FFI RAPPORT

OPERATIVE BESLUTNINGSSTØTTE-TJENESTER – FREMTID NBF

GAGNES Tommy, EGGEN Anders, HEDENSTAD Ole-Erik, RASMUSSEN Rolf, SLETTEN Geir

FFI/RAPPORT-2005/03584

OPERATIVE BESLUTNINGSSTØTTETJENESTER – FREMTID NBF

GAGNES Tommy, EGGEN Anders, HEDENSTAD Ole-Erik, RASMUSSEN Rolf, SLETTEN Geir

FFI/RAPPORT-2005/03584

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	2) SECURITY CLASSIFICATION	3) NUMBER OF PAGES
FFI/RAPPORT-2005/03584	UNCLASSIFIED	68
1a) PROJECT REFERENCE	**2a) DECLASSIFICATION/DOWNGRADING SCHEDULE**	
FFI-II/898/912	-	

4) TITLE

OPERATIVE BESLUTNINGSSTØTTETJENESTER – FREMTID NBF

INFORMATION AND INTEGRATION SERVICES FOR COMMAND AND CONTROL - FUTURE NETWORK BASED DEFENCE

5) NAMES OF AUTHOR(S) IN FULL (surname first)

GAGNES Tommy, EGGEN Anders, HEDENSTAD Ole-Erik, RASMUSSEN Rolf, SLETTEN Geir

6) DISTRIBUTION STATEMENT

Approved for public release. Distribution unlimited. (Offentlig tilgjengelig)

7) INDEXING TERMS

IN ENGLISH:	IN NORWEGIAN:
a) Service Oriented Architecture	a) Tjenesteorientert arkitektur
b) Network Based Defence	b) Nettverksbasert Forsvar
c) Ontology	c) Ontologi
d) Community of Interest	d) Interessefellesskap
e) Security	e) Sikkerhet

THESAURUS REFERENCE:

8) ABSTRACT

This report describes a conceptual solution for information and integration services for Command and Control in a short-term view (2008). We have used a long-term vision for 2014 as a basis, and from this derived a recommended solution for 2008. This will make the short-term solution a foundation for further expansion.

In 2008, the goal is to reach a flexible suite of services supporting bi-directional information sharing. Key elements are Service-Oriented Architecture based on open standards, a set of core services, and a Community of Interest (COI) for Command and Control. In the long-term vision additional elements are introduced. There will be more Community of Interests with respective ontologies and services. Also dynamic composition of the system and flexible security based on information object protection, are introduced.

9) DATE	AUTHORIZED BY	POSITION
	This page only	
2005-11-08	Vidar S Andersen	Director

ISBN 82-464-0981-6

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (when data entered)

SAMMENDRAG

Denne rapporten er utarbeidet i forbindelse med en arbeidspakke knyttet til ’P9268 – Variantbegrensning av Operative Beslutningsstøttetjenester’. Arbeidet er utført av FFI, etter oppdrag fra FK KKIS. Oppdraget har bestått i å utarbeide en beskrivelse av en konseptuell løsning for 2008. Det skal beskrives hvorfor løsningen er valgt og usikkerhet ved denne, egenskaper ved løsningen, samt eventuelle komponenter, grensesnitt og samhandling.

Vi har tatt utgangspunkt i og beskrevet en fremtidsvisjon for 2014, hvorav vi har avledet en løsning for 2008 som et skritt på veien. På denne måten blir løsningen en investering i en grunnmur å bygge videre på i fremtiden. For 2008 er målet å oppnå en fleksibel portefølje av funksjonalitet som støtter toveis informasjonsdeling. Følgende elementer bør inngå i et 2008-målbilde:

- En tjenesteorientert arkitektur basert på åpne standarder (Web Services og XML)
- Et sett av kjernetjenester
- En opprettelse av interessegruppen K2[1]
- Utvikling av en datamodell for interessegruppen K2
- Spesifikke tjenester for interessegruppen K2

For 2014 er målet at man skal ha en fleksibel, modulær portefølje av funksjonalitet som støtter (semi-)automatisk oppkobling av toveis informasjonsdeling med nye samarbeidspartnere. Følgende elementer bør utgjøre et målbilde for tjenesteinfrastrukturen i 2014 (en utvidelse av elementene listet over):

- En tjenesteorientert arkitektur basert på åpne standarder (Web Services og XML)
- Et sett av kjernetjenester
- En inndeling av brukere i interessegrupper med en ontologi (formell datamodell) for hver interessegruppe
- Spesifikke tjenester for hver interessegruppe
- Systemet kan komponeres etter behov, basert på prosessflyt
- Fleksibel sikkerhet på informasjonsnivå

I et 2014-perspektiv ser vi for oss tjenesteinfrastruktur-delen av INI realisert som en sikker og dynamisk tjenesteorientert arkitektur, med to hovedkategorier tjenester; kjernetjenester og tjenester som er mer spesifikke for en interessegruppe. Videre er den tjenesteorienterte arkitekturen basert på ontologier (formelle datamodeller) for å sikre at tjenester er interoperable.

[1] Vi mener her alle som er interessert i K2-relatert informasjon, og dermed også situasjonsinformasjon.

INNHOLD

OPERATIVE BESLUTNINGSSTØTTETJENESTER – FREMTID NBF

1 INNLEDNING

1.1 Bakgrunn

I forbindelse med P9268 – Variantbegrensning av Operative Beslutningsstøttetjenester har det blitt utarbeidet i alt 6 forskjellige arbeidspakker for fremskaffelsesløsning. FFI fikk i oppdrag av FK KKIS å utarbeide arbeidspakke 2 – Fremtid NBF. Oppdraget ble tildelt i juni, med leveranse 10. september 2005. Versjon 1.0 av rapporten ble levert i henhold til utsatt frist som var 23. september 2005.

Denne rapporten er i hovedsak lik rapporten som ble levert i P9268, men det er i etterkant tatt hensyn til noen tilbakemeldinger fra FLO/IKT.

1.2 Oppdrag

Oppdraget som ble tildelt FFI hadde følgende formulering:

”FFI skal utarbeide en beskrivelse av konseptuell løsning for 2008, gjerne som en UML-modell ved hjelp av Enterprise Architect. Det skal beskrives hvorfor løsningen er valgt og usikkerhet ved denne, egenskaper ved løsningen, samt eventuelle komponenter, grensesnitt og samhandling.”

1.3 Hensiktsformulering

Hensikten med oppdraget er å:

- Identifisere de viktigste faktorene i forhold til valg av fremskaffelsesløsning basert på strategier og trender innen sivil/militær IKT (eksempelvis SOA, standarder) og virksomheten forøvrig (eksempelvis NBF, omstilling, ressurstilgang)
- Bidra til at ny løsning tatt frem i P9268 er ett skritt i retning av NBF, og i det minste ikke vanskeliggjøre en senere tilnærming til NBF (i forhold til ressurser, teknologivalg, …)
- Skille klart mellom tanker om fremtiden (eks. 2014) kontra hva vi mer konkret kan ta hensyn til i forbindelse med P9268 som går i perioden 2006-2008.

1.4 Avgrensning

Ved gjennomføringen av oppdraget har vi lagt følgende tolkning og avgrensning til grunn:

- Ser kun på beslutningsstøtte for operativt domene (ikke operativt støttedomene)
- Fokus på konseptuell løsning som er realistisk i forhold til 2008
- Samtidig vil vi ta utgangspunkt i og beskrive en fremtidsvisjon for 2014

- Konseptuell løsning gjelder informasjonsinfrastrukturen (funksjonsvise beslutningsstøttetjenester og kjernetjenester)
- Ingen beskrivelser på virksomhetsnivå (virksomhetsarkitektur)
- Kostnadsvurderinger er utenfor vårt oppdrag (men bør gjøres av andre)

Dette dokumentet fokuserer på å beskrive langsiktig løsning (2014-perspektivet) i større grad enn det som ble angitt i opprinnelig oppdragsformulering. Dette gjøres for å sikre at den anbefalte løsningen for 2008 er forenlig med de tiltakene som vil være nødvendige på lenger sikt. Det legges også til grunn at Forsvarets fremtidige funksjonalitetsbehov ikke er kjent i tilstrekkelig grad til å gi grunnlag for vurdering her. Dette arbeidet fokuserer derfor på å beskrive de mer tekniske og systemmessige sidene av fremtidige løsninger.

1.5 Begrepsavklaring

COI – Community of Interest
En samling av mennesker som er interessert i informasjonsutveksling innen ett emneområde og som derfor må benytte samme terminologi for å dele informasjon.

Datamodell
Konseptuell modell av et domene (ofte mindre uttrykkskraft enn en ontologi).

Interessegruppe/Interessefellesskap
Se COI – Community of Interest.

Metadata
Metadata er data som beskriver andre data. Metadata kan innta mange former og ha mange funksjoner.

NGO – Non-governmental Organization
En organisasjon som ikke er en del av de offentlige myndigheter.

Ontologi
Formell, eksplisitt semantisk og konseptuell modell av et domene.

Syntaks
En representasjon av data.

Semantikk
Meningen (konteksten) til data.

SOA – Service-Oriented Architecture
Et sett av tjenester som kan benyttes, og som har tjenestebeskrivelser som kan publiseres og finnes.

Taksonomi
Prinsipper for klassifisering eller selve klassifiseringen.

Tjeneste
Her mener vi med tjeneste en selvstendig programvarekomponent med et klart definert grensesnitt, tilgjengelig over et nettverk. En tjeneste utføres av en tilbyder, og benyttes av en konsument.

Tjenesteorientert arkitektur
Se SOA – Service-Oriented Architecture.

Web Service
Her mener vi med Web Service en tjeneste realisert vha. WSDL (Web Services Description Language) for grensesnittbeskrivelse og SOAP for meldingsutveksling.

XML – eXtensible Markup Language
Et metaspråk, et sett med regler for å lage et språk. XML er plattformuavhengig (maskinvare, operativsystem, programmeringsspråk etc.). Har fått stor utbredelse i forbindelse med representasjon av informasjon for overføring.

Åpen standard
En ikke-proprietær og teknologinøytral standard, og fritt tilgjengelig for distribusjon. En åpen standard blir oftest utviklet i en åpen, inkluderende prosess der enhver organisasjon, bedrift eller offentlig enhet kan delta.

1.6 Forutsetninger

Nedenfor tar vi for oss føringer vi har basert oss på i arbeidet med et målbilde for en fremtidig operativ løsning. Uthevinger er gjort av oss, og illustrerer det vi kaller generelle behov.

1.6.1 St.prp. nr. 42 om informasjonsinfrastruktur

St.prp. nr. 42 (1) sier følgende om INI:

Ambisjonen er at det i 2008 er lagt et godt grunnlag for en felles infrastruktur for kommunikasjon og informasjonsutveksling i Forsvarets operative organisasjon, for å tilpasse kommandostrukturen til kravet om økt deployeringsevne, ***mobilitet og fleksibilitet****. Satsningen vil kunne medføre at investerings- og driftskostnadene for dette området kan øke. Informasjonsinfrastrukturen skal i størst mulig grad baseres på eksisterende* ***sivilt utviklet teknologi****, oppgradert og tilpasset Forsvarets behov.*

Administrative og forvaltningsmessige beslutningsstøttesystemer *vil i den grad det er hensiktsmessig bli utformet og* ***gjort anvendbare*** *for den operative organisasjonen og kommandostrukturen.*

Deler av Forsvarets informasjonsinfrastruktur, etablert for å ivareta Forsvarets primæroppgaver, bør ***kunne brukes av utvalgte instanser og brukersteder i en totalforsvarssammenheng****, for å forsterke samfunnssikkerhetsarbeidet.*

Og:

*Gjennom **deling og utveksling av informasjon på tvers i nettverket**, får våre styrker et mer fullstendig og oppdatert beslutningsgrunnlag. Forsvarets enheter får dermed økt mulighet til å handle raskere, mer effektivt og presist, i forhold til det situasjonen krever.*

Med andre ord trengs en løsning som understøtter hurtig tilgjengelige og anvendbare styrker som er alliansetilpasset, til tross for uforutsigbarhet.

1.6.2 Våre allierte

NATO Open Systems Working Group (NOSWG) skriver følgende:

***Service-based** and net-centric enabled architectures are beginning to replace the current system-of-systems architectural paradigms currently in use.*

Videre:

*Realizing NNEC can only be achieved by evolving the NC3TA to support a **system-of-services architecture paradigm**, through a transition from component-based architectures to web services and other web-enabled technologies, the NOSWG must begin to consider **evolutionary architectures** as they continue to emerge. Such a transition is essential if the level of information-sharing capabilities between coalition partners is to move from the simple sharing of data to include workflow and process/activity information consolidation.*

*Identifying and adopting **open standards** that provide the ability to represent standard **syntactic and semantic declarations** through the use of **controlled vocabularies** will be a considerable though necessary task. Issues such as syntactic conflict, semantic conflict, semantic accuracy, and data consolidation will need to be addressed, as will ontologies, though these are probably further in the future.*

Mer om hva som skjer i NATO kan bl.a. leses i (2). En foreløpig versjon av NATO NEC Feasibility Study er også tilgjengelig (25).

Amerikanerne har en rekke teknologiske initiativer. Uten å gå nærmere inn på detaljene kan vi nevne aktuelle termer som Global Information Grid (GIG) og Net-centric Core Enterprise Services (NCES). Web Services og XML står sentralt, sammen med satsning på tjenesteorienterte arkitekturer. Et eksempel på anvendelse av denne typen teknologier er ForceNet (29) hos US Navy.

1.6.3 Multilateral Interoperability Programme

Multilateral Interoperability Programme (MIP) er et samarbeid mellom 24 nasjoner (både innenfor og utenfor NATO) samt to NATO-kommandoer. MIP er ikke formelt styrt av NATO, men har tette koblinger til NATO.

Målet for MIP er å oppnå internasjonal interoperabilitet for KKI-systemer på alle nivåer fra korps og nedover, for å støtte flernasjonale og felles operasjoner.

Hovedproduktet fra MIP er en datamodell for informasjonsutveksling (26). Utviklingen foregår i samarbeid med NATO Data Administration Group (NDAG), og er NATOs felles datamodell for informasjonsutveksling. Datamodellen er sendt ut for ratifikasjon som STANAG 5525.

MIP leverer også to utvekslingsmekanismer; Message Exchange Mechanism (MEM) og Data Exchange Mechanism (DEM). MEM utveksler et sett med egendefinerte meldinger i henhold til samme syntaks som ADatP-3 (27), mens DEM benytter databasereplikasjon.

Noen stikkord om forholdet mellom MIP og NATO:

- Implementering av MIP er et NATO Force Goal (FG2802)
- NATO Standardisation Agreement SO 01-11 oppfordrer til implementering av MIP (ATCCIS)
- NATO har utgitt NATO Policy on MIP, som beskriver hvordan spesifikasjonene fra MIP skal tas inn i NATO
- Datamodellen fra MIP er spesifisert som en del av NATO C3 Technical Architecture
- Bi-SC Automated Information System vil bruke MIP-løsningen i landdelen for å utveksle informasjon med nasjonale K2IS

1.6.4 Variantbegrensning våren 2005

Fra (3) har vi hentet følgende sitat:

”Mange av de produkter som i dag eksisterer i de forskjellige beslutningsstøttesystemene er av en slik art, at man må ta alt eller ingenting. Det mangler beskrivelser av avhengigheter mellom komponentene i produktene. Videre er ***det manglende beskrivelse av tilgjengelige grensesnitt*** *og hvordan komponentene kan anvendes i andre konfigurasjoner. Før tjenestene kan tilbys som* ***selvstendige, fleksible og tilpasningsdyktige moduler*** *må den sterke binding som pr i dag eksisterer mellom modulene/komponentene reduseres/fjernes. I tillegg må det beskrives hvordan de kan gjenbrukes i nye konfigurasjoner.”*

Dokumentet identifiserer også en inndeling i flere grupper av funksjonalitet. Dette omtales nærmere i kapittel **5.1.3**. Videre sier dokumentet:

”Eksempler på konsept for den langsiktige arkitekturen kan være en tjenesteorientert arkitektur med mange tjenesteleverandører og løs kobling mellom de forskjellige tjenestene, eller man kan gå for et konsept med hvor alle tjenestene realiseres av ett system/applikasjon med sterk kobling mellom tjenestene. En hybrid mellom disse vil mest trolig være det riktige.

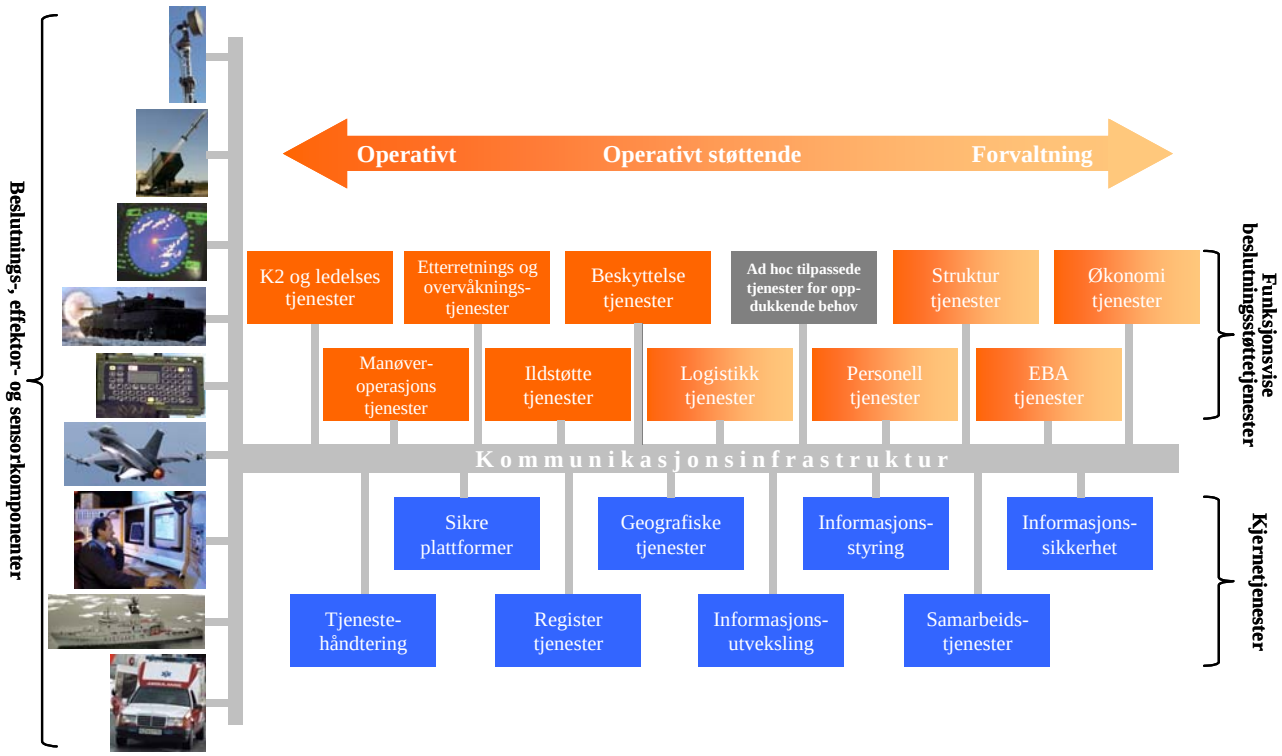
Her vil evne til understøttelse av et nettverksbasert forsvar, bruk av standarder, evne til gjenbruk, grad av fleksibilitet, interoperabilitet, driftskonsept etc måtte vurderes.”

1.6.5 Strategiske initiativer, NBF

I (4) beskrives resultatene av et arbeid for å vise veg i retning av et nettverksbasert forsvar. Her beskrives tre grader av NBF: Innledende, integrerende og gjennomgripende. Vi legger til grunn at løsningene vi skal beskrive må ha velutviklet støtte for innledende NBF, men at det også legges til rette for å utnytte mulighetene som ligger i integrerende og gjennomgripende.

Det presiseres i (4) at NBF ikke først og fremst handler om teknologi, men at teknologien utgjør et fundament i nettverksorganiseringen. En mulig oppsummering er at organisasjonen må utnytte de mulighetene som teknologien gir.

1.6.6 Referansemodell for informasjonsinfrastrukturen

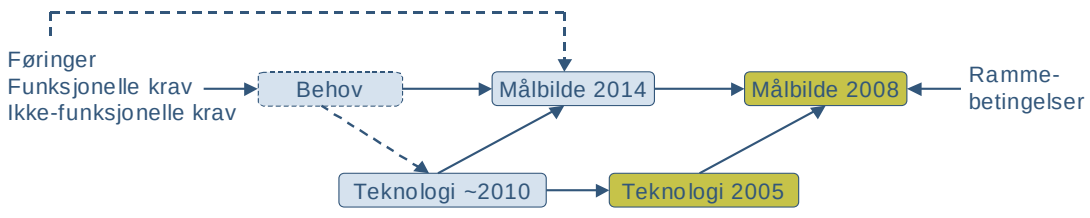


Figur 1.1 Referansemodell for informasjonsinfrastrukturen.

Forsvarets referansemodell for informasjonsinfrastrukturen (24) er delt inn i en kommunikasjonsinfrastruktur, kjernetjenester og funksjonsvise beslutningsstøttetjenester. For å oppnå interoperabilitet mellom tjenester som har behov for å utveksle informasjon, er det viktig å benytte standardiserte formater.

1.7 Gjennomføring

Figur 1.2 skisserer en prosess for å komme frem til en målbildebeskrivelse. Viktige føringer omtales i det følgende. Funksjonelle krav vil ikke bli konkretisert, men vi forutsetter generelle krav om fleksibilitet, dynamikk og interoperabilitet. Rammebetingelser for det nære perspektivet (2008) er forhold som tilgjengelige kommunikasjonsløsninger, økonomi og kompetanse.



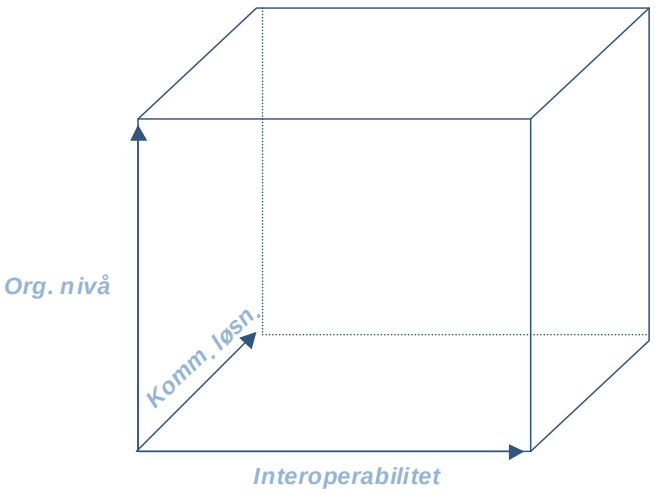
Figur 1.2 Prosessen frem mot et målbilde for 2008

Oppdraget dreier seg i hovedsak om å ta frem et målbilde for 2008, sammen med en gjennomgang av teknologi som kan understøtte målbildet. Dette er markert med grønt i figuren. For å komme frem til målbildet for 2008, har vi også tatt frem en del generelle behov og et målbilde i et lengre perspektiv. Disse er markert med blått i figuren.

Denne rapporten er bygget opp i en sekvens som stort sett gjenspeiler prosessen vist i figuren. Vi tar først for oss føringer og generelle behov før vi skisserer et målbilde for Forsvaret i 2014-perspektiv. Deretter ser vi på teknologi som kan understøtte både 2008- og 2014-målbildet, før vi drøfter hva som er mulig i et 2008-perspektiv. Vi presenterer deretter et generelt målbilde for 2008.

1.7.1 Vurderingsdimensjoner

Vi presenterer her fremgangsmåten vi har benyttet for å vurdere utfordringer og dimensjoner som en ny løsning bør kunne støtte. Det er viktig å merke seg at flere av disse dimensjonene kan opptre i forskjellige kombinasjoner. For eksempel kan man snakke om interoperabilitet på lavt nivå mellom nasjoner eller internt i Forsvaret. Vi mener, basert på de tre dimensjonene, at en ny løsning bør støtte stadig endrede krav, da det er vanskelig å si noe om hvilke oppdrag, samarbeidspartnere etc. man kommer til å måtte støtte i fremtiden. Figur 1.3 er en forenklet figur som viser tre hoveddimensjoner man må veie opp mot hverandre. Disse kan byttes ut med respektive underdimensjoner. Vi brekker opp hoveddimensjonene i sine underdimensjoner nedenfor.



Figur 1.3 Tre dimensjoner en ny løsning kan støtte

Den første dimensjonen i Figur 1.3 er interoperabilitet, og er illustrert langs x-aksen på figuren. Vi kan oppnå interoperabilitet med en rekke samarbeidspartnere, for eksempel følgende:

- utenlandske samarbeidspartnere
    - NATO, Partnership for Peace, EU
- internt i Forsvaret
    - K2, ISTAR[2], E-tjenesten, sjø, luft, land
- norske offentlige etater
    - FD, UD, PST[3]
- frivillige organisasjoner, NGOs[4]
    - Røde Kors etc.

Den neste hoveddimensjonen i Figur 1.3 er organisasjonsnivå. Denne strekker seg fra strategisk nivå ned til enkeltmannsnivå. I henhold til dagens terminologi får vi altså:

- Strategisk
- Operasjonelt
- Taktisk
- Stridsteknisk
- Enkeltmann

I henhold til NBF-tankegang kunne vi kanskje ha nøyd oss med inndelingene høyt og lavt, men poenget blir det samme. I tillegg bør en ny løsning støtte endringer i virksomheten, for eksempel dersom en velger å utføre oppgaver på andre nivåer, fjerne nivåer etc.

Den siste dimensjonen i kuben er kommunikasjonsløsningene en ny løsning kan baseres på. Som for interoperabilitet kan vi splitte opp kommunikasjonsløsninger i flere underdimensjoner.

- Båndbredde (overføringskapasitet)
    - Lav, middels, høy
    - Intra-nodal vs. inter-nodal
- Rekkevidde
    - Kort, middels, lang
    - Intra-nodal vs. inter-nodal
- Mobilitet
    - Trådløst, deployerbare, eller faste linjer
- Konnektivitet
    - Dynamisk eller planlagt
    - På tvers av interessegruppe eller ikke
- Kapasitet
    - Prosessering
    - Batteri
    - Minne
- Sikkerhet
    - På tvers av sikkerhetsnivåer eller ikke

[2] Intelligence, Surveillance, Target Acquisition and Reconnaissance
[3] Politiets sikkerhetstjeneste
[4] Non-Governmental Organization, En organisasjon som ikke er en del av de offentlige myndigheter.

I teorien kan vi for hvert punkt (x, y, z) innenfor kuben
, prioritere hva som er viktig. Den ideelle løsning støtter interoperabilitet med alle, på alle nivåer i organisasjonen, og over alle kommunikasjonsløsninger. En løsning bør derfor støtte:

- Et mangfold av interoperabilitet, mot forskjellige samarbeidspartnere, på flere organisasjonsnivåer (basert på åpne standarder)
- komponering av system basert på virksomhetens behov til enhver tid, fleksibilitet
- effektiv koding (for lav båndbredde og effektiv prosessering)
- automatisk oppkobling og interoperabilitet, nå og i fremtiden (når utstyret er tilpasset dette)

En mer realistisk tilnærming vil være gradvis å gå i de forskjellige retningene. Et eksempel på dette kan være interoperabilitet mellom hær og sjø på strategisk nivå over høy båndbredde, som vil kunne gi et felles land- og sjøbilde på FOHK. Et annet eksempel kan være interoperabilitet mellom luft og hær på stridsteknisk nivå over lav båndbredde, som vil kunne la en HV-soldat sende en anmodning om ildstøtte direkte til en F-16.

2 MÅLBILDE 2014

2.1 Utfordringer/fremtidige behov

Som nevnt i kapittel 1.6.1 er det behov for en løsning som understøtter alliansetilpassede styrker. Støtte skal gis i forhold til det situasjonen krever, noe som er forholdsvis uforutsigbart. En fremtidig K2IS-løsning må speile organisasjonens behov og ønske om organisk tilpasningsdyktige strukturer. Nye kapasiteter (sensorer) må kunne plugges inn, og interoperabilitet med logistikk- og støttevirksomhet vil også bli stadig viktigere.

Dermed står vi overfor en transformasjon av dagens løsninger, slik at informasjon (både strukturert og ustrukturert) kan deles mellom langt flere enheter enn i dag, og også på tvers i organisasjonen. En viktig faktor vil være å få alle kommunikasjonsnettverk til å spille sammen (interoperabilitet på datanivå), men dette er ikke alltid nok. For best mulig tilgang til informasjon, må vi også ha interoperabilitet på informasjonsnivå.

2.2 Krav til konseptuell løsning

Som nevnt over, bør en konseptuell løsning for K2IS i 2014 være fleksibel, slik at den er godt rustet for å imøtekomme nye behov som ikke fantes da systemutviklingen begynte. Løsningen vil måtte støtte et mangfold av ulike utvekslingsformater, protokoller, nettverksteknologier og ytelsesbegrensninger, både i nettverket og på maskiner. Interoperabilitet med andre organisasjoner, også sivile og frivillige, blir et viktig behov som en ny løsning må støtte. Det vil da være viktig å kunne filtrere informasjon som ikke skal deles med andre, avhengig av hvordan dette til enhver tid er definert.

I tillegg er det viktig å kunne tilpasse systemets funksjonalitet til gjeldende oppdrag og styrkesammensetning, noe som kan endres relativt raskt, i hvert fall i forhold til tiden det kan ta å rekonfigurere et system. En løsning bør kunne støtte håndholdte terminaler så vel som server-baserte kommandoplasser som har et eget lokalnett. I tillegg vil gjenbruk av programvarekomponenter være viktig, dette for å spare kostnader på lang sikt, ved for eksempel å gjenbruke rammeverk for kartbaserte applikasjoner.

Bruk av åpne standarder blir stadig viktigere for å sikre interoperabilitet med et mangfold av samarbeidspartnere. Det finnes mange definisjoner av en åpen standard, se blant annet (5). Vi gir her et sammendrag av elementer som inngår i flere definisjoner:

En åpen standard blir utviklet i en åpen, inkluderende prosess der enhver organisasjon, bedrift eller offentlig enhet kan delta. En slik standard er ikke-proprietær og teknologinøytral, og er fritt tilgjengelig for distribusjon.

2.3 Tjenesteorientert arkitektur i Forsvarets operative løsning

Forsvaret trenger en virksomhetsarkitektur som ivaretar slike behov som er beskrevet over. I tillegg bør systemet støtte endring i virksomhetsprosesser på en enkel måte. Et arkitekturparadigme som er ment å skulle forenkle slike utfordringer er tjenesteorientert arkitektur (dette paradigmet er beskrevet i kapittel 3). Basert på behovene vi ser Forsvaret vil få i fremtiden, samt retningen på teknologi og forskning, mener vi at Forsvarets operative løsning bør gå i retning av en tjenesteorientert arkitektur basert på åpne standarder. En tjenesteorientert arkitektur gjør oss best mulig rustet for stadig endring i samarbeidspartnere og operasjoner, og dermed krav til systemet. Fleksibel informasjonsdeling er sentralt, og blir i større grad mulig ved bruk av åpne standarder.

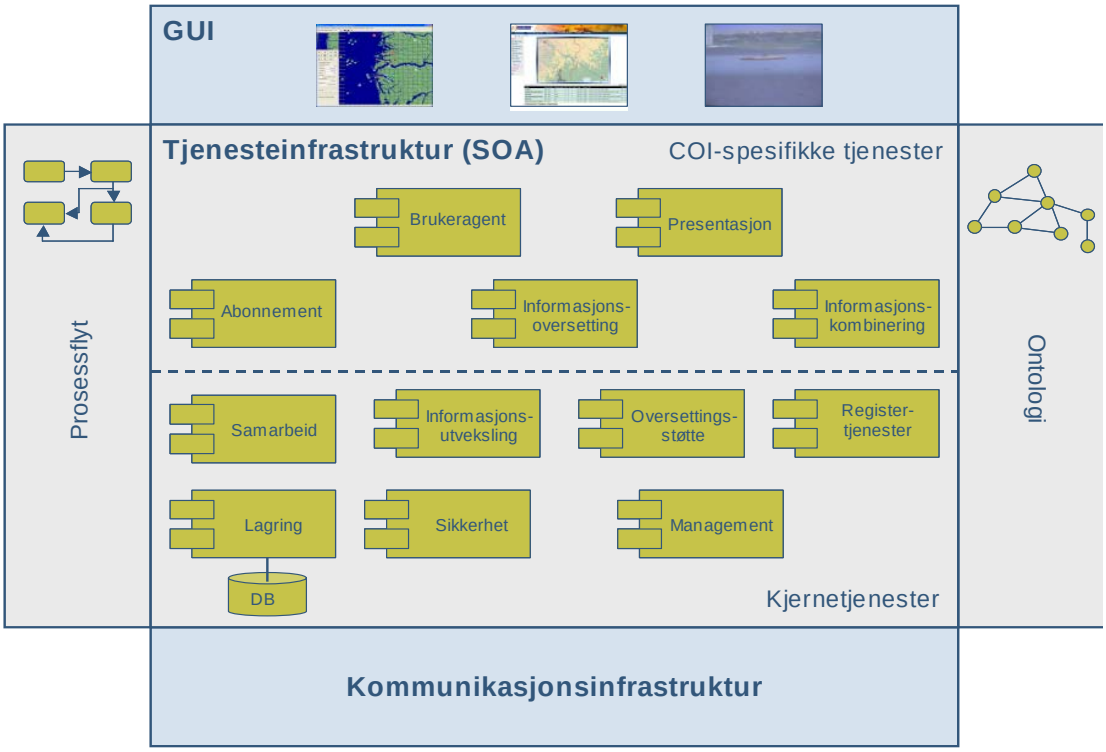
I en tjenesteorientert arkitektur er systemutviklingen konsentrert rundt tjenester; programvarekomponenter som tilbyr et klart definert grensesnitt og er tilgjengelig via et nettverk. Dermed kan tjenester brukes som byggeklosser når et system skal settes sammen. Tjenester blir utviklet etter behov, noe som muliggjør en evolusjonær utvikling. Basert på retningen vi ser at både teknologi og forskning går i, både i akademia og industri, mener vi at følgende elementer bør utgjøre et målbilde for tjenesteinfrastrukturen i 2014:

- En tjenesteorientert arkitektur basert på åpne standarder
- Et sett av kjernetjenester
- En inndeling av brukere i interessegrupper med en ontologi (formell datamodell) for hver interessegruppe
- Spesifikke tjenester for hver interessegruppe
- Systemet kan komponeres etter behov, basert på prosessflyt
- Fleksibel sikkerhet på informasjonsnivå

Figur 2.1 viser hvordan tjenesteinfrastrukturen ser ut i målbildet for 2014. Tjenesteinfrastrukturen ligger over kommunikasjonsinfrastrukturen, noe som gir en rekke

føringer for blant annet konnektivitet, båndbredde og sikkerhet. Vi ser at den tjenesteorienterte arkitekturen kan støtte flere applikasjoner (GUI), realisert ved å kombinere tjenester. Dette kan for eksempel være K2, ISTAR, blue force tracking eller operative støttefunksjoner. Ved å gjenbruke og komponere om tjenester kan nye applikasjoner eller ny funksjonalitet realiseres raskere.

I et 2014-perspektiv ser vi for oss tjenesteinfrastruktur-delen av INI realisert som en tjenesteorientert arkitektur. Det er delt inn i to hovedkategorier tjenester; kjernetjenester og tjenester som er mer spesifikke for en interessegruppe (vist som COI-spesifikke tjenester i figuren). Videre er den tjenesteorienterte arkitekturen basert på ontologier (formelle datamodeller) for å sikre at tjenester er interoperable. Til slutt er det også tegnet inn prosessflyt, da dette vil bli et viktig bindeledd mellom organisasjonens behov og hvordan tjenestene settes sammen til enhver tid. Vi går nærmere inn på disse elementene nedenfor.



Figur 2.1 Tjenesteinfrastruktur 2014

2.4 Kjernetjenester

I INI-modellen (se Figur 1.1) opererer man med begrepet kjernetjenester, et begrep som også kan brukes innenfor vår definisjon av tjenester. De fleste av disse vil være tilgjengelige for alle interessegrupper. Målet her er ikke å være uttømmende, og en fullstendig målarkitektur er utenfor rammen av denne leveransen. Derimot vil vi forsøke å illustrere hvordan tjenesteinfrastrukturen for automatiserte tjenester i en fremtidig INI bør se ut. Disse tjenestene må med andre ord kunne være en del av en tjenesteorientert arkitektur. Det vil også være behov for en infrastruktur som kan tilrettelegge for en tjenesteorientert arkitektur. Dette kan være for å

orkestrere (sette sammen) tjenester, koordinere meldingsflyt, sørge for garantert levering, håndtere et publish-subscribe kommunikasjonsmønster, samt administrasjon av systemet. Slike tjenester kan bli viktige, særlig ved stor informasjonsflyt. Eksempler på kjernetjenester kan være:

2.4.1 Samarbeid

I et NBF-perspektiv vil det være behov for tjenester som støtter samarbeid. Dette kan være for eksempel chat, diskusjonsforum eller lignende. I denne sammenhengen tenker vi kun på samarbeidstjenester som inngår i en tjenesteorientert arkitektur. For eksempel kan chat knyttet til situasjonsbildet bli en tjeneste som vil inngå i en situasjonsbildeapplikasjon.

2.4.2 Registertjenester

Vi deler her registertjenester inn i tre underkategorier: Tjenesteoppslag, Informasjonsoppslag og katalogtjenester.

Tjenesteoppslag
For å håndtere en stor mengde tjenester, potensielt med dynamikk i tilgjengeligheten, er det viktig å kunne gjøre oppslag i et tjenesteregister. Et slikt oppslag vil være basert på metadata om tjenester. Et slikt register kan ha flere former, og kan sammenlignes med gule sider eller en ”matchmaker”-tjeneste. Det vil være nødvendig å basere dette på en taksonomi for kategorisering av tjenester.

Informasjonsoppslag
Akkurat som for tjenester vil søk etter (ofte ustrukturerte) filer og dokumenter være viktig. For å få til dette, trengs metadata som beskriver innholdet i filene og dokumentene. Dermed trenger vi også en datamodell for metadata. Slike metadata bør eksistere ved siden av filene og dokumentene og kan inneholde informasjon om geografisk område, et sammendrag, informasjon om tid og sikkerhetsklassifisering, samt lokasjonen til filene og dokumentene. Et eksperiment for å teste ut disse prinsippene er beskrevet i (28).

Katalogtjenester
Felles katalogtjenester vil være en sentral del av tjenesteinfrastrukturdelen. Eksempler på dette kan være tilgangskontroll, epostlister, telefonlister etc.

2.4.3 Lagring

Lagring av informasjon er i mange tilfeller svært viktig. Visse typer informasjon kan være svært viktig å ta vare på, slik som situasjonsinformasjon. Lagring kan både være spesifikt for en applikasjon og generelt, og muliggjør bruk av informasjon fra forskjellige tidspunkter. Om lagring skal være en del av andre tjenester eller en egen tjeneste, er avhengig av i hvilken grad en ser for seg hele tjenesteinfrastrukturen som *ett* tjenesteorientert system. Logging er et annet aspekt, da det i et NBF kan være interessant å vite hvem som har fått vite hva. Dette har særlig relevans for informasjonsdeling med andre nasjoner og organisasjoner.

2.4.4 Sikkerhetstjenester

Ende-til-ende sikkerhetstjenester vil bli nødvendig for å oppnå større tilgjengelighet og fleksibilitet ved utveksling av informasjon enn situasjonen er i dagens systemer. Karakteristisk for dagens situasjon er atskilte sikkerhetsdomener som beskytter informasjon med forkjellig sensitivitet ved fysisk, kryptografisk og administrativ isolasjon. Eksempler på sikkerhetstjenester er bl.a. sikkerhetsmerking, kontroll av brukerprivilegier, aksesskontroll, autentisering, digital signering, signaturvalidering, kryptering, m.m.

2.4.5 Oversettingsstøtte

Når interoperabilitet med flere organisasjoner enn i dag blir viktigere vil det bli behov for oversetting av dataformater og megling mellom tjenester som i utgangspunktet er inkompatible. Transformasjon, mapping og inferens er blant tjenestene som vil inngå her. Mekanismene kan være generiske, slik at vi har valgt å plassere oversettingsstøtte blant kjernetjenestene.

2.4.6 Management

Tjenester for management vil bli viktige, og plasseres som kjernetjenester. Eksempler kan være konfigurasjon av tjenester fra sentralt hold, omdisponering av maskinressurser etc.

2.4.7 Informasjonsutveksling

Videre så finnes det en mengde eksisterende systemer og formater. Disse kan pakkes inn som tjenester, og brukes for å utveksle informasjon på den gamle måten, med gamle systemer, fra den nye tjenesteorienterte løsningen. Vi har valgt å kalle slike tjenester for utvekslingstjenester. Disse vil ofte være avhengige av tjenester for oversetting. Mekanismer for garantert levering etc. kan inngå her.

2.5 Sikkerhet

Hensikten med den tjenesteorienterte arkitekturen er å øke muligheten for å tilgjengeliggjøre og dele informasjon. Dette fører også til økt sårbarhet ved at mer data vil være tilgjengelig for en som klarer å bryte seg inn i systemet. Gode sikkerhetstjenester som ivaretar sikkerheten helt ut i endesystemene vil derfor bli svært viktig.

For å muliggjøre den dynamiske informasjonsflyten som man ser for seg i et NBF, må informasjonen som er nødvendig for å kunne utføre et oppdrag være tilgjengelig uavhengig av graderingsnivå. Det er brukerens aksessprivilegier som bør styre tilgangen til informasjonen, og ikke hvilket nettverk og system vedkommende er knyttet til. Det er derfor behov for å bevege seg bort fra sikkerhetsdomene-tankegangen og over mot beskyttelse av selve informasjonsobjektene ved bruk av sikkerhetsmerker, digitale signaturer og streng aksesskontroll basert på brukerens aksessprivilegier. Dette vil gjøre det mulig å gruppere informasjonen etter oppdrag og behov. Det vil være nødvendig å introdusere en dynamisk risikovurdering som en del av aksesskontrollen til informasjonen, hvor mulige kriterier for eksempel kan være:

- hvor stort behovet for tilgang til informasjonen er for å utføre oppdraget
- tiltro og privilegier til brukere av informasjonen
- type informasjonssystem
- sted, omgivelser og miljø
- hvor lenge informasjonen vil være gradert etc.

En slik dynamisk sikkerhetsløsning forutsetter en endring av dagens sikkerhetspolicy. Det vil også være nødvendig å innføre en sikkerhetsinfrastruktur og managementsystemer for å administrere privilegier og security tokens, samt tilgjengeliggjøre den informasjonen som er nødvendig for å utføre den dynamiske risikovurderingen.

2.6 Interessegrupper (COI)

En hensiktsmessig tilnærming til datamodelleringsarbeidet for en framtidig løsning, vil være å basere seg på en inndeling i interessegrupper. Vi definerer en interessegruppe som: En samling av mennesker som er interessert i informasjonsutveksling innen ett emneområde. Dette kan for eksempel være på grunn av ansvarsområde eller oppdrag. På engelsk kalles dette for Community of Interest, se for eksempel (7). Vi bruker forkortelsen COI for interessegruppe videre.

I US DoDs (8) Net-Centric Data Strategy defineres en COI som:

Communities of Interest (COIs) is the inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange.

Man ser for seg at forskjellige COI oppstår på forskjellig vis, og kan ha forskjellig grad av stabilitet.

Innenfor datamodellering ville den optimale teoretiske tilnærmingen (i følge en del) være *en* altomfattende modell. I praksis er dette ikke oppnåelig, av minst to grunner:

- en slik utvikling vil man neppe noensinne klare å bli ferdig med
- en slik modell vil uansett være for omfattende til at noen vil implementere den fullt ut

Den praktiske tilnærmingen blir derfor gjerne at man lager de modellene man trenger for de enkelte funksjonsområdene, og så ser man på hva som er relevant å utveksle utenfor disse områdene. Det er dette vi har kalt en ontologi tidligere. Ontologier er nærmere forklart i kapittel 2.7.

Tradisjonelt har arbeidet innenfor datamodellering nesten alltid tatt utgangspunkt i en COI, selv om det ikke alltid har vært kjent under dette begrepet. Det er det enkelte tilfelle som avgjør hva som er en COI. Noen er små, mens andre kan være store og inkludere andre COI delvis eller i sin helhet.

Frem mot 2014 bør det fokuseres på slike datamodeller for forskjellige interessegrupper, eksempelvis K2, slik at alle som defineres innenfor interessegruppen K2 kan dele informasjon med hverandre. I tillegg vil semantisk teknologi som ontologier kunne benyttes for mer smidig og rask informasjonsdeling og interoperabilitet med:

- andre interessegrupper i Forsvaret (logistikk, etterretning)
- andre nasjoners interessegrupper
- sivile institusjoner
- frivillige og NGOs
- nyhetsorganisasjoner etc.

En COI-datamodell utarbeides av en gruppe bestående av representanter fra alle grener av organisasjonen som har nytte av å utveksle et minste felles multiplum av informasjon seg imellom. Medlemmer fra forskjellige miljøer som tilhører samme interessegruppe må i samarbeid arbeide frem en slik modell der den ikke finnes. Der en slik modell finnes, for eksempel som en NATO standard, kan det beste være å benytte denne som utgangpunkt. Eksempler på andre interessegrupper kan være etterretning, ISTAR og ildledning. Vi tar ikke standpunkt til en slik inndeling i dette dokumentet, annet enn å identifisere K2 som en slik interessegruppe.

En sub-interessegruppe kan gjerne utvide datamodellen til sitt bruk, men for å oppnå kompatibilitet bør ikke det som er felles endres, annet enn gjennom arbeid i COI-modelleringsgruppen. En slik modell er svært viktig å ha på plass, da den utgjør grunnlaget for deling av informasjon innenfor en interessegruppe, i tillegg til at den definerer interessegruppens informasjonsinnhold for kommunikasjon med andre interessegrupper.

I en tjenesteorientert arkitektur er også en slik modell sentral dersom en skal oppnå gjenbruk av tjenester. Så lenge en er enige om semantikk og syntaks i meldingsformat, har det mindre betydning på hvilken måte data transporteres, så lenge interoperabilitet er mulig.

2.7 COI-ontologier

Det eksisterer i dag en rekke meldingsformater og datamodeller for utveksling av informasjon, samtidig som det utvikles nye systemer og datamodeller for nye virksomhetsområder. Akkurat som det vil hjelpe å kunne flest mulig språk når man reiser til forskjellige land, vil det være viktig for en ny norsk operativ løsning å kunne kommunisere med flest mulig. For å unngå tvetydighet og inkonsistens er det imidlertid viktig at informasjonsinnholdet er forankret i en overordnet konseptuell modell. Vi kaller dette for *ontologier* (formelle datamodeller). Hver COI vil ha sin egen ontologi som gjør dem i stand til å få samme forståelse av informasjon de deler med andre i interessegruppen. Dersom nye meldingsformater skal utvikles, bør dette gjøres med en slik overordnet ontologi som fundament. Dette kan bli viktig for å sikre konsistens, og også for å bidra til mer lettvint interoperabilitet. Oversettingstjenester som kan få inn informasjon på ett format og levere på et annet format vil bli sentralt for interoperabilitet. Dette er imidlertid avhengig av at det gjøres en manuell mapping mellom datamodeller. Å synliggjøre ontologier

gir derfor økt tilgjengelighet til informasjon, også informasjon som er bortgjemt i lukkede systemer.

Jo flere utvekslingsmetoder og formater/modeller som kan støttes, jo bedre vil vi være i stand til å dele informasjon med flest mulig. Dermed er det viktig at en ny løsning er bakoverkompatibel og rustet for interoperabilitet med nye samarbeidspartnere, enten de er nasjonale, internasjonale, sivile eller frivillige. Men akkurat som med språk er det noen formater som er viktigere å kunne enn andre.

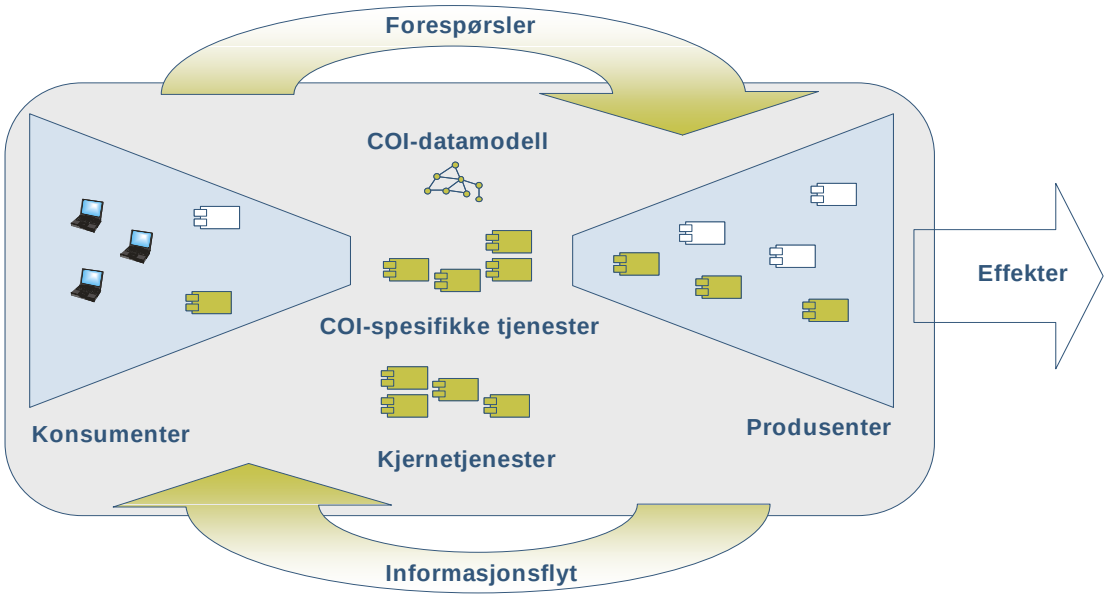
I tillegg kan noen utvekslingsmetoder og formater være mer effektive over lav båndbredde enn andre. Derfor er det viktig å ta vare på disse løsningene, også langt inn i fremtiden. Spesielt løsninger for trådløs kommunikasjon er kraftig begrenset av de fysiske lover, noe man må ta hensyn til.

2.8 Interoperabilitet og fleksibilitet

Målbildet for 2014 bør være at man har oppnådd en inndeling i interessegrupper, og at man har en felles datamodell (ontologi) for hver slik interessegruppe. Basert på dette bør man innenfor hver slik interessegruppe ha samlet opp *en fleksibel, modulær portefølje av funksjonalitet som støtter (semi-)automatisk oppkobling av toveis informasjonsdeling med nye samarbeidspartnere.* Dette kan ses på som et hovedmål for et 2014-målbilde. Slik funksjonalitet kan mappes til eller dekomponeres i tjenester, som bør være bygget på åpne standarder.

Målbildet for Forsvarets operative løsning i 2014 kan ses på som et anlegg for videreforedling av informasjon. Figur 2.2 viser en konseptuell skisse av dette, der man har produsenter av informasjon til høyre i figuren, og konsumenter til venstre. Det vil være et mangfold av produsenter og konsumenter, og systemets oppgave blir å distribuere informasjon, potensielt i videreforedlet form, fra produsentene til konsumentene. For å få til denne videreforedlingen, trengs et sett av tjenester som kan prosessere og sammenstille informasjon. For interessegruppen K2 kan dette for eksempel være kombinering og fusjon av informasjon. Dette kalles COI-spesifikke tjenester. Disse sørger for at innkommende data blir prosessert (potensielt av andre COI-spesifikke tjenester) og lagret i kjernetjenester som tilbyr lagring. COI-spesifikke tjenester vil også sørge for å tilby informasjon til konsumenter. I tillegg vil man trenge ting som kartdata og lagringstjenester.

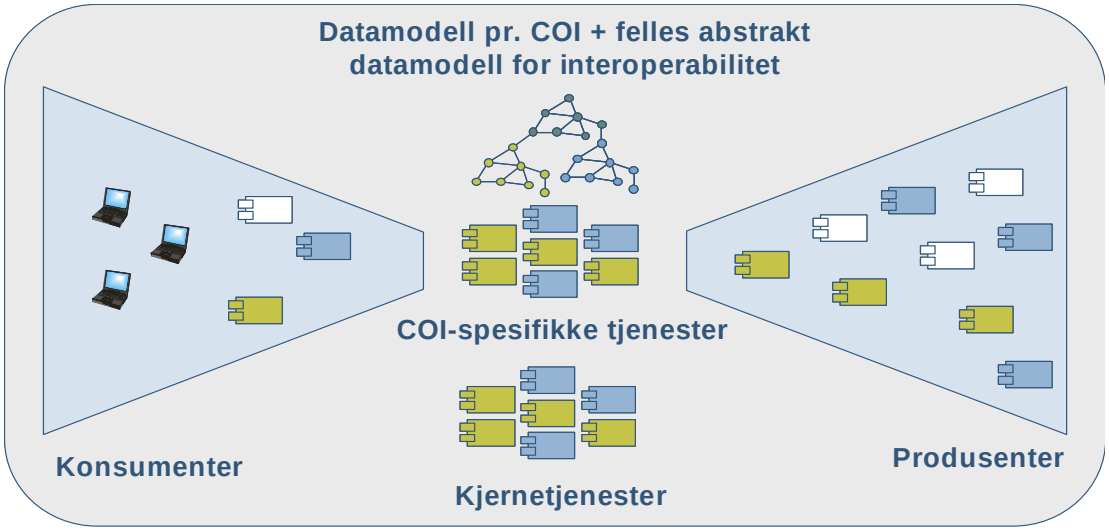
Et viktig poeng med denne tankegangen er at systemet vil være definert for å støtte hele verdikjeden, fra produsent til konsument. Følgelig vil systemet kunne tilpasses en rekke forskjellige konfigurasjoner, avhengig av hvem som er produsenter og konsumenter for et gitt oppdrag. Enheter kan ha både en produsentrolle og en konsumentrolle samtidig, slik at det er mulig både å produsere og konsumere for eksempel situasjonsinformasjon. Det er viktig å merke seg at alt dette skjer med COI-datamodellen som basis. Det er denne som sørger for at tjenestene kan settes sammen og fungere korrekt.



Figur 2.2 En systemkonfigurasjon for en interessegruppe

I andre interessegrupper vil man ha egne ontologier, andre tjenester og andre produsenter og konsumenter. Et eksempel på en annen interessegruppe kan være ISTAR, eller en sammenfallende interessegruppe fra en annen nasjon. Det er svært sannsynlig at det før eller senere kan oppstå behov for deling av informasjon *mellom* interessegrupper, selv om disse har forskjellige datamodeller. En måte å angripe denne utfordringen på er å si at vi da får en ny interessegruppe, som igjen kan arbeide frem sin datamodell for interoperabilitet. På denne måten ligger arbeidet først og fremst i å mappe datamodeller, utenfor programkode. Dette er arbeid som må gjøres uansett hvilken metode man benytter for å oppnå interoperabilitet. Da er det best å legge innsatsen her fra start, og få frem et miljø i Forsvaret som har dette som sin spesialitet.

Det er for interoperabilitet at en ontologi kan vise seg å bli svært viktig. Dersom det finnes forskjellige elementer i to COI-datamodeller som har samme mening (semantikk) men forskjellig meldingsformat (syntaks), kan man mappe slike elementer sammen. Dette kan gjerne gjøres ved hjelp av en ny felles abstrakt datamodell (ontologi) for de forskjellige interessegruppene. Dette er en manuell prosess, men etter at den er gjort (utenfor programkoden), kan man ved hjelp av semantisk teknologi automatisk få til en slik oversettelse. Dersom man har en semantisk beskrivelse av tjenestene i systemet, vil man, gitt en slik mapping, kunne få til en automatisk oppkobling av tjenester som i utgangspunktet er syntaktisk inkompatible. På denne måten kreves et minimum av innsats (selv om slik mapping kan være utfordrende) for å kunne tilpasse systemet til nye situasjoner, uten å endre programkode. Dette er illustrert i Figur 2.3, der tjenester fra to interessegrupper er satt sammen. I tillegg har vi nå trukket inn en tredje, overordnet ontologi som beskriver mappingen, og dermed en *bro* mellom de to forskjellige COI-datamodellene. En slik overordnet ontologi kan bli et viktig produkt i en fremtidig semantisk SOA, og behøver ikke nødvendigvis eies av en COI.



Figur 2.3 To interessegrupper, f. eks. K2 og ISTAR, som deler informasjon vha. en tredje ontologi

Et viktig moment i dette bildet er at det er mulig med en dynamisk oppkobling av tjenester for å tilfredsstille konsumenten (for eksempel en situasjonsbildebruker). Dersom vi nå forutsetter at forskningen innen lokasjonsbaserte tjenester har gitt resultater, kan vi tenke oss at det er mulig for en konsument å stille spørsmål av typen "Gi meg status for alle flyplasser i en radius 500 km fra Kandahar som støtter C130". Basert på dette kan systemet lete opp tjenester som potensielt kan tilby slik informasjon, spørre dem, og sette sammen svaret for konsumenten (brukeren). Eksempelet er modifisert fra et eksempel i (9).

Man kan også ved hjelp av (programvare-)tjenester nyttiggjøre seg en tjeneste i den virkelige verden, slik som å forandre innstillinger på en sensor eller rekvirere forsyninger.

Det er klart at sikkerhetsmekanismer, særlig for autorisasjon og integritet vil være viktig i dette eksempelet, noe som igjen indikerer at sikkerhet på informasjons-/applikasjonsnivå vil bli stadig viktigere (23). Vi tar for oss teknologier og forskning som vil kunne bidra til å realisere dette målbildet i kapittel 3.

Interoperabilitet mot stadig flere samarbeidspartnere genererer nye, store utfordringer på sikkerhetssiden. Vi ser at et nettverksbasert forsvar vil måtte medføre endringer i sikkerhetsregimet, og at vi bør arbeide i retning av en mer dynamisk sikkerhetspolicy. Basert på risikovurdering, oppdragets karakter, og hvem man kommuniserer med, bør sikkerhetsregler kunne defineres for hvert oppdrag. Disse bør også kunne endres under et oppdrag, basert på nye hendelser. En slik sikkerhetspolicy kan være fullstendig uavhengig av både nettverket og utvekslingsmetoden man benytter.

Et annet viktig aspekt er muligheten for å kunne kommunisere via legacy-formater der dette er nødvendig. Slike formater kan pakkes inn som tjenester, og man kan definere én- eller toveis mappinger eller transformasjoner for disse også. Det er da viktig at datamodellen for systemet

støtter alle informasjonselementer som inngår i disse formatene, slik at også denne informasjonen kan kommuniseres rundt i systemet. Pluggbarhet vil være viktig, slik at uventede grensesnitt raskt kan kobles inn i systemet, samt tilbys eksternt.

2.9 COI-spesifikke tjenester

Med COI-spesifikke tjenester mener vi tjenester som er spesielt tilpasset behov hos medlemmene i en interessegruppe. Slike tjenester har stort potensial for gjenbruk, og kan gjerne benytte kjernetjenester. Da oppnås gjenbruk også utenfor en COI. Vi beskriver her noen eksempler på COI-spesifikke tjenester.

2.9.1 Presentasjon

Et eksempel på presentasjonstjenester er tjenester som spesialtilpasser informasjon. Dette kan være å generere en webside for håndholdt utstyr basert på informasjonen, eller oversetting til et binært format.

2.9.2 Abonnement

I noen tilfeller vil det være viktig å kunne abonnere på forskjellige typer informasjon. Dette kan tenkes realisert som abonnementstjenester for forskjellige interessegrupper.

2.9.3 Informasjonskombinering

Etter hvert som mer informasjon fra flere kilder tilgjengeliggjøres, vil tjenester for kombinering av informasjon bli viktige. Eksempler på dette kan være korrelering av rapporter om objekter, fusjonering av slike rapporter etc.

2.9.4 Informasjonsoversetting

Som nevnt over vil oversetting av dataformater og megling mellom tjenester som i utgangspunktet er inkompatible kunne bli viktig. Transformasjon, mapping og inferens er generiske kjernetjenester, men disse er avhengige av menneskeutviklede mappinger. Det er imidlertid fullt mulig å realisere oversetting på en programmatisk (og ikke deklarativ) måte. I så fall vil tjenestene være spesiallaget for informasjonsoversetting mellom et fåtall spesifikke formater, og blir dermed COI-spesifikke.

2.9.5 Brukeragent

I andre tilfeller vil det være viktig å delegere oppgaver som har med informasjonsinnsamling å gjøre, for eksempel til en lokasjon som har bedre tilgang til informasjon. Slik informasjon kan for eksempel hentes fra World Wide Web (WWW). Da vil det være ønskelig å kunne sette ut en oppgave, for deretter å komme tilbake for å få den innsamlede informasjonen.

2.10 Orkestrering

Noen tjenester, både COI-spesifikke og kjernetjenester kan være orkestrerte tjenester, tjenester som benytter andre tjenester til å skape merverdi. Disse tjenestene kan kombinere for eksempel

kjernetjenester og tjenester for oversetting, samt innføre ekstra funksjonalitet.

Et eksempel på dette kan være å motta data på ett format, oversette til et annet, og lagre dataene. Et annet eksempel kan være å motta en forespørsel om informasjon fra en konsument, for så å finne aksessrettighetene til brukeren og deretter levere informasjon i henhold til gjeldende sikkerhetspolicy for informasjonen.

Orkestrering er et viktig element i en tjenesteorientert arkitektur. Dette benyttes for å konfigurere systemer basert på virksomhetsprosessene systemene skal støtte, ved hjelp av en portefølje av tjenester som allerede er utviklet.

3 TEKNOLOGI FOR INTEROPERABILITET OG INTEGRASJON

3.1 Overordnede teknologitrender

3.1.1 Tjenesteorientert arkitektur

Tjenesteorientert arkitektur er det norske begrepet for det som på engelsk kalles for Service-Oriented Architecture (SOA). En SOA er en arkitektur som består av en samling løst koblede tjenester, som igjen er en samling av funksjonalitet, se (10) og (11). Tjenester kan sammenlignes med komponenter, da disse også er basert på et klart definert grensesnitt, samt en datamodell for informasjonsutveksling. I tillegg kan tjenester utføres over et nettverk, noe som muliggjør distribusjon. Tjenester kan konfigureres sammen, slik at systemet utfører den ønskede funksjonalitet til enhver tid, basert på de virksomhetsprosesser som systemet skal støtte. Det er viktig at tjenester er basert på åpne standarder, slik at interoperabel kommunikasjon kan oppnås til tross for forskjellige maskinvareplattformer, operativsystem og programmeringsspråk. For å oppnå en løs kobling og gjenbruk er det viktig at tjenestene er grovkornede. Med dette menes at tjenestene er grove nok til å kunne gjenbrukes i andre sammenhenger. I tillegg bør en dokument-orientert tilnærming benyttes, slik at det overføres en større mengde informasjon én gang, i stedet for å gjøre flere, mer finkornede operasjoner. Det er viktig å huske at kommunikasjonen må kunne gå over et nettverk.

SOA er gjenstand for mye oppmerksomhet, og det er store forventninger til denne måten å bygge systemer på. Det er viktig å få frem at selve SOA-prinsippet er uavhengig av teknologien som benyttes for implementering, og at det finnes flere teknologier som støtter SOA i noen grad. SOA blir gjerne assosiert med kommunikasjon etter request-response-modellen, det vil si at man gjør en forespørsel til tjenesten, for deretter å få et svar. Dette er ikke nødvendigvis riktig, da det er fullt mulig med asynkron kommunikasjon i en tjenesteorientert arkitektur. Dette kalles gjerne for en hendelsesdreven arkitektur, eller Event-Driven Architecture (EDA). EDA støtter flere kommunikasjonsmodeller, blant annet garantert levering (på applikasjonsnivå) og abonnements-type kommunikasjon (også kalt publish-subscribe) der klienten registrerer seg, for siden å motta oppdateringer dersom en ny hendelse inntreffer. En slik arkitektur er i større grad avhengig av

en infrastruktur som kan mellomlagre og rute meldinger på applikasjonsnivå.

En av grunnene til at SOA, og spesielt SOA realisert ved hjelp av Web Services, har fått mye oppmerksomhet i det siste, er at det arbeides med teknologi som støtter rask endring av måten tjenestene er koblet sammen på. Dette kalles for orkestrering av tjenester, og kan settes opp ved hjelp av grafiske verktøy. Etter at dette er gjort kan orkestreringen utføres ved hjelp av et verktøy for dette. Med andre ord kan man deklarere ny programflyt eller samspill mellom tjenester uten å programmere. Orkestrering er ment å skulle understøtte stadig endring i virksomhetsprosesser, og vil være viktig for raskt å kunne møte nye behov som ikke tidligere har vært klart definert.

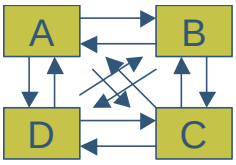
I tillegg arbeides det med tjenesteorientert teknologi basert på et spesifisert geografisk område, kalt lokasjonsbaserte tjenester (geospatial services (12)). Dette vil kunne muliggjøre å tilby kartlag via en tjeneste, slik at man for eksempel automatisk kan lese værdata fra en tjeneste, og plassere disse inn i kartrammeverket man benytter.

Som et siste punkt kan det nevnes at W3C, organisasjonen som arbeider med webstandarder, nylig har annonsert at de ønsker å arbeide i retning av å få WWW helt ut til små, mobile terminaler, Mobile Web Initiative (13). Det er grunn til å tro at noen av teknologiene som kommer frem her vil kunne benyttes også i forsvarssammenheng, for eksempel i forbindelse med soldatutrustning.

3.1.2 Syntaks, felles datamodeller og semantikk

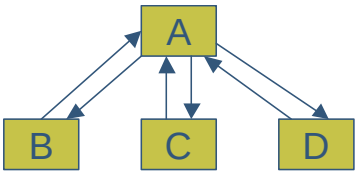
Selv om man har en SOA i en organisasjon vil det kunne by på utfordringer både å koble sammen egne tjenester, og å koble seg sammen med andre organisasjoner på en rask måte. For å løse dette best mulig, bør man ha en felles ontologi for tjenester som skal fungere sammen. En ontologi kan forklares som en felles formell datamodell for systemet. Har man ikke dette, risikerer man å måtte bruke tid på å oversette mellom forskjellige syntaktiske formater, basert på forskjellig terminologi. Dette er ikke alltid trivielt, særlig når man ikke kjenner konteksten eller betydningen av syntaksen.

Et eksempel på dette kan være at man har en tekst `armored_vehicle`. Et menneske ville forstått at det her dreier seg om en stridsvogn, som igjen er et kjøretøy. En datamaskin leser kun bokstavene a-r-m etc. Grunnen til at dette fungerer i dag, er at den som programmerer systemet legger inn hva som skal gjøres når teksten `armored_vehicle` inntreffer. Dette fungerer bra, helt til man skal koble sammen systemet (eller tjenesten) med et annet, som kanskje benytter teksten `stryker` for å representere samme type data. Dette kan i mange tilfeller løses ved at programmereren lager en oversettelse mellom de to systemene. En ulempe med dette er at det må gjøres for alle systemer, for hvert nytt syntaktisk format. I verste fall blir dette en alle-til-alle oversetting av syntaks, som gir en eksponentiell økning i antall oversettelser etter hvert som antallet systemer vokser. Dette er illustrert i Figur 3.1, der alle systemer har hver sin datamodell, og mapping gjøres punkt-til-punkt.



Figur 3.1 Punkt-til-punkt oversetting av dataformater

En bedre tilnærming vil være at alle fra en interessegruppe, i dette tilfellet en interessegruppe som utveksler informasjon om stridsvogner, kommer sammen og blir enige som en *felles abstrakt datamodell* som benyttes for kommunikasjon mellom alle systemer som arbeider med data om stridsvogner. En slik datamodell vil definere betydningen, eller semantikken til dataene. I eksempelet vårt definerer vi altså hva en stridsvogn er (en type kjøretøy), og at både en `armored_vehicle` og en `stryker` tilsvarer en stridsvogn. Dermed kan en datamaskin forstå sammenhengen. Benytter man en slik felles datamodell som et nav, kan man i beste fall få til en alle-til-én-oversetting, samt en én-til-alle oversetting, noe som medfører langt færre oversettinger ved integrasjon av nye systemer. I beste fall medfører dette en lineær økning i antall oversettelser etter hvert som antallet systemer vokser. På denne måten kan man tilrettelegge for en alle-til-alle informasjonsdeling. Se Figur 3.2.



Figur 3.2 Alle-til-en oversetting av dataformater

Det forskes mye på bruk av slike felles, abstrakte datamodeller, og de kalles gjerne for *ontologier*. En ontologi kan være alt fra en UML-modell (14) til en modell basert på formell logikk. Sistnevnte variant gir mulighet til å spesifisere ontologien eksplisitt og maskinprosesserbar utenfor programkode. En slik ontologi gjør at en datamaskin kan forstå relasjonene mellom konsepter og det blir mulig å automatisere en rekke ting. Dette står i kontrast til dagens bruk av datamodeller, der det er utvikleren som tar seg av tolkningen av datamodellen. For å få til dette må det gjøres et arbeid med å få frem en slik datamodell. I tillegg må mappinger utarbeides. Dette er manuelle prosesser som kan være utfordrende.

Videre inn i fremtiden ser vi at dagens teknologi for å realisere SOA har noen mangler, spesielt når det gjelder automatiserte prosesser og semantisk interoperabilitet. Ontologier er også fundamentet for mye av forskningen innen The Semantic Web. Dette er en visjon der man ser for seg langt større grad av presisjon og automatisering på WWW enn i dag, se (15). Denne visjonen ligger nok fremdeles litt frem i tid, men teknologien kan benyttes internt i og mellom virksomheter også, noe som ligger nærmere i tid.

Det gjøres i dag mye forskning på bruk av ontologier i en SOA. Ontologier kan ha flere roller,

men den viktigste rollen er som en formell representasjon av en felles datamodell, som beskrevet over. Ved å benytte en ontologi for dette formålet, er det mulig dynamisk å koble tjenester sammen, selv om de ikke kommuniserer ved hjelp av det samme meldingsformatet. Det trengs da blant annet en ekstra beskrivelse av tjenesten, der man hekter tjenestens syntaks opp i en felles, abstrakt datamodell. Å finne den best egnede tjenesten blant mange andre vil også kunne gjøres på en mer automatisert måte, siden dette vil kunne gjøres maskinelt, og ikke ved at brukerne sitter og blar seg igjennom en stor mengde tilgjengelige tjenester. Det vil sannsynligvis også bli mulig automatisk å orkestrere tjenester som kombinert gir ønsket totalfunksjonalitet. Tjenester som har semantiske beskrivelser i en eller annen form kalles Semantic Web Services (16).

Man har også nylig begynt å forske på kombinasjonen av lokasjonsbaserte tjenester og semantiske tjenester, dette for å oppnå høyere grad av automatisering og støtte til brukeren. I fremtiden vil man kunne få besvart komplekse spørsmål ved at systemet leter frem tjenester som kan gi et svar på dette, spør tjenestene, og sammenstiller informasjonen for brukeren. Se (9) for en beskrivelse av dette prosjektet.

Som en oppsummering må nevnes at mye av den nevnte forskningen dreier seg om utvidelser av dagens XML og Web Services-baserte teknologi. Dermed kan man ved å fokusere på de riktige tingene allerede i dag begynne å forberede seg på hva som kommer. Imidlertid er det utfordringer knyttet til dette. Disse diskuteres i kapittel 4.

3.2 Teknologier for SOA

Det finnes i hovedsak to standardiserte teknologigrupper for plattformuavhengige distribuerte systemer, CORBA og XML/Web Services. Begge disse kan brukes for å realisere en SOA, men Web Services er meldingsorientert og bedre egnet til å kjøres over et Wide Area Network (WAN). Standard bruk av CORBA kan også resultere i at tjenestene blir for finkornede, siden CORBA egentlig er en standard for distribuerte objekter. Det hevdes ofte at tjenester i en SOA ikke må være for finkornede. Selv om CORBA fortsatt er i utstrakt bruk, går trenden mer og mer i retning av Web Services. Dette gjelder også for kritiske applikasjoner, slik som i telecom og forsvarssystemer. En klar forskjell er i tilfeller der man har strenge sanntidskrav, og må ha en teknologi som støtter dette, slik som for eksempel i kampsystemer. Her vil nok sanntids CORBA og eventuelt det langt nyere OMG-initiativet Data Distribution Service (DDS) være viktige i lang tid fremover. Det er fullt mulig å pakke inn CORBA-objekter som tjenester, noe som også gir en mulighet til å benytte flere CORBA-objekter til å realisere en tjeneste, som dermed blir mer grovkornet.

Standardisering innen Web Services er dessverre preget av en uryddig standardiseringsprosess. Flere organisasjoner arbeider med standarder (W3C og OASIS), og ofte arbeider ulike grupperinger seg frem til forskjellige forslag til løsning på samme problem, hvilket er svært uheldig når det gjelder standarder.

Det har vært argumentert for at CORBA er for komplekst i forhold til Web Services, men dette

begynner langt på vei å bli feil. Organisasjonen WS-Interoperability (17) arbeider med retningslinjer for bruk av Web Services-standarder slik at interoperabilitet mellom forskjellige implementeringer kan garanteres.

Siden vi ser at trenden går i retning av XML og Web Services til å realisere en (semantikk-basert) tjenesteorientert arkitektur, legger vi vekt på denne gruppen teknologier når vi nå kort beskriver forskjellige teknologier. En mer detaljert gjennomgang av standarder finnes i vedlegg. Her forsøker vi også å skissere i hvilket tidsrom vi regner med at teknologien vil være standardisert. I tillegg har vi forsøkt å markere det der vi kjenner til tilgjengelige implementeringer av teknologiene. Denne gjennomgangen er ikke komplett (blant annet ser vi ikke på transaksjoner), men er ment å skulle gi et bilde av hvor man står i dag.

3.3 Standarder

3.3.1 Syntaks/meldingsformat

For syntaktisk (strukturell) interoperabilitet er XML, XML Schema Definition (XSD) for validering, samt teknologier relatert til Extensible Stylesheet Language (XSL) for transformasjoner modne pr. i dag. XML er forholdsvis tungt å prosessere, og inneholder mye overhead. Med det mener vi unødvendige data som skyldes formatet, og som ikke bidrar til informasjonsutvekslingen, slik at båndbreddeutnyttelsen blir dårlig. Det arbeides med mer effektive versjoner av XML, blant annet ITUs Fast Infoset (18). W3Cs Binary XML (19) er i oppstartsfasen. Det finnes allerede proprietære løsninger for binærkoding av XML, noe som vil kunne brukes i en transisjonsfase.

3.3.2 Meldingstransport

For transport av XML er basisstandarden i Web Services, SOAP, forholdsvis moden. Det finnes videre et mangfold av såkalte WS-* spesifikasjoner. Disse er utvidelser av basisstandardene, og på noen områder finnes flere initiativer. Det er grunn til å tro at disse dupliserte initiativene vil konvergere på sikt, og bli til én standard. Dette gjelder blant annet flere av standardene som muliggjør en hendelsesdreven arkitektur (EDA), WS-Notification, WS-BaseNotification, WS-ReliableMessaging, WS-Addressing etc.

Siden SOAP er basert på XML, er også Web Services relativt tungt å prosessere. Det finnes også her et initiativ for mer effektiv koding av Web Services, kalt Fast Web Services (20). Dette initiativet går ut på å kode ”konvolutten” som skal transportere innholdet (for eksempel Fast Infoset) mer effektivt.

I tillegg har Microsoft lansert en binding av SOAP til UDP, og NC3A arbeider med en binding mot MMHS. Dette er svært interessant, siden man da kan utnytte eksisterende kommunikasjons- og sikkerhetsinfrastruktur i Forsvaret maksimalt.

3.3.3 Beskrivelse og søk

For å beskrive tjenester benyttes i dag standarden Web Services Description Language (WSDL). WSDL beskriver grensesnittet og meldingene som en tjeneste leverer, men ikke hva den leverer. I tillegg kan Universal Description, Discovery & Integration (UDDI) benyttes som et register for å lagre eller referere til WSDL-beskrivelser. UDDI kan benyttes både i design-time (som en tjenestekatalog for utviklere) og i run-time (dynamisk binding til instanser av en tjeneste). Et UDDI-register er ikke en nødvendig bestanddel i en SOA, men kan gi større robusthet, siden erstatningstjenester kan finnes.

Microsoft m.fl. arbeider også sammen om en standard for å finne tjenester vha. Multicast på et lokalnett (LAN). Denne kalles WS-Discovery, og er et alternativ til UDDI på LAN. (WS-Discovery kan også benyttes for å lokalisere et UDDI-register). UDDI er modent, mens WS-Discovery er forholdsvis nytt ennå.

Det forskes også på oppslag av Web Services i mobile ad hoc nettverk, infrastrukturløse IP-nettverk der alle noder er rutere. Dette vil, kombinert med mer effektiv koding av XML, kunne muliggjøre en XML-basert SOA helt ut til terminaler med tekniske begrensninger (i form av prosessering) i fremtiden.

Som nevnt over, har man ikke pr. i dag noen måte å beskrive kapabiliteten til en Web Service. For å støtte målbildet for 2014, trengs det vi kaller semantiske tjenestebeskrivelser, slik at vi oppnår stor grad av automatisering. Dette er fokus for Semantic Web Services. En rekke initiativer finnes innenfor dette området i dag, alle med forskjellig fokus. Blant disse er OWL-S, WSDL-S, WSMO og FLOWS, der OWL-S er den mest modne, og WSDL-S har den tetteste koblingen mot dagens standarder. Ingen av disse teknologiene er spesielt modne riktig ennå.

3.3.4 Orkestrering og koordinering

Orkestrering av tjenester basert på modellering av virksomhetsprosesser får relativt mye oppmerksomhet i disse dager. WS-BPEL (21) er standarden som skal støtte dette. Det finnes en rekke produkter som støtter visuell modellering av systemer, samt ”eksekveringsmotorer” for å kjøre BPEL-prosesser. Dette vil sannsynligvis være modent i nær fremtid.

3.3.5 Semantikk og regler

For å beskrive semantikk og regler, finnes det flere muligheter. For visuell modellering av ontologier, arbeides det i Object Management Group (OMG) med tilpasning av UML for dette formålet. Web Ontology Language (OWL) er et formelt språk for å spesifisere ontologier eksplisitt. OWL er basert på logikk, og har vært en W3C-standard siden 2004. Det finnes flere verktøy som støtter denne standarden. Imidlertid er sammenhengen mellom SOA og ontologier fremdeles umoden verktøymessig, selv om det finnes produkter allerede i dag. Det er grunn til å tro at dette vil være kommet mye lenger i 2008. Andre standarder innenfor dette området er RDF, SPARQL og RuleML, henholdsvis for å representere fakta, spørre etter disse og for å definere regler i et XML-format. Disse er relativt modne i dag.

3.3.6 Sikkerhet

Det er viktig å ta sikkerhet med i betrakting når en ny løsning skal velges. Sikkerhet er blitt beskrevet som den største utfordringen i et NBF. Dermed vil det være viktig å designe inn sikkerhet i nye løsninger så tidlig som mulig. Det finnes i dagens systemer ingen sikkerhet på applikasjonsnivå eller informasjonsnivå. Dette vil sannsynligvis være enklest å få til ved bruk av XML-baserte løsninger, som kan gjøre det mulig å innføre generiske løsninger uavhengig av applikasjonene.

Det vanligste nivået å løse sikkerhet på i Web Services i dag er transportnivå (SSL/TLS). Dette er samme løsning som benyttes i for eksempel nettbanker, og fungerer fint dersom en kun har punkt-til-punkt kommunikasjon, og trenger er sikker tunnel. Men SSL/TLS sikrer ikke informasjonen fra endesystem til endesystem. Hvis informasjonen sendes via en mellomliggende node (for eksempel en ”proxy”) vil SSL/TLS-forbindelsen termineres og en ny gjenopprettes ved videresending, noe som gjør at informasjonen vil være i klartekst i denne noden og derfor må beskyttes på andre måter. Det er derfor behov for ende-til-ende sikkerhetsløsninger som beskytter informasjonen fra applikasjon til applikasjon. Dette ekskluderer ikke bruk av sikkerhetstjenester på lavere lag i tillegg for bl.a. å beskytte mot trafikkanalyser. Vedrørende trafikkanalyser forskes det på interessante metoder for anonymisering av datatrafikk.

Det finnes en rekke standarder og initiativer som arbeider med sikkerhet på Web Services-nivå og informasjonsnivå. Bruk av XML som utvekslingsformat muliggjør dessuten en generalisering og gjenbruk av sikkerhetsløsningene for de forskjellige tjenestene. XML Digital Signature, XML Encryption, WS-Security, osv. er forholdsvis modne spesifikasjoner og enkelte av disse er også standardisert. Dette gjør at man kan unngå proprietære sikkerhetsløsninger, som ofte er svært kostbare, og gir liten grad av interoperabilitet. Det finnes også spesifikasjoner for ”security tokens” (XrML, SAML assertions, XCBF, X.509,…), for utveksling av ”security tokens” (PKI, XKMS, SAML,…) og for å spesifisere og utveksle security policies (XACML). For en oversikt over standarder som kan brukes for å sikre XML informasjon, se (23).

3.4 Systemutvikling og produkter

3.4.1 Model-Driven Architechture

Model-Driven Architechture (MDA) er et initiativ fra OMG som fokuserer på bruk av modeller på flere abstraksjonsnivå som grunnlag for å utvikle plattformuavhengige løsninger. Modelleringen legger opp til konsistente overganger mellom nivåene – helt fra øverste virksomhetsnivå og ned til realisering av systemer. Konsistensen i overgangene skal sikre at systemene gir riktig støtte til virksomheten.

MDA har som bærende ide å kunne generere kjørbar programvare for valgfri maskinvareplattform, gitt at man har laget en tilstrekkelig presis modellbeskrivelse av systemet. Som overordnet tilnærming til systemutviklingsprosessen ser dette ut til å passe utmerket

sammen med en satsning på SOA som modell for implementeringen.

En fundamental premiss for MDA er verktøystøtte. UML-standarden har så langt vært hovedpilaren på modelleringssiden. Ellers har det som finnes av totalintegrerte MDA-løsninger vært leverandørspesifikke i større eller mindre grad. Men det teoretiske potensialet her er stort. MDA er derfor et område som bør overvåkes og utnyttes i fremtidig systemarbeid. OMG har også under arbeid en Ontology Definition Metamodel (ODM), som vil være interessant å følge videre med på.

3.4.2 Industristøtte

Et viktig vurderingsmoment for teknologi er hvorvidt det finnes kompetanse og produkter tilgjengelig ute i industrien. Toneangivende bedrifter som IBM, Microsoft, Sun, Oracle, BEA og HP er blant de vi tror vil være med i forkant av utviklingen fremover. En annen bidragsyter som blir stadig viktigere er den såkalte ”open source” bevegelsen, som omfatter sentrale produktfamilier som Apache og Eclipse. Alle disse organisasjonene arbeider i dag innen XML og Web Services.

I kapittel 3.2 ble teknologigruppen XML/Web Services omtalt. Disse teknologiene er tilstrekkelig modne til å tas i bruk. Arbeidet med XML/WS bør kunne starte nå.

3.4.3 Enterprise Service Bus

I forbindelse med blant annet EDA, er det kommet en ny produktkategori som kalles Enterprise Service Bus (ESB). De fleste solide aktører innen SOA leverer nå en ESB i en eller annen form. Slike produkter leverer infrastruktur for å realisere EDA, samt pålitelig levering av meldinger på applikasjonsnivå (ikke nettverksnivå). En del ESBer inneholder også elementer av koordinering og orkestrering, sikkerhet, management og støtte for XML-transformasjoner. Med andre ord er en ESB en klasse mellomvare spesiallaget for SOA med røtter i meldingsbasert mellomvare (MOM). Det er usikkert om en ny løsning vil trenge en ESB, da vi sannsynligvis vil kjøre flere instanser på forskjellige lokasjoner, adskilt av nettverk med lav båndbredde. Dette kan både føre til at å kjøre en ESB blir for tungt, eller at lisenskostnader blir uhensiktsmessig høye. I så fall vil en ”lettvekts-ESB” være det beste.

4 VURDERING AV TEKNOLOGIER I FORHOLD TIL MÅLBILDE

I dette kapittelet vurderer vi teknologiene som er presentert i kapittel 3 opp mot målbildet for 2014. Hensikten med dette er å få frem et realistisk målbilde for 2008 som er forankret i 2014-målbildet og som bygger på relativt moden teknologi.

4.1 Interoperabilitet

Plattformuavhengighet og åpne standarder er svært viktig for interoperabilitet. Eksempler på dette er HTML og e-post, åpne standarder som kan benyttes av flere applikasjoner på forskjellige plattformer. Men i vårt tilfelle er også domenespesifikke informasjonsmodeller

svært viktige, da en datamaskin trenger hjelp til å tolke informasjonen. Dette kan sees på som en kontrast til dagens World Wide Web, der mennesker tolker websider.

Det er viktig å merke seg at interoperabilitet kan skje på forskjellige organisasjonsnivåer. Informasjonsdeling med NGOs vil kanskje først og fremst skje på høyere nivå, mens norske styrker i INTOPS ofte ”plugges inn” på lavere nivå.

På området interoperabilitet er vi ganske sikre på at XML-basert teknologi og semantisk teknologi vil bli viktige i fremtiden. Dette er avhengig av en felles datamodell som informasjonselementene trekkes ut fra. XML og Web Services ligger an til å bli den mest populære måten å få til kommunikasjon mellom forskjellige systemer på. Imidlertid er det både syntaktiske og semantiske utfordringer, som bedre kan ivaretas ved å fokusere på dette allerede på et tidlig stadium. Dette kan gjøres ved å arbeide frem en COI-datamodell og XML-skjema for interessegruppen. Samtidig er det viktig å sikre bakoverkompatibilitet, og ta med seg alle viktige meldingsformater som støttes av dagens systemer inn i en ny løsning.

En klar fordel med bruk av XML er at man kan oppnå syntaktisk og strukturell interoperabilitet. XML er en åpen standard som gir plattformuavhengighet. Med plattformuavhengighet mener vi uavhengighet av maskinvare, operativsystem, programmerings- og kjøretidsmiljø. Ved hjelp av standard verktøy kan et meldingsformat (skjema) defineres på en enkel måte. Det gir grunnlag for å bruke fritt tilgjengelige parsere til å validere XML-dokumenter. En slik validering av andre typer meldingsformater tar lang tid å utvikle på egen hånd, mens en her har basismekanismene tilgjenglig.

En annen viktig fordel med XML er muligheten til å transformere dokumenter fra ett format til et annet på en deklarativ måte. Slike transformasjoner kan enkelt deles mellom systemer, slik at gjenbruk av disse vil være mulig. Dette, kombinert med muligheten for validering, sparer mye utviklingskostnader (bl.a. for feilsjekking), og gir bedre støtte for hurtig og fleksibel interoperabilitet. Se (22) for mer informasjon om nytten XML kan ha i NATO-sammenheng.

Fordelen med bruk av Web Services er at det er en standardisert, interoperabel mekanisme for å transportere XML-meldinger. Basisen for Web Services består av åpne standarder, og er også plattformuavhengig på samme måte som XML.

Interoperabilitet kan bety mer enn bare å benytte samme informasjonsmodell og syntaks. Vel så viktig er interoperabilitet på organisasjonsnivå og infrastrukturnivå. Sistnevnte kan være sikkerhet, bruk av oppslagstjenester etc.

4.2 Organisasjonsnivåer

Informasjonsflyten går i dag i stor grad oppover i organisasjonen. I et NBF, og dermed i en ny løsning, vil ikke dette være tilstrekkelig. Deling på tvers muliggjøres av initiativer rundt interoperabilitet. Informasjonsmodeller for alle nivåer i organisasjonen vil være viktig. De største begrensningene for informasjonsutveksling er sikkerhetsrestriksjoner og båndbredde, i

tillegg til mangelen på en felles informasjonsmodell og virksomhetsprosesser. Vi berører ikke virksomhetsprosesser her, annet enn å si at modellering av virksomhetsprosesser, og orkestrering av tjenester for å understøtte disse, kan vise seg å bli viktig. Dette vil på sikt støttes av Web Services-teknologier.

Når det gjelder kommunikasjonsløsninger på forskjellige organisasjonsnivåer, omtales dette nedenfor.

4.3 Nettverk og båndbredde

Begrensninger i kommunikasjonsløsninger kan føre til et skille mellom der systemene kan benytte XML og Web Services, og der disse ikke kan benyttes. Mulige årsaker til et slikt skille kan eksempelvis være båndbredde, prosessering, batterikapasitet, monolittiske terminalløsninger, tidskrav og trafikkmengde. Dersom en ny løsning tar med seg eksisterende meldingsformater, vil den kunne benyttes også ved lavere båndbredder. Særlig monolittiske terminalløsninger vil fremdeles gi et skille, avhengig av hva informasjonsbehovet er, men en ny løsning vil støtte interoperabilitet mellom flere systemer. Dermed også nye, mer fleksible typer terminalløsninger.

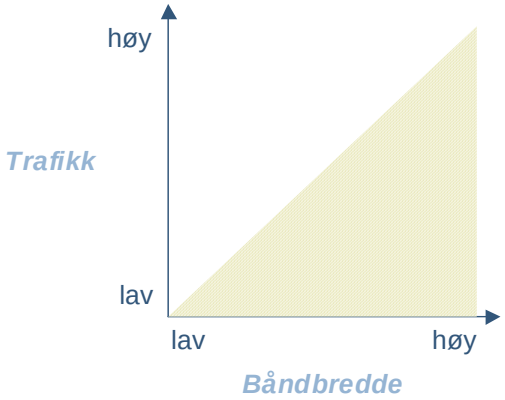
Vi antar at Forsvaret har de samme kommunikasjonsløsninger i 2008 som i dag, men at man vil få noe mer båndbredde på lang sikt. En migrasjon til IP-baserte nett, også med støtte for multicast, vil være viktig for bruk av åpne standarder for dynamisk oppkobling. Når det gjelder båndbredde i forhold til organisasjonsnivå, kan vår antakelse generaliseres på en enkel måte: Høyere organisasjonsnivå har relativt sett høyere båndbredde og lengre rekkevidde i forhold til lavere nivå.

Noen av utfordringene som er introdusert kan møtes i den konseptuelle løsningen for 2008 ved å bruke Web Services til å pakke inn eksisterende ikke-XML-baserte meldingsformater. En slik oversettelse kan gjøres på hver maskin (gitt at vi har med laptop og bedre å gjøre), avhengig av hvordan man velger å deployere systemet. Vi baserer målbildet for en ny løsning blant annet på gjenbruk av eksisterende meldingsformater i tillegg til XML-baserte formater. Dermed vil båndbreddebruken kunne bli tilsvarende dagens, gitt den samme bruken av systemet.

Effektiv koding av XML finnes allerede implementert, men er ikke standardisert. Når dette er standardisert, vil flere av utfordringene knyttet til XML over lav båndbredde unngås. Imidlertid trengs også effektiv koding av Web Services, slik at ikke bare nyttelasten i meldingene er effektivt kodet, men også ”konvolutten” som nyttelasten er pakket inn i. Standardiserte løsninger for effektiv koding av XML vil trolig komme mot slutten av perioden frem mot 2008.

Det vil være tilfeller der bruk av Web Services ikke er mulig i dag. Dette er det, som indikert over, vanskelig å si noe generelt om, blant annet fordi det vil være avhengig av trafikkmengden på nettverket. I mange tilfeller vil en oppdatering hver halvtime være en stor forbedring, mens det i andre tilfeller er krav om hyppigere oppdateringer.

Bruk av XML og Web Services kan være en utfordring over linker med lav båndbredde, høy trafikk og der en har korte tidsfrister. Figur 4.1 viser en generell kurve for når det kan være mulig å benytte XML og potensielt Web Services over et nettverk med begrenset båndbredde.



Figur 4.1 Generell kurve som viser hvor man kan bruke XML (nettverk)

Siden XML inneholder en del overhead, vil det for praktiske formål være en grense for hvor bruk av XML/Web Services er hensiktsmessig. Vi kan se av figuren at det i tilfeller med lav båndbredde og høy trafikk i nettverket vil være bedre å benytte mer optimaliserte formater. Det er mulig at enkelte eksisterende meldingsformater bedre ivaretar begrenset båndbredde. Dette er avhengig av flere ting, og spesielt intervallene mellom oppdateringer.

Da det er vanskelig å si noe generelt om bruk av XML og Web Services over lave båndbredder og på terminaler med tekniske begrensninger, vil dette måtte undersøkes nærmere gjennom eksperimentering.

4.4 Terminaler med tekniske begrensninger

Bruk av XML og Web Services kan være en utfordring der man har begrensninger i minne, lagringsplass, prosessor, og der man har lav batterikapasitet. Dersom terminalen ikke kan prosessere XML (gjelder enkle PDAer og nedover) er man nødt til å benytte proprietære løsninger.

En begrensning for å realisere en SOA helt ut til terminaler som Multi-rolle radio (MRR) og Link 16, er at man har en monolittisk applikasjon. Det er grunn til å tro at løsninger der en har lav batterikapasitet, slik som soldatutrustning (NORMANS, andre Blue Force Tracking og soldatutstyrsløsninger), kan betraktes som spesialtilpassede plattformer i lang tid fremover. Dermed vil de uansett ikke kjøre samme konfigurasjon som en laptop på for eksempel en kommandoplass. Like fullt vil *broer* mellom slike løsninger og de mindre mobile løsningene være nødvendig for interoperabilitet. Imidlertid kan enkelte terminaler benyttes som et modem kombinert med for eksempel en laptop-type terminal, og da er det teoretisk fullt mulig å konsumere tjenester, også via terminaler som MRR.

I visse tilfeller er batterikapasitet viktig. Dersom man ønsker å kjøre flere tjenester på én maskin kan dette være viktig å vurdere. En frittstående versjon av den tjenesteorienterte arkitekturen kunne være et eksempel på dette. Da oppnås gjenbruk av utviklede tjenester, uten noen form for optimalisering med tanke på batterikapasitet.

Bruk av batteri er spesielt avhengig av hvor mye prosessering som gjøres. XML og Web Services er tyngre å prosessere enn løsninger som er mer spesifikke for de enkelte programmeringsspråk. Dette kan for eksempel være intraprosess-kommunikasjon mellom tjenester, eller interprosess-kommunikasjon basert på mellomvare som er spesifikk for et programmeringsspråk. Eksempler på sistnevnte kan være Java Remote Method Invocation og .Net Remoting. Dermed kan det i visse tilfeller være uhensiktsmessig å benytte Web Services og XML, og en spesialtilpasset løsning må utvikles. Dette bør da gjøres i samme programmeringsspråk og med hensyn på optimalisert ressursbruk.

Dette betyr at det for en slik konfigurasjon (en SOA-instans på én maskin) altså kan være aktuelt å unngå bruk av åpne standarder. Dette er mest sannsynlig bare nødvendig der batterikapasitet er et problem. Om batterikapasitet representerer et problem eller ikke må undersøkes nærmere. Dersom XML/Web Services benyttes kun for utveksling av informasjon inn og spesielt ut fra terminalen, er det mer sannsynlig at terminalen kan klare dette.

Det må også her nevnes at det i dag finnes eksisterende systemer som kunne tatt en rolle som en lettvekts, frittstående applikasjon dersom et behov for mer batterieffektive løsninger finnes.

4.5 Dynamisk konnektivitet

I et NBF ser vi for oss større grad av dynamikk i hvem som er koblet opp mot hvem. Det blir vanskelig å forutsi hvilke produsenter konsumentene skal kunne velge blant. Dette støttes bra av en tjenesteorientert arkitektur, som muliggjør mange forskjellige og mer dynamiske systemkonfigurasjoner. For å oppnå dette må enhetene som skal delta være på samme nettverk og benytte samme mekanisme for å finne tjenester. Dette kan for eksempel være et IP-basert nettverk, og med Web Services-mekanismer for å finne tjenester. I dag er strukturen for informasjonsdeling i stor grad planlagt på forhånd. Imidlertid mener vi at XML og Web Services er riktig retning å gå i, da ledende forskning innen oppslag av tjenester bygger på disse teknologiene.

Den største nytten av en oppslagstjeneste får man der man ikke er begrenset av nettverket for å kunne få tilgang til alle tjenester. Her representerer forskjellige sikkerhetsdomener foreløpig en utfordring, da meldingstjenesten er den eneste gjennomgående bærer pr. i dag. Det gjøres imidlertid forskning på NC3A på å transportere SOAP over x.400, som er meldingstjenestens standard. Dagens kommunikasjonsløsninger kan dermed potensielt utvides med oppslagstjenester. Men siden bruk av en oppslagstjeneste gir økt trafikk på nettet, vil man med begrenset båndbredde ikke kunne få til full dynamikk på dagens taktiske nivå.

Sikkerhet (for tilgang til metadata) kan også bli viktig, da man publiserer informasjon om

tjenester tilgjengelig i nettet, og deres lokasjon på nettverket (og kanskje også geografisk i form av dekningsområde for sensorer). Dette omtales i kapittelet om sikkerhet.

Hvor dynamisk en automatisk oppkobling kan være, avhenger av uttrykkskraft i språket som benyttes for tjenestebeskrivelse. Men semantisk tjenestebeskrivelse er ikke noe poeng dersom man ikke har Web Services og en ontologi for ”domenet” på plass. Dette er også umodent, og ingen forent standard er på plass. Like fullt vil et arbeid med å ta frem en taksonomi over tjenester være viktig for å få til dynamisk oppkobling. Dette trenger ikke være veldig avansert i starten. For Web Services er det UDDI og WS-Discovery som er aktuelle, sistnevnte er ikke en standard og benytter multicast. Lokasjonen til et UDDI-registeret må distribueres til alle brukere før registeret kan tas i bruk. Dette er ikke desentralisert nok for et fullverdig NBF, men kan hjelpe oss et stykke på vei.

4.6 Militære standarder

Dagens versjon av NC3TA spesifiserer CORBA for distribuerte objekter, mens neste versjon trolig vil inkludere XML og Web Services. Dermed ser vi at NATO-standarder for interoperabilitet mellom tjenester også på sikt vil gå i en slik retning.

Det finnes i dag ingen XML-baserte NATO-standarder for K2-domenet. Imidlertid foregår det arbeid i MIP med en informasjonsmodell der XML for overføring vil komme i neste versjon. På lengre sikt vil det også komme ontologier som mer eksplisitt og formelt representerer informasjonsmodellen beskrevet i MIP. Uansett hva som vil komme vil det være viktig å støtte standarder som benyttes i dag videre.

Det er også viktig at det finnes informasjonsmodeller som kan benyttes på forskjellige nivåer i organisasjonen. Interoperabilitet mot eksterne organisasjoner vil sannsynligvis skje med XML.

4.7 Sikkerhet

Som beskrevet i kapittel 3 finnes en rekke spesifikasjoner og standarder relatert til sikkerhet i XML (for eksempel XML Signature, XML Encryption). OASIS har også utviklet en spesifikasjon som beskriver hvordan bl.a. XML sikkerhetsspesifikasjonene XML Signature og XML Encryption kan brukes for å sikre transportprotokollen SOAP i Web Services. I siste versjon (v3) av spesifikasjonen UDDI som definerer oppslagstjenesten i Web Services, har man introdusert bruk av XML Signature for autentisering og integritet. Det finnes også implementeringer av disse spesifikasjonene (både i programvare og maskinvare). Spesifikasjonene er et godt skritt i riktig retning, men er ikke alene tilstrekkelig for å innføre de sikkerhetsmekanismene som man ser for seg i et 2014+ perspektiv, med bl.a. merking av informasjonsobjektene og aksesskontroll basert på brukerprivilegier.

Når det gjelder sikkerhetsmerker finnes det pr. i dag ingen offisielle spesifikasjoner eller standarder basert på XML. Det finnes NATO- og IETF-standarder for sikkerhetsmerker som bl.a. brukes i militær meldingstjeneste og epost, men disse er definert i en annen syntaks

(ASN.1) og ikke XML. På FFI drives det forskning på dette området i samarbeid med andre NATO-nasjoner. Med fokus på internasjonale operasjoner er det viktig å velge løsninger basert på de samme standardene som våre samarbeidspartnere. Utviklingen av NATO Network Enabled Capabilities (NEC) vil være viktig for de teknologivalg vi må gjøre mot målbildet 2014+. Å delta i denne prosessen vil være viktig for å kunne være med å påvirke løsningene i en retning som også vil dekke våre behov nasjonalt.

Standardiseringsarbeidet innen W3C, OASIS og IETF gir gode indikasjoner på hvilke typer teknologier som vil bli tilgjengelige som hyllevare, men utfordringene ligger i å finne løsninger som man kan ha tilstrekkelig tiltro til med tanke på den anvendelsen man ser for seg i NBF. Dette gjelder bl.a. prosessen for å binde sikkerhetsmerker til informasjonsobjektene ved bruk av digitale signaturer, da disse sikkerhetsmerkene vil bli benyttet ved aksesskontroll og for slusing av informasjon mellom domener. Det er da viktig å kunne stole på at den som påfører sikkerhetsmerket og signerer vet hva hun signerer og at ikke noe annen informasjon utilsiktet har blitt lagt til av systemet. Det må også vurderes om de sivile spesifikasjonene og standardene kan brukes sammen med militære kryptoalgoritmer.

Sikkerhetsløsningene som er skissert for målbildet 2014+ forutsetter vesentlige endringer i security policy. Graden av tiltro som kreves for de ulike sikkerhetsløsningene vil være relatert til den aktuelle sikkerhetspolicy. Utviklingen av en mer fleksibel sikkerhetspolicy, hvor bl.a. risiko introduseres som en faktor under evalueringen av beskyttelsesnivå, vil være essensiell for å oppnå den fleksibiliteten i informasjonsutveksling som man ser for seg i NBF.

Management vil bli en utfordring på sikkerhetssiden. For å kunne innføre ende-til-ende sikkerhet med bl.a. sterk autentisering av brukere og prosesser, aksesskontroll på objektnivå og ende-til-ende kryptering, vil det måtte etableres en sikkerhetsinfrastruktur. Denne sikkerhetsinfrastrukturen er nødvendig for bl.a. å kunne administrere sikkerhetsmerker, security tokens, brukerprivilegier og kryptonøkler. Det finnes spesifikasjoner og standarder for bl.a. security tokens og administrering av disse. Den mest modne teknologien pr. i dag heter PKI (Public Key Infrastructure) og er bl.a. definert ved flere ITU- og IETF-standarder. For PKI finnes det en rekke sertifiserte produkter som i dag anvendes av flere nasjoner for militært bruk. Nasjonalt er det bl.a. startet et program for etablering av en nasjonal PKI-løsning for Forsvaret. Det er også denne teknologien NATO satser på og som vil være mest aktuell å benytte på kort til mellom-lang sikt bl.a. i forbindelse med innføring av digitale signaturer. Som nevnt i kapittel 3 har W3C og OASIS utarbeidet diverse XML baserte spesifikasjoner for ”security tokens” (XrML, SAML assertions, XCBF, …), for utveksling av ”security tokens” (XKMS, SAML,…) og for å spesifisere og utveksle security policies (XACML). Dette er spennende teknologier som må monitoreres nøye. Det finnes programvare- og maskinvareprodukter som implementerer flere av disse spesifikasjonene, men teknologiene er forholdsvis umodne og de er derfor mer naturlig å satse på i et 2014+ perspektiv enn på kortere sikt. Det må nevnes at selv om ikke standardene for PKI er XML-baserte, kan de brukes innen en tjenesteorientert arkitektur basert på utveksling av XML-informasjon, som for eksempel Web Services.

Utveksling av management-informasjon for å støtte ende-til-ende sikkerhetsløsninger vil kreve mye båndbredde ved bruk av dagens teknologi. Blant annet gjelder dette distribusjon av security tokens (sertifikater) og CRLs (Certificate Revocation Lists). Det må forskes mer for å utarbeide standardiserte løsninger som kan anvendes over ”trange kanaler”.

Ende-til-ende sikkerhetsløsninger bør være et mål for å muliggjøre en mer dynamisk og fleksibel utveksling av informasjon, men det introduserer også visse problemer. Ved å flytte sikkerhetsfunksjonaliteten nærmere applikasjonen vil man eksponere mer av protokollinformasjonen som brukes for kommunikasjon. Denne informasjonen kan brukes for trafikkanalyser for å se hvor informasjonen sendes. Det må vurderes om det er behov for å beholde kryptering på lavere lag i protokollstacken for å beskytte mot trafikkanalyser. Det forskes også på metoder for anonymisering av datatrafikk som er svært interessante og som bør følges nøye.

Det er viktig at man både har en ”top-down” og ”bottom-up” tilnærming i arbeidet med å møte de teknologiske sikkerhetsutfordringene i NBF. En ”top-down” tilnærming er nødvendig for å utarbeide en ny sikkerhetsarkitektur, sikkerhetspolicy og relaterte prosedyrer. Samtidig er det viktig å finne de teknologiske løsningene som gjør det mulig å innføre en ny sikkerhetspolicy hvor informasjon kan utveksles på en mer fleksibel måte enn i dag, samtidig som risikoen for kompromittering og fiendtlig manipulasjon av informasjonen er minimal.

4.8 Modenhet teknologi

Vi anbefaler åpne standarder som XML, XML Schema og Web Services (SOAP og WSDL) for utvikling av en ny løsning. Ulempen med dette er at standardiseringsarbeid tar tid. Utviklingen av standarder for Web Services preges av et uryddig standardiseringsarbeid, men basisteknologiene for utvikling av en Web Services-basert SOA er modne.

Når det gjelder semantisk teknologi, anbefaler vi å ta frem en Web Services-basert SOA basert på en felles informasjonsmodell før semantisk teknologi tas i bruk. Modenheten til en del semantisk teknologi er relativt god, men verktøystøtte og erfaringer med bruk av semantisk teknologi til dette formålet er fremdeles liten.

En felles informasjonsmodell kan inntil videre beskrives med UML og i tekstlig form. Det viktige er at det er enighet om hva som menes med begreper og hvilken relasjon disse har til hverandre.

Det er, gitt en standardisering av binærløsninger for XML, grunn til å tro at vi i et lengre perspektiv vil kunne basere mesteparten av løsningen på mer prosesseringsvennlige og båndbreddeeffektive versjoner av Web Services og XML. Standardiseringsinitiativer som binary XML, Fast Infoset og Fast Web Services vil kunne bidra til å flytte XML og Web Services ut til terminaler, og muliggjøre interoperabilitet på tvers også på lavt nivå der en har lav båndbredde. I tillegg finnes det som nevnt i dag allerede proprietære løsninger for binærkoding av XML.

4.9 Kompetanse

Dersom Forsvaret velger å gå i retning av en tjenesteorientert løsning, vil det være flere roller som må ivaretas. Vi mener at Forsvaret selv bør ta et arkitektansvar, dette for å sikre at porteføljen av tjenester ivaretar organisasjonens behov på best mulig måte. Personen(e) som fyller en slik rolle bør være involvert i all ny- og videreutvikling. På denne måten vil man ha forsvarsansatte personer som er med på en evolusjonær utvikling fra dagens systemer til en enkel SOA i 2008, til en mer automatisert og interoperabel (basert på informasjonssikkerhet) SOA i 2014. Dermed vil en i beste fall kunne unngå å hente inn konsulenter for å konfigurere systemet på nytt. En slik arkitekt(-gruppe) bør også ha en deltakende representant i datamodelleringsarbeidet for de forskjellige interessegruppene.

Den tradisjonelle forsvarsindustrien i Norge bør kunne forventes å ha kompetanse på de teknologier som her anbefales. Øvrig ”sivil” industri som eksempelvis konsulentbransjen er også en mulig bidragsyter når det gjelder teknologikompetanse.

4.10 Risiko

Det finnes mange former for risiko. Noe dekkes av begrepet sikkerhet, mens det vi her tenker på er faren for at våre anbefalinger om teknologivalg i ettertid kan vise seg å medføre uforutsette ulemper. I det følgende vil vi gi noen betraktninger knyttet til fremtidige teknologivalg.

IT-historien er full av teknologier som ikke har levd opp til forventningene. CORBA ble tatt frem som en universell løsning, men har ikke blitt like universell som antatt. Imidlertid er CORBA svært mye brukt. Ofte ”gjenfødes” teknologi i forbedret form, og dagens Web Services kan gjerne sees på som en reinkarnasjon av CORBA. Om WS representerer en universell løsning er det vanskelig å si noe om. Imidlertid er det langt mer interesse for XML og WS enn det er for CORBA i dag, selv om Web Services i dagens form ikke gjør noe særlig nytt. Det er ideen om en komponerbar, sikker, og semantisk SOA som er interessant for oss. Denne tilrettelegges det i stor grad for ved arbeid med en informasjonsmodell og bruk av XML/WS.

En viktig risikoparameter er hvordan markedet generelt vil forholde seg til våre teknologiske løsninger. Både kompetansetilgangen og utbudet av verktøystøtte avhenger av at løsningene har en tilstrekkelig stor brukergruppe på verdensbasis. Og ikke minst er de økonomiske kostnadene knyttet til bruken av teknologiene, avhengig av markedsutbredelsen. Dette er et forhold som bør overvåkes i tiden som kommer, og gjerne slik at konkrete anskaffelser gjøres på bakgrunn av en oppdatert revurdering av markedssituasjonen.

4.11 Kostnadseffekter

Dette arbeidet omfatter ikke konkrete kostnadsvurderinger. I forarbeidene til oppdraget ble det imidlertid uttrykt ønsker om at det i tilknytning til de teknologiske anbefalingene ble pekt på elementer som kunne kalles kostnadsdrivere. Uten å ta utgangspunkt i spesifikke systemer og en nærmere definert nåsituasjon – noe som ligger utenfor vårt mandat – vil betraktninger om kostnader måtte holdes på et overordnet nivå.

Innledningsvis når det gjelder kostnader er det viktig å huske at en økonomisk innsats kan gi gevinster på kortere eller lengre sikt. Begrepet ”grunnmur” er brukt om 2008-målbildet. Den gir som kjent liten kortsiktig verdi i seg selv, men er fundamental for helheten på lang sikt.

Det man ofte leter etter i planleggingsprosessen, er såkalte Quick Wins. De kjennetegnes av å gi verdi på kort sikt, men uten å gå på akkord med den langsiktige innretningen. Kortsiktig verdi er i løsningssammenheng oftest knyttet til funksjonelle krav, noe dette arbeidet ikke har gått konkret inn på. Vi må derfor nøye oss med å anbefale å identifisere slike Quick Wins i planarbeidet.

Kommunikasjonsløsninger for økt båndbredde er et viktig område for verdien av informasjonssystemene overfor brukerne. Det ligger utenfor rammen av dette arbeidet, men bør likevel pekes på som en konkret kostnadsdriver. Det å bygge ut kommunikasjonsinfrastrukturen vil kreve omfattende investeringer, og kostnadene til det vil øke med økende krav til ytelse.

Kompetanse er en forutsetning for å håndtere ny teknologi. Gitt at man fokuserer på allment utbredt teknologi, vil markedet generelt alltid ha kompetanse å tilby. Det å bygge opp ny kompetanse internt og eventuelt hos egne leverandører kan sees på som en kostnadskomponent på kort sikt.

Oppbygging av COI-spesifikke datamodeller er anbefalt som en grunnleggende aktivitet. Her er det også viktig å huske at innsatsen som må legges ned i utviklingsarbeidet er ment å gi gevinster på lang sikt. Og i praksis er man nødt til å oppnå en viss parallellitet, slik at datamodellene kan utvikle seg videre i nye versjoner etter at systemer er bygget på dem.

En annen aktivitet som har langsiktig gevinst, er gjenoppbygging (re-engineering) av systemer. Dersom dette gjøres helt uten å endre på funksjonaliteten, blir kortsiktig gevinst minimal. I praksis vil man ofte oppleve at en gjenoppbygging åpner for nye muligheter, eksempelvis innenfor området interoperabilitet.

Omfangskontroll er et kjent problem ved utvikling av løsninger. Manglende kontroll gir ukontrollerte utvidelser (såkalt ”scope creep”) som kan bli en betydelig kostnadsdriver sett i forhold til opprinnelige budsjetter.

Andre viktige kostnadsparametere er lisenser og kontrakter, og ikke minst eventuelle avtalebindinger av økonomisk og juridisk art. Vi går ikke nærmere inn på det her, men tillater oss å postulere at proprietære løsninger ofte vil være mer kostnadskrevende, noe vi har brukt til å underbygge vår anbefaling om bruk av åpne standarder.

En egenskap ved våre anbefalinger om SOA, XML og Web Services er at de vil kreve en viss prosesseringskapasitet. Konkret kan det bli en utfordring for maskinvaren i ”lav ende” (lav båndbredde / lavere organisasjonsnivå). Det kan bety kostnader til relativt sett sterkere

maskinvare eller alternativt til utvikling av spesialløsninger. Og en følge av dette er en risiko for – dersom kostnadene overstiger gevinsten - at de generelle løsningene ikke vil fungere på de laveste nivåene. For å avklare dette noe nærmere, kan eksperimentering og prototyping være nyttige redskaper.

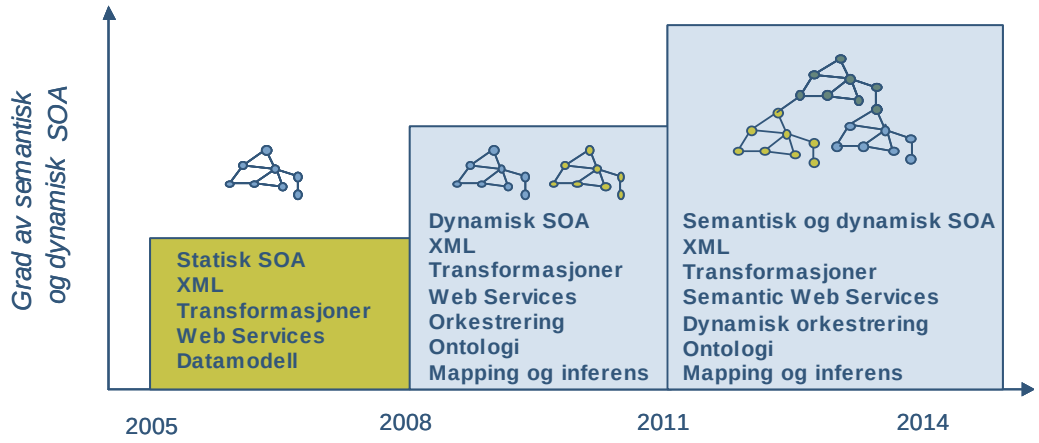
Et råd for å håndtere den relativt store usikkerheten som ligger i det generelle kostnadsbildet knyttet til de anbefalte teknologivalgene, er å gjennomføre utprøving av løsningsprinsippene (proof of concept) på en del-løsning som ventes å gi stor verdi på kort sikt (en Quick Win). Erfaringene fra utprøvingen vil gi grunnlag for en mer konkret vurdering av de ulike kostnadskomponentene som er beskrevet her. Kostnader og risiko bør også revurderes over tid etter hvert som ny informasjon kommer til.

4.12 Oppsummering

Som en oppsummering av dette kapittelet kan vi si at interoperabilitet muliggjøres av åpne standarder. Men det er i dag en avveining mellom åpne standarder og effektiv bruk av båndbredde og effektiv prosessering. Dette vil sannsynligvis endre seg de kommende år. Videre vil en endring av sikkerhetsregime sannsynligvis gi en forsinkelse i grad av dynamikk i informasjonsdeling og oppkobling. Vi velger å ta en teknologi-synsvinkel på dette, og se på hva som vil være mulig teknologisk.

Det viktigste er ikke å bruke XML/WS for enhver pris. Eksisterende formater vil etter alt å dømme benyttes i lang tid fremover, og bruk av XML og Web Services kan medføre problemer i visse tilfeller. Grunnen til at vi anbefaler XML og Web Services som et fundament, er at vi i fremtiden ser semantisk teknologi som en naturlig videreføring av denne familien av teknologier.

Som illustrert i Figur 4.2, anbefaler vi å vente med innføring av semantisk teknologi inntil verktøystøtte og bedre erfaring med dette er på plass. Vi vil likevel nok en gang fremheve viktigheten av en konsistent informasjonsmodell (datamodell i figuren) som grunnlag for de forskjellige XML Schema som benyttes som grunnlag for overføring av meldinger.



Figur 4.2 Anbefalt innføring av ny teknologi

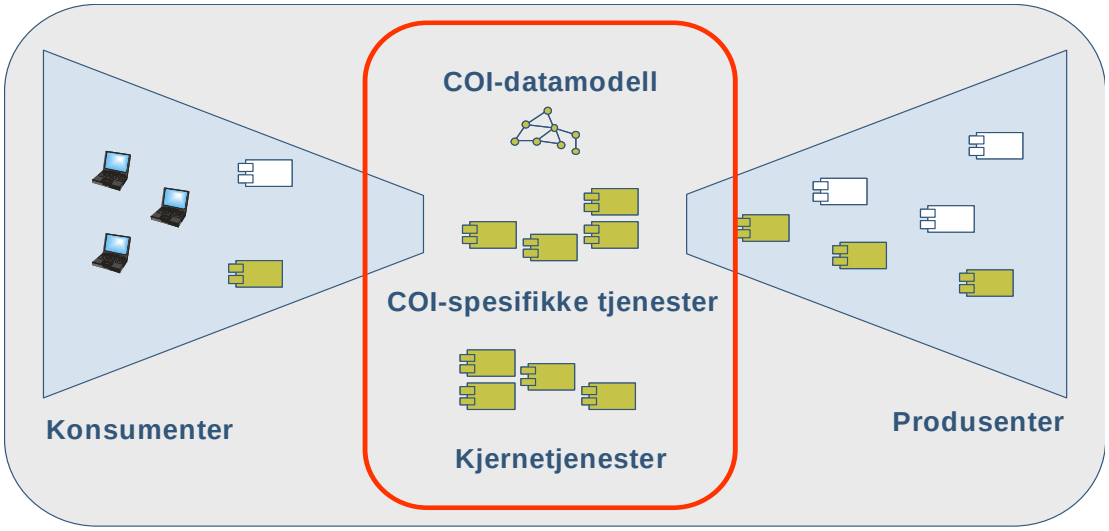
I figuren er aktuelle teknologiske målsetninger tegnet inn, og vi ser at frem mot 2008 vil målbildet være en statisk tjenesteorientert arkitektur, XML, Web Services, XML transformasjoner og en overordnet datamodell for meldingsformater. Denne datamodellen ligger ”utenfor” systemet i tidsperspektivet frem mot 2008, men vil i senere faser kunne tas inn i ontologier som inngår i den kjørbare delen av løsningen. Dette forutsetter et grundig arbeid med en slik felles modell. I neste kapittel beskriver vi målbildet for 2008 nærmere.

5 MÅLBILDE 2008

Basert på målbildet for 2014, og tilgjengelig teknologi i 2005, mener vi at en tjenesteorientert arkitektur vil være riktig vei å gå for Forsvarets operative løsning i 2008. Dette for å være best mulig rustet for å møte behov som ennå ikke er definert. En ny løsning bør utvikles på en evolusjonær måte, samt fokuseres mot interoperabilitet og dynamikk. Figur 5.1 viser relasjonen mellom målbildet for 2008 (rødt rektangel) og målbildet for 2014. Tanken er å starte i det små, ved å gjøre det viktigste først. Målbildet for en K2IS-løsning i 2008 trekker ut elementer fra det mer generelle målbildet for 2014. På denne måten blir løsningen en investering i en grunnmur å bygge videre på i fremtiden. Følgende elementer bør inngå i et 2008-målbilde:

- En tjenesteorientert arkitektur basert på åpne standarder
- Et sett av kjernetjenester
- En opprettelse av interessegruppen K2[5]
- Utvikling av en datamodell for interessegruppen K2
- Spesifikke tjenester for interessegruppen K2

[5] Vi mener her alle som er interessert i K2-relatert informasjon, og dermed også situasjonsinformasjon.



Figur 5.1 Fokus for målbilde 2008 i forhold til 2014

Vi ser for oss at en 2008-løsning består av en interessegruppe K2, som utvikler en datamodell for K2-informasjon. Videre utvikles et sett med kjernetjenester og et sett med K2-spesifikke tjenester som også inkluderer tjenester for oversetting. Oversettingsstjenestene tar imot informasjon på andre formater fra produsenter, og tilbyr informasjon ut til konsumenter. Vi beholder metaforen om et anlegg for informasjons-bearbeiding fra 2014-målbildet, der vi har produsenter og konsumenter, og der løsningen sørger for informasjonsdeling og lagring. Et hovedmål for en 2008-løsning blir derfor: *En fleksibel portefølje av funksjonalitet som støtter toveis informasjonsdeling.*

Løsningen bør i perioden frem mot 2008 baseres på et minimum av ny funksjonalitet som er basert på reelle behov. Dette gjør løsningen rustet for endringer i fremtiden. En slik tjenesteorientert arkitektur, basert på XML og Web Services vil gjøre løsningen klar for neste generasjon SOA-teknologi, basert på semantikk. På sikt vil dette, sammen med en ny sikkerhetsløsning, være teknologien som best støtter dynamiske koalisjoner med nye partnere og deres systemer.

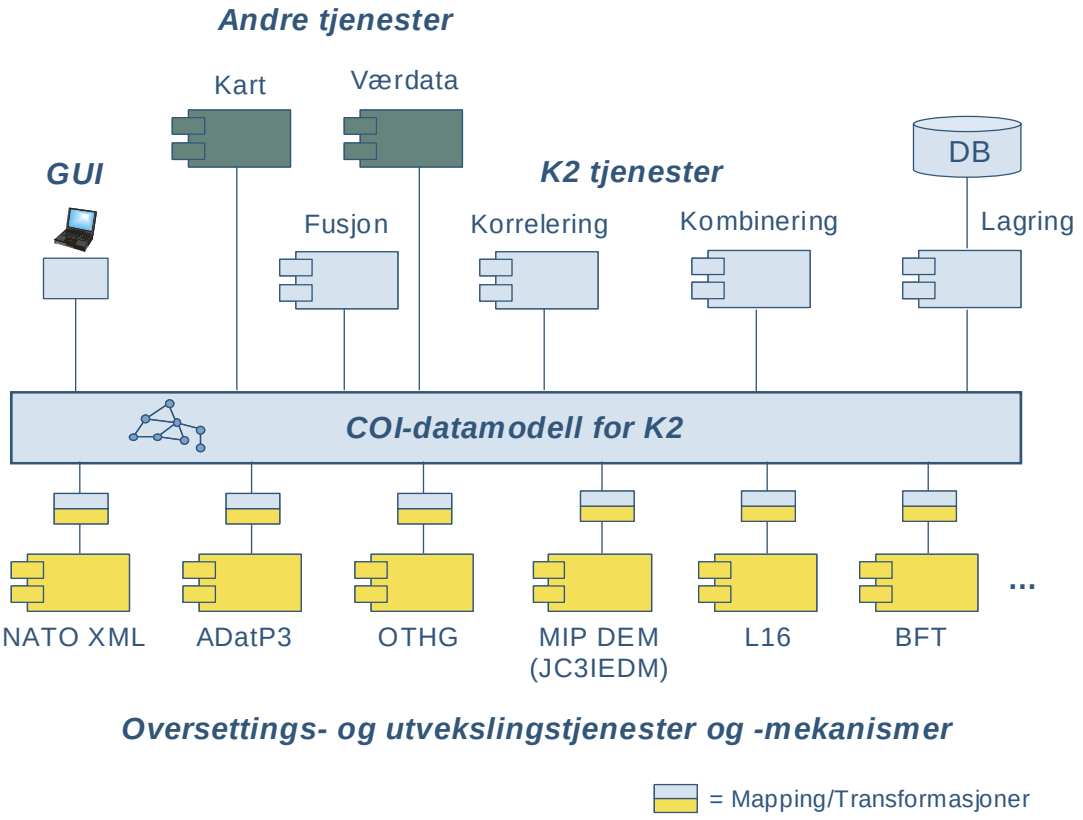
Siden det finnes systemer i dag som har gode løsninger for presentasjon, går vi ikke inn på dette her. Disse kan og bør gjenbrukes av en rekke grunner. Imidlertid ser vi for oss en dekomponering av eksisterende systemer i moduler, som på sikt vil konvergere og gi én løsning, potensielt med flere GUI for presentasjon.

Våre antagelser om kommunikasjonsløsninger i 2008 er at Forsvaret i stort har tilsvarende løsninger som i dag.

5.1 Tjenesteorientert arkitektur 2008

En tjenesteorientert arkitektur kan og bør innføres i forskjellige faser der man starter enkelt, og utvider etter hvert, basert på erfaringer. Nye tjenester bør kun tas frem basert på Forsvarets

langsiktige behov. Dermed blir det viktig å gå gjennom hva disse er. Å fremskaffe en SOA er ikke det samme som å fremskaffe en monolittisk applikasjon. Det kan for eksempel være flere leverandører inne i bildet. En vellykket SOA er resultatet av at tjenester er blitt utviklet basert på reelle, konkrete behov, for eksempel informasjonsdeling. Med andre ord bør en tjenesteorientert arkitektur utvikle seg gradvis. Dermed blir det igjen viktig å nevne behovet for en felles terminologi og datamodell i systemet. Vi ser på K2 som en interessegruppe, som følgelig bør arbeide frem en slik datamodell for sitt interesseområde.



Figur 5.2 Overordnet målbilde for 2008

Figur 5.2 viser en overordnet figur av en ny K2IS-løsning som en tjenesteorientert arkitektur. Vi ser at COI-datamodellen fungerer som et bindeledd mellom en rekke forskjellige tjenester, der en gruppe tjenester (markert med gult) sørger for utveksling med andre systemer, mens en annen gruppe tjenester er funksjonelle tjenester (markert med blått). Vi beskriver disse nedenfor. Det er også tegnet inn oversettelser i form av transformasjoner og mappinger mellom oversettings-/utvekslingstjenestene og datamodellen for K2IS.

5.1.1 Kjernetjenester 2008

Kjernetjenestene i et 2008-perspektiv vil være et utvalg av de kjernetjenester som er omtalt i beskrivelsen av 2014-målbildet.

I 2008-perspektiv ser vi for oss enkle tjenesteoppslag i kjøretid. En taksonomi over tjenester tas

frem og vi får dynamikk i tjenesteoppkopling. Semantiske tjenestebeskrivelser tas ikke i bruk i et 2008-perspektiv, men ambisjonen om en mer dynamisk tjenesteoppkopling kan oppnås som en videre påbygning. Tjenesteoppslag basert på Web Services ser vi for oss er mulig internt i noder/kommandoplasser, samt over fastnett hvor det er god kapasitet. På taktisk nivå og lavere ser vi for oss at det er mulig å tilby en kontrollert bruk av tjenesteoppslag ved bruk av taktisk profil i meldingstjenesten over dagens kommunikasjonsløsninger. Dette kan kombineres med binærkoding av XML og komprimering for ytterligere å redusere antall bit som overføres. Statisk bruk av tjenester (dvs. bruk av tjenester uten tjenesteoppslag) vurderes også som realistisk i et 2008-perspektiv. Disse mulighetene bør undersøkes nærmere gjennom videre arbeid og eksperimentering.

Oversettingstjenester vil være tilgjengelig, som enkle transformasjoner uten bruk av semantiske oversettingstjenester.

I 2008-perspektiv ser vi for oss at informasjonsoppslag basert på metadata er tilgjengelig kun over lokalnett og fastnett.

5.1.2 COI-datamodell for K2

For å komme i gang med å registrere behov, og dermed tjenester som vil være ønskelige, må representanter for medlemmene i en interessegruppe for K2 samles. Her kan for eksempel arkitekter, domeneeksperter og utviklere inngå. Dette er nødvendig for å få frem en terminologi og en konseptuell modell for informasjonen som skal deles internt i en interessegruppe.

En K2-datamodell skal støtte generering av meldingsformater for utveksling mellom tjenester. Det er mulig at en vil ha forskjellige meldingsformater mellom tjenester, noe som gjør det viktig at disse er forankret i en overordnet konseptuell modell. Denne kan baseres på en felles terminologi i interessegruppen. En slik datamodell er ikke nødvendigvis den samme som for utveksling mot andre interessegrupper. I NATO-sammenheng arbeider Multilateral Interoperability Programme (MIP) med en modell for deling av K2-informasjon mellom NATO-land. Dette kan være et naturlig utgangspunkt for et arbeid med en COI-datamodell. Se vedlegg for mer informasjon om MIP.

K2-datamodellen er en konseptuell datamodell som beskrives vha UML eller andre modelleringsteknikker. Den kan derfor karakteriseres som ”halvt formell” siden semantisk teknologi ikke tas i bruk.

5.1.3 K2-tjenester

Tjenestene tegnet med blått i Figur 5.2, er COI-spesifikke tjenester. Her tilsvarer dette tjenester for interessegruppen K2. Dette er tjenester som benyttes som byggeklosser i et K2IS. Disse bør kunne legges til og fjernes etter hvert som Forsvarets behov tilsier det, eller avhengig av hvordan systemet skal deployeres. Slike K2-tjenester vil kunne være for eksempel korrelering, kombinering, fusjon og klassifisering, og vil også kunne basere seg på kjernetjenester, eller tjenester fra andre interessegrupper, slik som kart og meteorologiske data (METOC). I det

tidligere variantbegrensningsarbeidet (3) er det identifisert flere grupper av funksjonalitet. Dette kan være et godt utgangspunkt for en diskusjon om hvilke tjenester som bør inngå i en interessegruppe for K2, og eventuelt andre interessegrupper som bør opprettes. Vi tar ikke standpunkt til en slik inndeling her, annet enn å foreslå dette arbeidet som et utgangspunkt for videre inndeling i tjenester og interessegrupper. Inndelingen som er gitt i (3), er:

- Common Operational Picture
- OOB Data Repository
- Assess Operational Situation.
- Prepare Plans and Orders
- Command Subordinate Operational Forces
- Plans and Orders Overlays
- Maritime C2 Services
- Air C2 Services
- Land C2 Services
- Intelligence (ISTAR)
- Targeting support
- Logistics support
- Crisis Management
- Information Management
- Rules of Engagement (ROE)
- Geographical Services
- Artillery Fire Support

Kombinering av data fra flere informasjonskilder vil bli viktigere etter hvert som det oppnås interoperabilitet med flere. For å kunne se situasjonsinformasjon i samme bilde må tjenester for datakombinering og fusjon utvikles.

I tillegg beskrev vi i målbildebeskrivelsen for 2014 noen generiske COI-spesifikke tjenester. Disse kan også inngå her.

5.1.4 K2 oversettingstjenester og -mekanismer

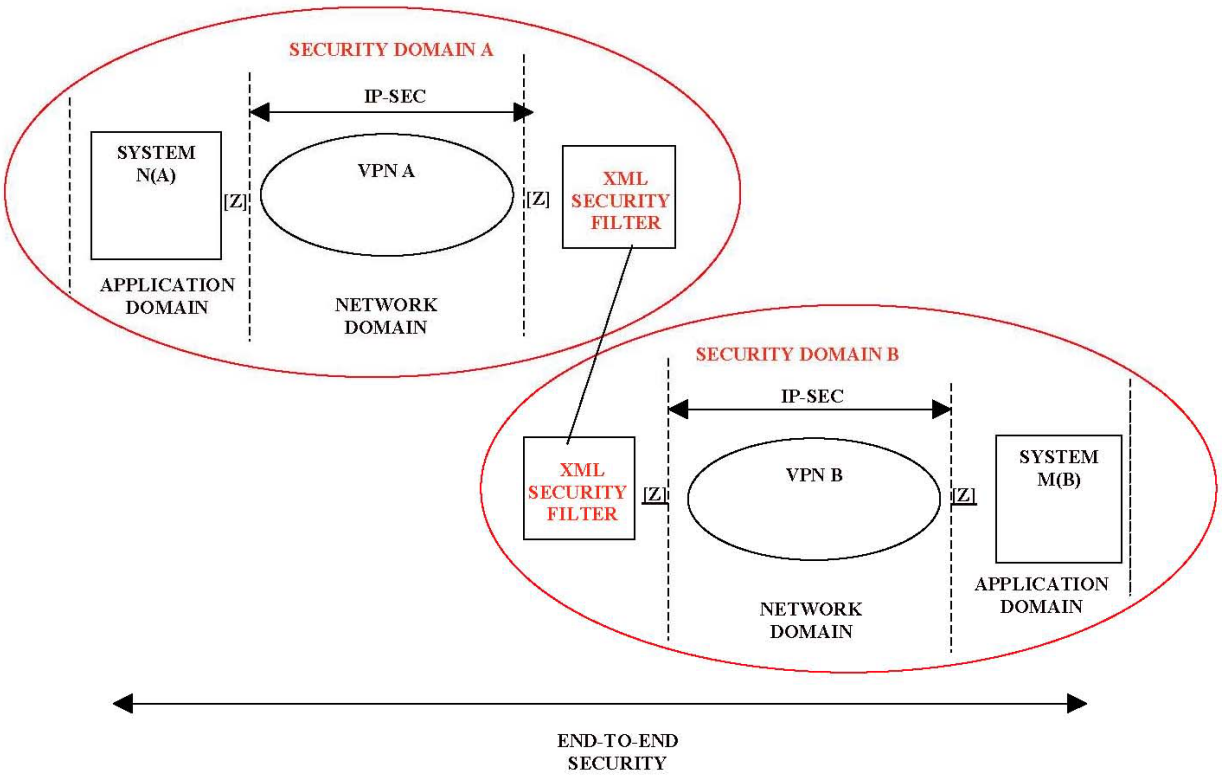
Med oversettingstjenester mener vi tjenester som sørger for informasjon inn til systemet, ut fra systemet, eller begge deler. Noen av disse vil være COI-spesifikke. Dette fordi man vil ha behov for å oversette mellom forskjellige formater innen et COI, og ikke alltid vil benytte deklarative måter å oversette på. Deklarativ oversetting gjør at man kan benytte mer generelle (kjerne-) tjenester for oversetting istedenfor å ha dedikerte oversettingstjenester. Et eksempel på deklarativ oversetting er XML-transformasjoner. Oversetting er nødvendig for å sikre interoperabilitet med samarbeidspartnere, og slike tjenester bør kunne legges til etter hvert som nye formater kommer til. Siden vi ikke kan forvente noen endring i kommunikasjonsløsninger frem mot 2008, bør utviklingen av en ny løsning ta hensyn til dagens kommunikasjonsløsninger og meldingsformater. Dette kan gjøres ved å pakke inn dagens formater som egne tjenester som leverer XML, og gjøre mappinger og XML-transformasjoner inn mot et felles COI-format. Figur 5.2 introduserer NATO XML og (nasjonal) Blue Force Tracking (BFT) som nye formater

som kan komme til å dukke opp i nær fremtid. Videre bør alle viktige meldingsformater som er i bruk i dag inngå i en ny løsning.

5.2 Sikkerhet

Sikkerhetsløsningene som er skissert for målbildet 2014 forutsetter vesentlige endringer i security policy. For målbilde 2008 vil det være lite trolig at man har klart å bevege seg bort fra den tradisjonelle inndelingen av informasjon i sikkerhetsdomener. Det man kan forsøke å få til i dette perspektivet er en mer automatisert flyt av informasjon mellom sikkerhetsdomenene. For å sende informasjon fra lavt nivå til høyt nivå eller mellom sikkerhetsdomener på samme graderingsnivå (for eksempel mellom nasjonal Hemmelig og NATO Secret), vil det være mulig å automatisere en filterfunksjon (dette gjøres til en viss grad i dagens formelle meldingssystem - MIF). Utfordringen ligger i å automatisere utvekslingen av informasjon fra høyt nivå til lavt nivå (for eksempel sende Begrenset informasjon fra et System High Hemmelig domene til et Begrenset domene), hvis det skulle være behov for det i 2008. Det vil være nødvendig å analysere behovet for informasjonsutveksling mellom sikkerhetsdomener og vurdere dette opp mot sikkerhetsløsningene som det vil være mulig å få akkreditert. Teknisk sett finnes løsningene, utfordringen ligger i å finne løsninger som lar seg akkreditere av sikkerhetsmyndighetene innenfor den sikkerhetspolicyen som vil gjelde i 2008. Det er lite trolig at den vil være vesentlig forskjellig fra dagens sikkerhetspolicy. En av de største utfordringene i realiseringen av et NBF på sikt, vil være å endre sikkerhetspolicy til å bli mer dynamisk i forhold til den reelle trusselen og risikoen.

I et 2008-perspektiv er det mest sannsynlig at man vil opprettholde bruk av IP-krypto for å sikre konfidensialiteten til informasjonen som utveksles mellom systemene/LANene i hvert sikkerhetsdomene. Som et supplement kan man vurdere å introdusere ende-til-ende sikkerhetstjenester for XML informasjon. Ende-til-ende sikkerhetstjenestene vil gjøre det mulig å beskytte informasjonen i selve systemene/LANene, samt åpne opp for muligheten til å kunne introdusere automatisert filtrering av informasjon mellom sikkerhetsdomener på samme nivå. Dette kan gjøres ved å binde sikkerhetsmerker som angir sensitiviteten til informasjonsobjektene ved bruk av digitale signaturer. Disse sikkerhetsmerkene kan deretter sjekkes av XML ”guards” når informasjonen er på vei inn og/eller ut av domenene. XML ”guard” funksjoner vil være nødvendig både i avsender- og mottakerdomenene. I et NBF må denne filterfunksjonen være automatisk for å møte kravene om sømløs informasjonsutveksling mellom alle involverte parter i en operasjon.



Figur 5.3 Utveksling av informasjon mellom to sikkerhetsdomener ved bruk av XML.

Figur 5.3 viser et eksempel på hvordan informasjonen som utveksles mellom to systemer M og N i to sikkerhetsdomener A og B, kan sikres. Innen hvert sikkerhetsdomene er det et applikasjonsdomene og et nettverksdomene. Informasjonen som utveksles innen hvert nettverksdomene blir beskyttet av IP kryptoapparater og danner sikre VPNs (Virtual Private Networks). Innen applikasjonsdomenet blir et sikkerhetsmerke bundet til informasjonen som skal utveksles ved bruk av en digital signatur. Signaturen og sikkerhetsmerket blir kontrollert for å avgjøre om det er tillatt å sende informasjonen til det andre sikkerhetsdomenet. På grensen til det andre domenet blir signaturen og sikkerhetsmerket kontrollert igjen for å forsikre seg om at informasjonen er sendt av en betrodd avsender (applikasjon/prosess/person) og at sikkerhetsmerke er i henhold til sikkerhetspolicyen i dette sikkerhetsdomenet. XML-informasjonen kan i tillegg være kryptert for å oppnå ende-til-ende konfidensialitet bl.a. for strengere need-to-know separasjon av informasjonen.

Den største utfordringen med å få godkjent dette konseptet vil være å utvikle løsninger med nok tiltro til den prosessen som påfører sikkerhetsmerket og kryptografisk binder dette til informasjonen med en digital signatur.

5.3 Teknologianbefalinger

Basert på behov og krav vi antar Forsvaret vil ha i fremtiden, ledende forskning og trender samt teknologisk status i dag (kapittel 3) kan vi komme frem til følgende teknologianbefalinger i et 2008-perspektiv.

Vi mener at SOA er det beste arkitekturprinsippet å bygge en ny K2IS-løsning på. Dette på grunn av at Forsvaret, og dermed også løsningene, må være best mulig rustet til å møte nye utfordringer. Et eksempel på dette kan være interoperabilitet med tjenester for operative støttefunksjoner. Siden både Web Services og XML er plattformuavhengige og åpne standarder vil bruk av disse standardene støtte interoperabilitet med nye samarbeidspartnere og gjenbruk i best mulig grad. Forskning på teknologier innen SOA og semantisk interoperabilitet bygger videre på XML og Web Services, slik at dette vil utgjøre et godt fundament å bygge en dynamisk NBF-løsning på. Leverandører av utviklingsverktøy, mellomvareprodukter og konsulentfirmaer har omfavnet SOA som et arkitekturprinsipp. Det er spesielt SOA realisert med teknologiene Web Services og XML som er gjenstand for mye oppmerksomhet. En rekke viktige teknologier som utfyller basisteknologiene vil bli tilgjengelige i perioden frem mot 2008.

På grunn av dette mener vi at XML-baserte Web Services (basert på SOAP og WSDL) bør benyttes der det er mulig. Dette fordi disse teknologiene er i ferd med å bli en standard for syntaktisk interoperabilitet mellom systemer som kjøres på forskjellige plattformer (maskinvare, operativsystem og programmeringsspråk). Følgelig kan man i fremtiden, forutsatt en datamodell som nevnt over, komponere tjenester basert på behovene i organisasjonen.

Vi anbefaler at tjenester som en hovedregel utvikles ved hjelp av Web Services-teknologi (SOAP og WSDL), og er basert på samme datamodell. Innholdet i Web Services-meldinger bør være XML, spesifisert ved hjelp av et XML Schema. For transformasjoner bør XSL/XSLT benyttes der man går fra ett XML-format til et annet XML-format. For innpakking av eksisterende meldingsformater, trengs sannsynligvis programkode som sjekker feil etc.

Selv om Web Services-teknologiene er åpne standarder, gir de dessverre rom for valgmuligheter som kan begrense interoperabilitet med andre systemer. Organisasjonen WS-Interoperability (WS-I) arbeider med å profilere standardene, slik at man kan oppnå interoperabilitet ved å følge profilene til WS-I. Det anbefales at både profiler og best practices utarbeidet av WS-I følges (17).

Det er videre en rekke utviklingsverktøy som støtter automatisk generering av WSDL tjenestebeskrivelser (11) fra programkode (for eksempel Java). Dette frarådes, da status i dag er at man får mindre kontroll over grensesnittene, som er det viktigste elementet i en SOA. Vi anbefaler en WSDL-først-tilnærming, basert på en felles COI-datamodell.

I en fullverdig SOA inngår oppslag etter tjenester, koordinering, og støtte for ruting og mellomlagring av SOAP-meldinger. Annen funksjonalitet kan være notification, management, transformasjon, logging og sikkerhet. Alt dette er tjenester som i varierende grad inngår i en ESB.

Det er imidlertid en viktig forskjell mellom eBusiness og en operativ løsning: På lavere nivå vil vi nemlig ha behov for å kjøre flere instanser av den tjenesteorienterte arkitekturen, potensielt på

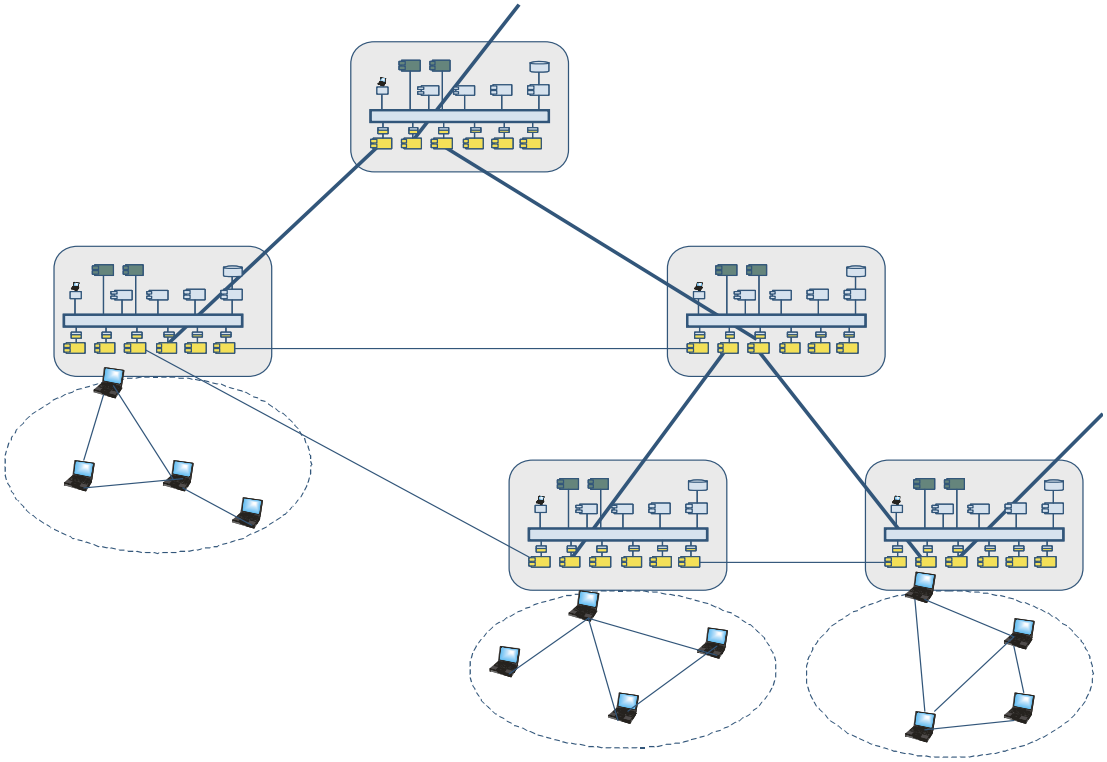
én maskin. Dette kan løses ved hjelp av en lettvekts-ESB eller BPEL-motor. En slik BPEL-motor er ofte en del av en ESB. Det er viktig å vurdere lisenskostnader i lys av dette.

Imidlertid kan XML og Web Services i dag i noen tilfeller medføre utfordringer, og da spesielt der en har strenge krav til batterikapasitet i forbindelse med kjøring av en SOA-instans på for eksempel en bærbar PC. Det er usikkert for oss om Forsvaret har slike behov i forbindelse med en ny løsning. I tillegg finnes det allerede løsninger for dette i dagens systemer. Dersom Forsvaret har et slikt behov kan en åpne for mer optimaliserte og proprietære løsninger mellom tjenester, inntil åpne standarder for effektiv eller binær XML foreligger. Dette kan for eksempel innebære bruk av proprietære løsninger for effektiv eller binær XML.

5.4 Eksempel på løsningsoppsett

Figur 5.4 viser et eksempel på et oppsett basert på en tenkt løsning med begrensede ressurser på laveste nivå. De avrundede rektanglene i figuren skal illustrere tjenesteorienterte instanser av systemet der man ikke er begrenset av eksisterende, monolittiske og lukkede terminaler. Dette kan for eksempel være kommandoplasser. De tykke linjene mellom rektanglene illustrerer kommunikasjonslinjer med god båndbredde. Her kan Web Services benyttes. De tynne linjene illustrerer kommunikasjonslinjer med dårlig kapasitet. Her må sannsynligvis eksisterende eller proprietære løsninger benyttes i større grad, kanskje også på grunn av interoperabilitet. Vi har også illustrert flere trådløse nettverk (ellipser), da det særlig er noder i slike nettverk som ikke umiddelbart kan kjøre Web Services. Vi får dermed et skille mellom noder i løsningen som kan kommunisere ved hjelp av mange meldingsformater, og noder som bare kommuniserer ved hjelp av ett format. Dette vil også kunne være avgjørende for informasjonsdelingens struktur, da man potensielt må ett eller flere nivåer opp i hierarkiet for å få gjort en oversettelse mellom to formater.

I figuren kjøres fem instanser av systemet (representert som grå rektangler). Disse kjører hver sin SOA-instans, og kan konfigureres til oppgaven som skal utføres på de forskjellige lokasjonene. Vi ser at noen trådløse systemer kjører sine egne løsninger, men at de logisk kan knyttes sammen ved å benytte SOA-løsningen på et høyere nivå, for deretter å kommunisere på tvers, og ned igjen. Denne formen for logisk konnektivitet vil ivareta arven på en best mulig måte, til tross for at systemene på laveste nivå ikke alltid er interoperable.



Figur 5.4 Eksempel på systemkonfigurasjon

Konnektivitet mellom slike nettverk og noder er avhengig av løsningen for den spesifikke terminal, men på sikt er det mulig å tenke seg XML-basert og kanskje også Web Services-basert kommunikasjon i og mellom slike nettverk.

En annen dimensjon som også bør diskuteres i denne sammenheng, er sikkerhet, og koblingen mellom forskjellige sikkerhetsnivåer og nettverk. Dette kan vise seg å bli det største hinderet for interoperabilitet i et NBF, og må få spesiell oppmerksomhet.

6 KONKLUSJON OG ANBEFALING

6.1 Konklusjon

Hensikten med å beskrive et målbilde med 2008-perspektiv må være å stake ut en kurs som er i samsvar med de mer langsiktige målene. Vi har tatt utgangspunkt i og beskrevet en fremtidsvisjon for 2014, hvorav vi har avledet en løsning for 2008 som et skritt på veien. På denne måten blir løsningen en investering i en grunnmur å bygge videre på i fremtiden.

Vi mener at SOA er det beste arkitekturprinsippet å bygge en ny K2IS-løsning på. Dette på grunn av at Forsvaret, og dermed også løsningene, må være best mulig rustet til å møte nye utfordringer. Vi anbefaler at tjenester som en hovedregel utvikles ved hjelp av Web Services-teknologi (SOAP og WSDL), og er basert på samme datamodell. Innholdet i Web Services-

meldinger bør være XML, spesifisert ved hjelp av et XML Schema.

Basert på behov og krav vi antar Forsvaret vil ha i fremtiden, ledende forskning og trender samt teknologisk status i dag (kapittel 3), har vi kommet frem til at følgende elementer bør inngå i et 2008-målbilde:

- En tjenesteorientert arkitektur basert på åpne standarder
- Et sett av kjernetjenester
- En opprettelse av interessegruppen K2
- Utvikling av en datamodell for interessegruppen K2
- Spesifikke tjenester for interessegruppen K2

Vi ser for oss at en 2008-løsning består av en interessegruppe K2, som utvikler en datamodell for K2-informasjon. Videre utvikles et sett med kjernetjenester og et sett med K2-spesifikke tjenester som også inkluderer oversettingstjenester. Disse tar imot informasjon på andre formater fra produsenter, og tilbyr informasjon ut til konsumenter. Et hovedmål for en 2008-løsning blir: *En fleksibel portefølje av funksjonalitet som støtter toveis informasjonsdeling.*

Løsningen bør i perioden frem mot 2008 baseres på et minimum av ny funksjonalitet som er basert på reelle behov. En slik tjenesteorientert arkitektur, basert på XML og Web Services vil gjøre løsningen klar for neste generasjon SOA-teknologi, basert på semantikk.

Det viktigste er ikke å bruke XML/WS for enhver pris. Eksisterende formater vil etter alt å dømme benyttes i lang tid fremover, og bruk av XML og Web Services kan medføre problemer i visse tilfeller, spesielt ved lav båndbredde og batterikapasitet. Dette kan for eksempel åpne for mer optimaliserte og proprietære løsninger mellom tjenester, inntil åpne standarder for effektiv eller binær XML foreligger. Grunnen til at vi anbefaler XML og Web Services som et fundament, er at vi i fremtiden ser semantisk teknologi som en naturlig videreføring av denne familien av teknologier.

Selv om Web Services-teknologiene er åpne standarder, gir de dessverre rom for valgmuligheter som kan begrense interoperabilitet med andre systemer. Det anbefales at både profiler og best practices utarbeidet av WS-Interoperability følges (17).

Dersom Forsvaret velger å gå i retning av en tjenesteorientert løsning, vil det være flere roller som må ivaretas. Vi mener at Forsvaret selv bør ta et arkitektansvar, for å sikre at porteføljen av tjenester ivaretar organisasjonens behov på best mulig måte. Personen(e) som fyller en slik rolle bør være involvert i all ny- og videreutvikling. På denne måten vil man ha forsvarsansatte personer som er med på en evolusjonær utvikling fra dagens systemer til en enkel SOA i 2008, til en mer automatisert og interoperabel (basert på informasjonssikkerhet) SOA i 2014. En slik arkitekt(-gruppe) bør også ha en deltakende representant i datamodelleringsarbeidet for de forskjellige interessegruppene.

Vi vil poengtere at det beskrevne målbildet for 2008 ikke gir noe grunnlag for å velge en strategi

der ett av dagens operative systemer velges som basis for ny løsning. Målbildet åpner derimot opp for en annen mulig strategi hvor de aktuelle systemene integreres over tid, slik at man til slutt ender opp med ett system.

6.2 Anbefaling til fremtidig konsept

Videre mener vi at følgende elementer bør utgjøre et målbilde for tjenesteinfrastrukturen i 2014:

- En tjenesteorientert arkitektur basert på åpne standarder (Web Services og XML)
- Et sett av kjernetjenester
- En inndeling av brukere i interessegrupper med en ontologi (formell datamodell) for hver interessegruppe
- Spesifikke tjenester for hver interessegruppe
- Systemet kan komponeres etter behov, basert på prosessflyt
- Fleksibel sikkerhet på informasjonsnivå

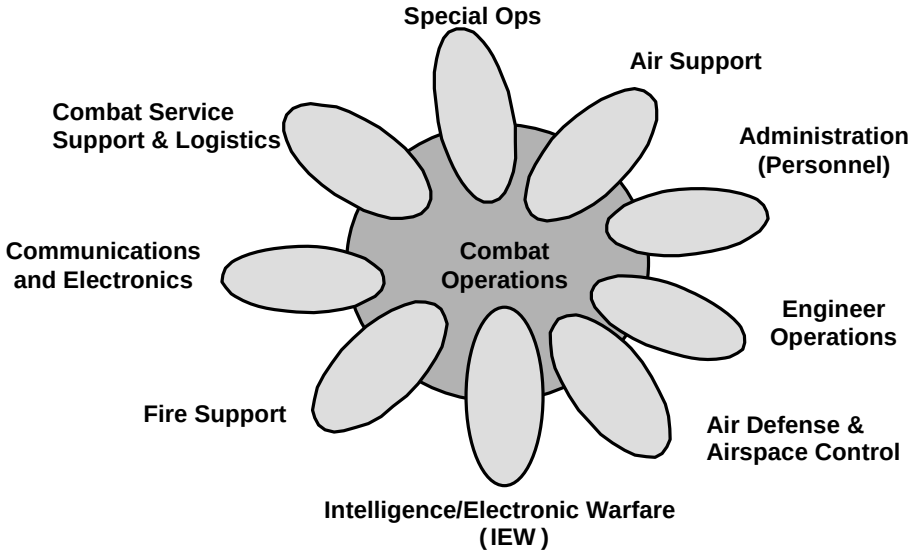
I et 2014-perspektiv ser vi for oss tjenesteinfrastruktur-delen av INI realisert som en tjenesteorientert arkitektur, med to hovedkategorier tjenester; kjernetjenester og tjenester som er mer spesifikke for en interessegruppe. Videre er den tjenesteorienterte arkitekturen basert på ontologier (formelle datamodeller) for å sikre at tjenester er interoperable.
Vi anbefaler å vente med innføring av semantisk teknologi inntil verktøystøtte og bedre erfaring med dette er på plass. Vi vil likevel nok en gang fremheve viktigheten av en konsistent informasjonsmodell som grunnlag for de forskjellige XML Schema som benyttes som grunnlag for overføring av meldinger.

Sikkerhetsløsningene som er skissert for målbildet 2014 forutsetter vesentlige endringer i security policy. For målbilde 2008 vil det være lite trolig at den vil være vesentlig forskjellig fra dagens sikkerhetspolicy. Det man kan forsøke å få til i dette perspektivet er bedre ”need-to-know” separasjon og evt. en mer automatisert flyt av informasjon mellom sikkerhetsdomenene. Teknisk sett finnes løsningene, utfordringen ligger i å finne løsninger som lar seg akkreditere av sikkerhetsmyndighetene innenfor den sikkerhetspolicyen som vil gjelde i 2008. En av de største utfordringene i realiseringen av et NBF på sikt, vil være å endre sikkerhetspolicy til å bli mer dynamisk i forhold til den reelle trusselen og risikoen.

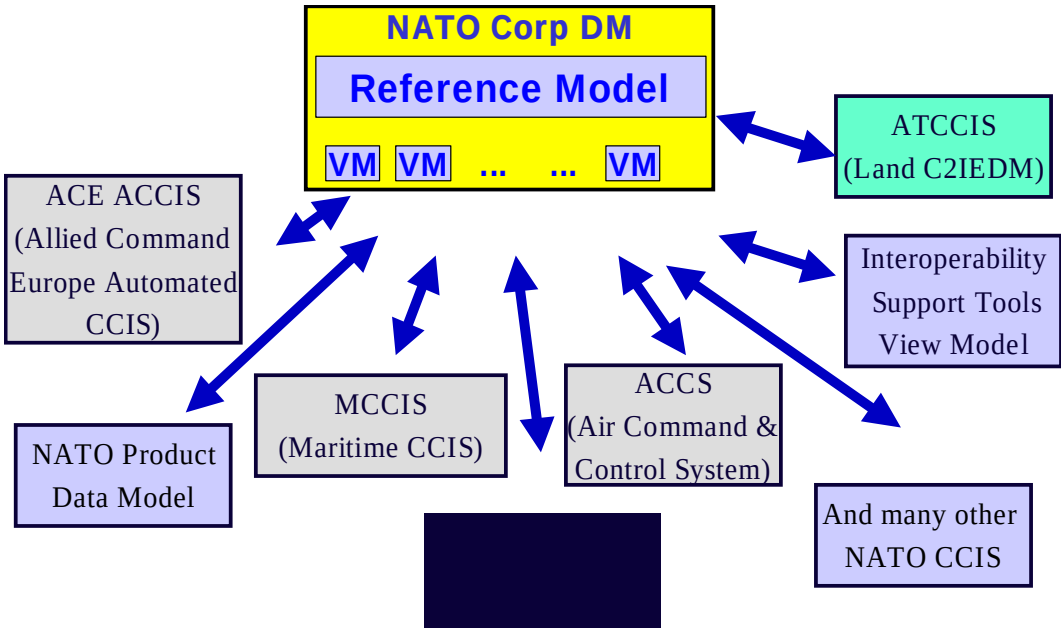
APPENDIKS

DATAMODELLERING OG BRUK AV COI

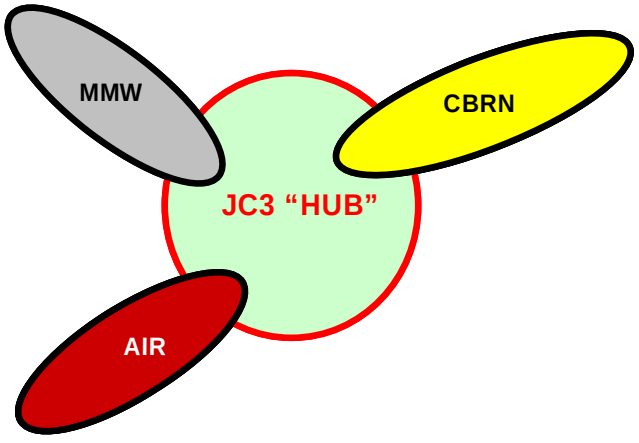
Ved oppstarten av datamodelleringen i Army Tactical Command and Control Information System (ATCCIS) i 1992, startet man med å definere en kjerne for kommando og kontroll, kalt Generic Hub. Dette var en utvekslingsmodell for informasjonsbehov mellom allierte hærstyrker. Rundt denne kjernen så man for seg at flere funksjonelle områder (COI) ville grense inn, men samtidig ha en del informasjonsbehov som ikke var relevant i kjernen, se figur nedenfor. Initielt startet man med å se på Ildstøtte, Ingeniør, Personelladministrasjon og Kommunikasjon, og fikk dermed innspill til hva som burde inngå i kjernen.



I 2000 besluttet NATO Data Administration Group seg for å lage en felles datamodell for NATO ved å ta utgangspunkt i Generic Hub fra ATCCIS. Dette skulle være en samlemodell som het Reference Model, mens forskjellige brukermiljøer (COI) kunne ha sin egen View Model. En VM ville inneholde en del som var felles med RM (et subsett), men kunne også inneholde informasjon utover det som fantes i RM. Figuren nedenfor viser tankegangen.



Tankegangen fra ATCCIS er også videreført etter sammenslåingen med Multilateral Interoperability Programme (MIP). Utviklingen av en felles datamodell for NATO har nå blitt et samarbeid mellom NDAG og MIP. Nå brukes også COI som begrep aktivt. Det beste eksemplet er CBRN-miljøet (tidligere kjent som NBC eller ABC). Med utgangspunkt i MIP-modellen har de laget seg en utvidelse som dekker deres behov innenfor sitt COI. Dette er en omfattende utvidelse, men det er kun de deler som de mener er relevante utenfor deres COI som de foreslår som utvidelser til den felles utvekslingsmodellen. Dette er illustrert i figuren nedenfor, og representerer fortsatt samme prinsippet som ble lagt til grunn i ATCCIS, selv om omfanget av kjernen er utvidet.



UTVEKSLINGSMETODER

I forbindelse med informasjonsutveksling, er det store skillet mellom strukturert og ustrukturert informasjon. Ustrukturert informasjon kan deles ved fildeling, web-sider, e-post osv. Svært mye informasjonsutveksling over landegrensene har vært ustrukturert. Selv om dette er til stor hjelp, så krever det fullstendig manuell behandling. Det kan selv for en operatør være tidkrevende å finne fram til essensen, siden det ikke er noen kjent struktur i informasjonen.

For å få mulighet til å behandle informasjon mer effektivt, har man innført varierende grad av struktur på den. En god tilnærming for menneskelig behandling er gruppering under faste punkter, slik som NATO har gjort i Information Exchange Requirements (IER). For å kunne benytte seg av datastøtte, må imidlertid strukturen være enda fastere. Ved å spesifisere syntaks og innhold i detalj får vi formaterte meldinger.

Det er to former for strukturert informasjonsutveksling som gjerne betraktes som ’motpoler’; meldingsutveksling og databasereplikasjon. Den prinsipielle forskjellen er imidlertid svært liten, det er valg som er gjort underveis i arbeidet med de forskjellige løsningene som har skapt forskjellene.

XML er en sivil standard som har fått stor utbredelse de siste årene, og som også har blitt tatt i bruk i militær sammenheng. XML har også fokus på informasjonsoverføring, men på et litt annet nivå. Mens meldinger og replikasjon har fokus på innholdet som skal overføres, er XML mer fokusert på hvordan dette innholdet skal formateres. XML kan benyttes både i forbindelse med meldinger og replikasjon, og både ADatP-3 og MIP har utviklet XML-representasjoner. Tilgangen på sivile verktøy reduserer behovet for spesialutviklet programvare, og gjør at det blir både lettere og billigere å implementere den overføringsmetoden man ønsker.

Interoperabilitet

I henhold til interoperabilitetsnivåene definert i NATO Policy for C3 Interoperability (hvor 0 er dårligst og 4 er best), medfører meldingsutveksling interoperabilitet på nivå 2, mens databasereplikasjon gir nivå 4. Tradisjonell meldingsutveksling som konsept krever manuelle inngrep, og kommer derfor på et lavere nivå for interoperabilitet enn replikasjon.

Meldinger

Meldinger er den eldste av dagens utvekslingsmetoder, og ble utviklet med tanke på bruk av telex eller lignende. Kravet om at innholdet måtte være menneskelesbart var da åpenbart. Dagens situasjon er at det kan forventes datamaskinstøtte både hos sender og mottager. Behovet for at meldingene skal kunne leses direkte av et menneske har derfor i praksis forsvunnet.

En melding inneholder et forhåndsdefinert oppsett av hva slags informasjon som skal sendes fra hvem til hvem under gitte forhold (eventuelt som periodisk statusrapport). Dette oppsettet er i

henhold til en felles syntaks for et sett av meldinger, men beskriver bare selve strukturen i meldingen.

Det er imidlertid normalt ingen felles beskrivelse for flere meldinger av hva slags informasjon som kan inngå i de forskjellige feltene. Det betyr at hver enkelt melding inneholder beskrivelsen av hva som kan stå i de forskjellige feltene. Denne beskrivelsen er ikke dokumentert utenfor meldingen, og det sies at meldingen kun har en implisitt datamodell. Dette medfører at det ofte er inkonsistenser mellom de implisitte datamodellene i de forskjellige meldingene.

Det er denne mangelen på en felles eksplisitt datamodell som er det grunnleggende problemet med det meste som finnes av meldinger i dag. Det var ikke noe behov for dette da utviklingsarbeidet startet, siden sendt og mottatt informasjon typisk ble lagret på papir. Sammenstillingen av informasjonen ble gjort i operatørenes hoder. I dagens situasjon er imidlertid tilgangen på informasjonen så stor, og tilgjengelig behandlingstid så lav, at operatørene trenger datamaskinstøtte. Derfor trenger man i dagens KKI-systemer å lagre innholdet i alle meldingene på en slik måte at totalbildet enkelt kan hentes ut igjen. Derfor må alle meldingene være innbyrdes konsistente, dvs at de overlappende delene må være definert ut fra samme ’verdensbilde’.

En sideeffekt av manglende eksplisitt datamodell i bunnen er at meldingene ikke inneholder entydige referanser til det meldingene refererer til (databasenøkler), slik at det er vanskelig for et datasystem å identifisere om en melding inneholder en oppdatering for et allerede kjent objekt, eller om det er et nytt objekt av samme type. Ved menneskelig behandling vil dette i de fleste tilfellene være klart for operatøren.

Bruk av meldingsformater

Innen NATO i dag finnes det flere meldingsformater som er i bruk. På landsiden er det ADatP-3 (27) som er det mest brukte formatet. Selv om dette er en ratifisert STANAG, så virker det som om bruken har vært mest internt i nasjoner. Mellom nasjoner har det vært et problem at det er forskjellige versjoner som er implementert i landene, samtidig som problemene nevnt over har medført at det har vært behov for å gjøre nasjonale tilpasninger for å bruke meldingene sammen med databaser. Meldingene i ADatP-3 er nå spesifisert i XML. Dette fører til at man ikke lenger trenger egenutviklede verktøy for å lese meldingene, og bidrar dermed til lavere kostnader og lettere bruk. De mer fundamentale problemene er imidlertid ikke løst.

Innen luft og sjø er det taktiske datalinker som er dominerende. Link 1, Link11 og Link14 har vært mye brukt, og Link 16 er nå vedtatt innført i Norge. Link-systemene kommer generelt mer som ’pakkeløsninger’, dvs at de også kommer sammen med hardware som har meldingsstandarden ferdig implementert. Dette har nok bidratt til større utbredelse enn for ADatP-3, men også her finnes det problemer med implementeringer som ikke snakker sammen. Ulempen med slike ferdige løsninger er at det blir et mer lukket system, slik at det blir verre å få til interoperabilitet med andre deler av Forsvaret.

OTH (Over-The-Horizon) Gold er et annet meldingsformat som er i bruk på sjøsiden. Dette er ikke en NATO-standard, men ligner utseendemessig på ADatP-3. OTH Gold har fokus på bildeoppbygging, som ADatP-3 støtter dårlig, slik at de to formatene utfyller hverandre godt. De overlappende delene er imidlertid ikke likt definert.

Det har i en årrekke nå eksistert et forum for interoperabilitetstester kalt CWID (Coalition Warrior Interoperability Demonstration) eller tidligere JWID (Joint WID). Nasjonene har her deltatt med systemer som er i operativ bruk. Bruk av tradisjonelle meldinger har tidligere vært enerådende her, men fra 2005 har de fleste nasjonene også hatt muligheter for å teste databasereplikasjon (MIP-løsning).

Databasereplikasjon

Etter hvert som bruk av databaser har gjort sitt inntog i så vel sivile som militære systemer, har det også blitt utviklet metoder for automatisk flytting av informasjon mellom databasene. I den sammenheng er det ikke noe krav om at informasjonen skal være menneskelesbar, ellers ligner replikasjon mye på meldinger. Man snakker gjerne om kontrakter i forbindelse med replikasjon, og hvis ønskelig kan man etablere kontrakter som tilsvarer de tradisjonelle meldingene. Ved replikasjon unngår man de problemene som meldingsbaserte systemer tradisjonelt er designet med. På den annen side forutsetter replikasjon at partene har en felles utvekslingsmodell som systemene forholder seg til. Det er ikke nødvendig at systemene bruker samme modell internt, men de være enige om en felles plattform for selve utvekslingen. Dette kan ses på som en begrensning.

Bruk av databasereplikasjon

Databasereplikasjon som teknologi har vært i bruk lenge, men har til nå vært mest brukt for informasjonsutveksling internt i systemer, dvs mellom noder som har samme system installert. For utveksling mellom systemer og nasjoner, kanskje basert på upålitelige kommunikasjonslinjer, er imidlertid databasereplikasjon relativt nytt.

En viktig grunn til at databasereplikasjon ikke har fått større gjennomslag tidligere er nettopp mangelen på et felles grensesnitt som kreves for å bruke replikasjon mellom ulike systemer. MIP (26) har som målsetting å gjøre noe med dette, og har en datamodell som er det beste initiativet i så måte innen NATO. Etter hvert som systemer basert på MIP-spesifikasjonene kommer i operativ bruk vil de få en felles datamodell å forholde seg til. Datamodellen i MIP er selve fundamentet som gjør at ellers ganske forskjellige systemer kan ha en felles basis for informasjonsutvekslingen.

En annen medvirkende faktor til liten utbredelse kan være en viss skepsis fra operative. Siden databasereplikasjon i prinsippet oppdaterer en annen database automatisk, og også sender informasjon til andre automatisk, føler en del operative at de mister kontrollen på hva som legges inn eller videresendes. Med den informasjonsmengden som er tilgjengelig i dag, er det imidlertid vanskelig å se for seg at en person kan holde kontroll over alle detaljer og samtidig

fatte riktige beslutninger. Man kan velge å motta informasjon fra/sende til bare de man stoler fullt på, og man kan også velge ut hva slags type informasjon man vil motta/sende. Etter hvert som de operative blir mer vant til datamaskiner, og de ser at de er et godt hjelpemiddel til å utføre de mer administrative rutinene, vil trolig også skepsisen avta.

Som nevnt over har også MIP replikasjonsmekanisme nå blitt tatt i bruk under CWID. Det er all grunn til å anta at omfanget av den tradisjonelle meldingsbruken vil bli sterkt redusert til neste år, til fordel for databasereplikasjon og XML-meldinger.

Bruk av XML i MIP

Hovedprinsippet for databasereplikasjonen i MIP har vært at både mottager og sender har en relasjonsdatabase, og at de forholder seg til samme utvekslingsmodell. Det vil imidlertid ikke alltid være tilfelle at alle parter har implementert replikasjonsmekanismen. Det er derfor behov for å finne metoder for å formidle informasjon til andre, uten å benytte databasereplikasjon.

For å løse dette problemet har MIP tatt i bruk XML. Hensikten er at man skal kunne sende informasjon til andre uavhengig av hva slags løsning de har. En mulighet er å tilby informasjon fra MIP gjennom Web Services og XML-meldinger. For å kunne tilby dette, er det utviklet XML-skjemaer som kan omdanne innholdet i databaser til XML-filer. Dermed kan man sende informasjon til databaser som ikke har implementert en MIP-replikasjonsmekanisme.

I den sammenheng er det utviklet en XML Exchange Mechanism (XEM), som vil være en tredje utvekslingsløsning fra MIP i neste versjon. Den er imidlertid tenkt brukt sammen med eksisterende løsninger for meldinger eller replikasjon. I prinsippet kan denne utvides til å erstatte den eksisterende DEM, men siden XML foreløpig har problemer med ineffektiv båndbreddebruk, er ikke dette noen anbefalt løsning på kort sikt. Det er imidlertid grunn til å anta at mer effektiv XML vil komme relativt snart, siden det er stor etterspørsel etter dette. På sikt kan det tenkes at XEM og DEM vil smelte sammen, siden replikasjonsmekanismen inneholder prosedyrer for å sikre semantisk kompletthet, som mangler i XEM.

Vurdering

I NATO er det veletablerte miljøer for både meldinger og datamodellering/ replikasjon, i form av to undergrupper av SC 5 ISSC under NC3Board, nemlig MTF og NDAG. Dessverre er ikke koblingen mellom disse gruppene god nok. NATO har erkjent behovet for utvikling av en felles utvekslingsmodell for NATO (gjennom NDAGs samarbeid med MIP), men MTF har så langt ikke begynt å bruke denne modellen som utgangspunkt for meldingene. Ved å gjøre dette, kunne man blitt kvitt problemene som er knyttet til meldingene.

Utvikling av nye KKI-systemer bør baseres på NATOs felles datamodell (STANAG 5525) og en utvekslingsmetode tilpasset denne. Selv om meldingene utviklet i NATO også er en standard, er det ikke hensiktsmessig å basere seg på disse før det har foregått en grundig gjennomgang for å gjøre dem konsistente.

MODENHET TEKNOLOGI

Vi presenterer her en grov oversikt over standardiseringsarbeid som pågår eller er fullført. Dette for å illustrere både hva som er tilgjengelig og for å illustrere utfordringene som man har i standardiseringsarbeidet. Vi følger samme inndeling som i kapittel 3.

Syntaks/meldingsformat

Teknologi	***Org.***	***Bruksområde***	***Modenhet***	***Impl.***	***Kommentar***
XML	W3C	Syntaks	Standard	Ja	
XML Schema Definition	W3C	Validering	Standard	Ja	
XSL(T)	W3C	Transformasjon	Standard	Ja	
Fast XML	ITU	Effektiv, generell koding	?	Ja	Bruker ASN.1 for mer effektiv koding
Binary XML	W3C	Binær koding	2007 ?	Proprietær	Ikke standardisert

Meldingstransport

Teknologi	***Org.***	***Bruksområde***	***Modenhet***	***Impl.***	***Kommentar***
SOAP	W3C	Transport	Standard		Gjelder versjon 1.2. Versjon 1.1. er ikke standardisert
SOAP/UDP	[Microsoft]	Transport	2005 ?		Ikke standardisert
WS-Attachments	IBM, Microsoft	Vedlegg			
SOAP w/Attachments	HP, Microsoft	Vedlegg			
MTOM	W3C	Vedlegg	Standard		Vil ta over etter WS-Attachments
WS-Addressing	W3C	Endepunkt-adressering	Standard 2005	Ja	
WS-Eventing	Microsoft, BEA ++	Publish-Subscribe			Ikke standardisert
WS-Notification	OASIS, IBM, HP ++	Publish-Subscribe		Ja	Ikke standardisert
WS-Reliability	OASIS	Garantert levering	Standard		
WS-ReliableMessaging	IBM, Microsoft	Garantert levering		Ja	

Beskrivelse og søk

Teknologi	*Organisasjon*	*Bruksområde*	*Modenhet*	*Impl.*	*Kommentar*
WSDL	W3C	Tjenestebeskrivelse		Ja	Verken 1.1 eller 2.0 er standardisert, men 1.1 er stabil
UDDI	OASIS	Tjenesteregister	Standard	Ja	
WS-Discovery	Microsoft, BEA, Canon, webMethods	Tjenestesøk på lokalnett			Ikke standardisert
WS-Policy	SAP, IBM, Microsoft, BEA	Rammeverk for policy	2005 ?		

Orkestrering og koordinering

Teknologi	*Org.*	*Bruksområde*	*Modenhet*	*Impl.*	*Kommentar*
WS-BPEL	OASIS	Prosessflyt	2005	Ja	
WS-Management	Microsoft, Sun			Ja	
WSDM	OASIS, HP, IBM, CA	Management	Standard	Ja	

Semantikk og regler

Teknologi	*Org.*	*Bruksområde*	*Modenhet*	*Impl.*	*Kommentar*
OWL	W3C	Ontologibeskrivelse	Standard	Ja	
RuleML	RuleML Initiative	Syntaks for regler	Standard	Ja	Har som mål en W3C-fremleggelse
RDF	W3C	Syntaks for setninger	Standard	Ja	
SPARQL	W3C	Spørringer på RDF-data			

Sikkerhet

Teknologi	*Org.*	*Bruksområde*	*Modenhet*	*Impl.*	*Kommentar*
XML Signature	W3C	Signering	Standard		
XML Encryption	W3C	Kryptering	Standard		
SAML	OASIS	Security Token	2005		
WS-Security	OASIS	Sikkerhetsrammeverk	Standard	Ja	
WS-Trust	Div. Industri	Etablering av “trust relationships”			Ikke standardisert
WS-SecureConversation	Div. Industri	Etablering og bruk av “security contexts”			Ikke standardisert
WS-Federation	Div. industri	Administrasjon av “trust relationships”			Ikke standardisert
XKMS	W3C	Distribusjoj og registrering av offentlige nøkler	Standard		
XACML	OASIS	Definisjon og utveksling av security policy	Standard		

Litteratur

(1) Forsvarsdepartementet (2004): St.prp. nr. 42 (2003-2004), Den videre moderniseringen av Forsvaret i perioden 2005–2008.

(2) F.E.Moxley, C.P.Blackman (2004): Architecture Engineering: An Essential Role for Net-Centric Enablement within NATO, NATO RTO IST-042 Symposium on "Coalition C4ISR Architectures and Information Exchange Capabilities", Haag, 27-28 september 2004.

(3) FK KKIS (2005): Variantbegrensning og modularisering av eksisterende operative beslutningsstøttetjenester, Beslutningsunderlag (Rapport fra arbeidsgruppe april 2005).

(4) FD (2005): Strategiske initiativer for tilnærming til et nettverksbasert forsvar (22. juni 2005).

(5) OASIS (2005): Open Standards, Technology Report, OASIS Web page.

(6) T.Gagnes, A.Langmyr (2004): User-defined access to situation information services: an experiment, FFI/RAPPORT-2004/04171.

(7) S.A.Renner (2001): A "Community of Interest" Approach to Data Interoperability, Federal Database Colloquium '01, San Diego.

(8) US DoD (2003): Department of Defense Net-Centric Data Strategy.

(9) J.Lieberman, T.Pehle, M.Dean (2005): Semantic Evolution of Geospatial Web Services: Use Cases and Experiments in the Geospatial Semantic Web, W3C Workshop on Frameworks for Semantics in Web Services.

(10) OASIS (2005): Service Oriented Architecture Reference Model, Working Draft 07, OASIS Web page.

(11) T.Gagnes (2004): A Survey of Service-Oriented Architecures, Event-Driven Architectures and the Current State of Web Services Technology , FFI/NOTAT-2004/04264.

(12) Open Geospatial Consortium (2005): Open Geospatial Consortium Web Page, http://www.opengeospatial.org/.

(13) W3C (2005): Mobile Web Initiative web page, http://www.w3.org/2005/MWI/.

(14) Object Management Group (2005): UML web page, http://www.uml.org/.

(15) T.Gagnes (2004): A Survey of the Current State of The Semantic Web, FFI/NOTAT-2004/03985.

(16) McIlraith, S. A., Son, T. C., Zeng, H. (2001): Semantic Web Services, IEEE Intelligent Systems, vol. 16, no. 2, pp. 46-53.

(17) WS-I (2005): WS-Interoperability web page, http://www.ws-i.org/.

(18) P.Sandoz, A.Triglia, and S.Pericas-Geertsen (2004): Fast Infoset, Sun Developer Network.

(19) W3C (2005): XML Binary Characterization Working Group Public Page, http://www.w3.org/XML/Binary/.

(20) P.Sandoz, S.Pericas-Geertsen, K.Kawagutchi, M.Hadley, and E.Pelegri-Llopart (2003): Fast Web Services, Sun Developer Network.

(21) OASIS (2005): Web Services Business Process Execution Language Version 2.0, OASIS Web page.

(22) K.Müller (2000): NATO and XML, Proceedings of the XML Europe 2000 Conference.

(23) A. Eggen, R. Haakseth (2005): A Survey of solutions for end-to-end security when using JXTA or Web Services, FFI/NOTAT-2005/00332.

(24) FD (2005): Policy for militær tilpasning og anvendelse av informasjons- og kommunikasjonsteknologi i Forsvaret (september 2005).

(25) NC3A (2005): NATO Network Enabled Capability Feasibility Study, version 1.0.

(26) MIP (2004): The Joint C3 Information Exchange Data Model, version 0.5.

(27) MTFWG (2004): Allied Data Publication Number 3 Baseline 12.2.

(28) Hafnor et al (2005): Experiment Report: "Ad Hoc Organisation Of Picture Compilation And Situation Awareness In Nbd" - Battle Griffin 2005, FFI/RAPPORT-2005/01492.

(29) George Galdorisi et al (2004): Composable FORCEnet Command and Control: The Key to Energizing the Global Information Grid to Enable Superior Decision Making. (The 2004 Command and Control Research Technology Symposium).