FFI RAPPORT

STANDARDISERINGSARBEID I NATO OG IETF INNEN MILITÆR MELDINGSTJENESTE OG ENDE-TIL-ENDE SIKKERHETSLØSNINGER

EGGEN, Anders

FFI/RAPPORT-2003/01521

FFIE/840/110

Godkjent
Kjeller 19. desember 2003

Torleiv Maseng
Forskningssjef

STANDARDISERINGSARBEID I NATO OG IETF INNEN MILITÆR MELDINGSTJENESTE OG ENDE-TIL-ENDE SIKKERHETSLØSNINGER

EGGEN, Anders

FFI/RAPPORT-2003/01521

FORSVARETS FORSKNINGSINSTITUTT
Norwegian Defence Research Establishment
Postboks 25, 2027 Kjeller, Norge

FORSVARETS FORSKNINGSINSTITUTT (FFI)
Norwegian Defence Research Establishment

P O BOX 25
NO-2027 KJELLER, NORWAY

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

REPORT DOCUMENTATION PAGE

1) PUBL/REPORT NUMBER FFI/RAPPORT-2003/01521	2) SECURITY CLASSIFICATION UNCLASSIFIED	3) NUMBER OF PAGES 34
1a) PROJECT REFERENCE FFIE/840/110	2a) DECLASSIFICATION/DOWNGRADING SCHEDULE -	

4) TITLE
STANDARDISATION OF MMHS AND RELATED END-TO-END SECURITY SOLUTIONS IN NATO AND IETF

5) NAMES OF AUTHOR(S) IN FULL (surname first)
EGGEN, Anders

6) DISTRIBUTION STATEMENT
Approved for public release. Distribution unlimited. (Offentlig tilgjengelig)

7) INDEXING TERMS

IN ENGLISH:	IN NORWEGIAN:
a) Military Message Handling System	a) Militære meldingssystemer
b) End-to-end security	b) Ende-til-ende sikkerhet
c) S/MIME	c) S/MIME
d) Tactical MMHS	d) Taktisk meldingstjeneste
e) P-Mul	e) P-Mul

THESAURUS REFERENCE:

8) ABSTRACT
This report summarises the contribution of the FFI project STAROS in international standardization of Military Message Handling Systems and related end-to-end security mechanisms. The report describes the involvement in the standardizations work in both NATO and the IETF, and gives an overview of the different standards. Related test activities in order to verify the solutions, are also described.

9) DATE	AUTHORIZED BY This page only	POSITION
19. December 2003	Torleiv Maseng	Director of Research

ISBN-82-464-0811-9

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

INNHOLD

Side

STANDARDISERINGSARBEID I NATO OG IETF INNEN MILITÆR MELDINGSTJENESTE OG ENDE-TIL-ENDE SIKKERHETSLØSNINGER

1 INNLEDNING

Hensikten med denne rapporten er å gi en oppsummering av det internasjonale standardiseringsarbeidet og de internasjonale demonstratorene som STAROS prosjektet ved FFI har vært involvert i. Arbeidet omfatter først og fremst militær meldingstjeneste og sikkerhetsløsninger for disse. Det er også lagt vekt på hvordan standardiseringsarbeidet er relatert til utviklingen av våre nasjonale meldingssystem, både når det gjelder meldingsfunksjonalitet og sikkerhetstjenester. Rapporten vil ikke gå i detalj når det gjelder funksjonalitet og systemløsninger, men vil gi en overordnet beskrivelse og henvise til andre rapporter og dokumenter for detaljer.

Standardiseringsarbeid er viktig for å oppnå internasjonal enighet rundt de løsningene som velges. Dette vil føre til at flere leverandører implementere løsningene, slik at det blir flere produkter å velge mellom. Standarder er det eneste verktøyet man har for å oppnå at implementasjoner fra forkjellige leverandører blir interoperable.

STAROS prosjektet har vært sterkt engasjert i internasjonalt standardiseringsarbeid, samtidig som vi har bidratt til utvikling av løsninger for våre nasjonale meldingssystemer. Vi har sett at disse oppgavene ikke kan løses uavhengig av hverandre, da våre nasjonale systemer også skal brukes mot våre allierte i NATO.

Arbeidet som er utført innen standardisering, er beskrevet i en rekke dokumenter og internasjonale standarder. I denne rapporten vil vi prøve å samle trådene og gi en kort beskrivelse av essensen i arbeidet. Vi vil derimot henvise til de ulike dokumentene for en mer utfyllende beskrivelse av arbeidet som er utført.

NATOs meldingssystem har inntil i dag vært basert på den gamle ACP 127 standarden som ble utviklet for fjernskrivere på 60 tallet. Systemene har blitt modernisert opp gjennom årene, men har klare begrensninger når det gjelder funksjonalitet, formater og informasjonsinnholdet til meldingene (bl.a. støttes ikke vedlegg i meldinger). Mange land har fremdeles ACP 127 systemer som sine nasjonale meldingssystemer.

Det norske Forsvaret var tidlig ute for å erstatte ACP 127 systemer nasjonalt, og hadde allerede i 1990 et operativt meldingssystem system, basert på første versjon av STANAG 4406. Interoperabilitet med NATO og andre nasjoner ble (og blir fremdeles) opprettholdt via en ACP 127 gateway. Det er først nå i 2003/2004 at NATO som organisasjon erstatter sitt ACP 127 system med et system basert på STANAG 4406. Det samme gjelder også for mange NATO nasjoner.

STAROS har bidratt på flere områder innen internasjonal standardisering, men hovedtyngden de senere årene har vært innen spesifikasjon av protokolløsninger for taktisk meldingstjeneste og ende-til-ende sikkerhetsløsninger for militær meldingstjeneste. Med ende-til-ende sikkerhetsløsninger mener vi løsninger for bl.a. integritet, autentisering og need-to-know separasjon av meldinger.

2 FORMELL MILITÆR MELDINGSTJENESTE

Som nevnt i innledningen, så har ACP 127 vært den gjeldende standarden for militær meldingstjeneste i NATO. Standarden ACP 127 ble utviklet for fjernskrivere og er derfor gammeldags i forhold til dagens moderne meldingssystemer. ACP 127 har også klare begrensninger som bl.a. at det ikke støtter vedlegg i meldinger. STANAG 4406 for MMHS (Military Message Handling Systems) ble introdusert på slutten av 80 tallet for å erstatte ACP 127. Første versjon var klar i 1991 og var basert på X.400 som da var den ledende sivile standarden for epost. Norge var et foregangsland allerede på dette tidspunktet fordi vi allerede hadde et X.400 basert militært meldingssystem som var i operativ bruk og som var interoperabelt med de gamle ACP127 systemene via en gateway.

Militær meldingstjeneste er en meget viktig brikke i et K2IS, noe som har blitt understreket fra flere hold:

- fra NC3A har MMHS blitt omtalt som; ”the lowest common denominator for information exchange in C2IS”.
- ”MMHS er i dag primærtjenesten for utøvelse av Kommando og Kontroll (K2)”, sitat ØKS Strong Resolve 02 .
- Fra SHAPE har det blitt uttalt at ”MMHS is the most important service for the command and control of joint operations”.

Det som gjør MMHS viktig er bl.a. følgende egenskaper:

- forankret i operative militære prosedyrer, og standarder
- ”store and forward” egenskaper som gjør tjenesten robust,
- ”push” tjeneste som informerer mottakeren om at det er ankommet ny viktig informasjon som evt. krever umiddelbar handling,
- gir sikker og garantert overføring av informasjon iht ”fire and forget” prinsippet (meldingene skal alltid komme frem, enten til en mottaker eller til et kommunikasjonssenter som kan bringe meldingen videre),
- ivaretar interoperabilitet med ”legacy” systemet ACP 127 (arven),
- knytter sammen alle avdelinger i Forsvaret og sentrale avdelinger i den sivile delen av Totalforsvaret (taktisk og strategisk, nasjonalt og i NATO) ,
- beskytter informasjonen iht. sikkerhetsloven,
- behandler informasjon iht. prioritet,
- innehar mekanismer dersom nettet blir degradert,
- er formell (autorisering, arkivering),
- kan brukes i fred, krise og krig

3 TAKTISK MELDINGSTJENESTE - STANAG 4406 ANNEX E

3.1 Gjennomgående taktisk og strategisk meldingstjeneste

STAROS har deltatt i NATOs arbeidsgruppe for militær meldingstjeneste AC/322(SC/5)WG/5 on Military Message Handling Systems (MMHS). Den norske innsatsen har de siste årene bl.a. vært fokusert rundt taktisk meldingstjeneste nasjonalt og i NATO.

FFI (STAROS) leder aktiviteten for taktisk MMHS i NATOs arbeidsgruppe MMHS WG og har fått gjennomslag for en protokoll-løsning for NATOs taktiske meldingstjeneste. Denne løsningen er nå utgitt som STANAG 4406 Annex E ("Tactical MMHS protocol and profile solution"). Protokolløsningen beskriver hvordan militær meldingstjeneste kan brukes over nett med lav datarate, hvor mottakerne for eksempel kan befinne seg i EMCON eller "radio silence". Protokollene som benyttes for overføring av informasjonen reduserer bruk av båndbredde betydelig i forhold til protokollene som benyttes i det strategiske nettet. Løsningen er basert på at man kan gjenbruke applikasjonene utviklet for den strategiske meldingstjenesten og at applikasjonene og brukergrensesnittet skal være felles. Løsningen gjør det mulig å oppnå en gjennomgående integrert militær meldingstjeneste både på strategisk og taktisk nivå i alle forsvarsgrener. De samme applikasjonene kan brukes overalt.

FO/I har vedtatt at denne løsningen for taktisk meldingstjeneste skal benyttes i det norske Forsvaret for alle forsvarsgrener, noe som vil gi oss en gjennomgående integrert militær meldingstjeneste både på taktisk og strategisk nivå. Dette vil være fordelaktig både når det gjelder interoperabilitet mellom systemer, opplæring, og drift og vedlikehold av systemene.

Hensikten med å utarbeide felles løsninger i NATO og nasjonalt, er at de samme systemene kan benyttes både nasjonalt og i internasjonale operasjoner.

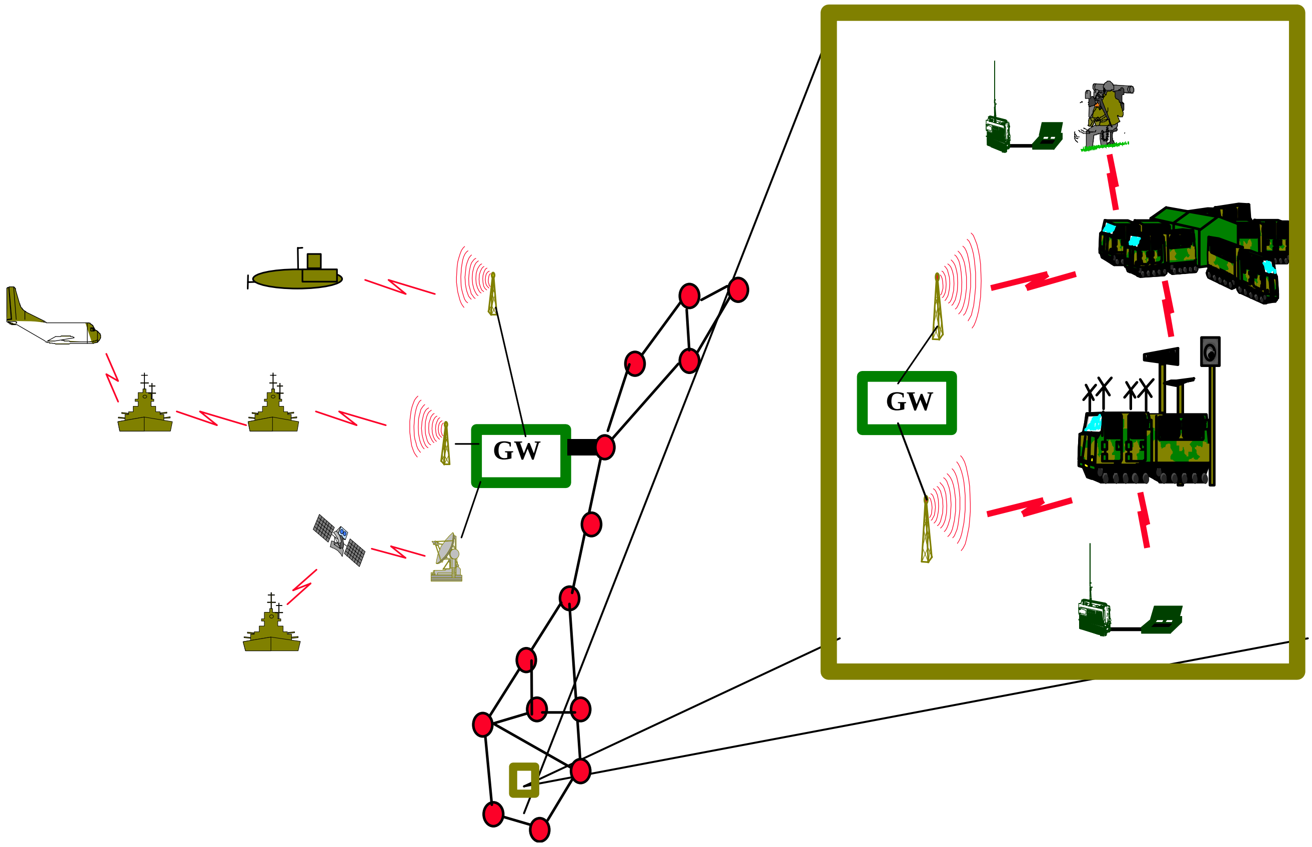
3.1.1 Funksjonaliteten og egenskapene til STANAG 4406 Annex E

Vi skal her gi en oversikt over funksjonaliteten og egenskapene til STANAG 4406 Annex E. En mer detaljert og fullstendig beskrivelse av protokollen er gitt i ref.(2).

STANAG 4406 Annex E definerer en protokolløsning for overføring av formelle militære meldinger over nett med lav datarate. Applikasjonene som benyttes, er de samme som i det strategiske nettet, men protokollene som benyttes for overføringen av meldingene er mer tilpasset egenskapene til nett med lav datarate.

Egenskapene til STANAG 4406 Annex E:

- egnet til å benyttes over taktisk datasamband med lav datarate (ofte lavere enn 2.4 Kbps).
- interoperabel med de strategiske NATO MMHS systemene og med ACP 127 systemer.
- kan benyttes over taktisk datasamband som bruker både full duplex, halv-duplex og simplex forbindelser (broacast).
- har funksjonalitet for å utnytte multicast over radio.
- har funksjonalitet for å håndtere "radio silence" (EMCON) scenarier.



Figur 3.1 STANAG 4406 Annex E kan bidra til en gjennomgående Meldingstjeneste i Forsvaret mellom alle strategiske og taktiske enheter.

Fleksibiliteten til Annex E gjør at den kan benyttes over de fleste taktiske kommunikasjonsløsninger i alle forsvarsgrener.

For å redusere bruk av overføringskapasiteten i nettet har vi fjernet mange av protokollene i de øvre lagene i den opprinnelige protokollprofilen, som brukes for det strategiske nettet. Denne protokollprofilen er basert på en full forbindelsesorientert OSI protokoll ”stack”, med opp- og nedkopling mellom de fleste lagene. Dette er veldig ressurskrevende for et nett med lav datarate og vil legge beslag på mye av kapasiteten. Radioer med lang ”snutid” er også dårlig egnet for forbindelsesoritenterte protokoller som hyppig veksler mellom trafikk i begge retninger.

Figur 3.2 og figur 3.3 viser hhv den strategisk og taktisk protokoll profilen som brukes i vårt nasjonale MMHS (XOmail). Vi vil bruke disse figurene for å vise forskjellen mellom strategisk og taktisk protokoll-profil i STANAG 4406.

3.1.2 Strategisk profil

RTSE og ACSE er applikasjonslagsprotokoller som brukes for å opprette en pålitelig forbindelse på applikasjonslaget (en assosiasjon) (se ref.(17) og (18) for detaljer). Presentasjons og sesjonslaget har funksjonalitet for bl.a. koding av informasjonene som skal overføres og opprettelse av en pålitelig forbindelse (sesjon) hvor man bl.a. har mulighet til å sette synkroniseringspunkter for å slippe å overføre alle data på nytt hvis for eksempel en sesjon skulle bli brutt. Presentasjons- og Sesjonslaget genererer mye overhead både ved opp- og nedkopling i tillegg til at de legger på headerinformasjon ved overføring av dataene.

<table>
<tr><td rowspan="2">7</td><td rowspan="2">Applikasjonslag</td><td>Message Storage
(MSSE, MASE, MRSE, ROSE)</td><td>UserAgent
(MSSE, MDSE, MASE, MRSE, ROSE)</td><td>Message Transfer Agent
(MSSE, MDSE, MASE, MTSE, ROSE)</td></tr>
<tr><td colspan="3">ACSE, RTSE</td></tr>
<tr><td>6</td><td>Presentasjonslag</td><td colspan="3">Presentation Protocol Specification for OSI for CCITT Applications (CCITT X.226)</td></tr>
<tr><td>5</td><td>Sesjonslag</td><td colspan="3">Session Protocol Specification for OSI for CCITT Applications (CCITT X.225)</td></tr>
<tr><td rowspan="3">4</td><td rowspan="3">Transportlag</td><td colspan="3">TP0</td></tr>
<tr><td colspan="3">TPTK</td></tr>
<tr><td colspan="3">TCP</td></tr>
<tr><td>3</td><td>Netverkslag</td><td>X.25</td><td colspan="2">IP</td></tr>
<tr><td>2</td><td>Data linklag</td><td>LAPB</td><td colspan="2">f.eks. STANAG 5066</td></tr>
<tr><td>1</td><td>Fysisk lag</td><td colspan="3"></td></tr>
</table>

Figur 3.2 Strategisk protokoll profil i STANAG 4406 Annex C

I transportlaget i den strategiske profilen benyttes 3 protokoller. Dette er unødvendig tungt og genererer ekstra mye overhead. Grunnen til at man har 3 transport protokoller, er at man her benytter ISO protokoller i de øvere lagene i OSI modellen og IETF protokollene TCP/IP på hhv transport og nettlaget. TP0 er en ISO transportprotokoll med minimalt med funksjonalitet, som benyttes over relativt pålitelige nett. Den er forbindelsesorientert og genererer derfor overhead ved opp- og nedkopling, samt at den genererer ekstra headerinformasjon ved overføring av dataene. TP0 benyttes, fordi Sesjonslaget forventer å operere over en ISO transport protokoll. TPTK er en IETF protokoll som brukes som et bindeledd for å kunne benytte OSI transport protokoller over TCP protokollen. TCP/IP benyttes fordi forsvaret har standardisert på TCP/IP. Alle disse transportprotokollene genererer overhead. I enkelte tilfeller kjøres også IP over X.25 som vist på figur 3.2.

3.1.3 Taktisk profil

Som vi ser av figur 3.3, så har vi fjernet flere av de forbindelsesorienterte protokollene i applikasjonslaget, presentasjonslaget, sesjonslaget og transportlaget og erstattet disse med de forbindelsesløse protokollene P_Mul (ACP 142) og WAP Wireless Datagram Protocol (WDP).

Applikasjonene i meldingssystemet er ikke endret og det er de samme applikasjonene som brukes både for det strategiske og det taktiske systemet. Eneste forskjell er protokoll-stacken under applikasjonen. Protokollene som brukes i meldingsapplikasjonen er forbindelsesorienterte, som for eksempel (MSSE, MDSE, MASE, MTSE, ROSE), og forventer et forbindelsesorientert grensesnitt fra RTSE protokollen. Siden vi har fjernet RTSE protokollen i den taktiske profilen og erstattet denne og de andre nevnte protokollene med en forbindelsesløs protokoll-stack, er vi nødt til å simulere dette grensesnittet. Dette er gjort ved å tilby det samme grensesesnittet til applikasjonene, men jukse med underliggende funksjonaliteten i tjenestelaget ”Adaptation Sub-layer”. Dvs. når applikasjonen forsøker å kople opp og kople ned en forbindelse vil ”Adaptation Sub-layer” gi beskjed til applikasjonen om at dette er utført, selv om det ikke er sendt noen opp- og nedkoplings PDUer over nettet.

<table>
<tr><td rowspan="3">7</td><td rowspan="3">Aplikasjonslaget</td><td>Message Storage
(MSSE, MASE, MRSE, ROSE)</td><td>User Agent
(MSSE, MDSE, MASE, MRSE, ROSE)</td><td>Message Transfer Agent
(MSSE, MDSE, MASE, MTSE, ROSE)</td></tr>
<tr><td colspan="3">Tactical Adaptation Sub-Layer
Protocol Adaptation
Compresion/ Decompresion</td></tr>
<tr><td colspan="3">P-MUL Sub-layer</td></tr>
<tr><td>4</td><td>Transportlag</td><td colspan="3">WAP Transport Layer (WDP), (UDP)</td></tr>
<tr><td>3</td><td>Netverkslag</td><td colspan="2">X.25</td><td>IP</td></tr>
<tr><td>2</td><td>Data Linklag</td><td colspan="2">LAPB</td><td>f.eks. STANAG 5066</td></tr>
<tr><td>1</td><td>Fysisklag</td><td colspan="3"></td></tr>
</table>

Figur 3.3 Eksempel på bruk av Taktisk protokoll profil (STANAG 4406 Annex E) over X.25 eller IP

Man kan si at ”Adaptation Sub-layer” simulerer tjenestene som applikasjonsprotokollene er vant med å se fra RTSE protokollen, slik at disse protokollene ikke behøver å forandres. Det eneste som ”Adaptation Sub-layer” slipper igjennom, er dataene som utgjør selve meldingen. I tillegg til funksjonaliteten for å integrere en forbindelsesorientert og en forbindelsesløs protokoll- stack, utfører også ”Adaptation Sub-layer” komprimering av hele meldingen som overføres (inkludert header-informasjon og konvolutt).

P-MUL Sub-Layer består av protokollen P-Mul som er definert av den militære standarden ACP142. ACP142 er opprinnelig tenkt integrert i meldingsapplikasjonen, men dette krever at applikasjonene må endres, noe som er kostbart. Vi har derfor definert et tjenestegrensesnitt til P-Mul protokollen i Annex E, som gjør P_Mul protokollen mer fleksibel når det gjelder hvor den kan plasseres i protokollstacken. Innføring av dette grensesnittet gjør det også mulig å anvende

P_Mul sammen med andre applikasjoner enn X.400 meldingssystemer.

P-Mul protokollen sørger for at alle dataene kommer frem til mottakerne ved at den fragmenterer meldingen i mindre PDUer, setter på sekvensnummer og sørger for retransmisjon av PDUer ved bruk av en selective-repeat mekanisme som bare re-transmitterer de PDUene som ikke er mottatt. P-Mul har også funksjonalitet for multicast d.v.s. at en melding kan sendes en gang til flere mottakere over et broadcast medium. Man slipper dermed å sende meldingen en gang for hver mottaker, noe som sparer ressurser i det underliggende transmisjonssystemet. P-Mul kan også håndtere mottakere i ”radio silence”, dvs. mottakere som kan ta imot informasjon, men ikke sende. De har derfor ingen mulighet til å kvittere på at meldingene er mottatt. P-Mul håndterer dette ved at den aksepterer at avsender ikke får kvittering fra mottakere som den vet er i ”radio silence”, før de kommer ut av denne tilstanden. For mer detaljer om P-Mul eller ACP 142, se ref.(19).

For å oppsummer er de båndbredde reduserende tiltakene følgende:

- De forbindelsesorienterte protokollene på OSI lag 7; RTSE (Reliable Transfer Service Element) og ACSE (Association Control Service Element) er fjernet.
- OSI forbindelsesorienterte Presentasjonslags- (lag 6), Sesjonslagsprotokoller (lag 5) og Transportlag (lag 4) er fjernet.
- Det forbindelsesorienterte transportlaget er erstattet med en forbindelsesløs transportprotokoll (WAP WDP el. UDP hvis IP benyttes).
- Hele meldingen (konvolutt, heading og innhold) komprimeres før sending.
- Forbindelsesløs (connection-less) overføring av informasjon (ingen opp- og nedkopling) i de ulike protokoll-lagene.
- Mulighet for å bruke korte addresseformater i meldingene (X400 O/R Terminal Form)
- Bruk av IP header compression, hvis IP brukes som nett protokoll.

For flere detaljer refereres det til ref.(2).

3.2 Endringsforslag til ACP 142 (P_Mul)

Som vi ser av protokoll-profilen som er vist i figur 3.3, så bygger STANAG 4406 Annex E på protokollen P_Mul (ACP 142). Funksjonaliteten til P_Mul er beskrevet i seksjon 3.1.3. Under testing av Annex E på FFI, ble det oppdaget svakheter med P_Mul protokollen som kunne forbedres. STAROS har derfor skrevet et endringsforslag til ACP 142 som bl.a. beskriver

- mer dynamiske løsninger for re-transmisjon av data,
- mer dynamiske løsninger for generering av acknowledgement,
- flytkontroll mellom en rask applikasjon og en treg radio,
- m.m…

Endringsforslaget er under behandling i NATO MMHS WG og vil deretter bli sendt videre til CCEB (Combined Communications Electronics Board) som et endringsforslag på vegne av NATO.

3.3 Testing

FFI prosjektene STAROS og SIGVAT/HF har drevet omfattende testing av løsningene i

STANAG 4406 Annex E. I 2000 var STAROS med å utvikle et pilotsystem av STANAG 4406 Annex E sammen med FLO/IKT, FLO/Land og Thales. Dette systemet har blitt brukt for å demonstrere og teste løsningen både nasjonalt og internasjonalt. Pilotsystemet har også vært viktig for å forbedre og justere protokoll-parametre. Foreløpig har Annex E blitt testet over nettsimulatorer og følgende radioløsninger:

- STANAG 5066 over Harris RF-5710 A HF modemer og radioer under øvelse FLOTEX og MARVIKA, og mellom Tuentangen og Jåtta,
- STANAG 4538 over Harris Falcon II radioer mellom jørstadmoen og FFI
- MRR X.25 grensesnitt i MRR på lab på Jørstadmoen

Se ref. (23) og ref. (24) for flere detaljer ang. denne testingen.

3.3.1 JWID 2002 - Demonstrasjon av taktisk meldingstjeneste (STANAG 4406 Annex E)

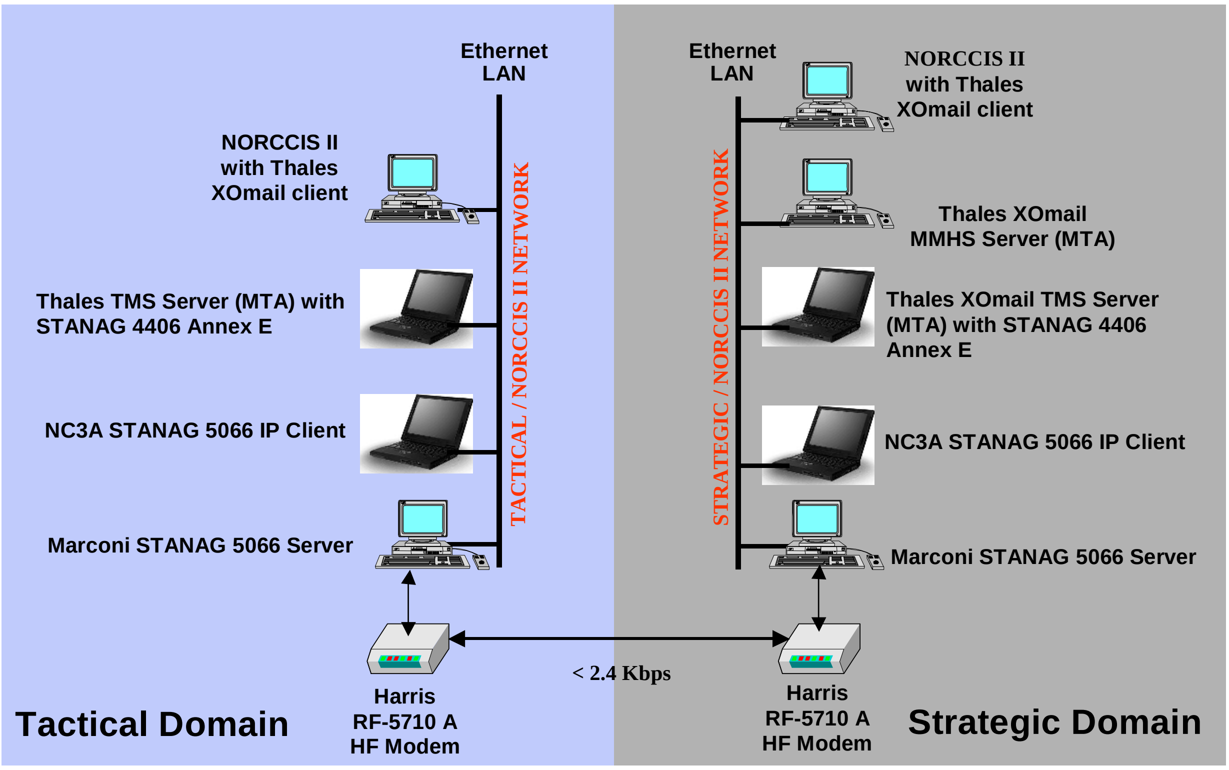
Som nevnt i forrige seksjon, så utviklet FFI, i samarbeid med FLO/IKT, FLO/LAND og THALES, en demonstrator for taktisk meldingstjeneste, basert på spesifikasjonen i STANAG 4406 Annex E. Under JWID 2002 ble denne demonstratoren vist som en integrert del av NORCCIS II (se figur 3.4). Det ble bl.a. demonstrert at overføring av meldinger mellom en taktisk og en strategisk NORCCIS II node, via en HF modem forbindelse med lav data rate (2,4 Kbps).

Figur 3.4 viser et taktisk og et strategisk domene. I det taktiske domenet, ser vi det taksiske MMHS systemet bestående av en Thales XOmail klient og en Thales XOmail server med den taktiske protokoll profilen (STANAG 4406 Annex E). Meldinger ble sendt fra den taktiske meldingsserveren via en IP-klient (utviklet av NC3A). IP-klienten setter oppe en forbindelse til en STANAG 5066 Server, som bl.a. har implementert et link lag over HF. Denne serveren ruter meldingen videre over HF modemet.

I det strategiske domenet er oppsettet nesten det samme som på taktisk side, bortsett fra at man her har en ekstra strategisk meldingsserver (MTA). Thales XOmail taktiske meldingsserver har to protokoll-stacker som gjør at den kan kommunisere ved bruk av både taktisk og strategisk protokoll profil. Den kan derfor fungere som en gateway mellom det taktiske og strategiske domenet.

Denne demonstratoren av STANAG 4406 Annex E ble senere videreutviklet av Thales til et produkt som har blitt integrert i XOmail.

For flere detaljer se ref.(14).

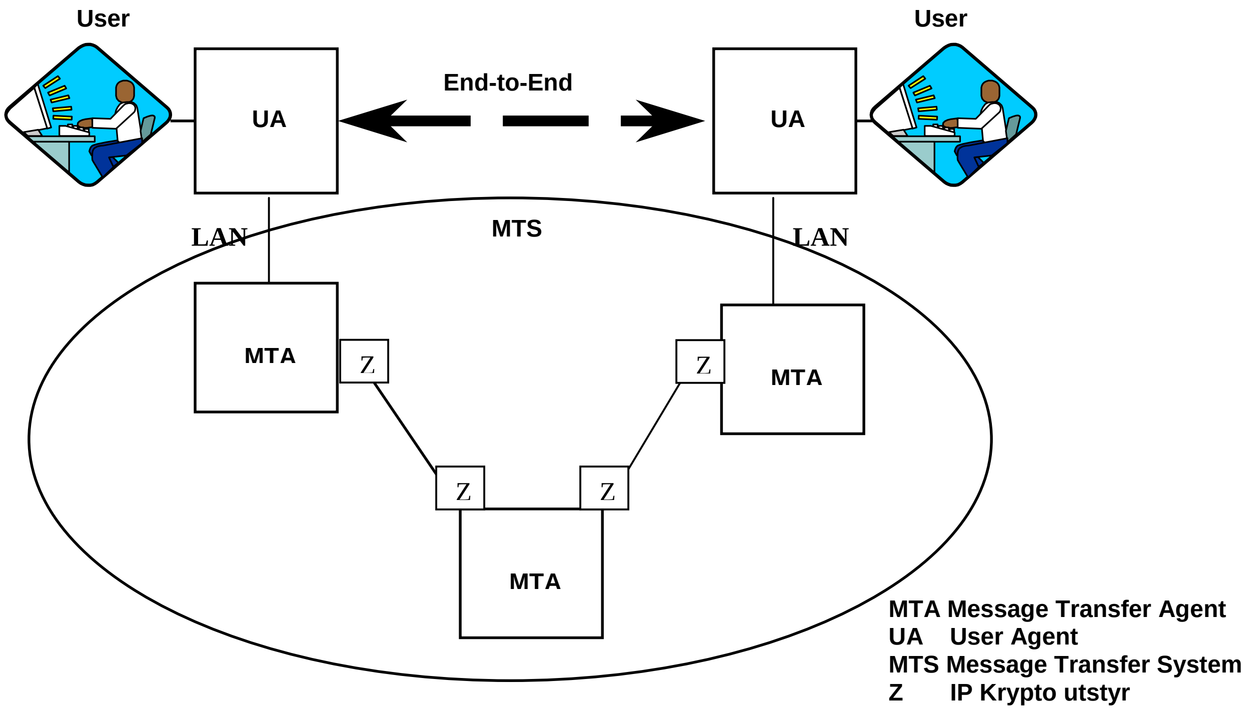


Figur 3.4 Demonstrator for integrasjon av taktisk og strategisk militær meldingstjeneste under JWID 2002

4 STANDARDISERING AV ENDE-TIL-ENDE SIKKERHETSLØSNINGER FOR MILITÆR MELDINGSTJENESTE

Konfidensialitetssikring av informasjon som skal overføres over nett har, i militær sammenheng, vanligvis blitt håndtert av kryptoutstyr på lavere lag i OSI modellen (f.eks. X.25 krypto, IP krypto og/eller bulk krypto). Dette vil antagelig også være tilfelle i en god tid fremover, når det gjelder informasjon av høyere graderinger. Grunnen til dette er strenge krav til sikkerhetsgodkjenning og akreditering av funksjonalitet og systemløsninger. Det er lettere å sikkerhetsgodkjenne en hardware-boks med en inngang og en utgang, enn programvare som er integrert i en eller flere applikasjoner. Dette utelukker derimot ikke behovet for å legge ekstra sikkerhetstjenester nærmere applikasjonene og brukerne, i tillegg til bruk av lavere lags krypto, for å overholde kravene til konfidensialitetsbeskyttelse for høyere sikkerhetsgraderinger.

NATO arbeidsgruppene Working Group on MMHS og Ad-Hoc Working Group on Application Security, har i de senere årene bl.a. arbeidet med ende-til-ende sikkerhetsløsninger for militær meldingstjeneste (MMHS). Hensikten har vært å legge visse sikkerhetsløsninger nærmere endesystemene og brukeren av informasjonen. Med lavere lags krypto, beskytter man informasjonen under overføring mellom systemene (eller organisasjonene), men disse løsningene begrenser ikke hvem som får tilgang til informasjonen etter at de har kommet inn i ende-systemene og lokalnettene. Med ende-til-ende sikkerhetsløsninger kan man sikre informasjonen hele veien fra avsender til mottaker. Som nevnt vil det være vanskelig å få godkjent sikkerhetsløsninger for høyere graderinger som kun baserer seg på ende-til-ende sikkerhetsmekanismer. Løsningen vil antagelig bli at man benytter lavere lags krypto for konfidensialitet og at man benytter ende-til-ende sikkerhet for autentisering, integritet og "need-to-know" separasjon.



Figur 4.1 Figuren er ment å illustrere at ende-til-ende sikkerhet går mellom bruker applikasjonene, mens IP krypto brukes mellom hver meldingssvitjs (MTA) i meldingsoverføringssystemet.

4.1 STANAG 4406 Ed. 1 Annex B - Protecting Content Type (PCT)

Standardiseringsarbeid er ofte en tidkrevende prosess fordi nasjonene ofte har nasjonale interesser å ivareta. Når en standard for ende-til-ende sikkerhet for militær meldingstjeneste (STANAG 4406 Ed.1) skulle bestemmes, var ikke nasjonene enige om hvilke sikkerhetsprotokoller løsningene skulle baseres på. I utgangspunktet ønsket man å benytte sikkerhetsprotokoller definert i den sivile X.400 standarden. Dette var ikke akseptabelt for enkelte nasjoner som allerede hadde valgt andre løsninger nasjonalt, og som ikke ønsket å konvertere. Til slutt endte man opp med en "equal pain" løsning som var basert på en tredje standard og som førte til at begge leire måtte konvertere. Denne sikkerhetsløsningen, som ble valgt for STANAG 4406 Edition 1, ble kalt PCT (Protecting Content Type) og var basert på IETFs S/MIME v3 standard, men med visse modifikasjoner som gjorde at de sivile standardiserte løsningene ikke kunne brukes direkte. PCT er basert på bruk av digitale signaturer, og kan brukes for autentisering av avsender og integritetsbeskyttelse av meldingen.

Under utarbeidelsen av PCT protokollen, var det hele tiden klart at dette bare var en midlertidig løsning og at man ønsket å arbeide videre med en løsning som var mer konform med S/MIME standardene. Norge (ved FFI/STAROS) og USA utarbeidet et forslag som ble akseptert av arbeidsgruppene NATO C3 Board (SC/4)AHWG Application Security og NATO C3 Board

(SC/5)WG MMHS. Denne løsningen er beskrevet i seksjonene 4.2 til 4.5.

4.2 STANAG 4406 Ed.2 Annex B – S/MIME v.3

FFI/STAROS har sammen med USA vært editor for STANAG 4406 Ed.2 Annex B, som beskriver ende-til-ende sikkerhet for militær meldingstjeneste i NATO. Annex B beskriver en overordnet arkitektur for hvordan sikkerhetstjenestene skal implementeres, samt hvilke av disse sikkerhetstjenestene som må støttes for at meldingssystemet skal være konform med Annex B. Annex B beskriver også hvordan sikkerhetstjenestene skal implementeres ved å henvise til dokumentet ”The NATO Profile for S/MIME CMS and ESS”. Figur 4.2 viser forholdet mellom de ulike dokumentene som til sammen spesifiserer sikkerhetsløsningen for STANAG 4406 Ed.2.

Nedenfor følger et utvalg av sikkhetstjenestene som er definert i Annex B, med en kort forklaring. For en mer detaljert beskrivelse se STANAG 4406 Ed.2 Annex B.

4.2.1 Access Control

Aksesskontroll er en tjeneste som gjør det mulig å bare la autoriserte brukere få tilgang til en melding. Sikkerhetsmerker (security labels) kan benyttes for å merke meldinger med bl.a. graderingsnivået på informasjonen i meldingen. Graderingsinformasjonen i et sikkerhetsmerke kan bl.a. kontrolleres mot et systems akkrediteringsnivå, for å avgjøre om en melding kan sendes via dette systemet.

Aksesskontroll vil utføres i hvert MMHS domene i henhold til den gjeldende sikkerhetspolicy. Nasjonale MMHS systemer må støtte både nasjonale og NATO sikkerhetspolicy. Med dette menes at nasjonale MMHS systemer må kunne overføre meldinger med enten nasjonale eller NATO sikkerhetsmerker. For å støtte disse kravene, har standardiserte maskinlesbare datastrukturer blitt etablert for sikkerhetsmerker. Behovet for sikkerhetsmerker vil sannsynligvis bli enda større i tiden som kommer for kunne håndtere informasjonsutveksling mellom ulike koalisjoner.

4.2.2 Authentication of Origin

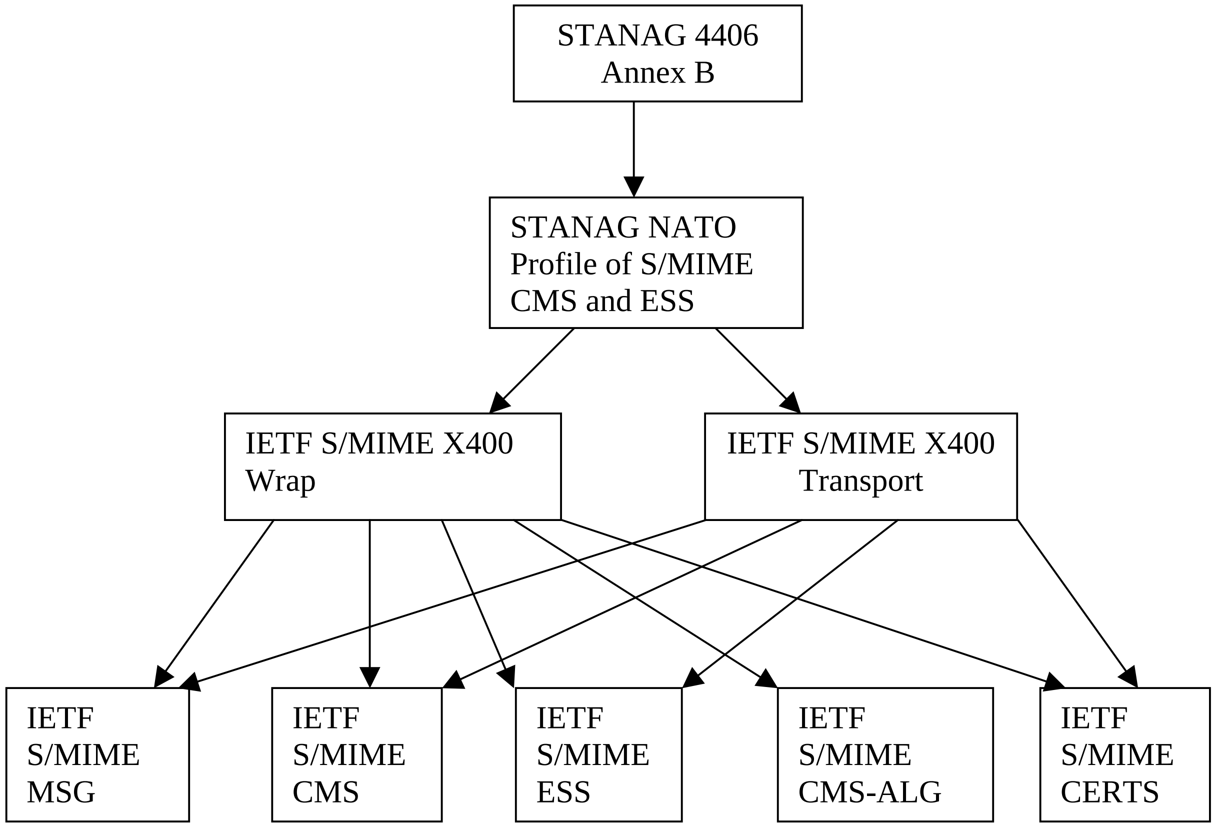
Tjenesten “Autentication of origin” gir tillit til identiteten til en entitet (en person eller et system). Det er metoden for å oppnå tiltro til at det er avsenderen som har sendt meldingen og at avsenderen er den han utgir seg for å være.

4.2.3 Non-repudiation of Origin

Tjenesten “Non-repudiation of origin” beskytter mot at avsenderen av meldingen i ettertid feilaktig kan nekte for at meldingen har blitt sendt eller tidspunktet som meldingen er sendt på.

4.2.4 Message Integrity

Tjenesten “Message Integrity” gir mottakerene av meldingen en indikasjon på om meldingen har blitt modifisert, slettet eller byttet ut, uten autorisasjon.



Figur 4.2 Figuren viser sammenhengen mellom de ulike STANAGene og IETF standardene(se referanseliste for henvisning til de ulike standardene).

4.2.5 Message Data Separation

Tjenesten “Message Data Separation” skiller kryptografisk data som er inneholdt i en melding fra data som er inneholdt i en annen melding, og ivaretar konfidensialiteten til dataene helt fra avsender til mottaker. Denne tjenesten kan være med å håndheve “need-to-know” restriksjoner, eller å bidra til at flere buker-miljøer kan anvende de samme systemene uten at de får innsyn til hverandres meldinger. Denne tjenesten er uavhengig av sikkerheten i nettet som transporterer meldingene.

4.2.6 Security Labels

Security Labels (eller sikkerhetsmerker) angir “security policy”, gradering, kategorier og andre indikasjoner på hvordan meldingen og informasjonsinnholdet skal håndteres. “Security labels” kan brukes for aksesskontroll og for indikasjon om hvordan meldingen skal rutes i meldingstransmisjonssystemet.

4.2.7 Non-repudiation of Receipt

Tjenesten “Non-repudiation of Receipt” gir en kryptografisk binding mellom en signert melding og en kvittering som er sendt som respons på mottak av meldingen. Tjenesten gir avsenderen en forsikring om at meldingen som ble sendt er mottatt av mottakeren, og at meldingen som ble mottatt er den samme som meldingen som ble sent.

4.2.8 Secure Mailing Lists

Tjenesten “Secure Mailing Lists” gjør det mulig for en “Mail List Agent” (distribusjonssystem for meldinger med mottakerlister) å ta en enkelt melding, utføre mottaker spesifikk sikkerhetsprosessering, og deretter re-distribuere meldingen til hvert medlem i ”mottakerlisten” (Mailing List). Tjenesten gjør det mulig å drive mer effektiv management av store “mottakerlister”, samt å inkludere mekanismer for å hindre ”mail-loops” (meldingen blir rutet i ring i meldingstransmisjonssystemet).

For en fullstendig liste av tjenestene, se STANAG 4406 Ed.2 Annex B.

4.3 The NATO Profile for SMIME CMS and ESS

FFI/STAROS har vært editor for dokumentet ”The NATO Profile for S/MIME CMS and ESS” som nå er sendt ut for ratifisering som en NATO STANAG under NATO C3 Board SC/4 Information Security (se ref. 5).

For å implementere de ende-til-ende sikkerhetstjenestene som er definert i STANAG 4406 Ed.2 Annex B, så må man benytte mekanismer og funksjonalitet som er definert i en rekke ulike IETF standarder. Disse standardene definerer ofte mye funksjonalitet, noe som det er påkrevd å implementere og annet som det er valgfritt å implementere. NATO profilen for S/MIME definerer hvilke standarder og hvilken funksjonalitet i disse standardene som må benyttes for å implementere de ende-til-ende sikkerhetstjenestene som er definert i STANAG 4406 Annex B.

Som vi ser av figur 4.2, så peker NATO profilen for S/MIME på to IETF standarder hhv. ”Securing X.400 Content with S/MIME” ref.(11) og ” Transporting S/MIME Objects in X.400” ref.(12). Dette er standarder som NATO har skrevet og som har blitt utgitt som sivile IETF standarder for å kunne bruke hyllevareløsninger for ende-til-ende sikkerhet i militære meldingssystemer basert på ITU X.400 standarden.

Løsningen blir dokumentert både som STANAG 4406 Ed.2 Annex H og som en egen STANAG under NATO C3 Board SC/4 Information Security.

Jeg henviser leseren til selve dokumentet for mer detaljer rundt NATO profilen for S/MIME (se ref.(5)).

4.4 IETF RFC “Securing X.400 Content with S/MIME”

FFI/STAROS har sammen med USA vært editor til IETF standarden ”Securing X.400 Content with S/MIME” (ref. (11)). I tråd med utviklingen av mer bruk av hyllevare i militære systemer, har løsningene for ende-til-ende sikkerhet i militære meldingssystemer blitt basert på internasjonale standarder for sikkerhet i epost systemer (SMTP). Standardene man har valgt som utgangspunkt heter IETF S/MIME V.3 og er brukt bl.a. i Microsoft Outlook .

4.4.1 Standardiseringsprosessen i IETF

IETF S/MIME v3 er et sett med standarder og er spesifisert med tanke på meldingsprotokollen SMTP (Simple Mail Transfer Protocol) og MIME kodingsformat. Formell meldingstjeneste i NATO er definert av STANAG 4406 som er basert på ITU X.400 og S/MIME v3 lar seg derfor ikke bruke over disse militære systemene direkte.

For å kunne bruke S/MIME over NATOs militære meldingssystemer basert på ITU X.400, var det behov for å spesifisere utvidelser til S/MIME standardene. I regi av NATOs arbeidsgruppe NC3B(SC/4) Ad-Hoc Working Group on Application Security, startet FFI/STAROS og USAs representant arbeidet med å spesifisere nye RFCer, med mål om å prøve å få disse akseptert i IETF som en del av settet av S/MIME standarder. Begrunnelsen for å prøve å utgi disse dokumentene som IETF standarder og ikke NATO STANAGer, var at vi mente at sivile standarder i større grad fremmer utviklingen av hyllevareprodukter enn militære standarder. USA hadde også gode kontakter inn i IETF organisasjonen og fikk med Paul Hoffman som medforfatter. Paul Hoffman har vært editor for flere av de andre S/MIME standardene og det var større sjanse for å få løsningen akseptert i IETF hvis han ble med som medforfatter. Arbeidet ble fordelt ved at FFI/STAROS skrev hoveddelen av dokumentet ”Securing X.400 Content with S/MIME” og Chris Bonatti fra USA skrev hoveddelen av dokumentet ” Transporting S/MIME Objects in X.400”. Paul Hoffman står som medforfatter på begge standardene og ga oss derved innpass på IETF arenaen.

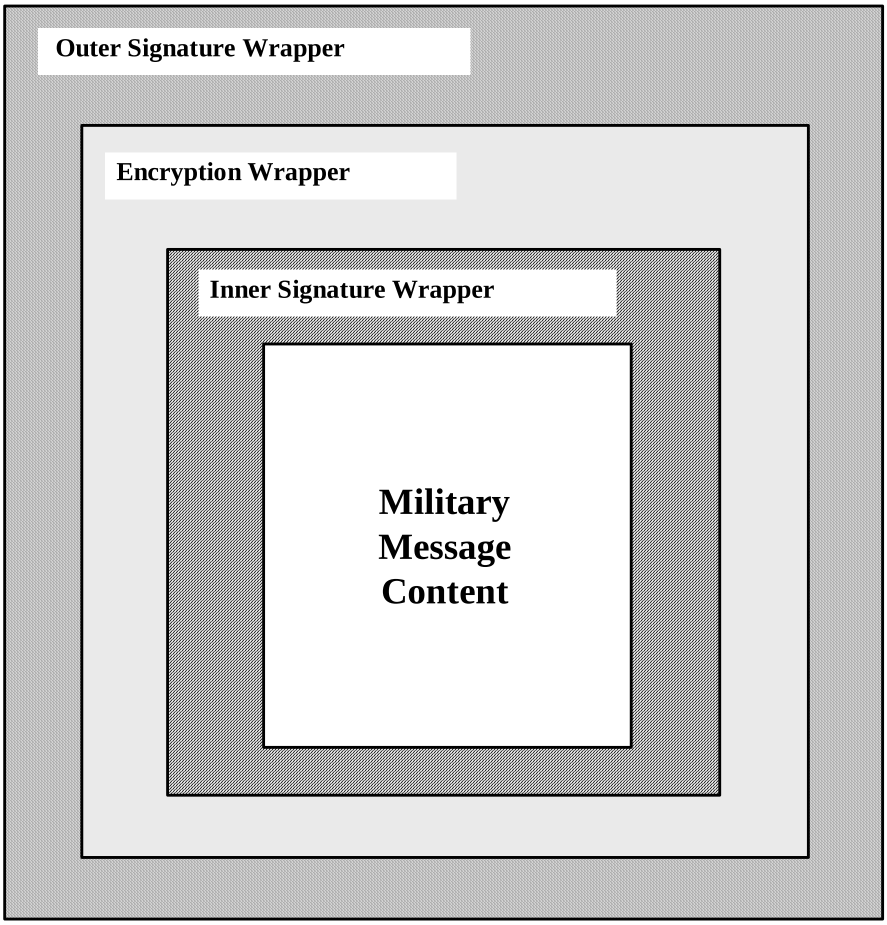
Etter flere runder med kommentarer og editeringer, ble forslagene akseptert i IETF (oktober 2003) og vil bli gitt ut som IETF RFC standarder (ref. (??)).

Standardene er allerede implementert av en rekke store leverandører bl.a. Mototola, Nexor, Clearswift, Boldon James, Thales m.fl.

4.4.2 Overordnet beskrivelse av standarden

Standarden ”Securing X.400 Content with S/MIME” beskriver hvordan S/MIME v3 kan benyttes for å sikre X.400 meldingsformater. Militære meldinger basert på STANAG 4406 er av typen X.400 meldingsformat. S/MIME definerer en innkapslingsteknikk hvor det benyttes ulike typer konvolutter for å gi meldingen forskjellig typer sikkerhet. Figur 4.3 viser en ”tripple wrapped message”, som vil si at meldingen er pakket inn med tre konvolutter (wrappers). Hver konvolutt inneholder en data del (som igjen kan inneholde en annen konvolutt) og et sett med parametere og attributter relatert til den sikkerhetsfunksjonaliteten konvolutten representerer.

- Den indre konvolutten (”Inner Signature Wrapper”) gjør det mulig å signere meldingen med en digital signatur, samt å binde et sett med attributter (som for eksempel et sikkerhetsmerke) til meldingen kryptografisk.
- Den andre konvolutten (”Encryption Wrapper”) gjør det mulig å kryptere innholdet, som i dette tilfellet er hele ”Inner Signature Wrapper” som utgjør den signerte meldingen.
- Den ytre konvolutten (”Outer Signature Wrapper”) gjør det mulig å legge på en ny signatur over ”Encryption Wrapper”. Hensikten med dette er bl.a. at den krypterte meldingen kan ha en annen sikkerhetsgradering enn den opprinnelige meldingen. Det kan derfor være hensiktsmessig å kryptografisk binde et nytt sikkerhetsmerke til den krypterte meldingen, for bl.a. å indikere at den nå ikke trenger like streng beskyttelse.



Figur 4.3 En ”tripple wrapped message” bestående av en indre signatur konvolutt, en konfidensialitetskonvolutt og en ytre signatur konvolutt.

En forskjell mellom en X.400 melding og SMTP melding, er at de kodes forskjellig. En X.400 melding blir kodet ved bruk av kodingsstandarden ASN.1, mens en SMTP melding kodes ved bruk av MIME. I en ”tripple wrapped message” av en SMTP melding, vil hver konvolutt ha en ekstra MIME innkapsling som introduserer veldig mye overhead og strengt tatt bare er nødvendig for bakoverkompatibilitet med forrige versjonen av S/MIME (v2). I de nye RFCene har vi valgt å fjerne MIME kodingen for ”tripple wrapped messages”, men å gjøre det valgfritt å benytte den over den ytterste konvolutten (enten det er single eller tripple wrapped) for å gjøre det mulig å transportere meldingen i et SMTP transportsystem hvor MIME-koding er påkrevet.

For mer informasjon se ref.(5).

4.5 STANAG 4406 Annex G ” Compatibility with PCT-Based MMHS Security”

FFI/STAROS og USA har sammen skrevet STANAG 4406 Annex G “Compatibility with PCT-Based MMHS Security”. Dette Annex’et beskiver hvordan systemer basert på sikkerhetsløsningene beskrevet i STANAG 4406 Ed.2 kan kommunisere med systemer som er basert på STANAG 4406 Ed.1. Forskjellen er at i Edition 2 så benyttes en full S/MIME løsning, mens Edition 1 er basert på PCT. I NATO vil man i en periode ha nasjoner som bruker forskjellige versjoner av STANAG 4406, og det er viktig at systemene kan kommunisere selv om deler av funksjonaliteten er forskjellig.

For mer informasjon og detaljer se STANAG 4406 Ed.2, Annex G.

5 TESTING OG DEMONSTRATORER

5.1 Testing og demonstrasjon av ende-til-ende sikkerhetsløsninger for MMHS

Både ende-til-ende sikkherhetsløsningene og den taktisktiske profilen for MMHS er testet både i nasjonale og internasjonale tester og demonstratorer. Internasjonal testing er nødvendig for å avklare tvetydigheter i standarder og få erfaring med integrasjon av systemer som MMHS, Directory og PKI. Norge har foreløpig ikke tatt i bruk en slik integrert løsning med ende-til-ende sikkerhet nasjonalt. I løpet av 2006 vil NATO begynne sammenkoblingen av NATOs NMS og nasjonale MMHS systemer. Testingen som er beskrevet i dette kapittelet har gitt oss nyttig erfaring med tanke på denne integrasjonen.

5.1.1 JWID 2002 - Demonstrator for ende-til-ende sikkerhetsmekanismer og integrering av MMHS, Directory og PKI

I JWID 2002 var FFI/STAROS involvert i arbeidet med en demonstrator for taktisk MMHS (beskrevet i seksjon 3.3.1), og en integrert løsning med MMHS, Directory og PKI for bl.a. å demonstrere ende-til-ende sikkerhetsløsninger. Disse løsningene ble vist som en integrert del av kommando- og kontroll-systemet NORCCIS II, som også ble demonstrert under øvelsen. Vi vil ikke komme inn på NORCCIS II i denne rapporten, da det var FLO/IKT som hadde ansvaret for denne demonstrasjonen.

Norge og Storbritannia demonstrerte en integrert løsning av MMHS (militær meldingstjeneste), Directory (katalogtjeneste) og PKI (Public Key Infrastructure). Alle disse komponentene er nødvendige for å ha et MMHS med ende-til-ende sikkhetsfunksjoner. Den norske demonstratoren var et samarbeid mellom FFI (ved STAROS), FLO/IKT, NSM og Thales. STAROS hadde ansvaret for demonstrasjonen av STANAG 4406 Annex E og for koordingeringen av MMHS, Directory og PKI aktiviteten nasjonalt og internasjonalt.

Som for MMHS, er det også for Directory og PKI utfordringer når det gjelder å oppnå interoperabilitet mellom systemer fra forskjellige nasjoner. Figur 5.1 viser systemene som var med i demonstrasjonen. Her ser vi det norske domenet, Storbritanias domene, samt ”Cooperativ zone” som er et felles domene som NC3A var ansvarlig for. De oransje boksene representerer militære meldingssystemer. De blå boksene representerer Directory systemer og grå boksene representerer PKI systemer.

5.1.1.1 PKI systemet

PKI CA (Certificate Authority) på figur 5.1 brukes for å utstede sertifikater og CRLer (Certificate Revocation List), og en PKI RA (Registration Authority) brukes for å registrere brukere som det skal utstedes sertifikater til. For å oppnå interoperabilitet mellom PKI systemer fra forskjellige ”security policy” domener, må man bl.a. bli enige om sertifikatformater og signatur algoritmer. Man må også bli enige om en ”trust modell” for å kunne ha tillit til sertifikater og CRLer som utstedes av et annet sikkerhetsdomene.

Hver nasjon har en rot-CA som autoriserer de andre CAene i et hierarki av CAer i et sikkerhetsdomene. I denne JWID demonstratoren bygger tillitsmodellen på en mekanisme som heter ”trust anchors” hvor et rot-sertifikat (som man har fullstendig tillit til) fra det norske sikkerhetsdomene blir lastet ned i de britiske meldingssystemene (og omvendt), via kurer eller en annen sikker mekanisme.

Når en melding signeres i det norske meldingssystemet, vil det bli lagt ved et sertifikat som er utstedt av den norske CAen, som igjen har et sertifikat som er utstedt av den norske rot-CAen. Informasjon om hele denne kjeden av sertifikater blir lagt ved meldingen. Dette er nødvendig for at et meldingssystem i Storbritanias domene skal kunne verifisere at sertifikatet, som autoriserer signaturen til meldingen, er gyldig og har en link til rot-CAen som man har fullstendig tillit til. Sertifikater kan enten distribueres i selve meldingen, eller i Directory. CAene kan også utstede CRLer (Certificate Revocation Lists) som brukes for å angi hvilke sertifikater som ikke er gyldige lengre. Når et sertifikat eller en CRL genereres av PKI CAen i demonstratoren, blir den lastet ned i Directory serveren. Denne informasjonen blir også distribuert i Directory slik at en mottaker av en melding kan slå opp for å sjekke om sertifikatet som er brukt til å signere en melding er gyldig eller ikke.

5.1.1.2 Directory systemet

Directory er her et støttesystem for MMHS som gjør det mulig å dele nødvendig informasjon som bl.a. meldingsaddresser, sertifikater, CRLer, o.l mellom de allierte. For å oppnå interoperabilitet mellom forskjellige Directory systemer, er det viktig å bli enige om et ”Directory Schema” (en modell for hvordan informasjonen skal organiseres), samt kommunikasjonsprotokollene som skal brukes for å utveksle informasjonen. I NATO har man skissert en Directory modell hvor hver nasjon har en ”border DSA”, dvs. en katalog server hvor man laster ned all informasjon som man ønsker å dele med andre nasjoner. Denne informasjonen blir så replisert ned til en ”Coalission Hub” som kan sees på som en felles Directory server. Fra denne felles Directory serveren, kan hver nasjon laste ned all informasjon som de andre nasjonene har lagt ut for distribusjon. Hensikten med en slik ”Coalission Hub” er at alle nasjonene kun trenger å være interoperabel men denne hub’en, i stedet for å måtte være interoperabel med alle andre nasjoners Directory systemer. ”Coalission Hub” tilbyr flere protokoll grensesnitt som nasjonene kan velge mellom, når de skal kople seg til. Directory informasjon fra hvert sikkerhetsdomene ble under denne demonstrasjonen automatisk replisert ned til (og hentet ut av) til ”Coalission Hub” hvert 15 min. Hvis for eksempel et sertifikat ble trukket tilbake (gjort ugyldig), så kunne man hente ut denne informasjonen fra sin lokale Directory etter maksimalt 15 minutter. Frekvensen på replikasjonen kunne konfigureres.

5.1.1.3 Meldingssystemet

Under JWID 2002 ble Thales XOmail system benyttet for både det strategiske og taktiske meldingssystemet på norsk side. I det norske domenet ser vi det taktiske meldingssystemet helt til venstre som er koplet sammen med en strategisk meldingsserver. Denne strategiske meldingsserveren er koplet til en Directory server som brukes for å hente ut meldingsaddresser, sertifikater og CRLer. Denne meldingsserveren er videre koplet til meldingssystemene til Storbritannia. Vår nasjonale ”Border DSA” og Storbritanias ”Border DSA” er begge koplet til

”Coalission Hub” som er beskrevet i forrige avsnitt.

Under demonstrasjonen viste vi bl.a. at vi kunne sende meldinger fra det taktiske meldingssystemet gjennom det norske strategiske meldingssystemet og til Storbritanias meldingssystem. Vi viste også at meldinger som ble signert på norsk side kunne verifiseres på britisk side og omvendt. Det ble også demonstrert automatisk replisering av Directory informasjon, som for eksempel sertifikater og CRLer, slik at mottakere på begge sider kunne sjekke CRLer i sitt lokale Directory for å kontrollerere om signaturene til meldingene ble mottatt var gyldige.

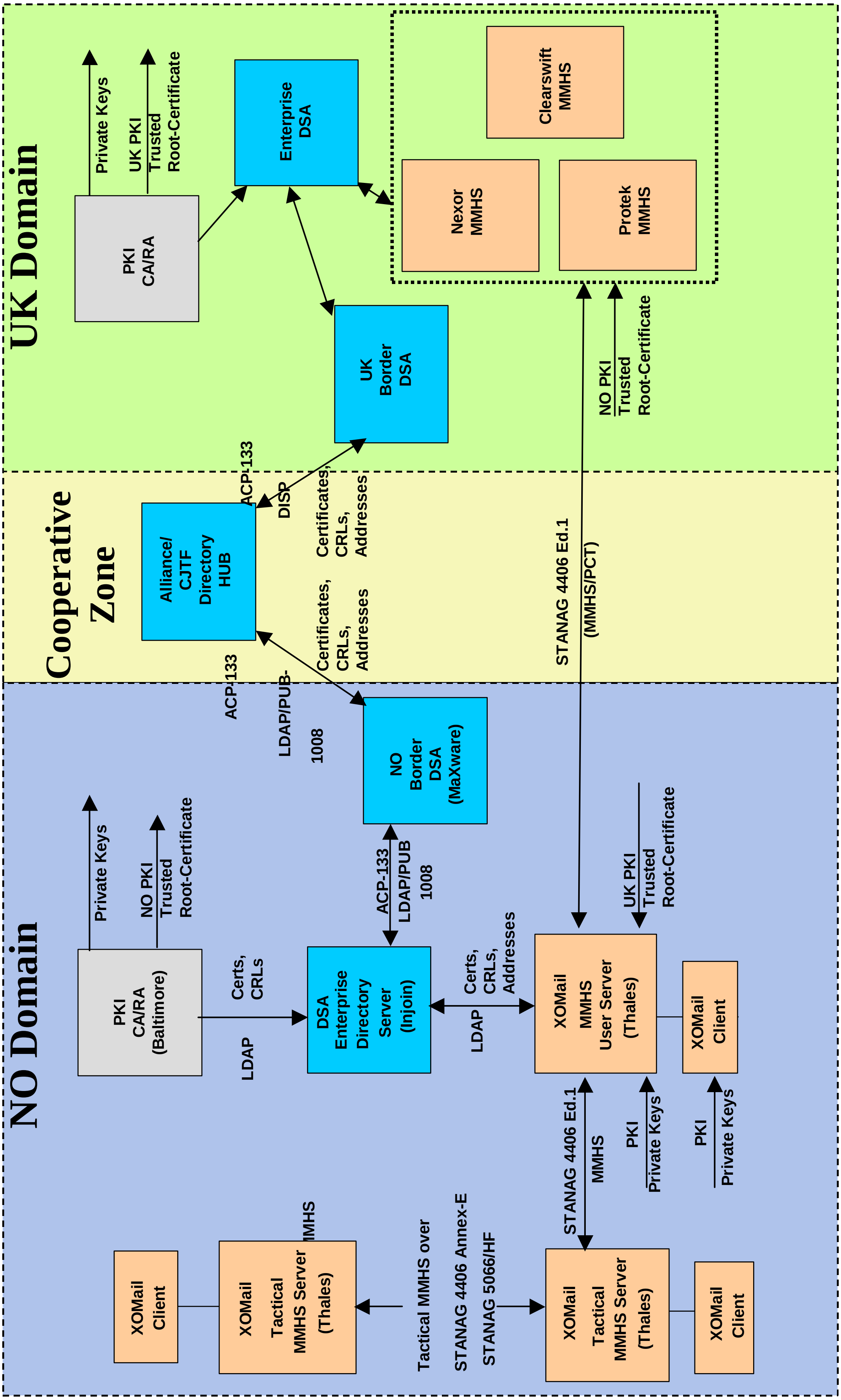
Se ref. (14) for en mer detaljert beskrivelse demonstratoren som ble vist under JWID 2002.

5.1.2 JWID 2003 - ACP 145 demonstrator

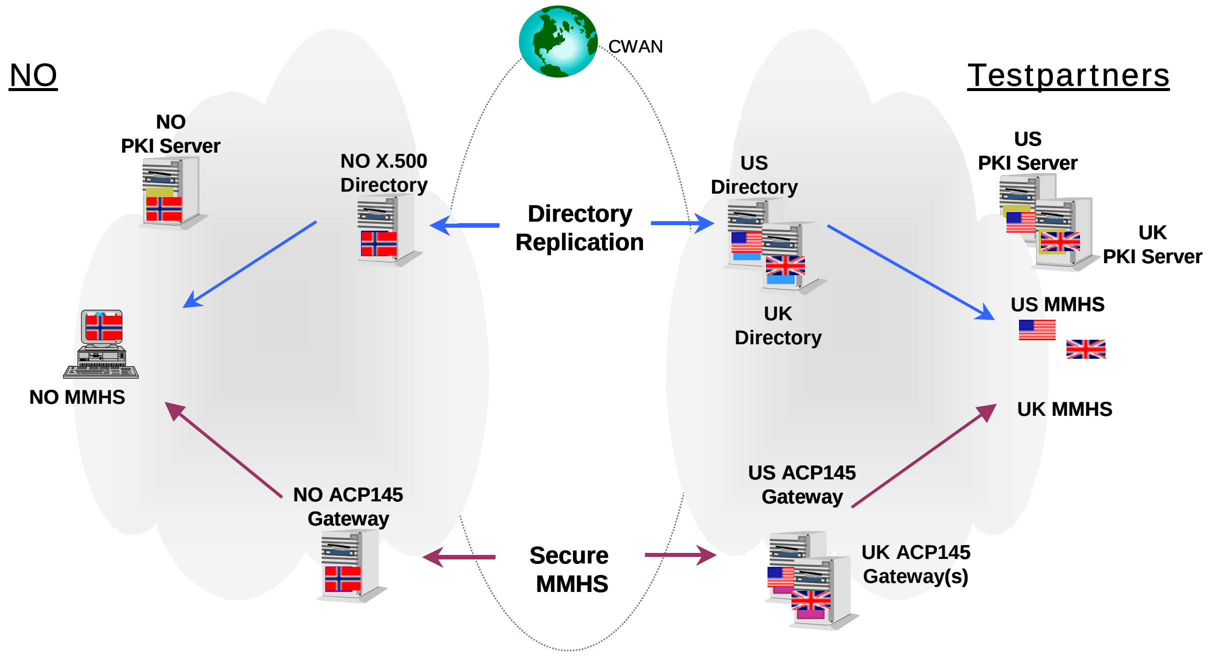
På JWID 2003 hadde Norge inngått samarbeid med Storbritannia og USA om en tilsvarende demonstrasjon som året før (se seksjon 5.1.1). Forskjellen var at systemene denne gangen var basert på standarden ACP 145 (som beskriver hvordan MMHS, Directory og PKI kan integreres). Dette er en standard som NATO ikke har adoptert (enda), men som er forholdsvis lik tilsvarende NATO løsninger. Vi vil ikke komme inn på forskjellen mellom ACP 145 og tilsvarende NATO løsninger i denne rapporten, men nysgjerrige lesere henvises til ref. (20).

Som for demonstrasjonen på JWID 2002 var arbeidet med ACP 145 demonstratoren, fra norsk side, et samarbeid mellom FFI (ved STAROS), FLO/IKT, NSM og Thales. FFI/STAROS hadde ansvaret for koordinering av arbeidet nasjonalt og internasjonalt, samt deler av spesifikasjonsarbeidet. Selve testingen mot de andre nasjonene ble utført av Thales og FLO/IKT på SHAPE i Mons (Belgia).

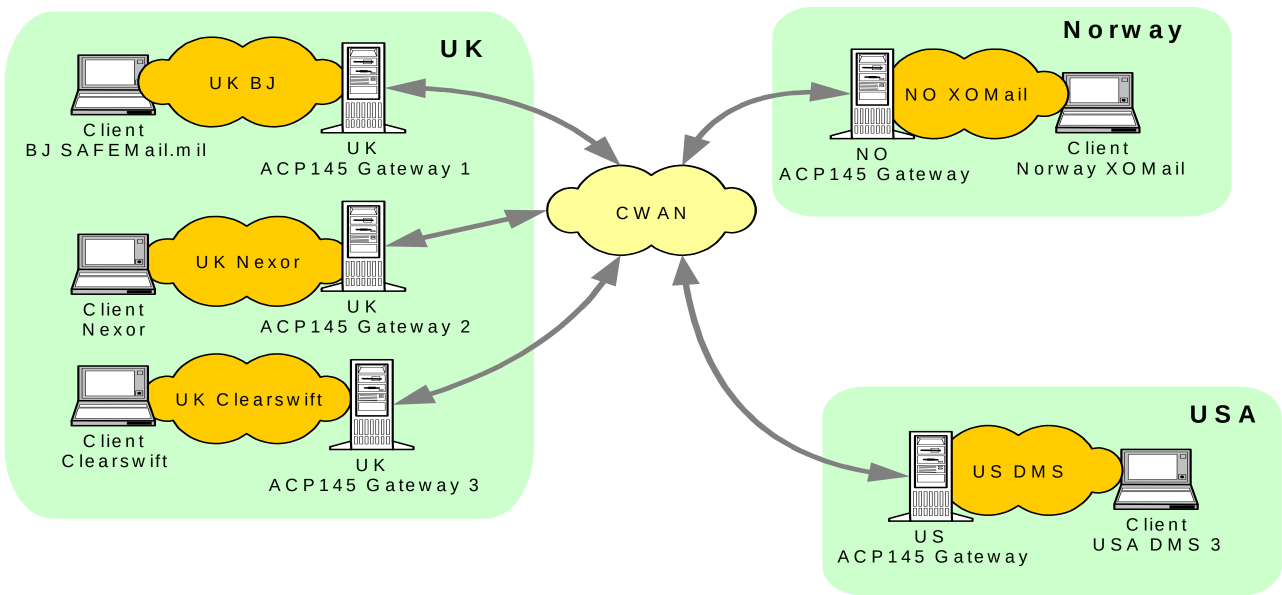
Figurene 5.2, 5.3 og 5.4 viser hvordan det norske systemet var koplet mot systemene fra Storbritannia og USA. Figur 5.2 viser en overordnet arkitektur, Figur 5.3 viser hvordan meldingssystemene fra de tre nasjonene var sammenkoplet over ”Coallision Wide Area Network” (CWAN). Figur 5.4 viser tilsvarende sammenkoplingen mellom Directory systemene. Som vi ser er demonstratoren forholdsvis lik demonstratoren fra JWID 2002, men som nevnt var protokollfunksjonaliteten forksjellig. For å beskrive forskjellene må vi ned på detaljnivå i protokollene, noe vi ønsker å unngå i denne rapporten. Vi henviser derfor til ref. (20) for detaljer.



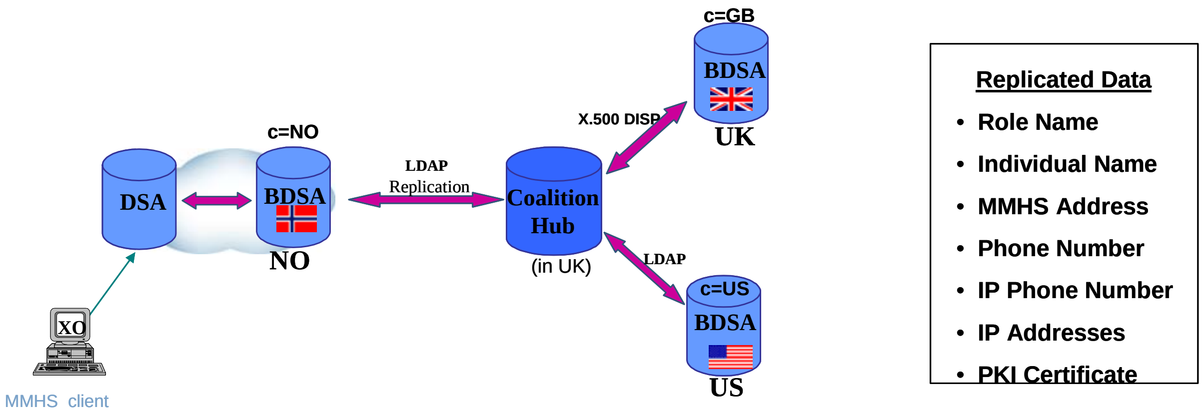
Figur 5.1 Norge og Storbritanias demonstrator under JWID 2002 som viste en integrert løsning av MMHS, Directory og PKI systemer.



Figur 5.2 JWID 2003: Demonstrasjonen av interoperabilitet mellom ACP 145 systemer fra Norge, Storbritannia og USA. ACP 145 spesiferer en løsning for hvordan MMHS, Directory og PKI kan integreres.



Figur 5.3 ACP 145 demonstratoren under JWID 2003, MMHS interoperabilitet.



Figur 5.4 ACP 145 demonstratoren under JWID 2003, Directory interoperabilitet.

5.1.3 MMHS Security Demonstrator Programme (MSDP)

MSDP (MMHS Security Demonstrator Programme) var en demonstrator som ble utført mellom flere NATO nasjoner (NO, GE, UK, US, FR, PT og TR) for å teste ende-til-ende sikkerhetsfunksjonaliteten i STANAG 4406 Ed.1 også kalt PCT (Protecting Content Type) (se seksjon 4.1). PCT er basert på S/MIME men inneholder bare et sub-sett av funksjonaliteten. PCT definerer hvordan man kan binde en digital signatur til en melding. PCT gir ende-til-ende sikkerhetstjenestene integritet og autentisering av avsender.

MSDP ble utført ved at alle involverte nasjoner testet mot et referansesystem på NC3A i Haag. Noen nasjoner testet over Internet, andre via ISDN forbindelser og noen installerte systemene i laboratoriet på NC3A.

MSDP ble inndelt i to faser. Den første fasen omfattet testing av meldingsfunksjonalitet uten sikkerhet, mens den andre fasen fokuserte på sikkerhetsfunksjonalitet og signerte meldinger.

Norge deltok med Thales sitt XOmail system, som er systemet som brukes i vårt nasjonale meldingssystem (MIF). FFI/STAROS var ansvarlig for koordineringen av den norske deltagelsen i MSDP nasjonalt og internasjonalt og representerte Norge både i MSDP Steering Committee og MSDP Technical Committee. Selve testingen ble utført av Thales over Internet mot referansesystemet i Haag.

Under MSDP testingen ble det oppdaget flere uklarheter i STANAG 4406 Ed.1 som hadde ført til at flere av leverandørene hadde tolket STANAGen forskjellig. Dette resulterte i at deler av funksjonaliteten til systemene ikke var interoperable. Dette er feil som har blitt rettet opp i Edition 2 av STANAG 4406.

For mer informasjon om MSDP se ref.(21).

6 MMHS- ACP 127 GATEWAY (STANAG 4406 ANNEX D)

STAROS har hatt ansvaret for oppdatering av Annex D (ACP 127 gateway) i NATO MMHS

WG. Dette arbeidet ble satt bort til Thales Communications i Trondheim. ACP 127 er en standard utviklet på 60 tallet, og som opprinnelig ble skrevet for utveksling av militære meldinger mellom fjernskrivere. I senere år har systemene blitt modernisert, men systemet er fremdeles gammeldags i forhold til dagens meldingssystemer. Gateway løsningen som er definert i Annex D av STANAG 4406 er nødvendig, fordi man ønsker interoperabilitet mellom X.400 baserte MMHS systemer og ACP127 systemer som fremdeles brukes i mange NATO nasjoner. I Norge så er alle strategiske ACP 127 systemer byttet ut med X.400 baserte STANAG 4406 systemer, men Sjøforsvaret benytter fremdeles ACP 127 systemer for utveksling av militære meldinger over kommunikasjonssystemer med lav data-rate (for eksempel HF radioer). STANAG 4406 Annex E (NATO Tactical MMHS protocol and profile) ble utviklet med tanke på å erstatte ACP 127 systemene på taktisk nivå.

7 OPPDATERING AV STANAG 4406 FRA EDITION 1 TIL EDITION 2

FFI/STAROS har deltatt i arbeidet med å oppdatere STANAG 4406 fra Edition 1 til Edition 2. Det ble opprettet en undergruppe under NATO MMHS WG bestående av representanter fra NO, FR, UK, US og GE. Denne gruppen fikk navnet ”The Red Team” og skulle utføre det konkrete arbeidet med å skrive et komplett sett av endringsforslag (Change Proposlas) til Edition 1 som ville bringe STANAG 4406 til Edition 2. Dette arbeidet medførte bl.a. å analysere resultatene fra MSDP testingen for å endre e.v.t. inkonsistenser, tvetydigheter og mangler i STANAG 4406 Ed.1, som hadde ført til at leverandører hadde tolket og implementert funksjonaliteten forskjellig. Vi skal ikke gå gjennom alle forskjellene mellom Edition 1 og Edition 2 da dette vil bli veldig detaljert, men kun nevne noen av endringene:

- Endring av sikkerhetsprotokoll fra PCT til S/MIME v3
- Retting av feil og tvetydigheter oppdaget under MSDP
- Flytting av sikkerhetsmerke fra meldingsprotokollen til S/MIME protokolen
- Ny ”loop” kontroll mekanisme for adresselister

For en fullstendig oversikt over endringene, se STANAG 4406 Ed.1 Implementors guide.

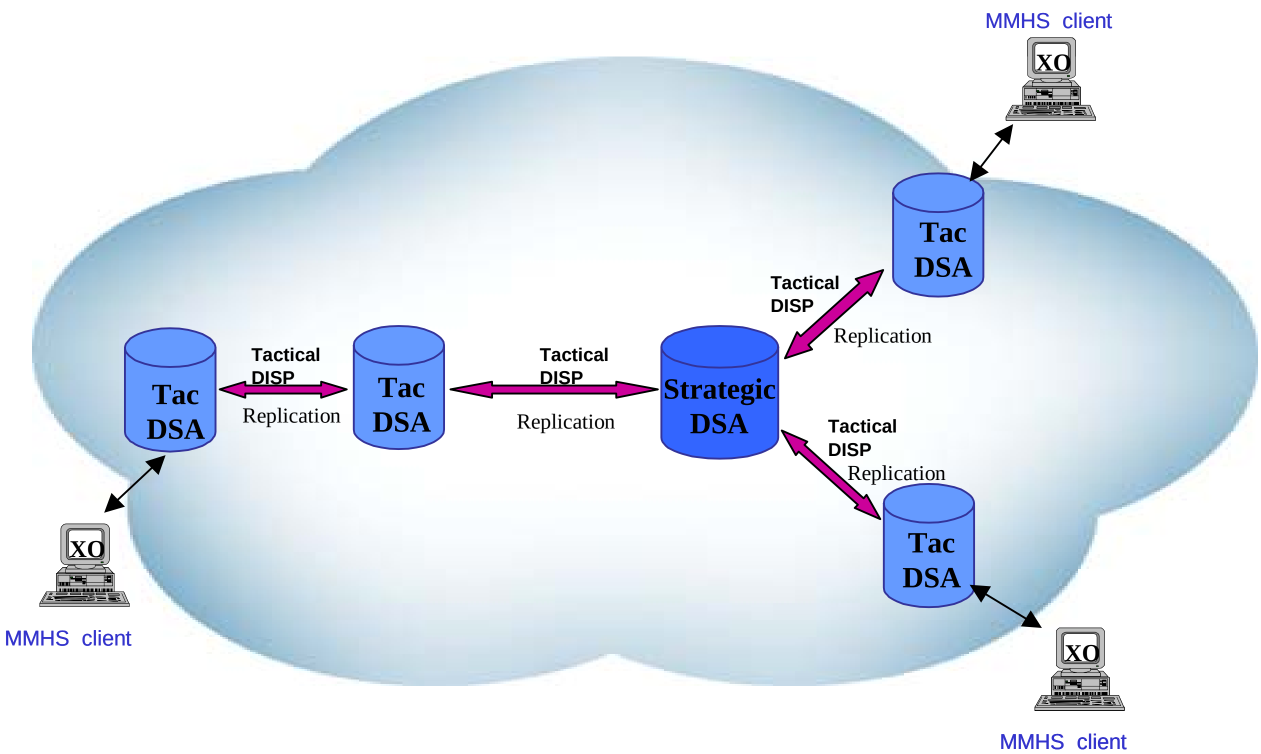
8 FORSLAG TIL PROTOKOLLØSNING FOR TAKTISK DIRECTORY I NATO

FFI/STAROS har spesifisert et forslag til en protokoll-løsning for taktisk Directory for NATO. Denne protokoll-løsningen er basert på løsningene som ble utarbeidet for STANAG 4406 Annex E (ref. (1)), som beskriver en taktisk protokoll-løsning for militær meldingstjeneste.

NATOs arbeidsgruppe NC3B(SC/5)WG on Directory Systems, har adoptert en Directory standard fra CCEB nasjonene som heter ACP 133 (ref. (3)). Denne standarden er basert på X.500 og LDAP standarden, men spesifiserer bl.a. et eget skjema som beskriver hva slags informasjon som kan lagres i katalogen og hvordan den skal organiseres. Den inneholder også en profil som angir hvilke deler av protokollene og skjema-informasjonen som må implementeres for å være konform med standarden.

ACP 133 er som STANAG 4406 skrevet for nett med høy data-rate, og protokollene er derfor veldig ressurskrevende for taktiske nett med lav data-rate. En katalogtjeneste (eller Directory) vil bli brukt sammen med militær meldingstjeneste for bl.a. å lagre informasjon om meldingsadresser, sertifikater og CRLer. Katalogtjenester vil også bli brukt som støttesystem for taktiske meldingssystemer (STANAG 4406 Annex E). FFI/STAROS har sett muligheten for å benytte den samme protokoll-løsningen for taktisk Directory. Det er behov for replikasjon av kataloginformasjon over de samme kanalene som man sender militære meldinger. En protokoll-profil tilsvarende STANAG 4406 Annex E for taktisk Directory er derfor nødvendig.

Det er bare spesifisert en taktiske Directory protokoll løsning for X.500 protokollen DISP (Directory Information Shadowing Protocol), som brukes for å replisere Directory informasjon mellom Directory servere (DSA- Directory System Agents). Grunnen til at det bare er fokusert på en av protokollene i X.500, er at vi antar at de andre X.500 protokollene som DAP (Directory Access Protocol) , DOP (Directory Operational Binding Management Protocol) og DSP (Directory System Protocol) ikke vil være like aktuelle å bruke over kanaler med lav datarate. Det antas at det meste av informasjonen i Directory vil være replisert ned til en lokal DSA knyttet til de taktiske enhetene i forkant av en eventuell operasjon og at det kun vil være oppdateringer som vil overføres over de taktiske lav-datarate forbindelsene v.h.a. taktisk DISP. Figur 5.5 viser hvordan den taktiske protokoll profilen for DISP kan brukes for replisering av informasjon mellom katalog servere.



Figur 5.5 Figuren viser hvordan den taktiske versjonen av DISP kan brukes for å replisere informasjon mellom strategiske og taktiske Directory systemer, samt direkte mellom taktiske Directory systemer.

For flere detaljer om den taktiske protokoll profilen for Directory, se ref.(22).

9 KONKLUSJON

Standardiseringsarbeid er viktig for å oppnå internasjonal enighet rundt de løsningene som velges. Dette vil føre til at flere leverandører implementere løsningene, og dermed flere produkter å velge mellom. Standarder er det eneste verktøyet man har for å oppnå at implementasjoner fra forkjellige leverandører blir interoperable. Vår erfaring er at det er svært viktig å arbeide med nasjonale og internasjonale løsninger i parallell. Det er da større sjanse for at våre nasjonale systemer blir interoperable med tilsvarende systemer hos våre allierte, noe som blir stadig mer aktuelt ettersom vi deltar mer aktivt i internasjonale fellesoperasjoner.

En annen erfaring er at det nettverket som etter hvert bygges opp, gir innpass i tilsvarende miljøer i andre nasjoner. Dette gir oss mulighet til å utveksle erfaringer og drøfte felles problemstillinger. I Norge har vi ofte svært små miljøer som arbeider med oppgaver som andre nasjoner bruker vesentlig mer ressurser på. Vi har derfor mye å hente på å samarbeide med, eller opprette kontakter med personer i disse miljøene. Å engasjere seg i internasjonalt standardieringsarbeid innen områder som er direkte relatert til våre nasjonale programmer og fremtidige systemer, er ut i fra vår erfaring utelukkende positivt. Det er derimot en forutsetning at man involverer seg i det arbeidet som gjøres i arbeidsgruppene og påtar seg verv og oppgaver. Man har en veldig stor innflytelse på resultatet av et dokument, når man har editor-ansvaret.

10 AKRONYMER OG DEFINISJONER

MMHS	Military Message Handling System
MTA	Message Transfer Agent
MS	Message Store
UA	User Agent
PKI	Public Key Infrastructure
Directory System	A distributed repository of information based on the ITU X.500 and IETF LDAP standard.
CRL	Certificate Revocation List
MMHS-Client	The MMHS User Interface application, which may be separate from the MMHS server
MMHS-Server	MMHS component containing the parts of the User Agent, Message Transfer Agent (MTA) and the Message Store (MS).
RA	Registration Authority
CA	Certificate Authority
HUB	A centralized unit which function is to make information available to other systems or to connect other systems together.
DSA	Directory Server Agent
DUA	Directory User Agent
DISP	Directory Information Shadowing Protocol
LDAP	Light Directory Access Protocol
Certificate	A certificate in PKI terms gives credibility to the binding of subject and a public Key
PCT	Protecting Content Type (PCT) is a security content type defined in STANAG 4406 Ed.1 Annex B.

P1	P1 is the X.400 protocol used between the MTAs, and describes the “Envelope” of the message.
P772	P772 is the NATO military message content type for formal messaging defined in STANAG 4406 Ed.1.
ACP 133	ACP 133 is the CCEB standard for Directory Systems adopted by NATO

11 REFERANSER

(1) [STANAG 4406 Ed.1] NATO STANAG 4406 Edition 1, “Military Message Handling Systems”

(2) [STANAG 4406 Ed.1 Annex E] AC/322(SC/5)N/224, Ratification Draft of STANAG 4406 (Ed. 1): Military Message Handling System, Annex E: Tactical MMHS Protocol and Profile Solution

(3) [ACP 133] ACP 133 – “Common Directory Services and Procedures”

(4) [ACP 127] ACP 127 - Allied Communication Publication (ACP) 127 (G), Communication Instructions Tape Relay Procedures

(5) [S/MIMEProfile] STANAG 4631 “Profile For The Use Of The Cryptographic Message Syntax (CMS) And Enhanced Security Services (ESS) For S/MIME”, AC/322(SC/4)N(2004)0016(INV)

(6) [CERT31] Ramsdell, B., Editor, "S/MIME Version 3 Certificate Handling", Internet-Draft draft-ietf-smime-rfc2632bis.

(7) [CMS] Housley, R., "Cryptographic Message Syntax", Internet-Draft draft-ietf-smime-rfc2630bis.

(8) [CMSALG] "Cryptographic Message Syntax (CMS) Algorithms", Internet-Draft draft-ietf-smime-cmsalg.

(9) [ESS] Hoffman, P., Editor "Enhanced Security Services for S/MIME", RFC 2634, June 1999.

(10) [MSG] Ramsdell, B., Editor "S/MIME Version 3 Message Specification", Internet-Draft draft-ietf-smime-rfc2633bis.

(11) [X400Wrap] Bonatti, C., Eggen, A., Hoffman, P., “Securing X.400 Content with S/MIME” RFC, November 2003.

(12) [X400Transport] Hoffman, P. and Bonatti, C., "Transporting S/MIME Objects in X.400", S/MIME” RFC, November 2003.

(13) [X.400] ITU-T X.400 Series of Recommendations, Information technology - Message Handling Systems (MHS). X.400: System and Service Overview; X.402: Overall Architecture; X.411: Message Transfer System: Abstract Service Definition and Procedures; X.420: Interpersonal Messaging System; 1996.

(14) Eggen A, Andreassen M, Hvinden Ø, Lægreid H, ” The Joint NO And UK Demonstration Of Integrated MMHS, PKI And Directory Systems At JWID 2002”, FFI/RAPPORT-2002/04655

(15) (1988): CCITT X.225 Session Protocol Specification for OSI for CCITT Applications.

(16) (1988): CCITT X.226 Presentation Protocol Specification for OSI for CCITT Applications.

(17) (1988): CCITT X.227 Association Control Protocol Specification for OSI for CCITT Applications.

(18) (1988): CCITT X.228 Reliable Transfer: Protocol Specification.

(19) ACP 142, P_Mul: A protocol for reliable multicast messaging in bandwidth constrained and delayed acknowledgement (EMCON) environments.

(20) ACP 145, Gateway-To-Gateway Implementation Guide For ACP 123 Messaging Service, CCEB

(21) Pink, J, MMHS Security Demonstrator Programme (MSDP), MSDP Report Version 02, March 06 2002

(22) Eggen, A, "A Protocol Solution for Replication of Information in a NATO Tactical Directory", FFI/RAPPORT-2003/01517.

(23) Jodalen V, Solberg B, Gronnerud O, Eggen A, Leere A B, **"**IP Over HF as a Bearer Service for NATO Formal Messages"**,** Ninth International Conference on HF Radio Systems and Techniques, IEE, pp 19-24, Bath, 2003.

(24) Leere A B, "Forsøk med taktisk meldingstjeneste, STANAG 4406 Annex E, over STANAG 5066 oktober til juni 2002", FFI/NOTAT-2004/00692.