjonssikring var utanfor rammene til [79]. Dei andre studia har lagt vekt på sikring av *sluttbrukarinformasjon* og *sluttbrukartenester*, men i liten grad kasta lys over sikring av *nettinformasjon* og *nett-tenester*. Denne rapporten dokumenterer eit studie der formålet har vore å ta føre seg dei grunnleggjande nett-tenestene i det IP-baserte målnettet og undersøkja om dei sivile sikkerhetsstandardane for IP-nett/Internett er tilstrekkelege for desse tenestene.

Målnettet for NbF vil vera eit distribuert kommunikasjonssystem med hovudoppgåve å overføra informasjon mellom sluttbrukarar. Sikring av kommunikasjonssystem har fleire sider. Å sikra overføringa av *sluttbrukarinformasjon* er *ei* side, og har ikkje vore tema for dette studiet. Å sikra tenestene som kommunikasjonsnettet tilbyr og informasjonen som ligg til grunn for desse tenestene, er ei *anna* side, og handlar om å kunna etablera og oppretthalda eit militært kommunikasjonsnett. Tilsvarande sikring av sivile kommersielle kommunikasjonsnett er gjerne eit operatøransvar.

1.2 Vilkår

Studiet har teke utgangspunkt i IP versjon 6 (IPv6) [36]. Når IPv6 vert innført, vil mange sikkerhetsløysingar som er spesifisert for IP versjon 4 (IPv4) [30], falla bort og verta erstatta av ein meir heilskapleg sikkerhetsarkitektur. Dette vil løysa mange av sikkerhetsproblema i eksisterande IPv4-nett. Dersom Forsvaret sjølv skal utvikla løysingar der dei sivile standardane ikkje er gode nok, er det viktig å vita kva for problemstillingar og utfordringar som, etter overgangen til IPv6, framleis er gyldige. Dette aspektet er dessutan viktig med tanke på eventuelle kortsiktige løysingar for noverande IPv4-nett.

Organa som spesifiserer og standardiserer protokollane for IP-nett er *Internet Engineering Task Force* (IETF) [14] og *Internet Engineering Steering Group* (IESG) [13]. Sjølve standardiserings-

arbeidet vert utført i arbeidsgrupper der industri, forskingsinstitutt og akademia deltek. Dei offisielle spesifikasjonane er dokumentert i *Request for Comments* (RFCs) som har *status* ut frå kor langt dei er komne i standardiseringsprosesssen. Ei rekkje spesifikasjonar har enno ikkje oppnådd status som *Internet Standard* sjølv om dei er implementert i kommersielle komponentar. Dei fleste spesifikasjonane av sikkerhetstenester og -mekanismar har førebels status som *Proposed Standard Protocol.* I denne rapporten ser me særleg på spesifikasjonar basert på IPv6. Mange har status som *Draft Standard Protocol*. Denne rapporten tek utgangspunkt i versjonane slik dei låg føre i desember 2006. På nokre område der IETF er komne kort i standardiseringsarbeidet, har me til ein viss grad òg sett på pågåande internasjonal forsking.

Spesifikasjonar som er feil eller dårleg implementert og implementasjonar som er feil eller dårleg konfigurert, vil medføra feilsituasjonar som i seg sjølv utgjer ein sikkerhetsrisiko. Vidare vil inntrengjarar utnytta feil og veikskapar i design, kode og konfigurasjon. Dette er svært viktige aspekt ved sikringa av nett-tenestene men er likevel utanfor rammene av denne rapporten. Rapporten føreset at spesifikasjonane vert implementert korrekt og sunt.

1.3 Definisjonar

IP vert brukt som samleomgrep for protokollar og tenester som er bygde rundt den opphavlege IP-spesifikasjonen.

Nett-teneste vert brukt som samleomgrep for tenester som nettet tilbyr sluttbrukar. Nett-tenester inkluderer funksjonar som ruting, differensiert tenestekvalitet og sikkerhet.

Nettinformasjon vert brukt som samleomgrep for informasjon som vert utveksla, prosessert og lagra i nettet for å realisera funksjonar som ruting, differensiert tenestekvalitet, sikkerhet, sjølvkonfigurering og drift og styring (*network management*). Nodane i eit kommunikasjonsnett utvekslar nettinformasjon ved hjelp av protokollmeldingar frå ei rekkje protokollar som opererer på ulike kommunikasjonslag.

Sluttbrukarinformasjon vert brukt som samleomgrep for informasjon til og frå applikasjonane som sluttbrukarane nyttar, til dømes tale, epost og lesing frå/skriving til databasar.

Nyttelast (*payload*) vert brukt om innhaldet i eit meldingsfelt når feltet fører data frå kommunikasjonslaga over. Sluttbrukarinformasjon vil til dømes vera ein del av nyttelasta i ein IP-pakke.

Ein *sikkerhetspolicy* delar systemet inn i sikre og usikre tilstandar, definerer krava til eit sikkert system og spesifiserer kva som er lov og ikkje lov i systemet. Ein slik policy kan skildrast på overordna nivå i form av normalt språk. For å vera verifiserbar, må ein policy vanlegvis uttrykkast meir eksakt og skrivast ved hjelp av modellar og eigne policy-språk.

Ein s*ikkerhetsmekanisme* er ein metode, verktøy eller prosedyre som implementerer og handhevar ein policy. Døme: Ein krypteringsalgoritme er ein sikkerhetsmekanisme som kan implementera

ein konfidensialitetspolicy.

Sikkerhetsnivå vert brukt synonymt med gradering og impliserer ein sikkerhetspolicy der subjekt og objekt kan tildelast ulike nivå.

Eit *sikkerhetsdomene* omfattar entitetane som er underlagt den same sikkerhetspolicyen.

Eit *rutingdomene* omfattar den delen av eit nett som er underlagt felles retningslinjer for ruting. Ruterane innan eit domene brukar ein og same rutingprotokoll.

Eit *tenestekvalitetsdomene* omfattar den delen av eit nett som er underlagt felles retningslinjer for tenestekvalitet.

I likskap med nyare spesifikasjonar for IP-nett, brukar me sikkerhetsdefinisjonar frå [45].

1.4 Avgrensingar

Alle kommunikasjonsnett må tilby tenester som skal sikra overføringa av sluttbrukarinformasjon. Sikring av sluttbrukarinformasjon og applikasjonstenester ligg utanfor rammene av dette studiet. Studiet er avgrensa til sikring av nettinformasjon og nett-tenester.

IP handterer i all hovudsak *nettlaget*, sjølv om fleire av tenestene i IP-nett kan implementerast over fleire kommunikasjonslag. Me ser på dei sentrale spesifikasjonane, uavhengig av kva for kommunikasjonslag som er involvert.

Studiet avgrensar seg til tre grunnleggjande nett-tenester: ruting, tenestekvalitet og sikkerhet. Me diskuterer om dei allmenne sikkerhetsfunksjonane som IPv6-nett tilbyr, kan brukast til å sikra ruting og tenestekvalitet. Andre viktige nett-tenester som topologikontroll, sjølvkonfigurering og ulike funksjonar knytt til drift og styring er ikkje handtert.

Me har ikkje utarbeidd trugsmålsmodellar av nett-tenestene i IP-nett. For å gje eit innblikk i korleis nett-tenestene vil bli sikra i framtidige sivile IP-nett, presenterer me derimot delar av arbeidet IETF utfører på dette området.

1.5 Oppbyggjing av rapporten

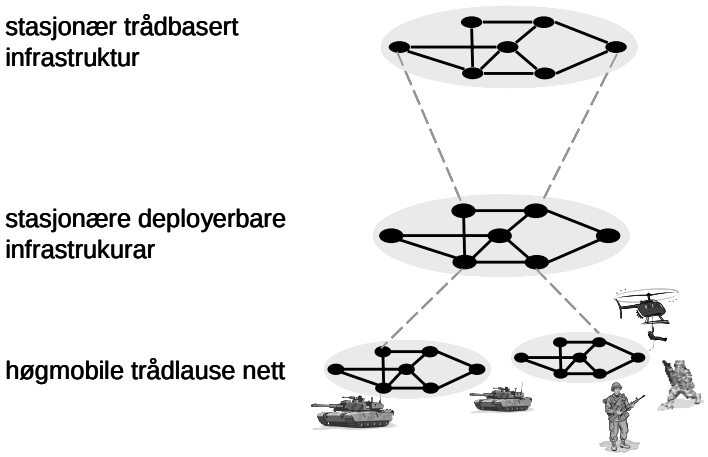
Kapittel 2 går i korte trekk gjennom dei grunnleggjande nett-tenestene og måten eit kommunikasjonssystem handterer informasjonen som ligg til grunn for slike tenester. Kapittel 3 ser på grunnleggjande aspekt ved sikring av nettinformasjon og drøftar ein framtidig sikkerhetspolicy for denne typen informasjon. I kapittel 4 går me kort gjennom IPv6. Kapittel 5 handlar om dei viktigaste standardarkitekturane for sikring av IPv6-nett. Standardane føreset eit underliggjande *fastnett*. Dei er allmenne og ikkje utvikla for å sikra *nettinformasjonen* spesielt. I kapittel 6 drøftar me om dei likevel kan vera eigna til dette og ser på arbeidet det internasjonale standardiseringsorganet gjer på dette feltet. Oppsummering og konklusjonar vert gitt i kapittel 7.

2 Målnettet for NbF

Målnettet for NbF er eit kommunikasjonssystem med tre delar [5]:

- Ein stasjonær infrastruktur som i all hovudsak er trådbasert
- Stasjonære deployerbare infrastrukturar som dels er trådbaserte og dels trådlause
- Høgmobile trådlause nett.

IP skal integrera ulike transmisjonsteknologiar. Figur 2.1 syner ei skisse av nettlaget (IP-laget) i målnettet. Dei tre delane av målnettet skal vera innbyrdes interoperable. I tillegg skal dei tre delane kvar for seg kunna operera saman med eksterne nett. Dette kan vera militære nett frå andre nasjonar i og utanfor NATO eller sivile nett. Frå sivile offentlege kommunikasjonsnett ventar ein gjerne at ulike delar av nettet er interoperable og likeeins at nettet kan tilby kommunikasjon med sluttbrukarar i nett eigd av andre operatørar. Det som skil NbF målnett frå mange sivile nett, er spekteret av bruksscenarium og systemarkitekturar for dei deployerbare og mobile delane av nettet. Særleg i desse delane av nettet kan krava til overlevingsevne, fleksibilitet, mobilitet, dynamikk og sikkerhet vera høgare enn i sivile nett.



Figur 2.1 Skisse av NbF målnett

Dette kapittelet skildrar to sider av målnettet for NbF. Som berar av sluttbrukarinformasjon skal nettet tilby sluttbrukar eit sett nett-tenester. Som informasjonssystem skal nettet forvalta sin eigen informasjon. Kapittelet går i korte trekk gjennom dei grunnleggjande nett-tenestene og korleis eit kommunikasjonssystem handterer informasjonen som ligg til grunn for desse tenestene.

2.1 Nettet som berar av sluttbrukarinformasjon

Informasjon kan overførast over ein trådbasert eller trådlaus fysisk kanal mellom to sluttbrukarar, til dømes ved hjelp av to radioar. I dette tilfellet har kommunikasjonssystemet *to* nodar. Gitt at nodane er innanfor rekkevidda til kvarandre, må *ein* link opprettast og vedlikehaldast for at sluttbrukarane skal kunna kommunisera. Når linken er oppretta, skal systemet syta for å gje best

mogleg kvalitet så lenge kommunikasjonen mellom sluttbrukarane pågår. Dette kan til dømes dreia seg om å gjera linken mest mogleg stabil og krev mellom anna at systemet er i stand til både å gjenkjenna og å tilpassa seg skiftande naturlege tilhøve. Eit moderne kommunikasjonssystem har vanlegvis langt fleire sluttbrukarar. Gitt fysisk konnektivitet mellom nodane, er systemet i stand til å oppretta logiske nett på fleire kommunikasjonslag. I motsetning til det enkle systemet skissert over, vil eit system med mange nodar difor vera operativt *uavhengig* av om sluttbrukarane kommuniserer, og vil såleis "leva sitt eige liv". Eit stort system må for dei ulike kvalitetsparametrane vega yteevne og kostnader for *heile nettet* mot omsynet til den *einskilde* linken mellom to nodar, eller til den *einskilde* ruta mellom to sluttbrukarar i nettet.

I dette avsnittet ser me på viktige oppgåver eit kommunikasjonssystem skal utføra. Slike oppgåver vert ofte kalla nettfunksjonar eller nett-tenester. Ruting og tenestekvalitet er døme på *grunnleggjande* nett-tenester NbF målnett må tilby. Dette vil seia at tenestene må vera til stades for at systemet skal kunna brukast til militære formål. Tenestene er skildra meir detaljert i til dømes [84]. Grunnleggjande nett-tenester må vera *gjennomgåande*. Dette vil seia at dei må finnast i alle tre delar av NbF-nettet og vera interoperable. Vidare må dei vera interoperable med tilsvarande tenester i eksterne nett. Me går i det følgjande raskt gjennom nokre grunnleggjande nett-tenester i NbF målnett.

2.1.1 Konnektivitet

Full konnektivitet inneber at kvar node i nettet kan kommunisera med alle andre. Full konnektivitet på nettlaget føreset at nettet heng saman på fysisk lag og at linklaget opprettar og vedlikeheld tilstrekkeleg mange linkar. Ruting på nettlaget krev at alle nodar kan adresserast, og adressene må direkte eller indirekte vera tilgjengelege for alle. Full konnektivitet bør vera *mogleg*. Om full konnektivitet er *ønska* er eit spørsmål om policy og kan variera.

Eit minimumskrav vil vera å oppretthalda ein konnektivitetsgrad som sikrar at sluttbrukarane kan nå alle dei treng å kommunisera med for å utføra eit visst oppdrag. Krav til konnektivitet kan difor vera avgrensa til spesifikke nodar. I slike tilfelle vil omsyn til redundans og overlevingsevne påverka talet på nodar som skal omfattast av konnektivitetskravet.

Å oppretthalda naudsynt konnektivitet er størst utfordring i dei deployerbare og mobile delane av målnettet, men det er ei viktig oppgåve i fastnettet òg.

2.1.2 Ruting

Ruting går føre seg på nettlaget og dreier seg om å flytta data frå kjelde til destinasjon over eit nett. Langs vegen frå kjelde til destinasjon vil det typisk vera minst *ein* IP-ruter. Ein ruter kan setjast opp manuelt med *statiske* ruter til dei andre ruterane i nettet. *Dynamisk* ruting vert realisert ved hjelp av rutingprotokollar.

Ruterane treng informasjon om nettet for å ruta data korrekt og effektivt. Informasjonsutveksling mellom ruterane set dei i stand til å kalkulera logiske ruter og til å senda og vidaresenda trafikk i samsvar med desse rutene. Rutingprotokollane syter for at tilstrekkeleg informasjon vert utveksla.

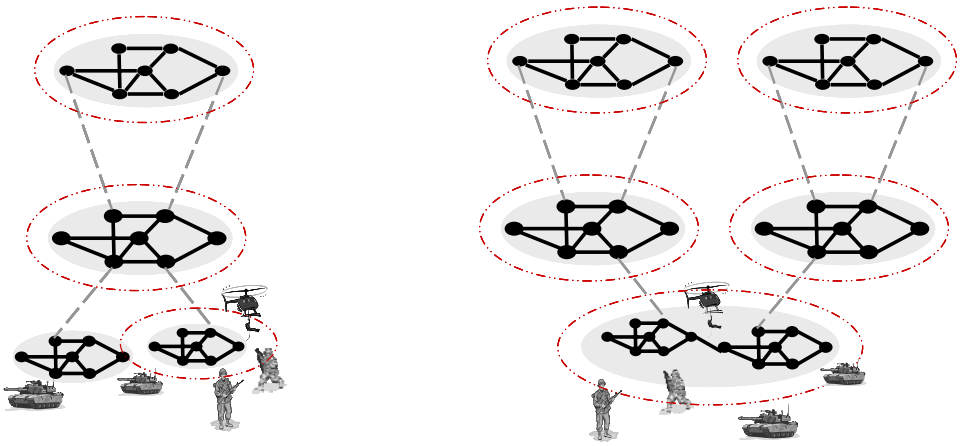
Protokollane er prosessessar som går i kvar ruter i nettet. Rutingprotokollar kan vera basert på ulike typar algoritmar. Effektive rutingalgoritmar har vore eit forskingsfelt sidan 1970-talet, men fekk kommersiell verdi først på midten av 80-talet då storskala IP-nett vart vanleg. Algoritmane nyttar ulike metrikkar (målbare og samanliknbare parametrar) for å kalkulera *optimale* ruter. Rutingalgoritmane er forma for ulike målsettingar, og kan klassifiserast etter ulike karakteristikkar. Rådande målsetting har vore å minimalisera talet på hopp frå kjelde til destinasjon. I seinare tid har ein lagt vekt på metrikkar som speglar rutekvaliteten, til dømes den tilgjengelege kapasiteten. Det er òg utvikla algoritmar som handterer ulike former for mobilitet. Dette gjeld så vel mobile endeterminalar i trådbaserte IP-nett som trådlause ad hoc-nett, der alle nettnodar flytter seg kontinuerleg. Likeeins går det føre seg mykje arbeid for å utvikla effektive protokollar for gruppekommunikasjon med multikastruting.

Den delen av eit nett som er underlagt felles retningslinjer for ruting vert i denne rapporten kalla r*utingdomene*. Ruterane innan eitt domene brukar ein og same rutingprotokoll. Gitt konnektivitet på lågare kommunikasjonslag, vil det vera full konnektivitet innan domenet. Eit anna liknande omgrep er *autonomt system* (*Autonomous System* (AS)). Eit AS er definert som ei gruppe av ruterar som utvekslar rutinginformasjon via ein felles rutingprotokoll [32]. Det globale internettet er inndelt i slike AS for å redusera global utveksling av rutinginformasjon og for å letta drifta av nettet.

Referansane [5] og [79] skisserer korleis NbF målnett kan organiserast i rutingdomene. Figur 2.2 syner korleis rutingdomene kan organiserast. Til venstre er ei løysing der den faste delen av nettet utgjer eitt rutingdomene, ein deployerbar del utgjer eit anna, medan eit trådlaust mobilt nett fungerer som eit tredje domene. Til høgre er ein variant der to mobile nett frå ulike nasjonar utgjer eitt rutingdomene. Nodar frå ulike nasjonar fungerer då som *eitt* IP-nett. Dette kan vera nyttig dersom nasjonane ikkje oppnår tilstrekkeleg konnektivitet ved hjelp av eigne nodar, eller dersom det er ynskjeleg at sluttbrukarar frå ulike nasjonar utvekslar informasjon direkte.

Einskilde rutingprotokollar opererer berre *innanfor* domene (intradomene), medan andre opererer *mellom* domene (interdomene). Referanse [79] går gjennom relevante sivile protokollar for både intradomene- og interdomeneruting. Dersom trafikken skal rutast gjennom alle delar av det framtidige nettet, må rutingprotokollane som vert nytta i dei ulike delane, vera interoperable. Sivile protokollar for intra- og interdomeneruting er interoperable. Desse protokollane er ueigna for mobile trådlause ad hoc-nett. Ruting i slike nett er eit aktivt forskingsområde. Førebels finns ingen standardar. Forskingsresultat så langt tilseier at representantar frå *ulike* kategoriar rutingprotokollar vil verta standardisert. Gode oversiktar over dei mest relevante rutingprotokollane finns i [89] og [9]. Dei viktigaste protokollkategoriane for ad hoc-nett er *proaktive* protokollar som kontinuerleg vedlikeheld ruter til alle andre nodar, dei *reaktive* som opprettar ei rute først når brukaren ber om det, dei *hierarkiske* som forenklar rutinga ved å utnytta nodeklynger som oppstår i nettet samt dei *geografiske* som sender pakkane i retning lokasjonen til destinasjonsnoden. Kva for kategori som er mest fordelaktig vil vera avhengig av gitt bruksscenarium. Nodane bør difor vera i stand til å operera under eit breitt spekter av protokollar. Så langt har forsking på ad hoc-ruting vore konsentrert om intradomene-ruting. Ruting mellom ad

hoc-nettdomene samt mellom ad hoc-nettdomene og domene i stasjonære nett er område der mykje er ugjort.



Figur 2.2 Døme på organisering av rutingdomene i NbF målnett

Gruppekommunikasjon er viktig i mange militære operasjonar. Kommunikasjonsnettet kan støtta slik kommunikasjon ved hjelp av multikastruting. For stasjonære nett finns det fleire protokollar for mulitkastruting, og ei rekkje protokollar er foreslått for ad hoc-nett. Eit logisk multikastnett kan byggjast opp og vedlikehaldast på ulike vis. For å vera effektivt, må eit slikt distribusjonsnett ta omsyn til organisatoriske tilhøve. Multikastgrupper må til dømes kunna opprettast, kombinerast, delast og oppløysast dynamisk. Dette kompliserer multikastruting samanlikna med ordinær unikastruting.

Dei vanlegaste rutingprotokollane i sivile stasjonære nett i dag er *Open Shortest Path First* (OSPF) *protocol* [32] for intradomene-ruting og *Border Gateway Protocol* (BGP) [66] for interdomene-ruting. Av protokollar som ligg langt framme i standardiseringsprosessen for ad hoc-ruting kan nemnast *Optimized Link State Routing* (OLSR) *protocol* [54], *Topology Based on Reverse Path Forwarding* (TBRPF) *protocol* [57] og *Wireless Open Shortest Path First* (W-OSPF) *protocol* [17], som alle er proaktive, og *Ad Hoc On Demand Distance Vector Routing* (AODV) *protocol* [53], *Dynamic MANET On-demand* (DYMO) *protocol* [18] *og Dynamic Source Routing* (DSR) *protocol* [28], som er velkjende reaktive protokollar. Berre W-OSPF er laga med tanke på interoperabilitet med rutingprotokollane i stasjonære nett.

2.1.3 Tenestekvalitet

Ulike typar trafikk har ulike krav med omsyn til prediktabel kvalitet. Dette kan uttrykkast som krav til datarate, tidsforseinking, jitter (variasjon i forseinkinga) og pakketap. Gitt knappe nettressursar er *best-effort*-tenesta som er standard i IP-nett, ikkje i stand til å tilfredsstilla denne typen krav. Kommersielle operatørar kan løysa problemet ved å syta for at nettressursane til ei kvar tid dekkar trongen. Dette er ikkje nokon farbar veg for Forsvaret. I dei trådlause delane av nettet, og særleg i dei mobile, vil ressursane alltid vera knappe. Dette gjeld i første rekkje

tilgjengeleg bandbreidde. Som ei følgje må NbF målnett vera i stand til å kontrollera tilgangen til ressursane, til å klassifisera påtrykt trafikk og til å handsama trafikklassane ulikt.

To standardarkitekturar er utvikla for faste IP-nett: *Integrated Services* (IntServ) [31] og *Differentiated Services* (DiffServ) [38]. IntServ brukar *Resource Reservation Protocol* (RSVP) [33] til å melda krav til nettelementa for så å reservera ressursar langs heile ruta. I tillegg til ordinær best-effort-teneste er to tenesteklassar definert. Den eine gir skrankar for ende-til-ende-forseinking, medan den andre garanterer skrankar for pakketap. Kvaliteten vert garantert per flyt, dvs per *Transmission Control Protocol* (TCP)-port. Dette gir ein granularitet som skalerer dårleg i store nett. For å unngå slike problem handterer DiffServ trafikken på basis av trafikkaggregat. Trafikken vert klassifisert ut frå *Per-Hop Behavior* (PHB) som spesifiserer trafikkhandtering per ruter. To typar PHB er spesifisert: Ein type legg vekt på forseinking, medan den andre skal sikra leveranse. Kvaliteten vert garantert per trafikk-klasse.

Referansane [5] og [79] skildrar korleis desse arkitekturane kan brukast og kombinerast i målnettet. Ei tilråding er å nytta IntServ med RSVP i kantnetta og for tenester som krev strenge kvalitetskrav, medan DiffServ kan nyttast i kjernenettet. Dersom tenestekvalitet skal vera gjennomgåande i det framtidige nettet, må relevante mekanismar finnast i alle delar av nettet, og dei må vera interoperable. Mest kritisk er tenestekvalitet i dei trådlause og mobile delane av nettet, der ressursane er knappast. I tillegg til å handtera den upålitelege og tidsvarierande radiokanalen skal desse mekanismane òg handtera ein nett-topologi som endrar seg dynamisk. Det er foreslått ei rekkje modellar inspirert av IntServ og DiffServ. Døme er *INSIGNIA* [80], *Stateless Wireless Ad hoc Networks* (SWAN) [1] og *Flexible QoS Model for Mobile Ad-Hoc Networks* (FQMM) [96]. Tenestekvalitet i mobile trådlause ad hoc-nett er eit nytt forskingsfelt, og mykje arbeid står att.

Vanlegvis er det *linklaget* som monitorerer kanalkvalitet og tilgjengeleg kapasitet. Å handtera tenestekvalitet lausrive frå *nettlaget*, kan føra til val av ineffektive ruter, og sannsynet for å oppnå ønska kvalitet kan verta redusert. Difor er det viktig at dei ulike rutingprotokollane kan ta omsyn til tenestekvalitetskrav. I motsetning til linklaget, har nettlaget oversyn over heile nettet og kan dermed ta globale omsyn. Overliggjande kommunikasjonslag må òg spela ein viktig rolle for å sikra at applikasjonane i størst mogleg grad får ønska kvalitetskrav innfridd. Tenestekvalitet er såleis ei fleirlagsoppgåve.

Handtering av krav om prioritet og forkøyrsrett (*pre-emption*) i nettet heng saman med evna til å differensiera tenestekvaliteten for ulike typar trafikk. Slike funksjonar er ikkje lagt vekt på i noverande sivile arkitekturar for tenestekvalitet i IP-nett. Den relativt låge kapasiteten i dei trådlause og mobile delane av målnettet tilseier at ein må handheva ein streng policy for prioritet og forkøyrsrett. Kva for informasjon som skal prioriterast, er avhengig av gitt bruksscenarium. Dessutan vil prioriteten kunna endra seg over tid. Difor bør denne tenesta kunna handterast dynamisk.

Den delen av eit nett som er underlagt felles retningslinjer for tenestekvalitet vert i denne

rapporten kalla *tenestekvalitetsdomene.* Eit tenestekvalitetsdomene kan, men treng ikkje, svara til eit rutingdomene. For å sikra gjennomgåande tenestekvalitet mellom ulike domene kan ein bruka *Service Level Agreements* (SLAs). I kommersielle nett der kunden betaler for tenestekvalitet, finns slike avtalar mellom nettoperatør og kunde eller mellom ulike nettoperatørar [55]. Mogleg bruk av SLA i taktiske nett er skildra i [92].

2.1.4 Sikkerhet

Nettet må kunna tilby sikker overføring av sluttbrukarinformasjon. I tillegg må nettet kunna syta for at nett-tenester som ruting og tenestekvalitet er sikre, dvs at nettinformasjonen vert overført, prosessert og lagra på ein sikker måte. Alle delar av nettet må tilby sikkerhetstenester slik at gjeldande policy for konfidensialitet, integritet og tilgjenge kan handhevast. Så vel sluttbrukarinformasjon som nettinformasjon kan sikrast av applikasjonane sjølve og/eller på eitt eller fleire kommunikasjonslag. *International Telecommunication Union – Telecommunication Standardization Sector* (ITU – T) spesifiserer ei rekkje tenester for konfidensialitet, integritet og tilgangskontroll. I tillegg vert mekanismar som kan implementera desse tenestene på ulike kommunikasjonslag, spesifisert [12]. For IP-nett har IETF spesifisert ei rekkje tenester, først og fremst på nettlaget. Dei viktigaste vert gjennomgått i kapittel 5. I IPv6 vil *Security Architecture for the Internet Protocol* (IPSec) [67] vera obligatorisk, og mange eksisterande spesifikasjonar og løysingar vil falla bort. Under Ipv6 vil IPSec mellom anna kunna brukast til å sikra data ende til ende på *nettlaget*. Ein annan, og kanskje motstridande trend er å lata *mellomvare* ta seg av ende-til-ende-sikring på eit høgare kommunikasjonslag. Mellomvare kan operera på vegne av alle applikasjonar, og ei slik løysing vil dermed erstatta applikasjonsspesifikke sikkerhetstenester.

IPv6 legg opp til at nett-tenester som ruting skal sikrast ved hjelp av IPSec. Dette vert gjennomgått i kapitla 5 og 6. Dersom nettinformasjonen skal delast inn i fleire sikkerhetsnivå, vil det vera ei utfordring å få til effektive nett-tenester. Spørsmålet vert drøfta i kapittel 3. Vidare vil det vera ei utfordring å sikra nett-tenestene når desse samstundes skal vera interoperable med tilsvarande tenester i eksterne nett, og når eitt og same kommunikasjonsnett omfattar ulike nasjonar. Mellom nasjonane finns dessutan sikkerhetsdomene som kan vera bi- eller multilaterale.

Den delen av eit nett som er underlagt den same sikkerhetspolicyen vert i denne rapporten kalla *sikkerhetsdomene.* Eit sikkerhetsdomene kan, men treng ikkje, svara til eit rutingdomene.

2.1.5 Drift og styring

Drift og styring av eit kommunikasjonssystem (*network management*) kan ikkje kallast ei nett-teneste. Mange reknar ruting og handtering av tenestekvalitet som ein del av den allmenne styringa av eit nett. Drift og styring vert utført av særeigne applikasjonar som handterer informasjon om nettet. Slike applikasjonar er avhengige av meir omfattande informasjon enn den som gjeld dei spesifikke nett-tenestene som vert tilbydd sluttbrukarane. For å vera styrbart må nettet difor vera i stand til å levera og motta informasjon frå drift- og styringsapplikasjonar. For stasjonære nett er slike applikasjonar per i dag sentraliserte. Sivile standardar delar vanlegvis drift og styring inn i fem funksjonsområde: feilhandtering, bruksregistrering, konfigurasjon, yteevne og sikkerhet [11]. Etter det me kjenner til finns ikkje drift- og styringssystem for mobile trådlause

ad hoc-nett. Det er heller ikkje forska mykje på dette feltet. Kva som er mogleg og ynskjeleg å overvaka og styra i slike nett, er ikkje opplagt. Den korte levetida til desse netta reduserer dessutan trongen for denne typen applikasjonar. Standardar for drift og styring er gjennomgått i [95], som òg drøftar sikringa av kommunikasjonsprotokollane mellom nettelementa og applikasjonen.

2.1.6 Kommentarar

Me har i dette avsnittet sett på viktige nett-tenester i IP-nett. Lista er langt frå fullstendig. Formålet har vore å syna at slike tenester er basert på tilstandsinformasjon om sjølve nettet. Rutingfunksjonalitet krev informasjon om topologien i nettet. Er protokollen basert på geografiske posisjonar, krevs lokasjonsinformasjon. Multikastruting krev informasjon om grupper og ruter. Tenestekvalitetsfunksjonalitet krev informasjon om effektiv datarate på linkane, om trafikkavviklinga i nettet og om gjeldande policy for sjølve tenesta. Sikkerhetstenester krev som regel hemmelege nøklar og anna informasjon knytt til ulike typar protokollar. Tilgangskontroll til nettressursane krev informasjon knytt til autentisering og autorisasjon. Drift- og styringsapplikasjonar krev at nettet genererer og leverer informasjon om dei fysiske nettelementa, om dei logiske netta, om fysisk og logisk konfigurasjon, om all funksjonalitet som skal overvakast og/eller styrast, samt om trafikken over dei ulike grensesnitta i nettet. I neste avsnitt skal me sjå på korleis nettet handterer denne informasjonen.

2.2 Nettet som informasjonssystem

Det enkle punkt-til-punkt-kommunikasjonssystemet nemnd i avsnitt 2.1 utvekslar nettinformasjon for å vedlikehalda linken mellom dei to nodane. Nettinformasjonen er enkel og oversiktleg og har ei levetid som samsvarar med tidsperioden dei to sluttbrukarane kommuniserer. I eit større kommunikasjonssystem som NbF målnett, vil nettinformasjon som ikkje er knytt til ein spesifikk pågåande sesjon, verta utveksla, prosessert og lagra *uavhengig* av om sluttbrukarar kommuniserer.

Eit kommunikasjonssystem som NbF målnett vil vera eit stort distribuert informasjonssystem. Rutingprotokollar er prosedyrar for utveksling, prosessering og lagring av informasjon om tilstanden i nettet. Protokollar og mekanismar for tenestekvalitet føreset òg at nettinformasjon vert utveksla, prosessert og lagra. Ulike protokollar og mekanismar krev ulik informasjonsmengde for at den aktuelle tenesta skal fungera tilfredsstillande. Protokollane skil seg òg med omsyn til distribusjon av nettinformasjonen. *Ein* node kan ha *all* informasjon om heile nettet, medan resten av nodane inneheld svært lite. Andre løysingar føreset at *alle* nodar har *delvis* informasjon om heile nettet. Ulike konsept kan eksistera i eitt og same kommunikasjonssystem. Delar av NbF målnett vil ha ein hierarkisk struktur medan andre delar kan ha ein flat. Delar av nettet vil ha ein fysisk infrastruktur, medan andre delar opererer utan slik infrastruktur. Saman med gjeldande domeneorganisering for ruting, tenestekvalitet og sikkerhet, vil dette påverka distribusjonen av nettinformasjon. I dette avsnittet føreset me at kvar node prosesserer og lagrar noko informasjon om nettet utanfor eigne domene. Noden vil ha langt meir informasjon om nettet som ligg innanfor dei respektive domena og i mange tilfelle svært detaljert informasjon om dei nærmaste

nabonodane. Vidare føreset me at kvar node utvekslar nettinformasjon med alle andre nodar innan eit domene, medan einskilde nodar utvekslar slik informasjon på tvers av domenegrenser.

2.2.1 Utveksling av nettinformasjon

Nodane utvekslar nettinformasjon først og fremst ved hjelp av ulike protokollar. Protokollane spesifiserer eit sett av meldingar. Meldingsformatet inneheld som regel eit meldingshovud som er felles for alle meldingstypar, og ein meldingskropp som er spesifikk for kvar meldingstype. Heile protokollmeldinga kan leggjast som nyttelast ei TCP-melding eller ei *User Datagram Protocol* (UDP)-melding som i sin tur vert nyttelast i ein IP-pakke. Protokollane kan skiljast med omsyn til meldingsdistribusjon, meldingsstorleik og meldingsfrekvens:

- *Distribusjon:* Protokollmeldingar kan kringkastast, multikastast eller unikastast. Innan ein protokoll vil distribusjonsreglar vera spesifisert for kvar meldingstype. I tilfelle kringkasting, kan det vera restriksjonar med omsyn til vidaresending: Skal meldinga i det heile vidaresendast og kven av nabonodane skal i så fall vidaresenda. Nokre meldingstypar krev kvittering frå mottakar, medan andre ikkje gjer det
- *Meldingsstorleik:* I praksis indikerer meldingsstorleiken informasjonsmengda som vert overført. Innan ein protokoll kan dette kan variera sterkt frå meldingstype til meldingstype. Det er òg stor skilnad mellom protokollar som er forma for faste nett og protokollar som er forma for trådlause nett. I det siste tilfellet har ein ofte ha lagt vekt på å gjera meldingane små
- *Meldingsfrekvens:* Protokollane sender ut meldingar periodisk (klokkestyrt) eller når spesifiserte hendingar oppstår i noden. Dette indikerer at meldingsfrekvensen vil kunna variera sterkt frå protokoll til protokoll og frå meldingstype til meldingstype innan ein og same protokoll. I mobile nett der topologien endrar seg dynamisk, må meldingsfrekvensen ofte vera høg for å sikra at nodane heile tida har eit mest mogleg korrekt bilete av gjeldande topologi.

Meldingsdistribusjon, meldingsstorleik og meldingsfrekvens avgjer omfanget av nettinformasjon. Ulike nett med ulik systemarkitektur vil ha ulik evne til å overføra nettinformasjon.

2.2.2 Prosessering av nettinformasjon

Nodane prosesserer nettinformasjonen i samsvar med protokollar eller andre spesifikasjonar. Inndata til prosessering vil vera informasjon generert av noden sjølv og/eller informasjon motteken frå andre nodar i nettet. Utdata vil verta lagra i noden og/eller sendt ut til andre nodar i nettet. Døme på prosessering er kalkulasjon av rutingtabell. Inndata er informasjon motteken frå andre nodar. Utdata vil verta lagra i noden sjølv, og avhengig av rutingprotokoll, vil delar av dette verta distribuert til andre nodar. Eit anna døme på prosessering er tilgangskontroll av trafikk som krev ein viss kvalitetsklasse. Ulike typar nodar vil ha ulik kapasitet og evne til prosessera nettinformasjon.

2.2.3 Lagring av nettinformasjon

Nodane har ei rekkje databasar der nettinformasjon er lagra. Rutingtabellane er eitt døme på slike databasar. Rutingprokollane vedlikeheld ofte mange andre databasar som inneheld lokal og global topologiinformasjon. Eit anna døme er dei mange databasane som inneheld drift- og

styringsinformasjon om noden. Einskilde protokollar lagrar ikkje motteken informasjon i det heile, men nyttar han direkte i ei tilbakekoplingssløyfe. SWAN er eit døme på dette, sjå avsnitt 2.1.3. Ulike typar nodar vil ha ulik kapasitet og evne til lagra nettinformasjon.

2.2.4 Kommentarar

Utan utveksling, prosessering og lagring av nettinformasjon, vil eit moderne kommunikasjonssystem ikkje fungera effektivt;- det vil ikkje fungera i det heile. Difor er nettinformasjonen i NbF målnett ein kritisk del av informasjonsinfrastrukturen til Forsvaret.

I den sivile verda er det nettoperatøren sitt ansvar å handtera og forvalta nettinformasjonen. For ein sluttbrukar artar nettinformasjonen seg som uønska *overhead* som konkurrerer med sluttbrukarinformasjonen om nettressursane. For nettoperatøren er det viktig å redusera omfanget av nettinformasjonen for å betra yteevna til nettet. I NbF målnett vil det vera viktig å redusera omfanget av nettinformasjon, særleg i dei mobile trådlause delane av nettet. Som me skal sjå i kapittel 3, er dette òg eit spørsmål om å sikra nettet best mogleg.

3 Grunnlag for sikre nett-tenester

NbF målnett vert eit stort distribuert informasjonssystem der informasjonen må sikrast. Dette kapittelet går først gjennom nokre grunnleggjande aspekt ved sikring av nettinformasjon. For å konkretisera problemstillingane syner me to konkrete døme før me diskuterer sider ved den framtidige sikkerhetspolicyen for nettinformasjon.

3.1 Allment om sikre nett-tenester

I dette avsnittet føreset me at det finns ein *sikkerhetspolicy* for nettinformasjon og nett-tenester. Ein slik policy spesifiserer krava som skal gjelda og kva som skal vera lov og ikkje lov med omsyn til informasjon og tenester. Dette handlar om kva for rettar subjekt som sluttbrukarar, applikasjonar og prosessar har over objekt som filer, databasar og nett-tenester. Rettane kan til dømes uttrykkast som les, skriv, opprett og slett. Me føreset at det finns ein policy for kvart av dei tre aspekta *konfidensialitet*, *integritet* og *tilgjenge* og ser på kva dette vil ha å seia for utveksling, prosessering og lagring av nettinformasjon.

Det er viktig å handtera aspekta *konfidensialitet*, *integritet* og *tilgjenge* kvar for seg. At ein og same *sikkerhetsmekanisme* kan understøtta meir enn eitt sikkerhetsaspekt, impliserer *ikkje* at desse tre aspekta er innbyrdes avhengige. Til dømes kan ein oppnå konfidensialitet ved å kryptera alt alle stader. Som *indirekte biprodukt* vil ein då kunna få ein viss grad av integritetsverifikasjon for informasjon *som er leseleg for menneske*, men dette betyr ikkje at komponentane konfidensialitet og integritet er innbyrdes avhengige. I denne rapporten handterer me dei tre grunnleggjande eigenskapane konfidensialitet, integritet og tilgjenge som tre *innbyrdes uavhengige* komponentar. Ved fleirnivå sikkerhet kan ein då handtera tre *uavhengige* dimensjonar. Me skal syna at dette opnar for meir fleksible løysingar samstundes som ein ivaretek krav om ein konsistent og verifiserbar sikkerhetspolicy.

3.1.1 Konfidensialitet

Konfidensialitet inneber at informasjon ikkje vert avdekka for ikkje-autoriserte entitetar [45]. Komponenten *konfidensialitet* er uavhengig av komponentane *integritet* og *tilgjenge*. Allment kan nettinformasjon avsløra mykje om topologien til nettet, elementa som utgjer nettet og om organisasjonen som nyttar det [95]. Avdekka nettinformasjon kan til dømes forenkla trafikkanalyse.

Ein *konfidensialitetspolicy* for nettinformasjon vil spesifisera krava som skal gjelda for ulike typar informasjon i ulike nett. Ut frå denne policyen må det definerast tenester som skal verna informasjonen mot ikkje-autorisert innsyn. *Ein* vanleg mekanisme for å handheva ein konfidensialitetspolicy er kryptering.

Dersom nettinformasjonen skal underleggjast konfidensialitetskrav, må desse krava omfatta utveksling, prosessering og lagring av informasjonen. I motsetning til sluttbrukarinformasjon, vert

nettinformasjon prosessert og lagra i kvar node i nettet. Dette inneber at kvar node må vera i stand til å handheva dei konfidensialitetskrava som gjeld for gitt type informasjon, i gitt type nett og i gitt bruksscenarium.

Dersom nettinformasjon skal graderast til ulike konfidensialitetsnivå etter same mal som sluttbrukarinformasjonen, vil dette få konsekvensar for informasjon i transitt så vel som for prosessering og lagring i nodane. Tabell 3.1 syner eit døme på ein enkel fleirnivå konfidensialitetspolicy. I dette dømet brukar me tre nivå: *høg*, *låg* og *ugradert*. (Høg og låg kan gjerne relaterast til skiftevis Hemmelig og Begrenset.) I dette dømet er rutingprotokollane subjekt, og rutinginformasjonen er objekt. Alle subjekt og alle objekt er tildelt sikkerhetsnivå, og konfidensialitetspolicyen regulerer kva for rettar subjekta har til å lesa og skriva til objekta. Dømet syner lese- og skriverettar tildelt på tradisjonelt vis [3]: Policyen tillet subjekta å lesa objekt på same eller lågare konfidensialitetsnivå. Rett til å lesa objekt på høgare konfidensialitetsnivå ville avdekka høgt graderte objekt for subjekt på lågt nivå. Subjekta kan skriva til objekt på same eller høgare konfidensialitetsnivå. Rett til å skriva til objekt på lågare konfidensialitetsnivå ville medføra informasjonsflyt frå høgt nivå til lågt nivå. Dette ville vera å avdekka høgt graderte objekt for subjekt på lågt nivå.

Objekt: / *Subjekt:*	Rutinginfo-Ugradert	Rutinginfo-Låg	Rutinginfo-Høg
Rutingprotokoll-Høg	Les	Les	Les, Skriv
Rutingprotokoll-Låg	Les	Les, Skriv	Skriv
Rutingprotokoll-Ugradert	Les, Skriv	Skriv	Skriv

Tabell 3.1 Døme på konfidensialitetspolicy for rutinginformasjon

3.1.2 Integritet

Integritet inneber at informasjonen kjem frå ei kjelde ein har tillit til, og at informasjonen deretter ikkje er endra, øydelagt eller tapt på ikkje-autorisert vis. Implisitt vil dette seia at informasjonen er korrekt og konsistent [45]. Komponenten *integritet* er uavhengig av komponentane *konfidensialitet* og *tilgjenge*.

Ein *integritetspolicy* for nettinformasjon vil spesifisera kva for krav som skal gjelda for ulike typar informasjon i ulike nett. Som konfidensialitetspolicyen vil integritetspolicyen spesifisera kva for rettar subjekta har over objekta, men i dette tilfellet ut frå omsynet til integritet. Ut frå policyen må det til dømes definerast tenester som skal verifisera at ei informasjonskjelde er den ho gir seg ut for å vera og at motteken informasjon ikkje er modifisert på ikkje-autorisert vis. Ein vanleg mekanisme for kjelde-autentisering er digitale signaturar. Til å verifisera at data ikkje er modifisert vert vanlegvis ulike *hash*-teknikkar brukt, gjerne saman med hemmelege nøklar.

Dersom nettinformasjonen skal underleggjast integritetskrav, må desse omfatta utveksling, prosessering og lagring av informasjonen. Sidan nettinformasjon vert utveksla, prosessert og lagra

i kvar node i nettet, må kvar node vera i stand til å handheva integritetskrav for gitt type informasjon, i gitt type nett og i gitt bruksscenarium.

Dersom nettinformasjonen skal graderast til ulike integritetsnivå, vil dette få konsekvensar for informasjon i transitt så vel som for prosessering og lagring i nodane. Tabell 3.2 syner eit døme på ein fleirnivå integritetspolicy for dei same subjekta og objekta som synt i Tabell 3.1. Subjekta har lese- og skriverettar på tradisjonelt vis her òg [3]: Policyen tillet subjekta å lesa objekt på same eller høgare integritetsnivå. Rett til å lesa objekt på lågare integritetsnivå ville minka integriteten til høgt graderte subjekt. Subjekta kan skriva til objekt på same eller lågare integritetsnivå. Rett til å skriva til objekt på høgare integritetsnivå ville medføra informasjonsflyt frå lågt til høgt nivå. Dette ville vera å minka integriteten til høgt graderte objekt.

Objekt: / *Subjekt:*	Rutinginfo-Ugradert	Rutinginfo-Låg	Rutinginfo-Høg
Rutingprotokoll-Høg	Skriv	Skriv	Les, Skriv
Rutingprotokoll-Låg	Skriv	Les, Skriv	Les
Rutingprotokoll-Ugradert	Les, Skriv	Les	Les

Tabell 3.2 Døme på integritetspolicy for rutinginformasjon

Dersom policyane for skiftevis konfidensialitet og integritet graderer subjekt og objekt etter same kriterium, ser me at dei to policyane er duale: Policyane utliknar kvarandre slik at alle kan lesa alt. Problemet kan løysast enkelt, men lite fleksibelt, ved at subjekta har rettar *berre* til objekt på same nivå som subjektet.

Dersom ein ser konfidensialitet og integritet som to ulike dimensjonar, kan ein bruka *ulike* kriterium når ein graderer for skiftevis konfidensialitet og integritet. Då ville graderingsnivåa Høg og Låg ha *eitt* innhald i Tabell 3.1 og eit *anna* i Tabell 3.2. Me kjem attende til dette i avsnitt 3.3.

3.1.3 Tilgjenge

Tilgjenge inneber at systemet (eller ein spesifikk systemressurs) kan aksesserast, er brukbart eller er operasjonelt i samsvar med spesifikasjonane på forespørsel frå ein autorisert systementitet. Eit system er såleis tilgjengeleg dersom det tilbyr tenester i samsvar med systemspesifikasjonane når autoriserte brukarar ber om det [45]. Omgrepet har to aspekt: Å sikra at autoriserte har best mogleg tilgjenge *og* å sikra at ikkje-autoriserte vert avvist. Komponenten *tilgjenge* er uavhengig av komponentane *konfidensialitet* og *integritet*.

Ein *tilgjengepolicy* for nettinformasjon spesifiserer kva for krav som må tilfredsstillast for at ulike typar informasjon og tenester skal vera tilgjengelege for autoriserte. Eit naudsynt grunnlag er god drift og styring. Kontroll av nettressursane krev først og fremst ei god løysing for aksess-kontroll. Ulike mekanismar kan nyttast. Nett-tenester vert i prinsippet tilbydd av kvar node i nettet. Dette

inneber at kvar node må vera i stand til å handheva tilgjengekontroll for gitt type informasjon, i gitt type nett og i gitt bruksscenarium.

Tilgjenge kan definerast for ulike systemaspekt. Dersom tilgjenge skal graderast, kan dette difor gjerast langs fleire "aksar". Det kan mellom anna vera ulike nivå med omsyn til oppetid, akseptabel nedetid, restriksjonar på bruk av ressursen, tilgjenge til kvalitetsklassar og til prioritet. Tabell 3.3 syner eit døme på ein fleirnivå tilgjengepolicy for ei applikasjonsteneste. I denne policyen er nivåa *høg* og *låg* knytt til korkje konfidensialitet eller integritet, men uttrykker ulike kvalitets- og prioritetsnivå som nettet kan tilby ein generisk sluttbrukar som spør etter tenesta.

Me føreset at policy for tilgjenge regulerer kva for kvalitetskrav subjekta har lov å be om for dei ulike tenestene, samt kva for prioritet dei har lov å krevja. I dette dømet føreset me at subjekta er sluttbrukarar med ulike *rollar* og at det er *rollane* som er autoriserte for ulike nivå av tilgjenge til ei spesifikk teneste.

Objekt: / *Subjekt:*	Applikasjonsteneste X			
	Allment tilgjenge	Forseinkingsgaranti	Leveringsgaranti	Prioritet
Lagførar	Høg	Høg	Høg	Høg
Soldat	Høg	Låg	Høg	Låg

Tabell 3.3 Døme på tilgjengepolicy for ei applikasjonsteneste

Me skal i det følgjande gå gjennom to praktiske døme og diskutera kva policy på desse tre områda vil seia i praksis.

3.2 Krav til konfidensialitet, integritet og tilgjenge, to døme

I dette avsnittet går me gjennom to praktiske døme på kva konfidensialitet, integritet og tilgjenge vil seia for utveksling, prosessering og lagring av nettinformasjon. Det første dømet gjeld rutinginformasjon. Her ser me på konfidensialitet og integritet. I det andre dømet ser me på tilgjenge til ei applikasjonsteneste der nettet tilbyr ulike tenestekvalitetsklassar og prioritet for autoriserte brukarar. I diskusjonen om fleirnivå-policy brukar me Tabell 3.1, Tabell 3.2 og Tabell 3.3. Problemstillingane er relevante for alle delar av NbF-nettet, men sidan utfordringane er størst i dei høgmobile netta, tek me eit mobilt trådlaust ad hoc-nett som utgangspunkt.

3.2.1 Rutinginformasjon

Introduksjon. Ein rutingprotokoll er implementert i kvar node og føreset i utgangspunktet at kvar implementasjon kan *lesa* rutinginformasjon frå alle samarbeidande implementasjonar innan rutingdomenet. Å *lesa* informasjon frå ein annan implementasjon inneber *å gjera bruk* av denne informasjonen, til dømes ved å kopiera eller prosessera informasjonen for *skriving* til eigne databasar. Dette vil seia at kvar protokoll-implementasjon er ansvarleg for å byggja opp og vedlikehalda sin eigen rutinginformasjon på basis av informasjonen han mottek frå andre

implementasjonar.

For at problemstillingane me ser på skal gjelda både eksisterande rutingprotokollar i stasjonære nett og fleire protokollkategoriar i ad hoc-nett, føreset me *proaktiv* ruting. Kvar node har då nok informasjon til å kalkulera ruter til alle andre nodar, gitt full konnektivitet i nettet. Desse rutene vert lagra i rutingtabellen til protokoll-implementasjonen. Både lokal og global informasjon trengs for å halda rutingtabellen så korrekt som mogleg. Noden utvekslar lokal informasjon med nabonodane ved hjelp av ein meldingstype som me kallar *lokale meldingar*. (I mange protokollar er dette kalla *Hallo-meldingar*). Lokale meldingar set noden i stand til å identifisera andre nodar i nabolaget og å oppretta linkar til desse. Delar av den lokale informasjonen vert spreidd til alle nodar i nettet. Denne globale informasjonen vert utveksla ved hjelp av ein meldingstype som me kallar *globale meldingar*.

Utveksling av rutinginformasjon. Protokoll-implementasjonane som skal ta del i eit rutingdomene må i utgangspunktet vera i stand til å *lesa* protokollmeldingane frå alle andre autoriserte implementasjonar. Dersom rutinginformasjonen skal vernast mot ikkje-autorisert innsyn, må i praksis protokollmeldingane krypterast. Ein *symmetrisk* krypteringsalgoritme inneber at same nøkkelen vert brukt til både kryptering og dekryptering. I prinsippet er det to måtar å organisera dette på: Kvar implementasjon har ein nøkkel felles med kvar einskild av dei andre, eller alle implementasjonane i domenet har *ein* felles nøkkel, ein *gruppenøkkel*. Ein *asymmetrisk* krypteringsalgoritme inneber at sendar krypterer rutingmeldingane med mottakar sin offentlege nøkkel, og mottakar dekrypterer med sin private nøkkel. Dette vert organisert ved at kvar implementasjon har ein privat og ein offentleg nøkkel samt dei offentlege nøklane til alle andre implementasjonar i domenet.

Ein fleirnivå konfidensialitetspolicy av typen synt i Tabell 3.1 skal hindra at høgt gradert rutinginformasjon vert avdekka for lågare graderte protokoll-implementasjonar. Det må sikrast at implementasjonar på lågt nivå ikkje kan lesa rutinginformasjon frå implementasjonar på høgt nivå, og at implementasjonar på høgt nivå ikkje kan skriva rutinginformasjon til implementasjonar på lågt nivå. Å handheva dette ved hjelp av kryptering, vil i utgangspunktet krevja eigne nøklar for kvart sikkerhetsnivå. Det kan vidare vera eit krav at sikkerhetsnivåa skal bruka ulike krypteringsalgoritmar.

Ein integritetspolicy vil krevja at protokoll-implementasjonane som skal ta del i rutingdomenet er i stand til å verifisera at meldingskjelda (meldingsoriginatoren) er den ho hevdar å vera. Dette vil i praksis krevja autentisering av kjelda. Kjelde-autentisering krev at kjelda kan identifisera seg som autorisert på ein måte som kan verifiserast av destinasjonen. Det er i prinsippet to ulike måtar å organisera dette: Dersom det ikkje er naudsynt å verifisera kjelda som anna enn ”autorisert medlem” vil det kunna vera tilstrekkeleg å til dømes prova kjennskap til ein symmetrisk gruppenøkkel som er felles for rutingdomenet. Er det eit krav at kjelda skal identifiserast spesifikt, kan i utgangspunktet digitale signaturar basert på eit asymmetrisk offentleg-nøkkel-system vera ei løysing.

I tillegg til å verifisera at meldingsskjelda er den ho hevdar å vera, må destinasjonen kunna verifisera at meldinga ikkje er endra på ikkje-autorisert vis etter at kjelda sende ho. Ei vanleg og effektiv løysing er å nytta ein hash-funksjon til å laga eit "fingeravtrykk" av meldinga. Kjelda signerer så fingeravtrykket og sender det saman med meldinga.

Ein fleirnivå integritetspolicy av typen synt i Tabell 3.2 skal hindra høgt graderte protokoll-implementasjonar i å lesa lågt gradert rutinginformasjon. Av praktiske omsyn kan ikkje dette sikrast ved å hindra protokoll-implementasjonar på høgt nivå i å lesa rutingmeldingar frå lågt nivå: I eit kommunikasjonsnett vil mottakarane ikkje vita kven som er kjelda før dei har lese meldingshovudet og autentisert kjelda. For å ivareta integriteten til høgt gradert rutinginformasjon, vil det difor truleg vera meir tenleg å tolka det å *lesa* informasjon som det å *gjera bruk* av informasjon. Restriksjonane må dermed gjelda for *prosessering* av informasjonen snarare enn for *utveksling* av informasjon.

Prosessering av rutinginformasjon. Prosessering av rutinginformasjon går som nemnd føre seg i alle ruterar i domenet. Dersom rutingmeldingane er krypterte, må mottakarane dekryptera dei før prosessering. Konfidensialitetskrav til rutinginformasjonen impliserer at prosessering av *ukrypterte* meldingar må sikrast i kvar node.

Berre implementasjonar med gyldig nøkkel vil kunna dekryptera og prosessera meldingane. I følgje fleirnivåpolicyen frå Tabell 3.1 vil protokoll-implementasjonar på lågt nivå ikkje kunna prosessera meldingar frå høgt nivå, medan implementasjonar på høgt nivå kan prosessera meldingar frå lågt nivå. Ut frå *konfidensialitets*krava er det dermed ikkje noko i vegen for at protokoll-implementasjonar på høgt nivå kan bruka rutinginformasjon frå lågare graderte implementasjonar når dei kalkulerer rutetabell. Dette medfører at høgt graderte rutingtabellar kan innehalda ruter til nodar med lågt graderte eller ugraderte implementasjonar, medan ingen rutetabellar kan ha ruter til nodar med høgare graderte implementasjonar.

Resultat av kjelde-autentisering og verifisering av at meldinga ikkje er endra på ikkje-autorisert vis må avgjera om meldinga inneheld gyldige inndata for til dømes kalkulasjon av rutingtabell. Integritetspolicyen frå Tabell 3.2 vil hindra protokoll-implementasjonar på høgt nivå i å prosessera og dermed *gjera bruk av* lågt gradert rutinginformasjon, medan ein implementasjon på lågt nivå kan prosessera høgare graderte meldingar. Ut frå *integritetskrava* er det såleis ikkje noko i vegen for at protokoll-implementasjonar på lågt nivå kan nytta rutinginformasjon frå høgare graderte nodar når dei kalkulerer til dømes rutetabell. Dette medfører mellom anna at lågt graderte rutingtabellar kan innehalda ruter til nodar med høgare graderte implementasjonar, medan ingen rutetabellar vil ha ruter til nodar med lågt graderte og ugraderte implementasjonar.

Me såg her eit døme på at policyane for skiftevis konfidensialitet og integritet er duale dersom ein brukar dei same sikkerhetsnivåa når ein graderer. Konsistens vil krevja at protokoll-implementasjonar har rettar *berre* i høve til rutinginformasjon på same sikkerhetsnivå og kan dermed ikkje prosessera andre meldingar enn dei som kjem frå implementasjonar på same nivå. Me ser nærmare på dette i avsnitt 3.3.

Lagring av rutinginformasjon. Ein protokoll-implementasjon lagrar prosessert informasjon i ulike databasar for lokal og global topologiinformasjon. Desse kan til dømes innehalda informasjon om linkane til nabonodar eller vera globale rutetabellar. I stasjonære nett med forholdsvis statisk nett-topologi vil denne informasjonen ikkje endra seg ofte. I mobile nett, derimot, vil informasjonen verta vaska ut heile tida og er difor gyldig berre for eit kort tidsrom.

Vanlegvis tenkjer ein seg at protokollen i eit rutingdomene er implementert på geografisk spreidde nodar, og at ein protokoll-implementasjon ikkje kan lesa rutinginformasjon frå andre implementasjonar på anna vis enn ved å lesa rutingmeldingane frå dei. Det kan òg tenkjast at fleire protokoll-implementasjonar er implementert på same node. I så fall må informasjonsflyt mellom dei regulerast av policy. Dersom det er konfidensialitetskrav til rutinginformasjonen, må desse òg gjelda når informasjonen er lagra. Skal rutinginformasjonen krypterast ved utveksling, bør han i prinsippet òg krypterast ved lagring. Integritetskontroll av mottekne meldingar vernar mot meldingsbasert informasjonsmanipulasjon, men det vernar ikkje mot direkte åtak på lagra rutinginformasjon og sjølvsagt heller ikkje mot ikkje-autorisert informasjonsflyt frå andre implementasjonar på same node. Policy for konfidensialitet og integritet må difor gjelda òg for lagra informasjon.

3.2.2 Bruk av applikasjonstenester, tenestekvalitet og prioritet

Introduksjon. I forrige avsnitt såg me på konfidensialitet og integritet for rutinginformasjon. Dei same problemstillingane er gyldige for kvalitetsinformasjon òg. Ikkje-autorisert tilgang til denne typen informasjon vil til dømes kunna avdekka kvar i nettet eit åtak vil ha stor effekt. I dette avsnittet let me konfidensialitet og integritet liggja og ser i staden på tilgjenge-aspektet; ein tilgjenge-policy til ei applikasjonsteneste som synt i Tabell 3.3.

Eit tenesteorientert nett vil tilby sluttbrukaren ulike applikasjonstenester, til dømes tale, epost, sertifikat-server eller bruk av ulike informasjonsbasar. Applikasjonstenestene krev i sin tur at nettet er i stand til å levera eit sett av nett-tenester som ikkje nødvendigvis er synlege for sluttbrukar.

For i det heile å kunna bruka ei teneste, må sluttbrukar kunna finna ho. Eit stasjonært nett vil i høg grad kunna garantera dette. Eit mobilt trådlaust nett vil ikkje på same måte kunna garantera tilgang til ei teneste, sjølv om tenesta er lokalisert innanfor rutingdomenet. Gitt at nettet er i stand til å tilby allmenn tilgang til tenesta (konnektivitet, ruting), vil det òg vera eit krav at nettet kan tilby differensiert kvalitet. Eksisterande arkitekturar for tenestekvalitet tilbyr vanlegvis ulike klassar av forseinkingsgaranti basert på tilgjengeleg bandbreidde ende til ende. Forseinkinga skal vera under spesifiserte grenser. I tillegg tilbyr dei ulike klassar av leveringsgaranti, der pakketapet må vera under spesifiserte grenser. Skal eit IP-nett kunna tilby kvalitet utover standard *best-effort*, må informasjon om kvaliteten på linkar og ruter utvekslast, prosesserast og lagrast av alle nodar, eller av ei delmengd.

Ein tilgjengepolicy som synt i Tabell 3.3, kan regulera kven som skal ha rett til ei

applikasjonsteneste, dei tilhøyrande kvalitetsklassane samt til prioritert bruk av tenesta. Eksisterande arkitekturar for tenestekvalitet tilbyr ikkje *prioritert* bruk av tenestene, men dette vil vera eit krav til NbF målnett, og me tek det difor med i dette dømet.

Tilgjenge til tenesta. Utfordringa i stasjonære nett er først og fremst å sikra at berre autoriserte kan nytta tenesta. I praksis trengs gjensidig *autentisering* av brukar og teneste, og tenesta må i tillegg kunna verifisera at brukaren er *autorisert* for bruk. Dette vil i seg sjølv ikkje hindra at *Denial-of-Service* (DoS)-åtak vert retta mot tenesta, men vil hindra misbruk av ho og dermed avgrensa effekten av eit DoS-åtak.

I eit mobilt trådlaust nett vil det i tillegg til å avvisa ikkje-autoriserte, vera ei stor utfordring å gjera tenesta tilgjengeleg for autoriserte sluttbrukarar. På grunn av den låge kapasiteten i denne typen nett, må ein vera svært restriktiv med omsyn til kva for tenester som skal tilbydast og kva for kvalitetsklassar som i sin tur skal realiserast. Settet av kritiske tenester vil kunna variera frå operasjon til operasjon. Det er til dømes ikkje gitt at dei kritiske tenestene er dei same i ein utrykkingsoperasjon som i ein patruljeoperasjon. Førstnemnde operasjon kan involvera svært mange aktørar, vera synleg og ha mange fellestrekk med ein sivil redningsoperasjon. Sistnemnde omfattar færre aktørar som gjerne skal minimalisera kommunikasjonen for å halda seg skjulte. Tilgjengepolicy for eitt og same subjekt vil dermed kunna variera frå operasjon til operasjon. Ein lagførar som i ein utrykkingsoperasjon treng høg garanti for tilgjenge til ei spesifikk teneste, kan i ein patruljeoperasjon kanskje greia seg med meir usikkert tilgjenge til den same tenesta.

Det er ikkje realistisk å rekna med at trådlause mobile nett vil kunna gje same kvalitet som stasjonære trådbaserte nett. Eit fornuftig utval av kritiske tenester samt ein restriktiv tilgjengepolicy for desse, vil vera naudsynt for at tenestene skal vera allment tilgjengelege for autoriserte sluttbrukarar. Tilgjenge kan aldri garanterast, og difor bør dei mest kritiske tenestene vera distribuerte til fleire server-implementasjonar innan domenet.

Tilgjenge til kvalitetsklassar. Eksisterande standardarkitekturar for tenestekvalitet kontrollerer at påtrykt trafikk er i samsvar med ein SLA. Arkitekturane omfattar i utgangspunktet ikkje autentisering og autorisasjonskontroll av sluttbrukarar og sluttbrukarapplikasjonar når desse spør etter ein spesifikk tenestekvalitet. For at tenestekvaliteten i NbF målnett i praksis skal vera *differensiert*, kan ikkje alle sluttbrukarar få same tilgang til alle trafikklassar. Dermed krevs autentisering og autorisasjonskontroll av sluttbrukarar (rollar) og sluttbrukarapplikasjonar.

Tilgjenge til prioritet og forkøyrsrett. Eksisterande arkitekturar for tenestekvalitet handterer i liten grad prioritet og forkøyrsrett for sluttbrukarar og applikasjonar. Policy for prioritet kan setjast opp for ulike typar subjekt. *Sluttbrukarar* (eller rollar) kan prioriterast slik at til dømes lagførar går føre soldat som synt i Tabell 3.3. På same vis kan *applikasjonstenester* prioriterast slik at til dømes eldleiing går før tale som i sin tur går føre epost. Meir komplekse policyar kan sjølvsagt setjast opp. For å hindra misbruk av prioritetsfunksjonen trengs autentisering og autorisasjonskontroll av sluttbrukarar (rollar) og applikasjonar.

3.3 Framtidig sikkerhetspolicy for nettinformasjon

Ein sikkerhetspolicy kan utviklast på bakgrunn av trugsmål mot systemet og ein konsekvens- og risikoanalyse av relevante informasjonsåtak. Trugsmål mot informasjons- og kommunikasjons-infrastrukturen, konsekvensar av og risiko for informasjonsåtak endrar seg over tid, frå stad til stad, og frå operasjon til operasjon. Ein sikkerhetspolicy kan prøva å unngå risiko eller ta omsyn til at risiko og konsekvens varierer. Informasjonssystem i Forsvaret er til ei kvar tid underlagt gjeldande sikkerhetspolicy. Som framheva i avsnitt 2.2, vil NbF målnett vera eit distribuert informasjonssystem. Nettinformasjonen må underleggjast ein sikkerhetspolicy som omfattar konfidensialitet, integritet og tilgjenge, men det er ikkje gitt at kommunikasjonssystemet bør underleggjast same policy som dei allmenne sluttbrukarsystema. Viktige aspekt ved val av policy og mekanismar for å handheva policy er *kompleksitet* og *yteevne*. Dei ulike delane av NbF målnett vil ha ulik kapasitet og ulik evne til å handheva ein sikkerhetspolicy. Avgrensa kapasitet til å handheva policy kan truleg ikkje vera nokon styrande parameter når ein fastset policy, men ein bør så langt forsvarleg unngå kompleksitet. Ved val av mekanismar derimot, vil avgrensa kapasitet leggja avgjerande føringar. Er policy enkel og har låg kompleksitet, kan ein truleg finna effektive mekanismar for å handheva han.

3.3.1 Konfidensialitet

Nettinformasjon avdekkar i utgangspunktet nett-topologi, trafikkparametrar og organisasjon. I dei stasjonære delane av NbF målnett er det mykje som talar for at nettinformasjonen bør underleggjast høge konfidensialitetskrav. Både den fysiske og den logiske topologien er statisk, og netta har relativt god kapasitet med omsyn til bandbreidde, prosessering, lagring og kraftforsyning. Det bør difor vera mogleg å tilfredsstilla høge konfidensialitetskrav. Per i dag er *kryptering* den vanlegaste mekanismen for å handheva konfidensialitetskrav. Det går føre seg mykje forsking for å finna "lette" krypteringsalgoritmar som krev lite prosessering. Uavhengig av krypteringsalgoritmar vil det vera ei utfordring å finna effektive algoritmar og system for dynamisk nøkkelhandtering. Høge konfidensialitetskrav medfører gjerne føringar vedrørande storleik og tal på nøklar så vel som utskiftingsfrekvens. Slike prosedyrar vil raskt kunna redusera yteevna til nettet.

I eit høgmobilt nett endrar nett-topologien seg raskt og mykje av nettinformasjonen vert vaska ut og erstatta med ny i takt med endringane. Nettinformasjonen har dermed kort levetid og er robust mot korrumpering. Omfanget av nettinformasjon er dessutan langt mindre enn i stasjonære trådbaserte nett. Alt i alt kan det vera forsvarleg å redusera eller ta bort krava om konfidensialitet på til dømes rutinginformasjonen. Dette ville mellom anna medføra at:

- Det vert lettare å organisera rutingdomene på ein dynamisk måte. I ein internasjonal operasjon vil fleire nasjonar lettare kunna organisera eit felles kommunikasjonsnett
- Ein unngår administrasjon av krypteringsnøklar.

Ein fleirnivå-policy er kompleks og vil i seg sjølv gjera nettet sårbart. Eventuelle krav om fleirnivå-konfidensialitet for nettinformasjon reiser viktige problemstillingar. Ein protokoll-implementasjon på lågt sikkerhetsnivå skal då ikkje kunna lesa informasjon frå implementasjonar på høgare nivå, noko som kan hindrast ved til dømes krypterte meldingar og kryptert lagring. I

tillegg må ein ha løysingar som sikrar skilje mellom nivåa under prosessering av dekrypterte meldingar. Eit spørsmål som må avklarast er om implementasjonar på ulike konfidensialitetsnivå kan køyrast på ein og same fysiske node. Dersom dette ikkje er forsvarleg, vil konsekvensen i praksis vera at ein må ha separate sett av terminalar og ruterar, med andre ord *eitt separat kommunikasjonsnett for kvart konfidensialitetsnivå*. Dette vil vera ressurskrevjande og upraktisk i både stasjonære og mobile nett. Eit anna spørsmål som må avklarast er om informasjon på ulike konfidensialitetsnivå kan prosesserast av ein og same protokoll-implementasjon.

3.3.2 Integritet

I alle kommunikasjonsnett er autentiseringsmekanismar avgjerande for sikker kommunikasjon. Det må vera mogleg å verifisera kven ein kommuniserer med og kven som opphavleg genererte ei motteken melding. Slik autentisering er særleg kritisk i trådlause nett sidan vilkårlege nodar kan senda protokollmeldingar inn i nettet. For å stola på informasjonen må ein i tillegg kunna verifisera at han ikkje er endra på ikkje-autorisert vis på vegen frå meldingskjelda eller under lagring. Dette er sjølvsagt òg grunnleggjande krav i stasjonære nett, men i slike nett, særleg i dei trådbaserte, vil det vera enklare å identifisera inntrengjarar. Desse delane av NbF målnett bør ha evne til å handheva høge krav til integritet for nettinformasjonen. Utfordringane kjem med dei mobile trådlause netta.

Ein integritetspolicy vert vanlegvis handheva ved ulike former for autentisering og dataintegritetskontroll. Eksisterande mekanismar for autentisering er i all hovudsak basert på å prova kjennskap til ein hemmeleg verdi. Dermed må ein i denne samanhengen òg finna effektive algoritmar og system for dynamisk nøkkelhandtering. Det er særleg ei utfordring å finna algoritmar som skalerer bra i mobile nett. Ei anna utfordring er å redusera autentiserings-parametrane som må vedleggjast protokollmeldingane, til dømes digitale signaturar. I mobile trådlause nett er protokollmeldingane ”strippa til beinet” og er vanlegvis langt mindre enn ein standard digital signatur. Mekanismar som syter for dataintegritetskontroll, er i all hovudsak basert på effektive hash-funksjonar, og det er ikkje på dette feltet dei største utfordringane vil vera.

Eventuelle krav om fleirnivå-integritet for nettinformasjon reiser viktige problemstillingar. Som me såg i avsnitta 3.1.2 og 3.2.1 er tradisjonelle policykrav for skiftevis konfidensialitet og integritet duale dersom ein nyttar *identiske* sikkerhetsnivå for dei to aspekta. Konsistens impliserer at protokoll-implementasjonane ikkje kan prosessera annan informasjon enn den som kjem frå implementasjonar på same nivå. Dette vil seia at *ingen* informasjonsflyt er tilleten mellom nivåa. Ei slik rigid løysing for nettinformasjonen vil gjera felles kommunikasjonsnett og felles rutingdomene på tvers av nasjonale og internasjonale sikkerhetsdomene umogleg.

Me har understreka at konfidensialitet og integritet er uavhengige sikkerhetsaspekt. Det er i utgangspunktet ingen grunn til at konfidensialitetsnivå og integritetsnivå skal representera identiske kriterium. Tvert om. Dersom konfidensialitet og integritet er *to* dimensjonar ved sikkerhet, er det naturleg å nivellera *to* aksar som representerer *ulike* eigenskapar/kriterium.

Nettinformasjonen er i utgangspunktet korrekt dersom han er generert, prosessert, lagra og utveksla i samsvar med protokollar og eventuelt andre spesifikasjonar. Gitt at kjelda for motteken nettinformasjon kan autentiserast og at det kan verifiserast at informasjonen ikkje er modifisert på uautorisert vis på vegen frå kjelda, vil ein kunna laga ein skala for integritet basert på *tillit* til meldingskjelda. Medan nivåa på konfidensialitets-aksen kan vera av typen Hemmeleg-Begrenset-Ugradert, kan nivåa på integritets-aksen dermed skildra ulike grader av tillit til at nettinformasjonen vert generert, prosessert, lagra og utveksla i samsvar med standard protokollar.

Ved å sjå konfidensialitet og integritet som uavhengige dimensjonar kan ein såleis definera policyar som er konsistente og samstundes fleksible nok til å mogleggjera kommunikasjonsnett der rutingdomene og tenestekvalitetsarkitekturar kan setjast opp dynamisk, til dømes på tvers av dei noverande nasjonale og internasjonale sikkerhetsdomena. Ved å sjå konfidensialitet og integritet som uavhengige dimensjonar, vil ein truleg òg gjera det enklare å utvikla ein meir risikodriven sikkerhetspolicy for nettinformasjon.

3.3.3 Tilgjenge

Ein tilgjenge-policy for tenester må for kvar teneste definera kva det vil seia at tenesta er tilgjengeleg. Policy må deretter spesifisera settet av tenester som skal vera tilgjengeleg for ulike subjekt som sluttbrukarar og applikasjonar. Gitt tilgjenge til ei teneste, må policy òg spesifisera kva som skal til for å vera autorisert til å bruka denne tenesta. I eit nett med avgrensa ressursar bør policy vera restriktiv og kunna differensiera tilgjenget for ulike typar subjekt. Ein fleirnivå-policy vil kunna gje fleksibiliteten som skal til for å utnytta ressursane optimalt. Policy bør difor òg spesifisera nivået dei ulike subjekta kan krevja.

Ein effektiv tilgjengepolicy for tenester vil truleg krevja at subjekta vert tildelt rollar, og at rollane i sin tur vert autoriserte for ulike nivå av tilgjenge til ulike tenester. For å handheva policyen vil effektive mekanismar for aksess-kontroll og autorisasjon vera naudsynt. Slike prosessar krev i sin tur autentiseringsmekanismar. Når subjektet er autentisert, kan autorisasjonskontrollen vidare utførast ved oppslag i sentraliserte eller distribuerte databasar. Ein annan metode er å lista autorisasjonar i digitale sertifikat som dermed kan brukast til å prova spesifikke rettar overfor ei teneste. Dersom tilgjengenivå er knytt til rollar, vil slike prosessar verta forenkla: Det vil vera tilstrekkeleg å prova ”medlemskap” i ein spesifikk rolle. I mange samanhengar vil dette òg kunna vera tilstrekkeleg som autentisering.

3.3.4 Kommentarar

Å sikra nettinformasjonen er ei fleirlagsoppgåve. Til dømes utvekslar alle kommunikasjonslag informasjon, og det er ikkje gitt kvar i protokollstakken dei ulike sikkerhetsmekanismane bør implementerast.

I dette kapittelet har me prøvd å syna at det trengs ein (særeigen) sikkerhetspolicy for informasjonssystemet NbF målnett. Basert på denne policyen og på den allmenne sikkerhetspolicyen for sluttbrukarinformasjon, trengs òg ein sikkerhetsarkitektur for systemet. Denne arkitekturen må omfatta *både* sikker overføring av sluttbrukarinformasjon *og* sikker

utveksling, prosessering og lagring av nettinformasjon.

Av dette kapittelet går det vidare fram at nettet må tilby nokre generiske sikkerhetstenester som til dømes autentisering av ulike subjekt. Autentiseringsprosedyrar mellom sluttbrukarar og ulike sluttbrukartenester/system vil truleg handterast av mellomvare som opererer på dei tre øvste laga i OSI-stakken. I den forenkla stakken som er nytta i TCP/IP-nett er desse tre laga slått saman og kalla *applikasjonslaget.* Som synt i dette kapittelet, vil det òg vera naudsynt med autentiseringsprosedyrar mellom sluttbrukar og entitetar på lågare kommunikasjonslag, til dømes ved forespørsel om prioritet eller ein tenestekvalitetsklasse. Vidare vil det vera naudsynt med autentiseringsprosedyrar mellom to entitetar på låge kommunikasjonslag, til dømes to rutingprotokoll-implementasjonar. Ein autentiseringsprosedyre er ressurskrevjande, og impliserer i utgangspunktet nøklar og nøkkeladministrasjon. Det er difor svært viktig at tenester av denne typen vert handtert som fleirlagstenester og planlagt med tanke på den totale ressursbruken i nettet. For å effektivisera kan det til dømes vera aktuelt å sjå på krysslagsløysingar.

Ei gjennomgåande autentiseringsteneste krev dessutan at nettarkitekturen spesifiserer fornuftige og konsistente *identitetar* på ulike kommunikasjonslag. Ein må til dømes vita om det er ein person, ein rolle, ei IP-adresse eller ei *Medium Access Control* (MAC)-adresse ein skal autentisera i dei ulike tilfella. Ein må òg ta stilling til om IP-adresse i det heile er ein fornuftig identitet på nettlaget.

4 IP versjon 6 versus IP versjon 4

Dei første IP-netta knytte saman forskingsmiljø som stolte på kvarandre. Det vart ikkje lagt vekt på å sikra kommunikasjonen. Ein del applikasjonar som Telnet og FTP kravde rett nok sluttbrukar-autentisering i form av passord, men dette var inkludert i sjølve applikasjonane. Den originale IP-arkitekturen mangla eit rammeverk for sikker kommunikasjon. Det er seinare spesifisert eigne sikkerhetsmekanismar for nokre av protokollane for nett-tenester. Dette gjeld til dømes rutingprotokollen OSPF, som i dag har ei svært enkel løysing og ressursreservasjons-protokollen RSVP. Fleire løysingar for sikker ende-til-ende-kommunikasjon har òg vorte utvikla. Døme på dette er *Secure Socket Layer* (SSL) og *Transport Layer Security* (TLS). IPSec kom først i 1998. Grunna problem knytt til interoperabilitet og yteevne er ikkje IPSec deployert i stor skala i IPv4-nett.

Forsvaret har førebels ikkje vedteke tidsplan for overgang frå IPv4 til IPv6. Det er i praksis tre ulike strategiar for overgang til IPv6. Strategien som vanlegvis vert tilrådd, er å støtta begge versjonar i kvar node i nettet. Ulike tunneleringsteknikkar er eit alternativ. Ein køyrer då IPv4 over IPv6 eller vice versa. Ein tredje strategi er å oversetja mellom IPv4 og IPv6.

I dette kapittelet listar me nokre av dei viktigaste endringane frå IPv4 [7] for å grunngje at studiet har teke utgangspunkt i denne versjonen.

4.1 Kva gir IPv6?

4.1.1 Utvida adresserom

Av historiske årsaker nyttar organisasjonar og styresmakter i USA 60% av adresserommet til IPv4. Resten av verda delar 40%. Raten for Internett-tilgang i Asia veks eksponensielt. Dette er ei årsak til at IPv6 er langt meir utbreidd der enn i Europa og USA. IPv6 utvidar adresseformatet frå 32 til 128 bitar. Dette held til å adressera kvart sandkorn på planeten. I tillegg mogleggjer det ei hierarkisk strukturering av adresserommet som vil vera fordelaktig med tanke på global ruting. Som i IPv4 er det grensesnitt (*interfaces*), ikkje nodar, som vert tildelt adresser. Kvart grensesnitt på ein node må ha minst *ei* unikast-adresse.

4.1.2 Sjølvkonfigurering

Sjølvkonfigurering utan tilstandsinformasjon (*stateless autoconfiguration*) er ein ny funksjon. Terminalar kan ved booting spørja etter adresse-prefix og få eitt eller fleire prefix frå ein IPv6-ruter. Ved hjelp av dette prefixet kan så terminalen konfigurera seg sjølv med ei eller fleire globale IP-adresser. Som tillegg til prefixet kan terminalen anten bruka MAC-adressa for vedkomande grensesnitt eller ei privat adresse som vert generert tilfeldig. Den private adressa kan konfigurerast manuelt eller ved hjelp av *Dynamic Host Configuration Protocol* (DHCP).

4.1.3 Enklare format på IP-hovudet

Det nye formatet på IP-hovudet er enklare og har ei fast lengde på 40 *bytes*. Dette mogleggjer raskare prosessering Figur 4.1 syner formatet. Som ein ser er det snakk om 2 * 16 *bytes* for skiftevis kjelde- og destinasjonsadresser og 8 *bytes* for allmenn informasjon.

Felt	*Lengde*	
Versjon	4 bits	Protokollversjon
Traffic class	1 byte	Skil ulike klassar av IP-pakkar
Flow label	20 bits	Merkar sekvensar av pakkar som skal handsamast likt
Payload length	2 bytes	Lengde på datafeltet som følgjer etter IP-hovudet
Next header	1 byte	Protokollnummer eller ein verdi for *Extension header*
Hop limit	1 byte	Talet på hopp. Kvar rutar på stien aukar feltet med *ein*.
Source address	16 bytes	
Destination address	16 bytes	

Figur 4.1 Formatet på meldingshovudet til IPv6 [7]

4.1.4 Betre støtte for opsjonar og tillegg

Medan IPv4 integrerer opsjonar i sjølve meldingshovudet, fører IPv6 opsjonane i såkalla tilleggshovud (*extension headers*), som vert sett inn berre når dei trengs. Dette medfører raskare pakkeprosessering. Tilleggshovuda vert plassert mellom IP-hovudet og hovudet til protokollen over. Vanlegvis er det berre destinasjonsnoden som les og prosesserer tilleggshovuda. Det er spesifisert seks tilleggshovud [36]:

- *Hopp-for-hop*p som fører informasjon som skal inspiserast av kvar node på stien
- *Ruting* som mogleggjer kjelderuting
- *Fragmentering* som mogleggjer fragmentering av IP-pakkar
- *Destinasjon* som fører informasjon som skal inspiserast av destinasjonen
- *Autentisering* som fører autentiseringsinformasjon
- *Kryptering* som fører krypteringsinformasjon.

Dei to siste utgjer funksjonaliteten i IPSec og vert gjennomgått i avsnitt 5.1.2.

4.1.5 Integrert sikkerhet

IPv6 er sikrare enn IPv4. I motsetning til IPv4, er IPv6 utvikla med tanke på at fundamental sikkerhetsfunksjonalitet skal vera del av protokollen. IPSec er til dømes obligatorisk i standard-implementasjonen av IPv6. Difor kjem IPv6-versjonane av protokollar som tidlegare hadde enkle sikkerhetsmekanismar innebygd, til å utelata desse mekanismane for i staden å bruka mekanismane i IPSec. Dette gjeld til dømes rutingprotokollen OSPF versjon 3 (OSPFv3) for IPv6 [43].

At sikkerhetsmekanismane er betre integrert, medfører ryddigare kommunikasjon, og det vert

mellom anna enklare å verifisera dei ulike løysingane. IPv6 mogleggjer dessutan ende-til-ende-sikkerhet på nettlaget. I staden for å implementera IPSec berre i IPSec-portar (*IPSec gateways*) kan ein implementera IPSec i alle maskiner. Dette gjer at ”skalsikringa” som kjenneteiknar IPv4-baserte nett, kan erstattast med ”djupne-sikring”.

4.2 Kommentarar

Resten av denne rapporten føreset IPv6. Det er tre grunnar til at me har valt dette utgangspunktet:

- IPv6 vil verta innført; det er berre eit spørsmål om tidspunkt. Mange sikkerhetsløysingar som er spesifisert for IPv4 vil då falla bort og verta erstatta av ein meir heilskapleg sikkerhetsarkitektur
- IPv6 løyser mange av sikkerhetsproblema i eksisterande IPv4- nett, men IPv6 løyser ikkje alt. Difor meiner me det er fornuftig å sjå på utfordringar som etter ein overgang til IPv6, framleis er gyldige
- IPv6 medfører i seg sjølv nye sikkerhetsutfordringar, særleg med omsyn til yteevna til IPSec.

5 Sikring av IPv6 - nett

Dette kapittelet går gjennom dei viktigaste standardkomponentane for sikring av IPv6-nett. Desse komponentane er samla innan to område:

- Sikkerhetsarkitektur for IP (*Security Architecture for the Internet Protocol*) som omfattar protokollane som samla utgjer *IPSec*
- Offentleg nøkkel-infrastruktur (X.509) (*Public-Key Infrastructure (X.509)*) som omfattar protokollane som utgjer *PKIX*.

Kapittelet syner òg korleis den offentlege nøkkel-infrastrukturen er tenkt brukt innan IPSec. I tillegg til desse arkitekturane finns frittståande standardar som til dømes TLS/SSL. IETF har dessutan ei rekkje arbeidsgrupper som spesifiserer sikring av delområde av IP-nett, til dømes sikker multikastruting.

5.1 Sikkerhetsarkitekturen for IPv6 (IPSec)

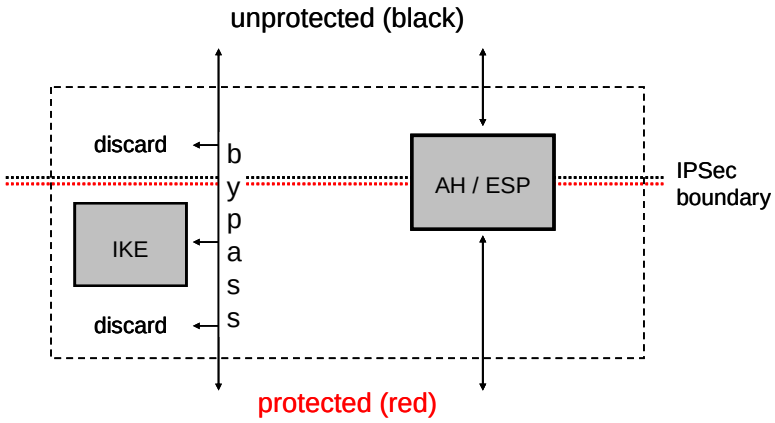
I IPv6 bør målet vera å sikra nettet best mogleg *samstundes* som ein sikrar sluttbrukardata ende til ende på nettlaget. IPv6 gir IPSec-funksjonalitet i kvar node. Dette mogleggjer begge desse aspekta. IPv6/IPSec mogleggjer dessutan ein identitetsbasert sikkerhetsmodell. Dette fører til at ein kan skilja sikkerhetspolicyen frå nettadressene. Dette er essensielt dersom nettet skal handtera til dømes sjølvkonfigurering og mobilitet på ein sikker og fleksibel måte.

For å sikra IPv4-baserte nett er det vanleg å nytta perimeterbrannmur og integrera *Network Address Translation* (NAT). Dette er òg mogleg i IPv6, men ei slik løysing utnyttar ikkje funksjonaliteten i IPv6. Eit mål med IPv6 er å oppretthalda ende-til-ende-konnektivitet ved hjelp av det store adresserommet, og NAT bør difor ikkje brukast. Dersom det er naudsynt å skjula intern nett-topologi, kan andre mekanismar nyttast. Å stola på perimetersikring kan vera farleg;- ein inntrengjar finn vanlegvis eit ope og usikra område på innsida.

Sikkerhetsarkitekturen er dokumentert på overordna vis i [67]. Arkitekturen skildrar sikring på nettlaget og er uavhengig av sikringstiltak på andre kommunikasjonslag. Rammeverket inneheld følgjande element:

- Krav og mekanismar på nettlaget
- Ein protokoll for kryptering
- Ein protokoll for autentisering
- Ein definisjon av sikkerhetspolicyar og sikkerhetsassosiasjonar mellom kommunikasjons-partar på same lag (*peers*)
- Nøkkelhandtering.

Figur 5.1 gir ein blokkskjematisk oversikt over dei ulike komponentane.



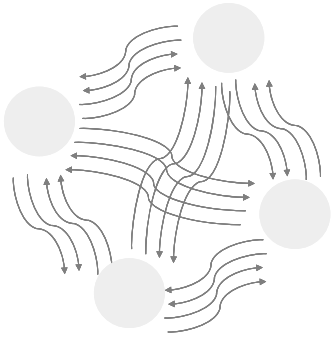
Figur 5.1 Sikkerhetsarkitektur for IP (IPSec) [67]

5.1.1 Sentrale omgrep

Verna og ikkje-verna område. Når ein konfigurerer IPSec, lagar ein ei grense mellom eit verna (*protected*) og eit ikkje-verna (*unprotected*) område. Denne grensa kan setjast rundt ei vertsmaskin eller rundt eit heilt nett. Eit sett med policy-reglar avgjer korleis kvar IP-pakke skal handterast ved grensa. For både innkomande og utgåande pakkar er det tre moglege utfall: pakken skal vernast (*protect*), pakken skal gå utanom sikkerhetsmekanismane (*bypass*) eller pakken skal kastast (*discard*).

Sikkerhetsassosiasjon (*Security Association*) (SA). SA vert sett opp for ein pakkestraum mellom kommunikasjonspartar på same lag (*peers*). Ein SA er ei semje om følgjande tre element: ein nøkkel, ein autentiserings- *eller* ein krypteringsalgoritme og til sist parametrar for vald algoritme. Ein SA er unidireksjonal, og kvar teneste krev sin eigen SA. Dette inneber at to kommunikasjonspartar som ynskjer både å autentisera og kryptera tovegstrafikk, treng fire assosiasjonar. SA vert forhandla ved hjelp av protokollen *Internet Key Exchange version 2* (IKEv2) [71]. IKEv2 sørgjer for gjensidig autentisering av partane og etablerer ein SA mellom dei. Nøkkelen som vert forhandla er hemmeleg. Slike nøklar bør ikkje brukast for uavgrensa tidsrom og for uavgrensa datamengder. Det bør difor setjast grenser for levetida for kvar nøkkel, i praksis for kvar SA. Reforhandling av SA vert initiert ved eigne protokollmeldingar.

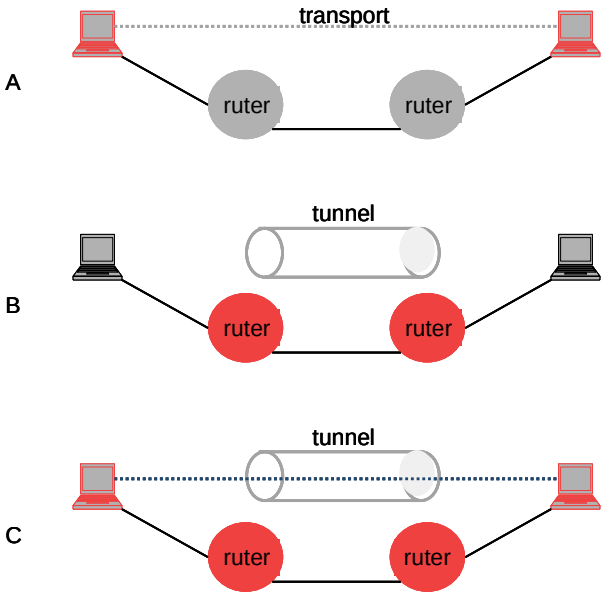
Figur 5.2 syner naudsynte sikkerhetsassosiasjonar mellom fire nodar som autentiserer og krypterer innbyrdes trafikk.



Figur 5.2 Sikkerhetsassosiasjonar mellom fire IPSec-nodar

Transportmodusar. IPSec skil mellom transport- og tunnelmodus:

– I transportmodus definerer SA autentisering *eller* kryptering for *nyttelasta* i IP-pakken. Figur 5.3 A) syner eit døme på SA for transportmodus. SA er her sett opp mellom to vertsmaskiner som begge implementerer IPSec



Figur 5.3 Døme på bruk av SA [71]

– Tunnelmodus er vanlegvis brukt mellom to sikkerhetsportar (*security gateways*). SA definerer då autentisering *eller* kryptering for *heile* IP-pakken, inkludert hovudet. Dette vert gjort ved å kapsla den originale IP-pakken inn ved hjelp av eit nytt IP-hovud. Tunnelmodus er grunnlaget for virtuelle private nett (*Virtual Private Networks*) (VPN). Figur 5.3 B) syner eit døme på SA for tunnelmodus. SA er sett opp mellom to ruterar som fungerer som IPSec-portar (*IPSec gateways*). Ruterane er endepunkt for tunnelen. Denne tunnelen kan brukast for ende-til-ende-trafikk av vertsmaskinene som sjølve ikkje implementerer IPSec. Figur 5.3 C) syner eit døme der både vertsmaskiner og tunnel-endepunkta implementerer IPSec.

Transport-SA'ar mellom vertsmaskinene er omslutta av tunnelen mellom IPSec-portane. SA i tunnelmodus kan omfatta mange transport-SA'ar mellom IP-adresser i dei einskilde lokalnetta.

5.1.2 Funksjonalitet

Som nemnd i avsnitt 4.1.3, er funksjonaliteten i IPSec knytt til to tilleggshovud som IP-pakken kan bruka. Tenester som skal brukast, vert forhandla under oppretting av SA og gjeld ende til ende på *nettlaget*.

Autentiseringshovud (*Authentication Header*) (AH) er spesifisert i [68] og legg til rette for autentisering og integritetssjekk av nyttelasta i ein IP-pakke. Autentisering og integritetssjekk gjeld ende til ende på *nettlaget*, og må ikkje forvekslast med ende-til-ende-sikring på *applikasjonslaget*. Figur 5.4 syner formatet til AH.

Felt	*Lengde*	
Next header	1 byte	Identifiserer typen til påfølgjande hovud
Payload length	1 byte	Lengde på AH i 4 byte einingar
Reserved	2 bytes	Feltet er ikkje brukt og er sett til null
Security Parameter Index	4 bytes	SPI knyter innkomande pakke til rett SA
Sequence number	4 bytes	Monotont aukande sekvensnummer
Authentication data	variabel	Sjekkverdi for dataintegritetsverifikasjon

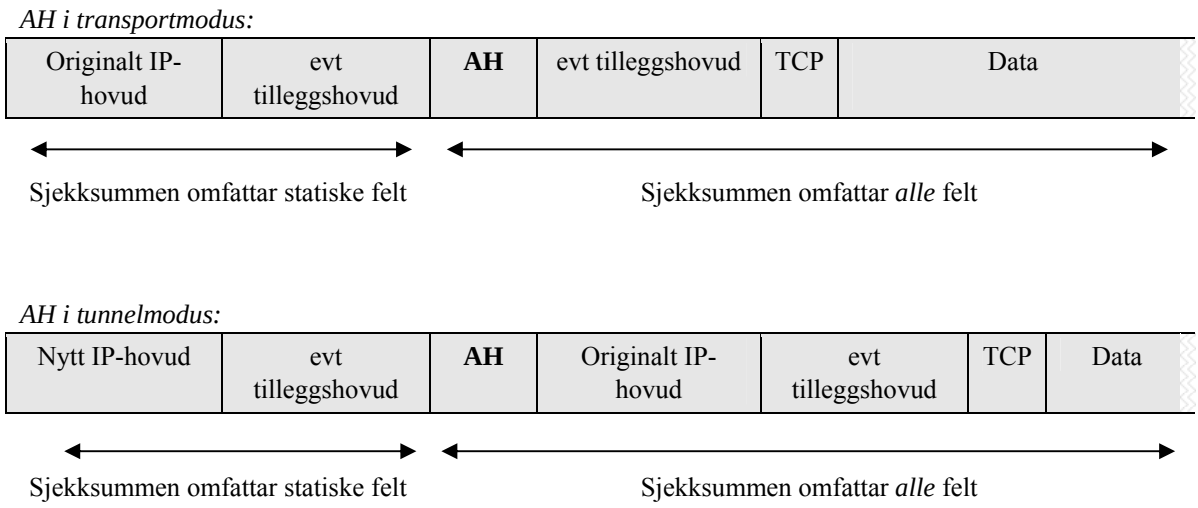
Figur 5.4 Formatet på AH [7]

AH i transport- og tunnelmodus er synt i Figur 5.5. I transportmodus vert AH plassert mellom det originale IP-hovudet og hovudet til protokollen over, til dømes TCP som synt i figuren. (Av praktiske omsyn kan eitt av tilleggshovuda vera plassert både før og etter AH). Sjekksummen som vert nytta til å verifisera dataintegritet vert kalkulert over følgjande felt:

- Alle felt i IP-hovud og tilleggshovud som *ikkje* skal endrast i transitt (statiske felt). Døme på felt som vert endra i transitt er *traffic class*, *flow label* og *hop limit*, sjå Figur 4.1
- Alle felt i AH
- Nyttelasta.

I tunnelmodus vert AH plassert mellom det nye og det originale IP-hovudet. Medan det originale IP-hovudet inneheld adressene til kjelde og destinasjon, finn me adressene for tunnel-endepunkta i det nye IP-hovudet. Sjekksummen vert kalkulert over følgjande felt:

- Alle felt som ikkje skal endrast i transitt i det nye IP-hovudet
- Den komplette originale IP-pakken.



Figur 5.5 AH i transport- og tunnelmodus

Av dei tre sikkerhetsaspekta me diskuterte i avsnitt 3.1, støttar AH *integritet*. AH påverkar ikkje direkte det autoriserte *tilgjenget* til informasjonen, men kan sjølvsagt understøtta ulike former for aksesskontroll som baserer seg på autentisering av den opphavlege IP-adressa.

AH gjer det mogleg for mottakar å verifisera at dei felta *som er omfatta av sjekksummen* ikkje er endra på vegen frå første til siste *IP-adresse* på ruta. I tunnelmodus skal mellomliggjande nodar ikkje endra verdiar i det *originale* IP-hovudet, og sjekksummen omfattar difor *heile* den originale IP-pakken. IPSec opererer på nettlaget og gir dataintegritet for nyttelasta berre så lenge nyttelasta er del av ein IP-pakke. Med omsyn til autentisering, er det viktig å merka seg at IPSec ikkje autentiserer kjelda for *nyttelasta* men kjelda for *IP-pakken*: Den opphavlege IP-adressa vert autentisert, sluttbrukar og applikasjon vert ikkje autentisert. AH kan nytta ulike autentiseringsalgoritmar. Dei tilrådde algoritmane nyttar nøkla meldings-autentiseringskodar (*keyed Message Authentication Codes* (MACs)) basert på symmetriske krypteringsalgoritmar [70]. Kjelde og destinasjon nyttar då same nøkkel. Sjekksummen vert rekna ut av hash-funksjonar.

Ved hjelp av sekvensnummeret gir AH òg støtte for vern mot ikkje-autorisert gjentaking (*replay*) av IP-pakken.

Innkapslande sikkerhetshovud for nyttelast (*Encapsulating Security Payload header*) (ESP) er spesifisert i [69] og legg til rette for konfidensialitet, dataintegritetssjekk, autentisering av meldingskjelde, vern mot ikkje-autorisert gjentaking samt avgrensa konfidensialitet for trafikkflyt av nyttelast transportert i ein IP-pakke. ESP mogleggjer både autentisering og kryptering, men ei av tenestene kan om ynskjeleg utelatast. Figur 5.6 syner formatet til ESP.

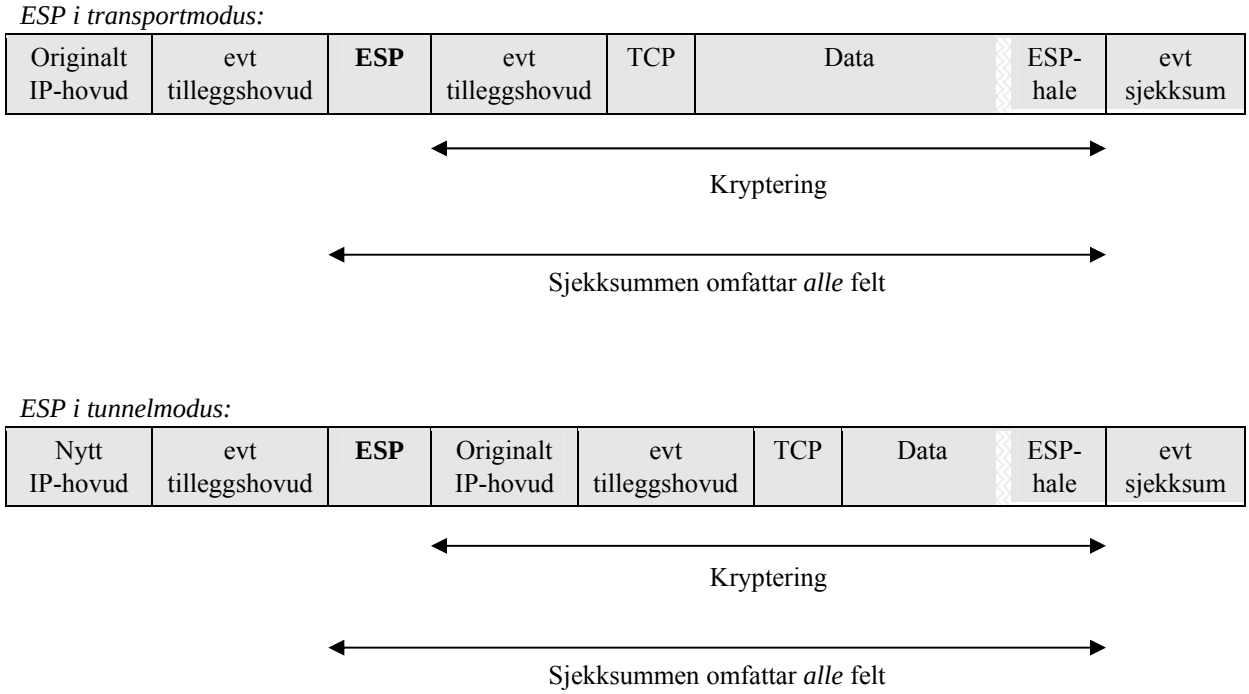
Felt		*Lengde*	
Security Parameter Index		4 bytes	SPI knyter innkomande pakke til rett SA
Sequence number		4 bytes	Monotont aukande sekvensnummer
Payload data		variabel	Kryptert data og eventuell initialiseringsvektor
Padding	←ESP→ trailer	0-255 bytes	
Pad length		1 byte	
Next header		1 byte	Identifiserer typen til påfølgjande hovud
Authentication data		variabel	Valfri sjekkverdi for dataintegritetsverifikasjon

Figur 5.6 Formatet på ESP [7]

ESP i transport- og tunnelmodus er synt i Figur 5.7. I transportmodus vert ESP plassert mellom det originale IP-hovudet og hovudet til protokollen over, til dømes TCP som synt i figuren. (Av praktiske omsyn kan eitt av tilleggshovuda vera plassert både før og etter ESP).

Mellomliggjande nodar må kunna lesa IP-hovudet for i det heile å kunna ruta pakken. Difor vert korkje IP-hovudet eller eventuelle tilleggshovud kryptert. Sjekksummen som vert nytta for dataintegritet og autentisering omfattar alt frå og med ESP-hovudet til og med ESP-halen. Merk at sjekksummen ikkje omfattar dei statiske felta i IP-hovudet og eventuelle tilleggshovud, slik han gjer ved bruk av AH.

I tunnelmodus vert ESP plassert mellom det nye og det originale IP-hovudet. Som ved bruk av AH inneheld det originale IP-hovudet adressene til kjelde og destinasjon, medan det nye IP-hovudet inneheld endepunkta for tunnelen. Pakken vert ruta etter parametrane i det nye IP-hovudet, og heile den originale IP-pakken kan difor krypterast. Sjekksummen for dataintegritet og autentisering omfattar alt frå og med ESP-hovudet til og med ESP-halen. Det vil seia at sjekksummen omfattar *heile* den originale IP-pakken. Merk at sjekksummen ikkje omfattar dei statiske felta i det nye IP-hovudet og eventuelle nye tilleggshovud, slik han gjer ved bruk av AH i tunnelmodus.



Figur 5.7 ESP i transport- og tunnelmodus

Av dei tre sikkerhetsaspekta me diskuterte i avsnitt 3.1, støttar ESP-hovudet både *konfidensialitet* og *integritet*. Som AH påverkar ikkje ESP direkte det autoriserte *tilgjenget* til informasjonen, men kan som AH støtta ulike former for aksesskontroll som baserer seg på autentisering av den opphavlege IP-adressa.

ESP gjer det mogleg å kryptera nyttelasta, men det er viktig å merka seg at konfidensialiteten gjeld berre så lenge nyttelasta er del av ein IP-pakke. I tunnelmodus vert heile den opphavlege IP-pakken kryptert, noko som gir konfidensialitet for det originale IP-hovudet. Dette medfører at ESP gjer det vanskelegare å analysera trafikkmønster mellom IP-adresser. På same vis som AH kan òg ESP verifisera at data ikkje er endra på vegen frå første til siste IP-adresse på ruta. Skilnaden er at sjekksummen ikkje omfattar statiske felt i det *rutbare* IP-hovudet og i tilleggshovuda når ein brukar ESP. Dette inneber at endringar av statiske adressefelt i desse hovuda ikkje vil verta detektert.

I tillegg til autentiseringsalgoritmane som AH kan nytta, støttar ESP fleire symmetriske krypteringsalgoritmar [70]. Kva for krypteringsalgoritme som skal nyttast kan forhandlast under oppretting av SA eller setjast dynamisk i nøkkelhandteringsprosessen, sjå avsnitt 5.1.3.

Kombinerte algoritmar for kryptering og autentisering legg til rette for både konfidensialitet og integritet. Slike algoritmar vil effektivisera IPSec, men førebels er ingen slike algoritmar støtta.

Kombinasjon av AH og ESP. AH og ESP kan nyttast i kombinasjon. I så fall må AH plasserast framfor ESP slik at mottakar kan autentisera avsendar og integritetssjekka pakken før dekryptering.

5.1.3 Nøkkelhandtering

IPSec legg til rette for ei rad sikkerhetsmekanismar. Dei fleste nyttar kryptografiske nøklar.
Eit separat sett av prosedyrar og protokollar er definert for å handtera desse nøklane (*key management*). IPSec støttar både manuell og automatisk handtering. Å konfigurera og handtera nøklar manuelt er tidsøydande. Referanse [67] seier at IKEv2 skal brukast for automatisk nøkkeldistribusjon, men andre mekanismar kan òg brukast. Når ein SA vert forhandla, utvekslar partane to par av meldingar. Det første meldingsparet forhandlar kryptografiske algoritmar og utvekslar nøklar ved hjelp av Diffie-Hellman-algoritmen. Deretter vert identitetar og eventuelt sertifikat utveksla. Kvart endepunkt har sin eigen policy vedrørande levetida til SA. Dette medfører at endepunktet med kortast levetid må initiera reforhandling.

5.1.4 Databasar

IPSec omfattar tre sentrale databasar:

- *Security Policy Database* (SPD) spesifiserer policyar for korleis ein port (*gateway*) eller vertsmaskin skal handtera lokal og global trafikk. Bruk av SPD-policy fører til ein av tre moglege prosesseringsreglar: kast (*discard*), la gå utanom (*bypass*) eller vern (*protect*)
- *Security Association Database* (SAD) registrerer kvar SA med parametrar
- *Peer Authorization Database* (PAD) gir ein link mellom protokollen som handterer SA, til dømes IKEv2, og SPD.

5.1.5 Yteevne

Låg yteevne har hittil vore ei årsak til at til IPSec er lite utbreidd. *Benchmarking Methodology Working Group* (BMWG) [2], ei arbeidsgruppe innan IETF, har utarbeidd terminologi [27] og metodar [20] for testing av yteevna til dei ulike IPSec-elementa.

5.2 Offentleg nøkkel-infrastruktur for IP (PKIX)

Sidan 1995 har IETF ved arbeidsgruppa for PKIX [87] utvikla IP-standardar for ein X.509-basert infrastruktur for offentlege nøklar. Arbeidsområdet er seinare utvida til å omfatta standardar for allmenn bruk av X.509-basert infrastruktur i det globale internettet. Ein oversikt over arbeidet er gitt i [19]. X.509-baserte infrastrukturar føreset bruk av sertifikat [10]. PKIX handterer to typar sertifikat:

- Sertifikat for *offentlege nøklar* som inneheld den offentlege nøkkelen til ein entitet samt noko anna informasjon.
- Sertifikat for *attributtar* som inneheld attributtane til ein entitet samt noko anna informasjon.

Begge sertifikattypar vert signert med den private nøkkelen til sertifiseringsinstansen som skriv ut sertifikata. Alle systementitetar må ha den offentlege nøkkelen til denne instansen for å verifisera sertifikata.

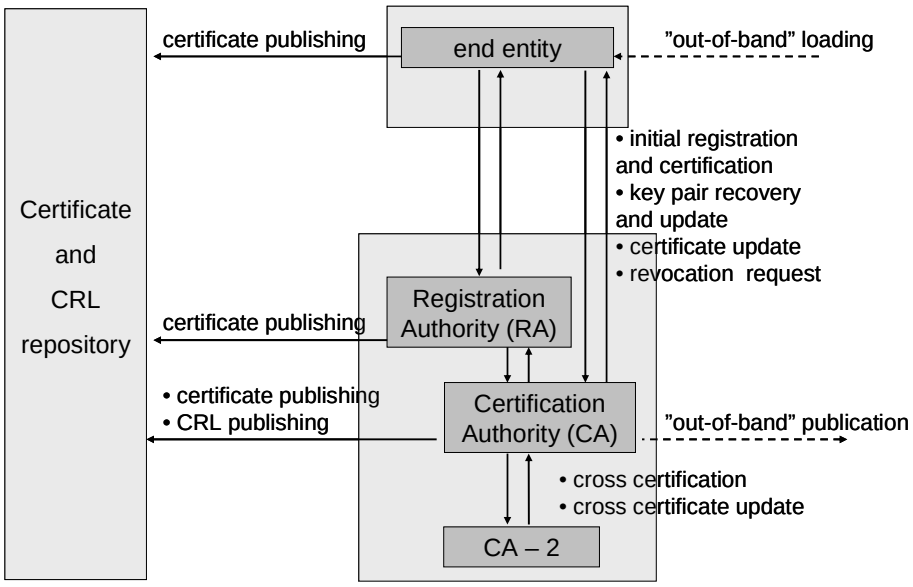
5.2.1 Infrastruktur for offentlege nøklar

PKIX definerer *Public Key Infrastructure* (PKI) som *The set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke public key certificates based on public-key cryptography*.

Infrastrukturen er tradisjonell og inneheld fem komponenttypar:

- Registreringsinstans (*Registration Authority*) (RA) som garanterer bindinga mellom offentlege nøklar og identiteten til innehavarane av sertifikata
- Sertifiseringsinstans (*Certification Authority*) (CA) som skriv ut og trekkjer attende offentleg nøkkel-sertifikat
- Innehavarar av utskrivne sertifikat som kan signera dokument digitalt med private nøklar
- Klientar som kan validera digitale signaturar ved hjelp av ein kjend offentleg nøkkel frå sertifiseringsinstansen
- Register som lagrar sertifikat og tilbakekallingslister (*Certificate Revocation List*) (CRLs) og gjer desse tilgjengelege.

Sjølve sertifikatet er basert på X.509-standarden frå ITU-T. Denne vart publisert i 1988 som del av rekommandasjonane for *X.500 Directory*. Fleire tillegg til det opphavlege sertifikatformatet er seinare standardisert innan ITU-T. Figur 5.8 syner ein oversikt over arkitekturmodellen som IETF nyttar for PKIX.



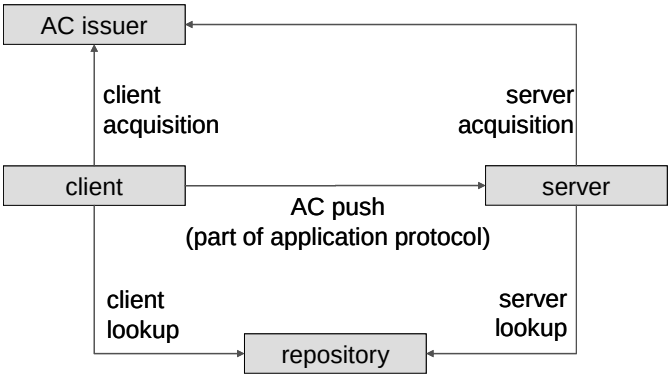
Figur 5.8 Arkitekturmodellen for PKI [63]

5.2.2 Infrastruktur for handtering av privileg

PKIX definerer *Privilege Management Infrastructure* (PMI) som *The set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke attribute certificates.*

Infrastrukturen inneheld fem komponenttypar:
- Attributtinstans (*Attribute Authority*) (AA) som skriv ut og trekkjer attende attributtsertifikat
- Sluttbrukarar som prosesserer attributtsertifikat
- Verifiserarar som sjekkar validiteten av eit attributtsertifikat for deretter å bruka resultatet
- Klientar som spør etter ein aksjon som treng autorisasjon for å verta utført
- Register som lagrar sertifikat og tilbakekallingslister og gjer dei tilgjengelege.

Figur 5.9 syner korleis attributtsertifikat vert utveksla. IETF føreset til dømes at attributtsertifikat vert brukt i prosedyrar for autentisering, autorisasjon og bruksregistrering i samband med nettaksess [47].



Figur 5.9 Utveksling av attributtsertifikat [52]

5.2.3 Spesifikasjonar

Ei rekkje spesifikasjonar er utarbeidd på fem ulike felt. I det følgjande vert nokre av dei nemnd:

Profilar. Eit X.509-sertifikat for offentlege nøklar er ein svært kompleks datastruktur. Strukturen inneheld grunnleggjande informasjonsfelt, men opnar for svært mange tillegg. Dette gir stor fleksibilitet, men samstundes vert det vanskeleg å laga uavhengige interoperable implementasjonar. IETF har difor utvikla ein *profil* av sertifikatet, *the Internet PKI Profile*. Denne profilen spesifiserer kva for tillegg som skal, kan og ikkje skal støttast. PKIX-gruppa foreslår verdisett for fleire av desse tillegga. Profilen er spesifisert i [51], [72] og [75]. På same vis er ein profil for attributtsertifikat spesifisert i [52].

Operasjon. Desse spesifikasjonane dreier seg om dei systema som må til for å distribuera sertifikat og tilbakekallingslister og gjeld bruk av register- og katalogsystem ved hjelp av

Lightweight Directory Access Protocol (LDAP) [40], ein ny protokoll som hentar ut informasjon om sertifikatstatus uavhengig av tilbakekallingslister [41], bruk av protokollane *File Transfer Protocol* (FTP) og *Hyper-Text Transfer Protocol* (HTTP) til å henta sertifikat og tilbakekallingslister [42] samt nøkkelforhandlingsalgoritmar som kan brukast dersom kommunikasjonspartane ikkje har interoperable offentlege nøklar [46].

Sertifikathandtering. Protokollar trengs for å få til interaksjon mellom sluttbrukarane og drift- og styringssystema, til dømes mellom eit klientsystem og ein sertifiseringsinstans eller mellom to sertifiseringsinstansar ved kryss-sertifisering. *Certificate Management Protocol* (CMP) er spesifisert i [63]. Tilhøyrande meldingsformat er definert i [64].

Sertifikatpolicy. For å laga ein sikker infrastruktur for offentlege nøklar trengs ein sertifikatpolicy og mekanismar som kan handheva denne. PKIX har utarbeidd eit rammeverk som identifiserer element som bør eller kan vera med i ein sertifikatpolicy [56]. Det vert ikkje definert nokon spesifikk policy.

Tidsstempling og datasertifisering. Tidsstempling er ei teneste der ein tiltrudd tredjepart, ein tidsstemplingsinstans (*Time Stamp Authority*) (TSA), signerer ei melding for å prova at meldinga *eksisterte* på det aktuelle tidspunktet. TSA legg til eit tidspunkt og signerer så meldinga utan å verifisera at ho er *korrekt*. Ettersom desse spesifikasjonane kan vera patenterte, er arbeidet ikkje vidareført. I staden har PKIX spesifisert *Data Validation and Certification Server* (DVCS) *protocol* [48]. I dette konseptet er DVCS ein tiltrudd tredjepart som i motsetning til TSA, òg verifiserer at ei melding var *korrekt* på det aktuelle tidspunktet. Dette gir eit betre vern mot ikkje-autorisert gjentaking og styrkar dermed ikkje-fornektingsfunksjonen (*non-repudiation*). DVCS kan delegera valideringsfunksjonen til ein annan server ved hjelp av ein definert signaturpolicy.

5.2.4 Tillitsmodellar

Fleire tillitsmodellar har vore utvikla og utprøvd. Det sentrale spørsmålet i desse modellane er kvar i domenet dei tiltrudde entitetane skal lokaliserast. Ein av dei første modellane var ein hierarkisk modell der den tiltrudde sertifiseringsinstansen er toppinstansen (*root*) for heile domenet. I ein slik modell er underinstansar organisert i eit hierarki. For å verifisera eit sertifikat må kvart sertifikat på stien frå det lågaste nivået til toppen verifiserast. Det er òg foreslått ein lokal modell der ein per definisjon har tiltru til den instansen som har skrive ut sertifikatet. Ved forespørsel om eit "framandt" sertifikat, kan lokale sertifiseringsinstansar setja opp tillitskjeder seg i mellom. I desse tilfella må kvart sertifikat på stien mellom dei to aktuelle instansane verifiserast. Eit tredje alternativ er å la sluttbrukar avgjera kva for instansar han godtek sertifikat frå. I dette tilfelle trengs ingen kryssertifisering mellom instansar. Eit fjerde er å basera seg på eit sett av reglar, dvs ein policy, der ein spesifiserer eksakt kven ein har tiltru til i ulike samanhengar.

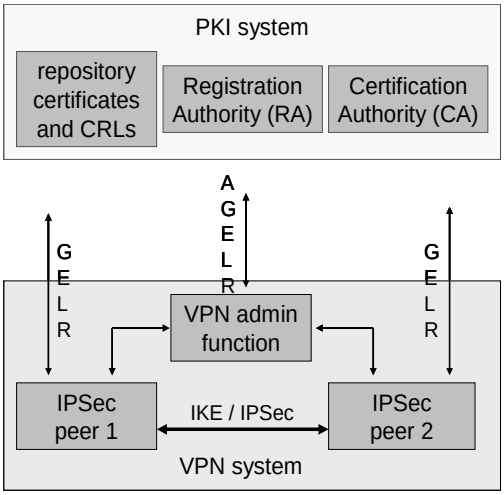
5.2.5 Namn

Infrastrukturen er "namnesentrisk" i det at sertifikata bind ein offentleg nøkkel eller eit attributtsett til *namnet* på innehavaren. I sertifikatet har innehavaren minst eitt namn. Namnet kan vera eit X.509 *Distinguished Name* (DN). Dersom ein tek i bruk eit tillegg til sertifikatprofilen,

kan til dømes epost-adresse, IP-adresse og *Uniform Resource Locator* (URL) vera gyldige namn.

5.3 Bruk av offentleg nøkkel-infrastruktur i IPSec

At X.509-sertifikat skal brukast, er spesifisert i IPSec, men det er ikkje klart *korleis* dei skal brukast. Dette kan vera ei årsak til at svært få IPSec-implementasjonar nyttar sertifikat. Ein annan grunn kan vera at det manglar metodar for korleis eit IPSec system skal kommunisera med eit PKI-system på ein effektiv måte. Difor har IETF sett ned arbeidsgruppa *Profiling Use of PKI in IPSEC* (pki4ipsec) [85]. Arbeidsgruppa har mellom anna laga to *Internet-Drafts*: [29] og [25]. Førstnemnde draft foreslår ein PKIX sertifikatprofil som kan nyttast i samband med IKE og IPSec. Dokumentet understøttar dermed spesifikasjonen av IKE som føreset at det eksisterer eit system for offentlege nøklar, men som ikkje adresserer dette området særskilt. Sistenemnde draft skildrar det naudsynte samspelet mellom IPSec og PKIX når ein skal bruka og vedlikehalda offentleg nøkkel-sertifikat i IPSec-applikasjonen VPN. Figur 5.10 syner eit døme på korleis ein tenkjer seg at dei to systema IPSec og PKIX skal operera saman.



A:	Authorization: public key certificate (pkc) issuance
G:	Generation: public and private keys, and pkc request
E:	Enrollment: sending pkc request, verifying and confirming pkc response
L:	Lifecycle: rekey, renew, update, revoke and confirm
R:	Repository: posting and look-up

Figur 5.10 Bruk av PKI i eit VPN med IPSec [25]

5.4 Andre arkitekturar

Som tidlegare nemnd, er det innan IETF utvikla fleire sikkerhetsarkitekturar som dekkar avgrensa område. Av dei mest kjende er TLS [73] som er vidareutvikla frå SSL. Arkitekturen skal sikra protokollar på applikasjonslaget, i første rekkje HTTP, og inneheld mekanismar som ligg dels mellom transportlaget og applikasjonslaget og dels på applikasjonslaget. Mekanismane sikrar sesjonane mellom klientar og tenarar, og tilbyr konfidensialitet og integritet for nyttelasta. Siste

tida har det særleg vore arbeidd med å finna nye og betre algoritmar for kryptering og autentisering [93].

Eit arbeid som kan vera relevant for NbF målnett, vert utført i ei arbeidsgruppe for *Protocol for carrying Authentication for Network Access* (PANA) [86]. Bakgrunnen for arbeidet er scenarium der ein IP-basert terminal må autentisera seg for nettet før han kan bruka det. Slik autentisering krev ein protokoll som kan støtta mange ulike autentiseringsmetodar og dynamisk val av tenestetilbydar. I dag nyttar ein ei rekkje løysingar for ulike kommunikasjonslag, men mykje tilseier at nettlaget kan tilby ei reinare løysing. Ved hjelp av PANA kan ein terminal autentisera seg ved bruk av IP-protokollar. PANA er ingen ny autentiseringsprotokoll, men heller ein generisk berar av autentiseringsprotokollar, som til dømes *Extensible Authentication Protocol* (EAP) [34] som autentiserer adresser på lågare kommunikasjonslag. Identitetar som kan autentiserast via PANA kan til dømes vera ei IP-adresse, ei linklag-adresse eller eit portnummer på ein switch. PANA-gruppa har utarbeidd trugsmålsanalyse [61] og kravspesifikasjon [62]. Eit rammeverk [23] og sjølve protokollen [24] er under arbeid. Av særleg interesse er arbeidet med interoperabilitet mellom PANA og IPSec [22].

5.5 Kommentarar

I dette kapittelet har me sett på dei viktigaste reiskapane for å sikra IPv6-nett. Sidan korkje IPv6 eller IPSec per i dag er deployert i stor skala, er det usikkert i kor stor grad sikringsløysingar som er utvikla primært for IPv4, vil overleva under IPv6/IPSec.

Eit anna viktig moment er at så vel arbeidet med IPSec som arbeidet med PKI føreset eit underliggjande *fastnett*. Så langt me kjenner til er det utført svært få studiar av IPv6 i trådlause nett. Det same gjeld IPSec og tradisjonelle PKI-løysingar som PKIX.

6 Er sikkerhetsstandardane gode nok ?

I kapittel 5 presenterte me IPSec og PKIX. Begge arkitekturane tilbyr allmenne sikkerhetstenester. Dei er ikkje utvikla for å sikra *nettinformasjonen* spesielt. Dette kapittelet presenterer nokre døme frå IETF sitt arbeid med å sikra denne typen informasjon. Me undersøkjer òg kor vidt arkitekturane frå kapittel 5 kan ivareta krava til konfidensialitet, integritet og tilgjenge frå kapittel 3, og om dei kan gje løysingar som er fleksible og effektive nok for nettinformasjonen i NbF målnett. Me ser særskilt på protokollane som er aktuelle for NbF målnett, sjå avsnitta 2.1.2 og 2.1.3.

6.1 Sikker ruting

I dette avsnittet skal me undersøkja om arkitekturane frå kapittel 5 kan nyttast til å sikra rutinga i IP-nett. Ein kort og god oversikt over relevante problemstillingar innan sikker ruting er gitt i [81]. Å sikra rutinginformasjonen var ikkje eit viktig omsyn då dei eksisterande rutingprotokollane vart utvikla. Hittil har det ikkje vore standardkrav til sikker ruting. For å bøta på dette har IETF sett ned fleire arbeidsgrupper som utfører eit omfattande arbeid. Ei sentral gruppe er *Routing Protocol Security Requirements Working Group* (RPSEC) [88] som skal dokumentera krav til sikring av nestegenerasjon rutingsystem. Arbeidsgruppa har hittil publisert fleire *Internet-Drafts* vedrørande trugsmål mot og veikskapar i eksisterande rutingprotokollar. Ei anna gruppe er *Secure Inter-Domain Routing Working Group* (SIDR) [90]. Denne gruppa skal utarbeida ein arkitektur for sikker ruting mellom domene. Når autonome system utvekslar ruter til destinasjonsadresser, er autentisering og autorisasjon særleg viktig. Gruppa skal òg spesifisera mekanismar i samsvar med krav utarbeidd av RPSEC, og har hittil publisert eit *Internet-Draft* vedrørande digitale sertifikat for nettressursar. I dette avsnittet presenterer me noko av arbeidet til desse gruppene.

6.1.1 Generiske trugsmål mot rutingprotokollar

Referanse [45] definerer eit trugsmål som *a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm*. RPSEC-gruppa har utarbeidd ein generisk trugsmålsmodell for rutingprotokollar [74]. Denne modellen byggjer på åtak som har vore kjent frå sivile IP-nett i ei årrekkje. Me presenterer denne modellen fordi han kan vera nyttig i framtidig utforming av tilsvarande modellar for NbF målnett og fordi han gir bakgrunn for å ta stilling til kor vidt IPSec og PKIX kan nyttast til å sikra rutinginformasjon. Motivasjonen for ein generisk modell er følgjande fellestrekk ved (dei aller fleste) rutingprotokollar:

- Dei brukar eit subsystem for å transportera rutingmeldingar. Dette kan vera protokollar som UDP, TCP eller IP
- Dei vedlikeheld tilstandsinformasjon om nabonodane
- Dei vedlikeheld databasar med informasjon om topologien i heile eller delar av kommunikasjonsnettet
- Dei har grovt sett to typar meldingar:
  - Meldingar som inneheld informasjon om tilstanden i kommunikasjonsnettet

- Meldingar som inneheld informasjon om tilstanden i sjølve rutingprosessen.

Modellen kategoriserer trugsmåla etter kjelde og konsekvens:

- *Kjelde*. Ei trugsmålskjelde har motiv og kapabilitetar som må analyserast spesifikt for kvar kjelde. Kjelder vert delt inn i to grupper: Utanforståande kjelder som ikkje er legitime deltakarar i rutingprotokollen og byzantinske[1] kjelder som er legitime deltakarar. Fiendtlege aktørar er døme på utanforståande, medan eigne ruterar med feil er døme på byzantinske trugsmålkjelder
- *Konsekvens*. Ein aksjon kan vera retta mot datatrafikken til eit spesifikt subnett eller mot ei maskin, men aksjonen kan like gjerne vera retta mot heile nettet. Modellen skil mellom fire ulike konsekvensar:
  - At rutinginformasjon vert *avdekka* når ikkje-autoriserte får tilgang. Sjølv om slik avdekking representerer ein risiko, er rutingprotokollar sjeldan utforma for å handtera rutinginformasjon med konfidensialitetskrav
  - At ein legitim ruter vert *lurt* når han til dømes mottek ei falsk rutingmelding og prosesserer denne som om ho var autentisk. Dette følgjer når ruteren ikkje er i stand til å autentisera meldingskjelda og verifisera integriteten til meldinga
  - At IP-nettet vert *forstyrra* og trafikken eventuelt avbroten. Dette kan til dømes vera resultat av at falsk rutinginformasjon er lurt inn i systemet. Legitime byzantinske kjelder kan òg korrumpera rutingsinformasjon med *trafikkavbrot* som følgje
  - At heile eller delar av IP-nettet er *overteke* av angripar ved at denne har fått kontroll over tenester og funksjonar som legitime ruterar tilbyr. Dette kan til dømes vera resultat av at nøye planlagt falsk rutinginformasjon er lurt inn i systemet. Legitime byzantinske kjelder kan òg medverka til at utanforståande oppnår kontroll.

Konsekvensane vert vidare analysert ut frå tre andre aspekt:

- *Verknad.* Åtak retta mot ei eller fleire spesifikke nettadresser, kan til dømes føra til at trafikk mynta på desse adressene vert avlytta og eventuelt reruta for seinare trafikkanalyse, at trafikken vert forseinka, går i evig sløyfe i nettet eller at adressene vert isolerte frå resten av nettet. Er åtaket retta mot heile nettet, kan det til dømes medføra trafikkopphoping og metting, at store trafikkmengder vert reruta mot spesifikke nodar (*black holes*), rutingsløyfer (*loops*), at nettet vert delt i fleire partisjonar, store variasjonar i måten pakkar vert vidaresende (*churn*), ustabilitet og unormalt stor rutingtrafikk
- *Omfang*. Dette kan vera frå ein einskild link eller ein einskild ruter til det globale internettet
- *Periode*. Einskilde truslar vil ha ein konsekvens så lenge åtaket pågår. Andre truslar har konsekvensar som varer lengre.

RPSEC-gruppa identifiserer ei rekkje konkrete trugsmål og nyttar modellen til å analysera dei. Dette gjeld trugsmål som informasjonsavdekking, identitetstjuveri, informasjonsforfalsking, overbod, feilbod, trafikkanalyse og overlast.

[1] Ei såkalla byzantinsk kjelde oppfører seg vilkårleg når ho feilar. Ein slik node kan til dømes senda tilfeldige meldingar på tilfeldige tidspunkt eller utføra andre operasjonar som er i strid med protokollane.

Konsekvensar av trugsmål kan kvantiserast langs fire dimensjonar. Dimensjonane ser ut til å vera fornuftig valde. Modellen gjer det mogleg å skilja mellom indre og ytre kjelder, og mellom åtak med og utan intensjon. Det siste har kanskje ikkje mykje å seia med omsyn til konsekvensar, men kan ha mykje å seia for risikovurdering og policy. Risiko for trugsmål er ikkje med i modellen, men dette aspektet kan kvantiserast og enkelt inkorporerast.

Modellen gir eit godt utgangspunkt for å analysera relevante trugsmål mot rutingprotokollane i NbF målnett. Modellen er utarbeidd på grunnlag av røynsler frå ruting i fastnett. Sidan modellen er generisk, kan han brukast og detaljerast for ulike typar nett og scenarium. Sjølv om trugsmål, konsekvens og risiko kan vera noko annleis i ad hoc-ruting bør ein modell av denne typen òg kunna brukast for slike nett.

6.1.2 Korleis kan rutingprotokollane sikrast?

I dette avsnittet ser me nærmare på dei mest relevante rutingprotokollane i lys av trugsmålsmodellen presentert i avsnitt 6.1.1 og sikkerhetsarkitekturane presentert i kapittel 5. Alle dei aktuelle rutingprotokollane er utvikla utan sikkerhet som viktig aspekt. Sikkerhetstenester har kome til seinare.

OSPF. Ein viktig skilnad på OSPFv2 for IPv4 og OSPFv3 for IPv6 er at sistnemnde baserer seg på AH og ESP i IPSec, sjå avsnitt 5.1.2. Autentiseringstenesta som er innbygd i OSPFv2 er teken bort. RPSEC-gruppa har laga ein sårbarhetsanalyse av OSPF v2 [21], og mykje i denne analysen er òg relevant for OSPFv3. OSPF er i utgangspunktet sårbar overfor generiske åtaksteknikkar som avlytting, ikkje-autorisert innsetting/sletting/modifisering/gjentaking av meldingar, *man-in-the-middle* og *denial-of-service*-åtak. Den svake autentiseringstenesta i OSPFv2 gjer protokollen svært sårbar overfor ikkje-autoriserte protokollmeldingar. Ein angripar som sender meldingar med feilinformasjon, vil raskt kunna gjera stor skade. Dette gjeld særleg globale meldingar som skal *floodast* til heile nettet. Analysen går gjennom alle meldingstypar og skildrar konsekvensar av ikkje-autorisert endring av informasjonen. IPSec tilbyr ei sterkare sikring av protokollen. OSPF køyrer direkte over IP, og eit viktig aspekt er at IPSec, i motsetning til den særeigne OSPFv2-autentiseringa, sikrar IP-hovudet. Dette gjer at OSPFv3 vil vera mindre sårbar overfor generelle åtak på IP. Det er ikkje slik at IPSec under IPv6 vil tetta alle hol som vert påvist i analysen. Det vil difor vera naudsynt med ein nøye gjennomgang før overgang til IPv6. Det vert vidare understreka at autentiseringsprosedyrar gjer protokollen sårbar overfor ein inntrengjar som sender mengder av meldingar til ein ruter som i sin tur brukar prosesseringskapasitet berre for å forkasta meldingane etterpå.

IPSec opererer på nettlaget, og ein kan merka seg at autentiseringa gjeld *IP-adressa*, ikkje *OSPF-identiteten* som er kjelda for OSPF-meldinga. Meldinga ligg som nyttelast i IP-pakken. IPSec autentiserer ikkje *originatoren av nyttelasta* korkje i transportmodus eller i tunnelmodus.

BGP. BGP versjon 4 (BGP-4) er i dag *de facto* rutingprotokoll for interdomeneruting i det globale internettet, men har ingen sikringsmekanismar innebygd. Standarden krev no at TCP-sesjonane vert verna ved hjelp av MAC. Den aktuelle autentiseringsalgoritmen, *TCP-MD5*, er

spesifisert i [35] og er ei enkel minimumsløysing. Den første heilskaplege arkitekturen for sikker interdomeneruting, *Secure BGP* (S-BGP), vart foreslått i 2000 [78]. Sentralt i S-BGP er eit autorisasjons- og autentiseringssystem basert på ein offentleg nøkkel-infrastruktur og X.509-sertifikat. Sikring av BGP har seinare vorte eit aktivt forskingsområde.

RPSEC-gruppa har laga ein kravspesifikasjon for sikkerhet i BGP-4 [15]. Det vert særleg lagt vekt på dataintegritet og autentisering av meldingskjelde, men spesifikasjonen nemner ikkje konkrete infrastrukturar som IPSec og PKIX. Det gjer derimot den tidlegare nemnde SIDR-gruppa. Gruppa har arbeidd med ein profil for X.509 ressurssertifikat. Ressurssertifikat er tidlegare spesifisert i [60]. Eit ressurssertifikat spesifiserer assosiasjonen mellom sertifikatinnehavaren og dei nettressursane han kan kontrollera, og kan til dømes spesifisera dei destinasjonsadressene eit AS har lov å annonsera overfor andre AS. Sertifikatet vil òg kunna ha ei rekkje andre bruksområde innanfor interdomeneruting. Den nye standardprofilen spesifiserer mellom anna kva for felt som må vera til stades for at sertifikatet skal vera gyldig. Arbeidet byggjer vidare på BGP-S. SIDR-gruppa har vidare spesifisert policy for dette området [26] samt reglar for sertifiseringsautoritet og sertifikatregister [16].

Det er uklart korleis BGP vil verta implementert i IPv6. Det finns ingen IPv6-versjon av protokollen, men IPv6 og BGP-4 kan operera saman sidan BGP-4 har tilleggsfunksjonalitet for å utveksla informasjon med andre nettlagsprotokollar enn IPv4. Dei generelle fleirprotokolltillegga til BGP-4 er spesifisert i [76]. Dessutan er det spesifisert eit ”BGP-tillegg” til IPv6 [39]. Det vil vera naudsynt med ein nøye gjennomgang av tilgjengelege sikkerhetstenester for BGP før overgang til IPv6.

Multikastruting. Ein god oversikt over sikkerhetsspørsmål i multikastkommunikasjon er gitt i [82]. Artikkelen går gjennom ulike arkitekturar for sikker gruppehandtering, handtering av gruppenøklar samt autentiseringsløysingar for kjelder og destinasjonar. For dette området har IETF oppretta arbeidsgruppa *Multicast Security* (MSEC) [83] som har som formål å standardisera protokollar for sikker gruppekommunikasjon over IP, særleg over det globale internettet. Gruppa har utarbeidd ein arkitektur for sikker multikastruting [59], og har på grunnlag av denne fremja ei rekkje rfc’ar og draft for delområde innanfor dette feltet.

Ad hoc-ruting. Dei mest relevante rutingprotokollane for mobile trådlause ad hoc-nett vart i likskap med dei tradisjonelle, utvikla for scenarium der alle nodar er tiltrudde. Protokollane som er med i standardiseringsarbeidet til IETF er døme på slike. Sikkerhetsløysingar har vorte foreslått *etter* at protokollane har teke form. Rutingprotokollane er limet i ad hoc-nett. Utan ein fungerande rutingprotokoll vil ein i beste fall stå att med ei samling isolerte eitthopp-nett. Samstundes er desse protokollane meir sårbare enn protokollar i trådbaserte og stasjonære nett. Sikker ad hoc-ruting er eit aktivt forskingsfelt. Gode oversiktar over generelle åtak på rutinginformasjon i ad hoc-nett finns i [4] og [77]. Ein kan her merka seg at trugsmål og åtaksteknikkar i stor grad er dei same som skildra i trugsmålsmodellen presentert i avsnitt 6.1.1. Det vil vera ein viss skilnad på proaktive og reaktive protokollar med omsyn til kva for funksjonar som er sårbare og til konsekvensen av ulike typar åtak. Eit konkret åtak vil sjølvsagt ta

utgangpunkt i protokollspesifikke veikskapar.

6.1.3 Diskusjon

I avsnitt 3.2.1 såg me på rutinginformasjon med omsyn til konfidensialitet og integritet. Både IETF-dokumenta og det meir forskingsbaserte arbeidet med sikring av ad hoc-protokollar har nokre fellestrekk:

- Det er ikkje *konfidensialitetskrav* for rutinginformasjonen. Det kan difor vera grunn til å tru at sivile aktørar ikkje vil gå i bresjen for å utvikla løysingar for dette. Det er vidare grunn til å tru at det er lite røynsle med til dømes krypterte rutingmeldingar. Sidan rutingmeldingar ligg som nyttelast i ein IP-pakke, vil IPSec gjera det mogleg å kryptera dei
- Det vert derimot lagt stor vekt på *integritetskrav* for rutinginformasjonen. Dette gjeld autentisering av meldingskjelder, verifikasjon av at meldinga ikkje er modifisert på ikkje-autorisert vis på vegen frå kjelda samt at meldinga er ny og gyldig. Som me har sett tidlegare, gir IPSec støtte for dette. Det er uklart om IETF tenkjer seg at IPSec og PKIX skal integrerast for å sikra rutinginformasjonen
- Sikkerhetsdokumenta frå IETF handterer berre *utvekslinga* av rutinginformasjon. Sikring av *prosessering* og *lagring* vert ikkje omtalt. Etter det me kjenner til, gjeld dette òg forskinga på sikker ad hoc-ruting
- Dokumenta handterer ikkje sikkerhetsproblematikk knytt til portar (*gateway*s) mellom to ulike rutingprotokollar, til dømes OSPF og BGP, eller OSPF og W-OSPF. Etter det me kjenner til, gjeld dette òg forskinga på sikker ad hoc-ruting
- Dokumenta handterer ikkje fleirnivå sikkerhetsmodellar, som dei me såg på i kapittel 3. Etter det me kjenner til, gjeld dette òg forskinga på sikker ad hoc-ruting, men det finns publiserte konsept som opnar for fleirnivå sikkerhetsmodellar for rutinginformasjon [97] og [94].

Ut frå spesifikasjonane vil IPSec kunna tilfredsstilla både eventuelle krav til konfidensialitet og krav til integritet ved utveksling av rutinginformasjon. Det er ikkje dermed sagt at IPSec vil vera ei *god* løysing. Det er ei rekkje spørsmål som reiser seg ved bruk av IPSec. Nokre av dei er knytt til det å sikra rutingmeldinga ved å sikra heile IP-pakken. Andre er knytt til sjølve IPSec-arkitekturen.

Døme på den første typen spørsmål er: Dei globale rutingmeldingane skal vidaresendast av mottakarane, ofte ved full eller delvis flooding. I mange tilfelle skal mottakaren endra verdiar i einskilde meldingsfelt før han vidaresender. Dette inneber at ein IP-pakke med rutingmelding må pakkast ut for kvart hopp. Rutingmeldinga skal så modifisert og leggjast i ein ny IP-pakke. Dette vil seia at IPSec-basert konfidensialitet og integritet vil gjelda hopp for hopp. Ei løysing basert på rutingmeldinga *åleine*, ville enkelt kunna halda felt som skal modifiserast utanom. Dette ville truleg både vera sikrare og i tillegg redusera prosesseringsarbeidet for kvar node.

Spørsmåla knytt til sjølve IPSec-arkitekturen er mange. Som synt i avsnitt 5.1.1, trengs 4 SA'ar dersom kommunikasjonen mellom to entitetar skal sikrast av både konfidensialitets- og integritetstenester. Proaktive *link-state* rutingprotokollar som til dømes OSPF og OLSR, krev i utgangspunktet at kvar node kan kommunisera med alle andre. Det må difor setjast opp SA'ar

mellom alle par av nodar. Dette vil seia talet på SA'ar gitt ved:

$$4 * (n(n-1))/2 = 2(n(n-1)), \text{ der } n \text{ er talet på ruterar.} \quad \text{(I)}$$

Me ser at dette ikkje skalerer bra. Det skal forhandlast *ein* nøkkel per SA. Det vil seia at eit nett med 20 nodar må handtera 760 ulike nøklar samstundes. For eit nett med 40 nodar er tilsvarande tal 3120. Med ein fleirnivå sikkerhetsmodell kan dette lett verta mange nøklar. Eit anna aspekt er at noden ikkje bør bruka dei same nøklane for både rutinginformasjon og sluttbrukarinformasjon. Dette kan løysast ved å setja opp fleire SA'ar, ikkje nødvendigvis mellom alle par av nodar, men mellom alle par av nodar der sluttbrukarane må kunna kommunisera sikkert. Eit tredje aspekt er kor lengje kvar SA skal vara. Dette er først og fremst eit spørsmål om kor lengje ein kan tillata at ein og same nøkkel er i bruk. Eit nett der SA'ar har kort levetid vil i prinsippet vera sikrare enn eit nett der levetida er lang. På den andre sida vil stadig fornying av SA'ane og reforhandling av nøklar krevja mykje nettressursar.

Me kjenner ikkje til publiserte framlegg om å bruka IPSec til å sikra rutingprotokollar i mobile trådlause ad hoc-nett. Som tidlegare nemnd, er det eit mål at IPv6 skal mogleggjera IPSec-funksjonalitet på kvar maskin. Skaleringsproblema knytt til oppsettet av SA'ar vil dermed lett kunna verta eit stort problem i faste nett òg.

Det kan sjølvsagt argumenterast med at ein ikkje treng å bruka den dynamiske nøkkelhandteringa som IPSec tilbyr gjennom IKE. Ein kan heller førehandskonfigurera alle naudsynte SA'ar med ein og same nøkkel. Dette er sjølvsagt mogleg dersom *ein felles* nøkkel er sikkert nok for eit rutingdomene. I tillegg til å vera lite robust, vil statisk nøkkelkonfigurering vera ei lite fleksibel løysing med tanke på rask samanslåing, oppsplitting og omorganisering av rutingdomene. Løysinga vil ikkje understøtta dynamikken ein ynskjer seg i NbF målnett.

Dei fleste rutingprotokollar kringkastar meldingane. IPv6 handterer kringkasting som eit spesialtilfelle av multikast. IPSec er spesifisert for å handtera multikast-SA'ar. Det er ikkje utenkjeleg at multikastfunksjonalitet kan redusera administrasjonen av SA'ar og nøklar. Dersom kvar node vert definert som kjelde i ei multikastgruppe der alle andre nodar er mottakarar, og kvar multikastgruppe har felles nøkkel, kunne ein i prinsippet få til ei lineær skalering. Dei same føresetnadene som me brukte i (I), vil då gje 4*n* multikast-SA'ar og tilsvarande tal på gruppenøklar. Samspelet mellom IPSec og eksisterande multikastspesifikasjonar er førebels uklart og det er ikkje opplagt at ei slik løysing er i tråd med intensjonane for dette samspelet.

Som før nemnd er skaleringsproblem ei årsak til at IPSec ikkje er implementert i mange IPv4-baserte nett. Ein analyse av prosesseringstider for dei ulike elementa i IPSec er dokumentert i [91]. Ikkje uventa finn forfattarane at generering av signaturar er den mest tidkrevjande operasjonen i IKE, medan kryptering er den dyraste operasjonen i prosesseringa av ESP-sikra IP-pakkar. Ein analyse av overføringstid i trådbaserte og trådlause nett er dokumentert i [6]. Analysen samanliknar ulike kombinasjonar av AH og ESP og ulike filstorleikar for applikasjonslagprotokollane HTTP og *Simple Mail Transfer Protocol* (SMTP). Begge analysane

har konsentrert seg om IPSec i tunnelmodus. Me er ikkje kjent med at det er publisert yteevne-analysar som er i tråd med retningslinjene til BMWG-gruppa, sjå avsnitt 5.1.5. Slike analysar bør utførast før ein går inn for å bruka IPSec til å sikra rutingprotokollar i dynamiske nett med låg overførings- og prosesseringskapasitet.

6.2 Sikker tenestekvalitet

I dette avsnittet skal me sjå korleis spesifikasjonane frå kapittel 5 kan nyttast til å sikra tenestekvalitetsarkitekturane i IP-nett. Me skal sjå på to aspekt: Det eine er å sikra sjølve kvalitetsinformasjonen som ligg til grunn for dei ulike kvalitetsklassane. Det andre er å sikra at berre autoriserte entitetar får tilgjenge til ein gitt tenesteklasse eller ein gitt prioritet. Dette omfattar signalering av kvalitets/prioritetskrav samt naudsynt verifikasjon av identitet og autorisasjonar.

6.2.1 Generiske trugsmål mot tenestekvalitetsarkitekturar

I avsnitt 6.1.1 presenterte me ein trugsmålsmodell for rutingprotokollar. Me kjenner ikkje til at det er utarbeidd ein tilsvarande modell for tenestekvalitetsarkitekturane. I utgangspunktet kan det sjå ut til at både trugsmålskjelder, risiko og konsekvensar vil kunna handterast på same vis som i modellen for ruting. Allment kan ein seia at korrumpert kvalitetsinformasjon vil kunna få same konsekvensar som korrumpert rutinginformasjon. Det same gjeld ikkje-autorisert tilgjenge til kvalitetsklassar og prioritet. Begge delar vil raskt kunna medføra store køar, forseinkingar og pakketap. Ikkje-autorisert tilgjenge vil dermed raskt kunna snu *Quality of Service* til *Denial of Service* for dei autoriserte brukarane. Mobile trådlause nett vil vera særleg sårbare for ikkje-autorisert tilgjenge til tenestekvalitetsmekanismane.

6.2.2 Korleis kan tenestekvalitetsarkitekturane sikrast?

I dette avsnittet ser me nærmare på dei mest relevant tenestekvalitetsarkitekturane. Desse arkitekturane har vore utvikla utan sikkerhet som viktig aspekt. I den grad det finns sikkerhetstenester, har dei vorte lagt til etter at arkitekturane var forma.

Signalering av tenestekvalitetskrav i IPv6. IPv6 har ikkje særeigne mekanismar for tenestekvalitet men kan støtta ulike arkitekturar. I IPv6-hovudet er det to felt som kan nyttast til å formidla krav om spesifikke tenesteklassar: *Traffic Class* [37] og *Flow Label* [58], sjå Figur 4.1.

Traffic Class-feltet vert òg kalla *DS field.* DiffServ skal bruka dette feltet. Innan eit DiffServ-domene har kvar DiffServ-ruter eit kjent sett med rutinar (PHBs), sjå avsnitt 2.1.3. Verdien i feltet vert omsett til ein spesifikk rutine, og ruteren handterer pakken i samsvar med denne. Det er såleis verdien i dette feltet som avgjer kva for tenesteklasse pakken får. Når ei kjelde skal spørja etter ein spesiell tenesteklasse, kan *Flow Label*-feltet brukast. Ein flytmerke (*flow label*) er assosiert med ein spesifikk flyt frå kjelde til destinasjon. Dette understøttar ein arkitektur som tildelar tenesteklassar per flyt, til dømes IntServ med RSVP, sjå avsnitt 2.1.3. Eit par av tilleggshovuda i IPv6 kan òg brukast til å formidla forespørsel om spesifikke tenesteklassar.

Korrekte verdiar i IP-hovudet er såleis eit vilkår for at ein pakke skal handterast i samsvar med

ein gitt tenesteklasse. Dei to aktuelle felta må vera leselege for alle ruterar på stien frå kjelde til destinasjon og kan dermed ikkje krypterast med mindre alle ruterar kjenner nøkkelen. IPSec tilbyr ikkje kryptering av desse felta. Det er vidare verdt å merka seg at desse to felta heller ikkje er omfatta av dataintegritetsprosedyren i IPSec. IPSec kan difor heller ikkje garantera integriteten til desse felta.

DiffServ. Ein DiffServ-arkitektur kan byggjast opp på mange ulike måtar [79]. Nokre fellestrekk finns likevel: Alle DiffServ-ruterar lagrar informasjon om relevante PHBs, men funksjonalitet og prosessering er ikkje like i alle ruterane. DiffServ krev i utgangspunktet lite tilstandsinformasjon om nettet, og utvekslinga av nettinformasjon er difor minimal. På den andre sida, dersom DiffServ skal fungera effektivt, trengs system og mekanismar som overvaker, kontrollerer og styrer tenestekvalitsmekanismane, system som handterer policy [55] og system som handterer avtalar om tenestekvalitet (SLAs). Styresystema skal kunna fjernkonfigurera ruterane og treng difor oppdatert informasjon om nett-topologi, ruter og tilgjengeleg kapasitet på linkane. Kommunikasjonen mellom desse styresystema og ruterane i nettet må sikrast. Det er ikkje gitt at IPSec vil kunna gje tilstrekkeleg konfidensialitet og integritet for denne kommunikasjonen.

IntServ og RSVP. Ein IntServ-arkitektur kan òg byggjast opp på mange ulike måtar. Medan DiffServ handterer tenestekvalitet per hopp for aggregat av pakkar, tilbyr IntServ tenestekvalitet per flyt. Til grunn for kvalitetsgaranti ligg ein flytspesifikk *ressursreservasjon* frå kjelde til destinasjon, altså ende til ende på transportlaget. For at ruteren skal kunna handtera forespørslar frå applikasjonane, må IntServ ha tilgang til global tilstandsinformasjon. RSVP hentar inn mykje av denne, men først og fremst brukar IntServ RSVP til å setja opp ei rute med ønska tenestekvalitet. For å reservera, må dei ønska nettressursane sjølvsagt vera tilgjengelege. I tillegg må brukaren vera autorisert til å gjera reservasjonen.

Sikkerhetsløysingane for RSVP støttar ikkje konfidensialitetskrav. Med omsyn til integritetskrav, definerer [44] ei autentiseringsteneste for RSVP. Ei RSVP-melding må kunna lesast og skrivast til av alle RSVP-ruterar. Dette inneber at meldinga kan sikrast berre hopp for hopp mellom RSVP-ruterar. Referanse [65] gir ei god oppsummering av mange sikkerhetsaspekt knytt til RSVP og dei ulike mekanismane som i dag vert brukt for å sikra protokollen. Mange forbetringar vert foreslått. Både [44] og [65] understrekar at autentiseringstenesta i IPSec er ueigna for RSVP slik spesifikasjonane er i dag. Ei viktig årsak er at IPSec set opp SA'ar mellom kjelde- og destinasjonsadressa for den aktuelle flyten. RSVP-trafikk som er knytt til ein flyt, følgjer ikkje nødvendigvis den same stien som sjølve flyten. Autentiseringstenesta for RSVP tek omsyn til dette. Eksisterande sikkerhetsmekanismar for RSVP er evaluert i [8], som konkluderer med at desse ikkje er gode i trådlause nett.

IPv6 Label Switch Architecture (6LSA). Dette er ein ny arkitektur som er basert på bruken av det før omtalte feltet *Flow Label* i IPv6-hovudet. Ideen er å knyta IP-pakkar til *Forward Equivalent Classes* (FECs). Arkitekturen er svært lik *Multiprotocol Label Switching* (MPLS), men ein viktig skilnad er at 6LSA nyttar IPv6 feltet *Flow Label* i staden for *shim*-hovudet til MPLS. 6LSA er eit heilt nytt konsept og ein må rekna med noko tid før det vert ein standard.

Tenestekvalitet i Ad hoc-nett. Dette er eit aktivt forskingsområde, men me kjenner ikkje til publiserte tenestekvalitetsmodellar der sikkerhet er ein viktig faktor. Dette er ein mangel ved dei foreslåtte arkitekturane.

6.2.3 Diskusjon

Konfidensialitet og integritet. Arkitekturane for både DiffServ og IntServ/RSVP kan byggjast opp på ulikt vis. Ein inntrengjar vil utnytta arkitekturspesifikke veikskapar. Tenestekvalitetsarkitekturar i store nett prosesserer og lagrar store mengder tilstandsinformasjon om nettet. Dersom det er konfidensialitetskrav til rutinginformasjonen, bør det vera minst tilsvarande krav for kvalitetsinformasjonen. Rutinginformasjonen er gjerne ein del av kvalitetsinformasjonen. Vidare er integritetskrav for kvalitetsinformasjonen minst like viktig som for rutinginformasjon. Dette gjeld særleg informasjonsutvekslinga mellom ruterane og dei systema som styrer og fjernkonfigurerer tenestekvalitetsmekanismar på desse ruterane. Det finns ulike protokollar for denne typen kommunikasjon. I utgangspunktet skal IPSec kunna gje den naudsynte sikringa, men dette må sjølvsagt analyserast for den spesifikke arkitekturen og dei spesifikke protokollane som vert valt for NbF målnett. I denne samanhengen er det på nytt verdt å merka seg at IPSec autentiserer *IP-adresser*. IPsec autentiserer ikkje andre typar identitetar. Dette er ingen "feil" ved IPSec, men ein konsekvens av at IPSec opererer på nettlaget. Det *finns* applikasjonar som baserer seg autentiserering av IP-adresser, men ynskjer ein betre granularitet på autentiseringa, må mekanismane implementerast på eit høgare kommunikasjonslag, eller applikasjonen må modifiserast slik at ein sluttbrukar/rolle vert assosiert med ei IP-adresse.

IntServ er basert på rutereservasjon ved hjelp av RSVP. Det er ingen standardar som støttar *konfidensialitetskrav* til reservasjonsprosessen. Med omsyn til *integritetskrav* er som nemnd IPSec ueigna for RSVP. Autentiseringstenesta for RSVP støttar integritetskrav hopp-for-hopp mellom RSV-ruterar som ofte er eit subsett av dei mellomliggjande IP-ruterane, men standarden støttar ikkje krav om integritet ende til ende frå kjelde til destinasjon. Dette kan vera viktig å merka seg sidan rutene vert vedlikehaldne ved hjelp av RSVP-meldingar, til dømes feilmeldingar. RSVP har òg meldingar som tek ned reservasjonar. Å gjera RSVP sikker nok for NbF målnett vil truleg vera ei stor utfordring.

Både DiffServ og IntServ føreset at krav om ein gitt kvalitetsklasse vert formidla ved å merka kvar IP-pakke. Som me har sett, støttar IPSec korkje konfidensialitetskrav eller integritetskrav til dette merket.

Tilgjenge. I avsnitt 3.2.2 såg me på tilgjenge til tenester, tenestekvalitet og prioritet. Me argumenterte for differensiert tilgjenge og ein streng policy. Både DiffServ og IntServ utfører tilgangskontroll (*admission control*) for trafikken. Dette er først og fremst ein kontroll av om påtrykt trafikk er i samsvar med avtalar og policy-reglar og ein kontroll av om nettet er i stand til å levera forespurt kvalitet. Som tidlegare nemnd omfattar arkitekturane i utgangspunktet ikkje autentisering og autorisasjonskontroll av sluttbrukarar og applikasjonar som spør etter ein spesifikk tenestekvalitet, men RSVP har fått eit tillegg som mogleggjer autentisering av

sluttbrukar og applikasjon [50].

Det er fleire måtar å utøva autorisasjonskontroll. Ei rekkje moglege mekanismar for autentisering og autorisasjonskontroll er som tidlegare nemnd, diskutert i [65]. Ein måte er å gjera bruk av PKIX attributtsertifikat, sjå avsnitt 5.2.2. Tradisjonelle offentleg nøkkel-infrastrukturar som PKIX, har fleire grunnleggjande trekk som gjer dei ueigna for bruk i mobile og dynamiske nett: Infrastrukturane er sentraliserte og tilgjenget til tenesta vil difor vera usikker. Protokollane for dynamisk sertifikatadministrasjonen er ressurskrevjande. Sertifikata er dessutan store og vil stela mykje kanalkapasitet. På same vis som for IPSec bør yteevna analyserast grundig før ein går inn for å bruka desse infrastrukturane i nett med låg overførings- og prosesseringskapasitet.

Korleis ein DiffServ-arkitektur kan autentisera og utøva autorisasjonskontroll av sluttbrukarar og applikasjonar, er uklart. Dette er kanskje heller ikkje naudsynt sidan NbF målnett truleg kjem til å implementera DiffServ berre i kjernenettet. I så fall kan ein tenkja seg at kantnettet, der IntServ er implementert, tek seg av naudsynt autentisering og autorisasjonskontroll på vegne av kjernenettet.

Det er ikkje spesifisert korleis ei prioritetsteneste skal implementerast på nettlaget i NbF målnett, men ei slik teneste krev sjølvsagt sterk autentiserings- og autorisasjonskontroll. Det er grunn til å tru at ei slik teneste krev konfidensialitet og integritet på applikasjonslaget. Det vil vera ei utfordring å sikra denne tenesta ettersom kvar involvert ruter må kunna lesa og prosessera pakken i samsvar med innvilga prioritet. Dette tilseier at kvar IP-pakke må merkast, men som synt tidlegare: IPSec gir ingen integritetsgaranti for dei relevante felta i IPv6-hovudet.

7 Oppsummering og konklusjonar

Målnettet for NbF er eit distribuert kommunikasjonssystem der IP inngår som gjennomgåande og integrerande teknologi. Studiet som denne rapporten dokumenterer, er i hovudsak avgrensa til nettlaget (IP-laget), og frå denne synsstaden har me sett på to sider ved kommunikasjonssystemet: *Som berar av sluttbrukarinformasjon* tilbyr nettet sluttbrukaren eit sett grunnleggjande nett-tenester som ruting, tenestekvalitet, prioritet og sikkerhet. Som *informasjonssystem* forvaltar systemet sin eigen informasjon ved å utveksla, prosessera og lagra nettinformasjonen som ligg til grunn for nett-tenestene. Brennpunkt for studiet er i kva for grad nett-tenesta *sikkerhet* kan brukast til å sikra nett-tenestene *ruting* og *tenestekvalitet*.

Me har studert kva dei tre komponentane konfidensialitet, integritet og tilgjenge har å seia for nettinformasjonen, og har synt at det trengs ein særeigen sikkerhetspolicy for *informasjonssystemet* NbF målnett. Basert på *både* policy for nettinformasjon *og* på den allmenne sikkerhetspolicyen for sluttbrukarinformasjon bør det utarbeidast ein sikkerhetsarkitektur for NbF målnett. Både policy og arkitektur er naudsynt for å kunna ta stilling til kor vidt sivile sikkerhetsstandardar for IP-nett kan brukast til å sikra nettinformasjonen i NbF målnett.

Om ein handterer konfidensialitet, integritet og tilgjenge som tre innbyrdes uavhengige komponentar, kan ein fastsetja policy for komponentane *kvar for seg*. Ved fleirnivå-policy kan dei tre dimensjonane då graderast ut frå *ulike* sett av kriterium. Dette vil kunna gje ein policy som er sikker, og som i tillegg kan føra til presise og fleksible løysingar. Dette er særleg viktig i NbF målnett dersom nettet skal vera i stand til å handtera rutingdomene og tenestekvalitetsdomene dynamisk.

Me har teke føre oss sivile standardar og andre spesifikasjonar utvikla av *Internet Engineering Task Force* (IETF), men har ikkje sett på sikkerhetsløysingane i noverande militære nett. Utgangspunkt er sikkerhetstenestene som *IP versjon 6* tilbyr. I motsetning til IPv4, er IPv6 utvikla med tanke på at fundamental sikkerhetsfunksjonalitet skal vera del av protokollen. IPv6 er sikrare og meir verifiserbar enn IPv4. Sidan sikkerhetsarkitekturen for IP (IPSec) vert obligatorisk med IPv6, vil sikkerhetstenestene verta ryddigare. IPSec skal til dømes kunna erstatta protokollspesifikke sikkerhetsløysingar.

Studiet har ikkje omfatta sikring av sluttbrukarinformasjon. Me vil likevel understreka at IPSec gir sikkerhetstenester på *nettlaget*. IPSec gir konfidensialitet og integritet for overført informasjon så lenge denne ligg som nyttelast i ein IP-pakke. Sikringa gjeld mellom IP-adressene til kjelde og destinasjon. Det er viktig å vera klar over at dette medfører viktige avgrensingar. Eit godt døme er autentisering av ei meldingskjelde: IPSec autentiserer *IP-adresser*. IPsec autentiserer ikkje andre typar identitetar som til dømes sluttbrukarar, rollar og applikasjonar. Dette er ein konsekvens av at IPSec opererer på nettlaget. Ynskjer ein betre granularitet på autentiseringa, må mekanismane implementerast på kommunikasjonslag over nettlaget.

Me har gått gjennom dei to viktigaste sikkerhetskomponentane: IPSec og den offentlege nøkkel-infrastrukturen PKIX. Rapporten syner at desse komponentane slik dei er spesifisert i dag, ikkje er tilstrekkelege for å sikra nett-tenestene ruting og tenestekvalitet. Årsakene til dette kan delast i tre kategoriar:

1. ***Standardar og spesifikasjonar har veikskapar og manglar***. IETF utfører eit omfattande arbeid for å sikra nett-tenestene i framtidige IP-nett. Likevel er spesifikasjonane på mange felt enno uklare og uferdige. Dette gjeld til dømes samspelet mellom IPSec og offentleg nøkkel-infrastrukturen PKIX, kva for rolle IPSec skal ha i ressursreservasjonsprosessen i samband med tenestekvalitet og, ikkje minst, sikker interdomene ruting. Det er verdt å merka seg at IETF i liten grad har arbeidd med å sikra nettinformasjonen i mobile trådlause ad hoc-nett.

   Fleire av dei sivile standardane for ruting og tenestekvalitet legg stor vekt på å støtta *integritetskrav* som autentisering av meldingskjelde og verifikasjon av at ei melding ikkje er modifisert på ikkje-autorisert vis. Ingen av desse standardane er utforma med tanke på å støtta *konfidensialitetskrav*. Derimot skal IPSec i utgangspunktet kunna støtta både integritetskrav og konfidensialitetskrav til denne typen informasjon, med dei avgrensingane som er nemnde over.

   Dei sivile standardane manglar eksplisitt støtte for *fleirnivå* sikkerhetsmodellar. Dette vil ikkje seia at det er umogleg å få til slike løysingar basert på standardane.

   Eit grunnleggjande problem ved IPSec er at det må opprettast sikkerhetsassosiasjonar mellom alle par av IPSec-nodar som skal kommunisera. Å bruka IPSec til å sikra rutinginformasjon medfører assosiasjonar mellom alle par av ruterar i nettet. I eit trådlaust mobilt ad hoc-nett vil det seia assosiasjonar mellom alle par av nodar. Om ikkje dette vert endra i IPSec, vil IPSec vera ueigna til å sikra nettinformasjonen i ad hoc-nett og truleg by på store skaleringsproblem i faste nett òg.

   Tradisjonelle offentleg nøkkel-infrastrukturar som PKIX, har fleire grunnleggjande trekk som gjer dei ueigna for bruk i mobile og dynamiske nett: Infrastrukturane er sentraliserte og tilgjenget til tenesta vil difor vera usikker. Sertifikatadministrasjonen er ressurskrevjande og sertifikata er store.

   Det bør gjerast grundige analysar før ein eventuelt går inn for å nytta IPSec og PKIX for å sikra nettinformasjonen i dei mobile delane av NbF målnett

2. ***IPSec tilbyr sikkerhetstenester på nettlaget***. Dette medfører viktige avgrensingar med omsyn til sikre nett-tenester. I fleire protokollar for ruting og tenestekvalitet skal ruterane modifisera meldingane før vidaresending. Protokollmeldingane ligg som nyttelast i ein IP-pakke. Dersom sikring av desse protokollane skal baserast på IPSec åleine, vil sikringa berre gjelda hopp for hopp. Samtlege ruterar på stien mellom kjelde og destinasjon må dermed vera

tiltrudde.

Nokre felt i IP-hovudet er ikkje omfatta av sikkerhetstenestene i IPSec. Om desse felta vert endra på ikkje-autorisert vis, vil IPSec ikkje oppdaga det. Dette vanskeleggjer sikker tenestekvalitet. Dersom desse felta skal brukast til å krevja ein gitt prioritet og forkøyrsrett gjennom nettet, vil dette vanskeleggjera ei sikker prioritetsteneste òg

3. ***Standardane dekkar berre informasjonsutvekslinga.*** Dokumenta frå IETF handterer berre *utvekslinga* av nettinformasjon. Sikring av *prosessering* og *lagring* vert ikkje omtalt. Dokumenta handterer heller ikkje sikkerhetsproblematikk knytt til portar (*gateways*) mellom to ulike rutingprotokollar, til dømes mellom intra-og interdomeneprotokollar og mellom fastnett og adhocprotokollar.

Rapporten identifiserer dessutan nokre område som må takast særleg hand om i det vidare arkitekturarbeidet:

- Det må avklarast på kva for kommunikasjonslag det er fornuftig å plassera dei ulike sikkerhetsmekanismane. Dette er viktig; både med omsyn til sikkerhet og med omsyn til den totale ressursbruken
- Styresystem for tenestekvalitetsarkitekturen vil i utgangspunktet vera sårbare punkt i nettet. Åtak på desse vil lett kunna få store konsekvensar. NbF målnett vil dessutan innehalda drift- og styringsinformasjon (*management information*) som ikkje er direkte knytt til ruting og tenestekvalitet. Sikring av denne informasjonen må òg med i det vidare arkitekturarbeidet.

At dei sentrale sikkerhetsspesifikasjonane ikkje strekk til for nett-tenestene, vil sjølvsagt ikkje seia at det er umogleg å sikra slike tenester i IP-nett. Dersom det er ynskjeleg å bruka sivile standardar, bør ein arbeida innanfor standardiseringsorgana å gjera standardane best mogleg. Eit alternativ er å utvikla eigne løysingar på grunnlag av dei sivile standardane. I så fall bør slike løysingar vera kompatible med dei sivile standardane for å ivareta kravet om dynamikk og interoperabilitet i alle delar av målnettet for det nettverksbaserte Forsvaret.

Forkortingar

6LSA	IPv6 Label Switch Architecture
AA	Attribute Authority
AH	Authentication Header
AODV	Ad Hoc On Demand Distance Vector Routing
AS	Autonomous System
BGP	Border Gateway Protocol
BGPv4	BGP versjon 4
BMWG	Benchmarking Methodology Working Group (arbeidsgruppe i IETF)
CA	Certification Authority
CMP	Certificate Management Protocol
CRL	Certificate Revocation List
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DN	Distinguished Name
DoS	Denial-of-Service
DSR	Dynamic Source Routing protocol
DVCS	Data Validation and Certification Server Protocol
DYMO	Dynamic MANET On-demand
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload header
FEC	Forward Equivalent Classe
FQMM	Flexible QoS Model for Mobile Ad-Hoc Networks
FTP	File Transfer Protocol
HTTP	Hyper-Text Transfer Protocol
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange version 2
IntServ	Integrated Services
IP	Internet Protocol
IPSec	Security Architecture for the Internet Protocol
IPv4	IP versjon 4
IPv6	IP versjon 6
ITU	International Telecommunication Union
ITU-T	ITU-Telecommunication Standardization Sector
LDAP	Lightweight Directory Access Protocol
MAC	Medium Access Control
MAC	Message Authentication Code
MPLS	Multiprotocol Label Switching
MSEC	Multicast Security (arbeidsgruppe i IETF)
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NbF	Nettverksbasert Forsvar
OLSR	Optimized Link State Routing protocol
OSPF	Open Shortest Path First
PAD	Peer Authorization Database
PANA	Protocol for carrying Authentication for Network Access (arbeidsgruppe i IETF)
PANA	Protocol for carrying Authentication for Network Access
PHB	Per-Hop Behavior
PKI	Public Key Infrastructure
PKI4IPSEC	Profiling Use of PKI in IPSEC (arbeidsgruppe i IETF)
PKIX	Public Key Infrastructure (X.509) (arbeidsgruppe i IETF)

PKIX	Public Key Infrastructure (X.509)
PMI	Privilege Management Infrastructure
QoS	Quality of Service
RA	Registration Authority
RFC	Request for Comments
RPSEC	Routing Protocol Security Requirements Working Group (arbeidsgruppe i IETF)
RSVP	Resource Reservation Protocol
SA	Security Association
SAD	Security Association Database
S-BGP	Secure BGP
SIDR	Secure Inter-Domain Routing Working Group (arbeidsgruppe i IETF)
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SPD	Security Policy Database
SSL	Secure Socket Layer
SWAN	Stateless Wireless Ad hoc Networks
TBRPF	Topology Based on Reverse Path Forwarding protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security (arbeidsgruppe i IETF)
TLS	Transport Layer Security
TSA	Time Stamp Authority
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VoIP	Voice-over-IP
VPN	Virtual Private Network
W-OSPF	Wireless Open Shortest Path First protocol
X.509	Standard frå ITU-T

Referansar

[1] G.-S. Ahn et al, "SWAN: Service Differentiation in Stateless Wireless Ad Hoc Networks," in Proceedings of the Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE InfoCom), 2002.

[2] Benchmarking Methodology Working Group (BMWG). http://www.ietf.org/html.charters/bmwg-charter.html

[3] A. Bishop, Computer Security, Art and Science Addison-Wesley, 2003.

[4] B. Dahill et al, "A Secure Routing Protocol for Ad Hoc Networks," in *Proceedings of the IEEE International Conference on Network Protocols (ICNP)*, 2002.

[5] T. Gjertsen et al, "Migrasjon av Forsvarets kommunikasjonssystemer (BEGRENSET)," FFI Rapport 2005/00290, 2005.

[6] G. C. Hadjichristofi et al, "IPSec Overhead in Wireline and Wireless Networks for Web and Email Application," in *Proceedings of the IEEE IPCCC*, 2003.

[7] S. Hagen, *IPv6 Essentials* O'Reilly, 2006.

[8] Ø. Heskestad, "Authenticated QoS in Wireless Networks," Master Thesis, University of Oslo, Department of Informatics, 2005.

[9] X. Hong et al, "Scalable Routing Protocols for Mobile Ad Hoc Networks," *IEEE Network*, vol. July/August, pp. 11-21, 2002.

[10] International Telecomunication Union-Telecommunication Standardization Sector (ITU-T), "Recommendation X.509, Information Technology - Open Systems Interconnection - The Directory: Authentication," 1997.

[11] International Telecomunication Union-Telecommunication Standardization Sector (ITU-T), "Recommendation X.700, Management Framework for Open Systems Interconnection for CCITT Applications," 1992.

[12] International Telecomunication Union-Telecommunication Standardization Sector (ITU-T), "Recommendation X.800, Security Architecture for Open Systems Interconnection for CCITT Applications," 1991.

[13] Internet Engineering Steering Group (IESG), http://www.ietf.org/iesg.html

[14] Internet Engineering Task Force (IETF), http://www.ietf.org/

[15] Internet Engineering Task Force (IETF), "Internet-Draft, BGP Security Requirements draft-ietf-rpsec-bgpsecrec-06,"2006.

[16] Internet Engineering Task Force (IETF), "Internet-Draft, Certificate Policy (CP) for the Internet IP Address and AS Number (PKI), draft-ietf-sidr-cp-00.txt," 2006.

[17] Internet Engineering Task Force (IETF), "Internet-Draft, DB Exchange for OSPFv2 Wireless Interface Type, draft-clausen-manet-ospf-dbx-00," 2004.

[18] Internet Engineering Task Force (IETF), "Internet-Draft, Dynamic MANET On-demand (DYMO) Routing, draft-ietf-manet-dymo-06," 2006.

[19] Internet Engineering Task Force (IETF), "Internet-Draft, Internet X.509 Public Key Infrastructure: Roadmap, draft-ietf-pkix-roadmap-09.txt," 2002.

[20] Internet Engineering Task Force (IETF), "Internet-Draft, Methodology for Benchmarking IPsec Devices, draft-ietf-bmwg-ipsec-meth-01," 2006.

[21] Internet Engineering Task Force (IETF), "Internet-Draft, OSPF Security Vulnerabilities Analysis, draft-ietf-rpsec-ospf-vuln-02.txt," 2006.

[22] Internet Engineering Task Force (IETF), "Internet-Draft, PANA Enabling IPsec based Access Control, draft-ietf-pana-ipsec-07.txt," 2005.

[23] Internet Engineering Task Force (IETF), "Internet-Draft, Protocol for Carrying Authentication for Network Access (PANA) Framework, draft-ietf-pana-framework-07," 2006.

[24] Internet Engineering Task Force (IETF), "Internet-Draft, Protocol for Carrying Authentication for Network Access (PANA), draft-ietf-pana-pana-13," 2006.

[25] Internet Engineering Task Force (IETF), "Internet-Draft, Requirements for an IPsec Certificate Management Profile, draft-ietf-pki4ipsec-profile-reqts-01.txt," 2005.

[26] Internet Engineering Task Force (IETF), "Internet-Draft, Template for an Internet Registry's Certification Practice Statement (CPS) for the Internet IP Address and AS Number (PKI), draft-ietf-sidr-cps-irs-00.txt," 2006.

[27] Internet Engineering Task Force (IETF), "Internet-Draft, Terminology for Benchmarking IPsec Device, draft-ietf-bmwg-ipsec-term-08," 2006.

[28] Internet Engineering Task Force (IETF), "Internet-Draft, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR), draft-ietf-manet-dsr-10.txt," 2004.

[29] Internet Engineering Task Force (IETF), "Internet-Draft, The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX, draft-ietf-pki4ipsec-ikecert-profile-11," 2006.

[30] Internet Engineering Task Force (IETF), "rfc 0791, Internet Protocol, DARPA Internet Program, Protocol Specification," 1981.

[31] Internet Engineering Task Force (IETF), "rfc 1633, Integrated Services in the Internet Architecture: an Overview," 1994.

[32] Internet Engineering Task Force (IETF), "rfc 2178, OSPF Version 2," 1997.

[33] Internet Engineering Task Force (IETF), "rfc 2205, Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification," 1997.

[34] Internet Engineering Task Force (IETF), "rfc 2284, PPP Extensible Authentication Protocol (EAP)," 1998.

[35] Internet Engineering Task Force (IETF), "rfc 2385, Protection of BGP Sessions via the TCP MD5 Signature Option," 1998.

[36] Internet Engineering Task Force (IETF), "rfc 2460, Internet Protocol, Version 6 (IPv6) Specification," 1998.

[37] Internet Engineering Task Force (IETF), "rfc 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," 1998.

[38] Internet Engineering Task Force (IETF), "rfc 2475, An Architecture for Differentiated Services," 1998.

[39] Internet Engineering Task Force (IETF), "rfc 2545, Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing," 1999.

[40] Internet Engineering Task Force (IETF), "rfc 2559, Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2," 1999.

[41] Internet Engineering Task Force (IETF), "rfc 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," 1999.

[42] Internet Engineering Task Force (IETF), "rfc 2585, Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP," 1999.

[43] Internet Engineering Task Force (IETF), "rfc 2740, OSPF for IPv6," 1999.

[44] Internet Engineering Task Force (IETF), "rfc 2747, RSVP Cryptographic Authentication," 2000.

[45] Internet Engineering Task Force (IETF), "rfc 2828, Internet Security Glossary," 2000.

[46] Internet Engineering Task Force (IETF), "rfc 2875, Diffie-Hellman Proof-of-Possession Algorithms," 2000.

[47] Internet Engineering Task Force (IETF), "rfc 2904, AAA Authorization Framework," 2000.

[48] Internet Engineering Task Force (IETF), "rfc 3029, Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols," 2001.

[49] Internet Engineering Task Force (IETF), "rfc 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)," 2001.

[50] Internet Engineering Task Force (IETF), "rfc 3182, Identity Representation for RSVP," 2001.

[51] Internet Engineering Task Force (IETF), "rfc 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," 2003.

[52] Internet Engineering Task Force (IETF), "rfc 3281, An Internet Attribute Certificate Profile for Authorization," 2002.

[53] Internet Engineering Task Force (IETF), "rfc 3561, Ad hoc On-Demand Distance Vector (AODV) Routing," 2003.

[54] Internet Engineering Task Force (IETF), "rfc 3626, Optimized Link State Routing Protocol (OLSR)," 2003.

[55] Internet Engineering Task Force (IETF), "rfc 3644, Policy Quality of Service (QoS) Information Model," 2003.

[56] Internet Engineering Task Force (IETF), "rfc 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," 2003.

[57] Internet Engineering Task Force (IETF), "rfc 3684, Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)," 2004.

[58] Internet Engineering Task Force (IETF), "rfc 3697, IPv6 Flow Label Specification," 2004.

[59] Internet Engineering Task Force (IETF), "rfc 3740, The Multicast Group Security Architecture," 2004.

[60] Internet Engineering Task Force (IETF), "rfc 3779, X.509 Extensions for IP Addresses and AS Identifiers," 2004.

[61] Internet Engineering Task Force (IETF), "rfc 4016, Protocol for Carrying Authentication and Network Access (PANA) Threat Analysis and Security Requirements,"2005.

[62] Internet Engineering Task Force (IETF), "rfc 4058, Protocol for Carrying Authentication for Network Access (PANA) Requirements," 2005.

[63] Internet Engineering Task Force (IETF), "rfc 4210, Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)," 2005.

[64] Internet Engineering Task Force (IETF), "rfc 4211, Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)," 2005.

[65] Internet Engineering Task Force (IETF), "rfc 4230, RSVP Security Properties," 2005.

[66] Internet Engineering Task Force (IETF), "rfc 4271, A Border Gateway Protocol 4 (BGP-4)," 2006.

[67] Internet Engineering Task Force (IETF), "rfc 4301, Security Architecture for the Internet Protocol," 2005.

[68] Internet Engineering Task Force (IETF), "rfc 4302, IP Authentication Header," 2005.

[69] Internet Engineering Task Force (IETF), "rfc 4303, IP Encapsulating Security Payload (ESP)," 2005.

[70] Internet Engineering Task Force (IETF), "rfc 4305, Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)," 2005.

[71] Internet Engineering Task Force (IETF), "rfc 4306, Internet Key Exchange (IKEv2) Protocol," 2005.

[72] Internet Engineering Task Force (IETF), "rfc 4325, Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension," 2005.

[73] Internet Engineering Task Force (IETF), "rfc 4346, The Transport Layer Security (TLS) Protocol Version 1.1," 2006.

[74] Internet Engineering Task Force (IETF), "rfc 4593 Generic Threats to Routing Protocols," 2006

[75] Internet Engineering Task Force (IETF), "rfc 4630, Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," 2006.

[76] Internet Engineering Task Force (IETF), "rfc 4760, Multiprotocol Extensions for BGP-4," 2007.

[77] M. Jakobsson et al, "Stealth Attacks on Ad-Hoc Wireless Networks," in *Proceedings of the IEEE Vehicular Technology Conference (VTC)* 2003.

[78] S. Kent et al, "Secure Border Gateway Protocol (S-BGP)," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 4, pp. 582-592, 2000.

[79] Ø. Kure and I. Sorteberg, "Network architecture for network centric warfare operations," FFI Rapport 2004/01561, 2004.

[80] S.-B. Lee et al, "INSIGNIA: An IP-Based Quality of Service Framework for Mobile ad-Hoc Networks," *Journal on Parallel and Distributed Computing*, vol. 60, no. 4, pp. 374-406, 2000.

[81] D. Mongomery and D. Murphy, "Toward Secure Routing Infrastructures," *IEEE Security & Privacy*, vol. September/October, pp. 84-87, 2006.

[82] M. J. Moyer et al, "A Survey of Security Issues in Multicast Communications," *IEEE Network*, vol. November/December, pp. 12-23, 1999.

[83] Multicast Security, http://www.ietf.org/html.charters/msec-charter.html

[84] NATO Consultation, Command and Control Agency (NC3A), "NATO Network Enabled Capability Feasibility Study," 2006.

[85] Profiling Use of PKI in IPSEC (PKI4IPSEC), http://www.ietf.org/html.charters/pki4ipsec-charter.html

[86] Protocol for carrying Authentication for Network Access (PANA), http://www.ietf.org/html.charters/pana-charter.html

[87] Public Key Infrastructure (X.509), http://www.ietf.org/html.charters/pkix-charter.html

[88] Routing Protocol Security Requirements Working Group (RPSEC), http://www.ietf.org/html.charters/rpsec-charter.html

[89] E. M. Royer and C.-K. Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," *IEEE Personal Communications*, vol. April, pp. 46-55, 1999.

[90] Secure Inter-Domain Routing Working Group (SIDR), http://www.ietf.org/html.charters/sidr-charter.html

[91] C. Shue et al, "Analysis of IPSec overheads for VPN servers," in *Proceedings of the Secure Networks Protocols (NPSec)*, 2005.

[92] I. Sorteberg and Ø. Kure, "The Use of Service Level Agreements in Tactical Military Coalition Force Networks," *IEEE Communication Magazine*, vol. 43, no. 11, pp. 107-114, 2005.

[93] Transport Layer Security (TLS), http://www.ietf.org/html.charters/tls-charter.html

[94] E. Winjum et al, "Trust Metric Routing to Regulate Routing Cooperation in Mobile Wireless Ad Hoc Networks," in *Proceedings of the European Wireless Conference*, 2005.

[95] E. Winjum, "Arkitekturar og standardar for drift og styring av kommunikasjonsnett," FFI Rapport 2001/04331, 2001.

[96] H. Xiao et al, "A Flexible Quality of Service Model for Mobile Ad-Hoc Networks," in *Proceedings of the IEEE Vehicular Technology Conference (VTC)*, 2000.

[97] S. Yi et al, "A Security-Aware Routing Protocol for Wireless Ad Hoc Networks," in *Proceedings of the World Multi-Conference on Systemics, Cybernetics and Informatics (SCI)*, 2002.