FFI-rapport 2013/00932

Sluttrapport for FFI-prosjekt Tjenesteorientering og semantisk interoperabilitet i INI

Rolf Rasmussen, Trude H. Bloebaum, Eli Gjørven,
Jonas Halvorsen, Bjørn Jervell Hansen,
Raymond Haakseth, Frank T. Johnsen, Ketil Lund,
Nils A. Nordbotten, Espen Skjervold,
og Audun Stolpe

FFI Forsvarets forskningsinstitutt

Sluttrapport for FFI-prosjekt Tjenesteorientering og semantisk interoperabilitet i INI

Rolf Rasmussen, Trude H. Bloebaum, Eli Gjørven, Jonas Halvorsen, Bjørn Jervell Hansen, Raymond Haakseth, Frank T. Johnsen, Ketil Lund, Nils A. Nordbotten, Espen Skjervold, og Audun Stolpe

Forsvarets forskningsinstitutt (FFI)

15. juni 2013

FFI-rapport 2013/00932

1176

P: ISBN 978-82-464-2256-5
E: ISBN 978-82-464-2257-2

Emneord

Tjenesteorientering

Semantiske teknologier

Sikkerhetsløsninger

Informasjonsdeling

Arkitekturarbeid

Godkjent av

Rolf Rasmussen	Prosjektleder
Anders Eggen	Avdelingssjef

Sammendrag

Dette dokumentet gir en oversikt over arbeidet som er gjort i FFI-prosjekt 1176 *Tjenesteorientering og semantisk interoperabilitet i INI*. Rapporten er forsøkt holdt på et oversiktsnivå, dog slik at de enkelte temaene har fått en selvstendig forklaring. Prosjektets teknologiske innsatsområder og resultater blir oppsummert, og det er lagt vekt på å henvise til publikasjoner som prosjektet har medvirket til.

Basert på prosjektavtalens inndeling i fire områder har prosjektet vært gjennomført i form av fire parallelle aktivitetsområder: Tjenesteorientering, semantiske teknologier, sikkerhetsløsninger og arkitekturarbeid. Disse områdene berører en betydelig del av det som sammen med ulike former for kommunikasjonstjenester skal utgjøre det vi ser på som muliggjørende elementer i Forsvarets informasjonsinfrastruktur (INI).

De teknologiske resultatene fra prosjektet beskrives i underpunkter til hvert aktivitetsområde. I tillegg beskrives eksperimentinnsats og utvalgte internasjonale samarbeidsaktiviteter. Rapporten inneholder også en omfattende liste av publikasjoner.

Prosjektets resultater har i stor grad et teknisk preg. En viktig målgruppe for prosjektet anses å være de INI-relaterte leveranseprosjektene som gjennomføres i Forsvaret. Prosjekt 8009 blir således pekt på som et miljø det er lagt stor vekt på å gi avtapninger til. Et innspill til videre arbeid er å holde fokus på relevante militære anvendelser av tilgjengelige teknologiske løsninger.

English summary

This document presents an overview of the work performed in FFI-project 1176 (*Service orientation and semantic interoperability in INI*). The report aims to describe a high-level view, but the topics selected for presentation are described in some more detail. The technological priority areas and results are summed up, with an emphasis on explicit references to publications from the project.

Based on the division of the formal project agreement into four areas, the project execution has evolved along four parallel activity areas: Service orientation, semantic technologies, information security solutions and architecture-work. These areas touch upon a significant part of what, along with various kinds of communication services, will constitute the enabling elements of the information infrastructure (INI) for the Armed Forces.

The technological results from the project are described in subsections to each activity area. Further, experiment participation and selected international collaborations, are described. The report also contains an extensive list of publications.

The results of the project are largely technical. An important target audience for this project is the INI-related delivery projects that are being executed within the Armed Forces. Project 8009 is pointed to as a community to which deliverables and technical support have been prioritized. An input to further work is to keep focus on military utilization of the technological solutions being made available by research.

Innhold

1 Innledning

Denne rapporten gir en oversikt over resultater og anbefalinger fra FFI-prosjekt 1176 *Tjenesteorientering og semantisk interoperabilitet i INI*[1]. Arbeidet i prosjektet har pågått i vel tre år, fra januar 2010 til ut mars 2013, hvorav de siste tre månedene var en vedtatt forlengelse som skyldtes lavere innsats enn budsjettert i den normerte treårsperioden.

Hensikten med denne rapporten er å peke på publikasjoner og andre resultater som har vært produsert i prosjektet, samtidig som det gis en overordnet beskrivelse av de viktigste faglige innsatsområdene. Anbefalinger fremmes i den grad de foreligger.

Prosjektet bygger på forutsetningen om at effektiv informasjonsutveksling er grunnleggende for et nettverksbasert forsvar (NbF), og at tjenesteorientering og service-oriented architectures (SOA) er en teknologisk utviklingsretning som vil sikre nødvendig fleksibilitet for fremtidige behov. Semantiske teknologier har et potensial for å gjøre det mulig for datamaskiner å behandle selve meningsinnholdet i informasjonen, og fagområdet Information Management (IM) har som ambisjon å skaffe "rett informasjon til rett beslutningstaker til rett tid". Sikkerhetsløsninger som muliggjør tilstrekkelig fleksibilitet i informasjonsutvekslingen, har også vært en del av prosjektets mandat.

Det er på denne bakgrunn at prosjektavtalen beskriver fire områder for prosjektets innretning:

- SOA-teknologier på ulike operative nivåer
- Semantiske teknologier
- Informasjonsstyring (herunder informasjonsmodeller og systemarkitektur)
- Ende-til-ende sikkerhetsløsninger i SOA

Det er vurdert som viktig for Forsvaret å ha og videreutvikle relevant kompetanse innenfor disse områdene. En viktig mekanisme for dette har vært å ha gode samarbeidsrelasjoner, både norske og ikke minst internasjonale. Eksperimenter har gitt verdifull læring og erfaring, samtidig som de har vært gode arenaer for å synliggjøre hvordan teknologiske løsninger kan gi operativ nytteverdi. Det har også vært et mål å levere bidrag til INI-relaterte materiellprosjekter i Forsvaret.

Arbeidet i prosjektet har i hovedsak bestått i fordypning innenfor de fire aktivitetsområdene. En prosjektintern studie [24] av sammenhengen mellom fagområdene SOA og semantiske teknologier, peker på at mens SOA-området er orientert mot tjenester, prosesser og arbeidsflyt, er semantiske teknologier i sin natur data-orientert og beskrivende (deklarative). Det ligger klare synergier i kombinasjonen av fagområdene, men prosjektets primærfokus har vært spesialisering.

[1] INI benyttes som betegnelse på Forsvarets informasjonsinfrastruktur

Denne rapporten skrives på norsk, til forskjell fra majoriteten av prosjektets øvrige publikasjoner som har vært utgitt på engelsk av hensyn til distribusjon og gjenbruk internasjonalt. Beskrivelsene her er forsøkt holdt på et mest mulig lettlest og ikke-teknisk nivå, i håp om stor utbredelse og godt mottak i et bredt lag av Forsvarets organisasjon i Norge.

2 Teknologiresultater og anbefalinger

Dette hovedkapitlet tar for seg et sett av sentrale områder som det er riktig å fremheve sett i lys av innsats og resultater i prosjektet. Kapitlet beskriver aktivitetsområdene tjenesteorientering, semantiske teknologier og sikkerhetsløsninger, samt en omtale av prosjektets forhold til arkitekturarbeidet i Forsvaret.

2.1 Tjenesteorientering

Dette området har vært det relativt sett største innen prosjektet. Det har vært gitt betydelige bidrag inn i Natos arbeid med kjernetjenester, noe som omtales nærmere i kapittel 4.1. Nato har identifisert Web services som en nøkkelteknologi i NATO Network Enabled Capabilities (NNEC), og prosjektet har konsentrert seg om Web services for realisering av løsninger for SOA. Det er også gjort vurderinger av hvordan løsninger for Enterprise Service Bus (ESB) bør utnyttes [26] og det er gjennomført arbeider knyttet til tjenestekvalitet (Quality of Service, QoS) [23].

En teknisk løsning som ikke har vært fokusert i prosjektet, men som er i utstrakt bruk i industrien, eksempelvis internt på et kjøretøy, er Data Distribution Service (DDS). Prosjektets tidlige befatning med DDS er beskrevet i [5], og innbød ikke til ytterligere innsats da. DDS nevnes her likevel som et eksempel på løsninger det i fremtiden kan bli viktig å kunne forholde seg til i form av standardiserte grensesnitt.

Videre bør det nevnes at et medlem av prosjektet fikk prisen for beste FFI-rapport 2011 for [7], som gir en inngående oversikt over hvordan Web services kan brukes i militære nett. Juryens kommentar ”Relativt lettlest om et faglig vanskelig tema” bør være en god anbefaling.

I det følgende vil vi se nærmere på tre viktige faglige innsatsområder der prosjektet har skapt viktige resultater, nemlig service discovery, publish/subscribe og optimaliseringer av SOA med henblikk på bruk i taktiske nett.

2.1.1 Service discovery

Service discovery (SD) betegner prosessen man benytter for å oppdage tjenester som er tilgjengelige for bruk. SD kan foregå i planleggingsfasen av et system (såkalt *design-time* SD) eller mens systemet er i bruk (såkalt *run-time* SD).

I tilfellet design-time SD finnes og konfigureres tjenestens endepunktadresse i enten en konfigurasjonsfil eller WSDL, og adressen forandres ikke ved senere bruk av tjenesten med mindre en administrator gjør endringer for eksempel i forbindelse med deployering i et nytt

nettverk eller liknende. Run-time SD er primært beregnet for dynamiske nettverk slik som militære taktiske nett. Der er det viktig å finne de til enhver tid tilgjengelige, relevante tjenestene.

Det finnes tre standarder som omhandler service discovery, alle under OASIS:

- Universal Description, Discovery and Integration (UDDI),
- electronic business using XML (ebXML), og
- WS-Dynamic Discovery (WS-Discovery).

UDDI og ebXML er registerløsninger som støtter både design-time og run-time SD. WS-Discovery er ment for mer dynamiske omgivelser enn registrene, og støtter kun run-time SD. I Natos SOA baseline [75] har man foreslått UDDI for SD (den såkalte *Service Discovery Service*), mens ebXML har blitt valgt som metadataregister (den såkalte *Metadata Registry Service*).

Registrene er laget for bruk i store nettverk med fast infrastruktur. De er ikke egnet for bruk i mobile ad hoc nettverk (MANET), som karakteriseres av at man har mobile noder og ustabile forbindelser, noe som kan føre til at ikke alle noder kan kommunisere med hverandre hele tiden.

I slike nettverk kan man få problemer med *liveness* og tilgjengelighet (*availability)*:

- Livenessproblemet oppstår hvis en tjeneste blir utilgjengelig etter å ha blitt publisert i et register. En klient vil da fortsatt kunne finne tjenesten i registeret, men tjenesten kan ikke brukes. Gjentar man oppslaget i registeret er resultatet fortsatt det samme. Dette problemet oppstår fordi de standardiserte registrene krever at man aktivt avregistrerer tjenester som ikke lenger skal kunne oppdages, noe man ikke er i stand til dersom tjenesten forsvinner på grunn av f.eks. nettverkspartisjonering.

- Tilgjengelighetsproblemet oppstår når registeret havner i en annen nettverkspartisjon enn klienten. Klienten vil da ikke kunne slå opp noen tjenester i det hele tatt, ettersom den ikke kan kople til registeret. Selv om en aktuell tjeneste skulle befinne seg i samme partisjon som klienten så vil den ikke kunne benyttes fordi den ikke kan oppdages.

Dette betyr at i dynamiske nettverk hvor partisjoner kan oppstå, bør man fortrinnsvis benytte SD-mekanismer som ikke har disse problemene. Taktiske mobile nett har gjerne færre noder enn et infrastrukturbasert nettverk, noe som betyr at det er mulig å benytte desentraliserte SD-mekanismer der. En desentralisert mekanisme løser tilgjengelighetsproblemet ved å spre informasjonen om tjenester til alle noder den kan nå. Dersom mekanismen samtidig har en form for timeout slik at tjenester som forsvinner fra nettverket også forsvinner fra SD-mekanismen, så vil også *liveness*-problemet kunne løses ettersom man ikke lenger aktivt må avregistrere tjenester.

I prosjektet har vi sett på krav til og utfordringer ved SD i ulike militære nettverk, og konkludert med at på grunn av den store forskjellen mellom de ulike nettverkene så kan ikke en enkelt mekanisme benyttes over alt. Man trenger ulike mekanismer i ulike nettverk, slik at man kan bruke den mekanismen som er best for hvert enkelt tilfelle.

I militære taktiske nett, og da spesielt såkalte disadvantaged grids[2], bør ikke registerbaserte løsninger benyttes og man må se seg om etter andre mekanismer. For eksempel kan man vurdere å bruke WS-Discovery med komprimering i nettverk der man har støtte for IP multicast. Gitt at man finner fornuftige mekanismer for de ulike nettverkene kan man få støtte for SD i alle militære nett. Interoperabilitet er svært viktig, så det er også behov for gjennomgående SD (såkalt *pervasive SD*) på tvers av heterogene nettverk.

Vi har sett på ulike teknikker for å oppnå gjennomgående SD, og har konkludert med at man bør benytte gateways for å oversette mellom protokoller. Dette er den enkleste tilnærmingen til å oppnå protokollinteroperabilitet (og vil dermed også være den mest kosteffektive). En slik gateway vil typisk kunne plasseres i koplingspunktet mellom heterogene nettverk som benytter ulike SD-mekansimer. Denne tankegangen er for øvrig i tråd med de såkalte *interoperability points* som NNEC feasibility study [76] diskuterer.

2.1.2 Publish/subscribe

Publish/subcribe (pubsub) er et paradigme for informasjonsutveksling som baserer seg på at informasjonskonsumenter (konsument) melder sin interesse for ulike informasjonstyper gjennom en abonnements-mekanisme. Pubsub er et alternativ til det mer utbredte Request/response-paradigmet, der hver respons krever en forespørsel og konsumenten er avhengig av å sende hyppige forespørsler for til enhver tid å ha oppdaterte responsdata.

WS-Notification er en OASIS-godkjent standard, og er valgt av Nato Core Enterprise Services Working Group (CESWG) for Web Service pubsub. WS-Notification omfatter tre deler: WS-BaseNotification, WS-BrokeredNotification og WS-Topics. Til sammen gjør de det mulig for konsumenter (eller en annen node på vegne av konsumenten) å abonnere hos en ”broker” (eller en annen node som innehar rollen ”subcription manager”), på informasjon som publiseres under et gitt emne (topic). Én eller flere informasjonsprodusenter (produsent) publiserer informasjon til en broker under et gitt topic, og brokeren leverer deretter informasjonen til alle konsumenter som abonnerer på dette topicet. Leveransen av informasjonen gjøres via en utgående forbindelse fra brokeren til konsumenten, og kalles push-basert meldingsleveranse.

Pubsub har flere fordeler fremfor tradisjonell Request/response. Frikobling (decoupling) innebærer at konsumenter ikke behøver å ha kjennskap til produsenter. De behøver kun kjennskap til brokeren, som formidler informasjon på vegne av mange produsenter. Push-basert levering gjør at informasjonen leveres til klientene straks den foreligger. Dette gjør at konsumentene ikke behøver å forespørre en tjener om data, noe som kan være fordelaktig da det eliminerer overflødig datatrafikk i nettverket[3].

[2] Nettverk som har særlige begrensninger på områder som kapasitet, datarate og forsinkelse/pakketap

[3] Når konsumenter jevnlig forespør data risikerer de å forespørre uten at det faktisk foreligger nye data, og dermed introdusere ekstra trafikk i nettverket og ekstra last på serversiden. Man kan minimere denne belastningen ved å forespørre sjeldnere, men innfører da forsinkelse i dataflyten, noe som er uønsket for mange typer data og scenarioer.

Orienteringen rundt informasjonstyper (f.eks. uttrykt gjennom topics) gjør også at pubsub-løsninger støtter både én-til-mange og mange-til-mange prinsippene for spredning av data. I SOA-piloten (se kapittel 3.1) ble det i stor grad benyttet pubsub-løsninger for spredning av informasjon mellom de militære informasjonssystemene og aggregerings- og visualiseringsapplikasjonene. I etterkant av SOA-piloten har prosjektet tatt frem en egen implementasjon av de viktigste delene av WS-Notification som en frittstående, lettvekts java-implementasjon kalt microWSN. Denne har vist seg svært nyttig for prosjektet, til eksperimentering og samarbeidsaktiviteter, samt forskning på utvidelser til standardene den er basert på.

Forskningen på pubsub har også avstedkommet en ny komprimeringsprotokoll spesielt egnet for pubsub-nettverk. Protokollen er kalt ZDiff, og ble publisert ved MILCOM 2012 [71]. Ytterligere en pubsub-basert transmisjonsprotokoll for taktiske nett og disadvantaged grids kalt REAP er under utvikling. Gjennom et doktorgradsarbeid er det også tatt frem en ny pubsub-protokoll kalt Mist [53][67]. Protokollen benytter epidemisk spredning av data mellom noder, og trenger ingen underliggende ruting-mekanisme for å fungere. Tester har vist at Mist er svært effektiv i nettverk med dynamisk topologi.

Vårt arbeid har vist at pubsub er en effektiv distribusjonsmekanisme, også i radionett. Nettverkstrafikken reduseres, samtidig som mottakerne er sikret oppdatert informasjon raskt. Vi har imidlertid erfart at WS-Notification-standarden mangler enkelte funksjoner. Først og fremst gjelder dette muligheten for å få tak i meldinger som er sendt ut før man begynte å abonnere. I tillegg har vi sett et behov for å kunne sjekke status på egne abonnement. Dette er ting vi har begynt å se på i samarbeid med NATO Communication and Information Agency (NCIA).

Videre ser vi at ved innføring av pubsub får man et behov for å kunne klassifisere informasjonstypene som tilbys fra slike tjenester. Vanlig service discovery vil kunne finne pubsub-tjenester, men vil ikke kunne si noe om hva slags informasjon de tilbyr. Det er derfor behov for å utvide service discovery med en form for informasjon discovery. Vi har derfor begynt å se på bruk av såkalte topics for dette formålet.

2.1.3 Optimaliseringer for taktiske nett

Den vanligste og mest modne teknologien for å implementere en SOA er Web services, og mange Nato-nasjoner har allerede begynt å implementere støtte for denne teknologien i sine informasjonssystemer.

Web services muliggjør interoperabilitet mellom ulike systemer, men teknologien har en del overhead ettersom den bygger på det tekstbaserte XML-formatet, noe som gir økte krav til tilgjengelig kommunikasjonskapasitet. I sivile nettverk er dette vanligvis ikke noe problem, men i militære radiobaserte nett er sitasjonen en annen. Der må man forholde seg til den ofte svært begrensede båndbredden som utstyret gir.

Vi har identifisert tre konkrete aspekter ved Web services som må håndteres i militære nett:

1. Fjerne behovet for ende-til-ende-forbindelser.
2. Skjule nettverksheterogenitet.
3. Redusere overhead av Web services (som nevnt over).

I prosjektet har vi undersøkt ulike tilnærminger til å håndtere disse aspektene, og vi har fått en del erfaring med ulike teknikker gjennom nasjonale og internasjonale eksperimenter. Avhengigheten av forbindelse ende-til-ende kan fjernes ved bruk av en «mellommann» (såkalt *proxy*) i kommunikasjonen. Det å skjule nettverksheterogeniteten er, til en viss grad, løst ved å benytte IP som nettverksprotokoll i alle nettverk (dette er i tråd med anbefalingene i NNEC Feasibility Study [76]). Forskjeller i nettverkskapasitet håndteres ved å legge på forsinkelsestoleranse (delay tolerance), og i mange tilfeller vil det være nødvendig med mekanismer for håndtering av tjenestekvalitet.

I prosjektet har vi sett på ulike måter for å redusere overhead ved XML og Web services for å gjøre det mulig å benytte teknologien i taktiske nett:

- Bruk av komprimering for å redusere overhead ved XML: Her har vi vurdert ulike algoritmer, bl.a. GZIP og den nylig standardiserte EXI. EXI komprimerer best, tett fulgt av GZIP.
- Alternative transportprotokoller: Vi har kikket på ulike alternativer her, og har så langt ingen konkrete anbefalinger. Det er tidligere vist at det er mulig å sende SOAP over Forsvarets meldingstjeneste, selv om dette ikke nødvendigvis er å anbefale.
- Redusere overhead ved å optimalisere applikasjonens kommunikasjonsbehov. Dette er applikasjonsspesifikt og man kan for eksempel forsøke å redusere mengden data som sendes, samt å redusere frekvensen på meldingene.

De første to teknikkene kan benyttes med enhver Web service, mens den siste må vurderes for hver enkelt tjeneste. Dermed bør ikke den siste optimaliseringen være en del av mellomvaren, ettersom mellomvaren ikke bør behøve å kjenne til applikasjonsdata. Tvert imot bør denne funksjonaliteten plasseres i applikasjonen eller eventuelt i proxyer, som er en god tilnærming til det å gjøre optimaliseringer mellom kommersielt tilgjengelige (COTS) klienter og tjenester.

For å støtte Web services på tvers av heterogene nettverk (inkludert disadvantaged grids) så har prosjektet utviklet en prototyp som vi kaller Delay and Disruption Tolerant SOAP Proxy (DSProxy) [45]. Den er laget for bruk på tvers av heterogene militære nettverk, og har blitt benyttet med hell i flere eksperimenter nasjonalt og internasjonalt. DSProxy har blitt brukt for å få ytterligere erfaring med teknikkene som nevnes ovenfor, og gjør blant annet komprimering, støtter ulike transportprotokoller, samt innfører forsinkelsestoleranse til SOAP. Disse erfaringene viser at man alltid bør benytte komprimering av informasjon i taktiske nett, men at hvilken komprimeringsmetode man bruker er underordnet, så lenge man bruker en som er kompatibel med det som kommunikasjonspartnerne bruker. Videre har vi erfart at man, i alle nettverkstyper som har avbrudd i kommunikasjonen, bør ha forsinkelsestoleranse.

2.2 Semantiske teknologier

Forsvarssjefen slår i sin plan for NbF [31] fast at Forsvarets evne til å skape, prosessere, distribuere og utnytte informasjon står sentralt i alle typer av operasjoner. Prosessering og utnytting av informasjon er i dag dominert av manuelle prosesser, og vi forventer at et NbF, med sitt fokus på økt tilgjengeliggjøring av informasjon, vil føre til enda større mengder informasjon som skal prosesseres. Dette øker sjansen for informasjonsoverlast på de som skal behandle og utnytte denne informasjonen, og for å motvirke dette bør Forsvaret anskaffe systemer som støtter disse prosessene. Metoder for automatisk sammenstilling av informasjon fra ulike heterogene kilder samt automatisert analyse og mulighet til å stille spørringer mot den samlede informasjonen har potensial til å gi viktige bidrag til slike systemer. Prosjektet har derfor fokusert på hvordan semantiske teknologier kan bidra til slike metoder.

Ved hjelp av semantiske teknologier kan man bygge systemer med en høy grad av autonomi. Dette gjør systemene i stand til å håndtere situasjoner der forutsetningene endrer seg hyppig. Slike endringer kan f.eks. skyldes at informasjonen endrer seg, at informasjonskilder kommer og går eller at brukerens informasjonsbehov endrer seg. Bruk av semantiske teknologier gjør det mulig å endre systemers oppførsel ved kun å endre modeller som ligger utenfor selve systemene. Dette forventes å gjøre det enklere og mindre kostnadskrevende å integrere informasjon fra forskjellige systemer. US DoD har for eksempel besluttet at ontologier skal brukes i deres Business Enterprise Architecture for å få ned IT-kostnadene samt fremme interoperabilitet mellom DoDs anslagsvis 2000 informasjonssystemer [32][33].

I arbeidet med semantiske teknologier har prosjektet konsentrert seg om teknikker for å behandle strukturert informasjon. Skal disse teknikkene tas i bruk på ustrukturert informasjon som tekst, bilder, lydklipp, statistiske data eller lignende, må informasjonen gjennom et preprosesseringssteg for å trekke ut og strukturere den essensielle informasjonen. Det har vært planlagt en CD&E-aktivitet i prosjektet som skulle se på hvordan man kan benytte teknikker fra semantiske teknologier på ustrukturerte tekstdokumenter, men aktiviteten har så langt ikke blitt gjennomført på grunn av manglende ressurser hos sponsoren i Forsvaret.

Sentrale deler av teknologiene og standardene som utgjør semantiske teknologier, har nådd et modenhetsnivå som gjør dem egnet til mer operativ uttesting i form av pilotprosjekter. Dette gjelder først og fremst teknologiene og standardene utviklet under W3Cs Semantic Web-initiativ. Modenheten kan sees gjennom at disse teknologiene nå er gjenstand for kommersialisering og tas i bruk av betydelige aktører og for å løse reelle problemstillinger. Som eksempler på bruk av disse teknologiene kan nevnes:

- EPIM ReportingHub [74]: Oljebransjens løsning for rapportering av oljevirksomhet på norsk sokkel
- Hafslund Sesam [39]: Løsning for informasjonsintegrasjon, arkivering og søk hos Hafslund,
- SemanticDB (Cleveland Clinic [40]): Løsning for å integrere informasjon fra helsesystemer,

- US DoDs satsing på W3Cs Semantic Web-standarder i sin Business Enterprise Architecture [33], som skal bidra til å styre informasjonssystemporteføljen og bedre integrasjonen av informasjonssystemene i US DoD.

Et viktig punkt for prosjektet har vært å studere hvordan semantiske teknologier kan utnyttes sammen med reelle militære systemer. Dette har vært gjort i de to eksperimentene SOA-pilot (kapittel 3.1) og CWIX 2012 (kapittel 3.2), og omfatter Nato-systemene JOCWatch og MEDWatch samt NORCCIS II.

Vi anbefaler derfor, som en videreføring av uttestingen som er gjort mot reelle militære systemer i lab-omgivelser, at Forsvaret og FFI i samarbeid finner egnede områder der teknologiene kan testes ut operativt.

Et enkelt grep som bør settes i verk for å legge til rette for utprøving av disse teknologiene nå og i fremtiden, er å gjøre utvalgte database-baserte militære systemer i stand til å gjøre informasjon tilgjengelig via SPARQL-endepunkter. Dette er moden teknologi og standarder, vist militært bl.a. i Natos TIDE-prosjekt [35] og sivilt hos store databaseleverandører som IBM [41] og Oracle [42], og det er tiltak som kan gjøres parallelt med eksisterende utvikling uten at det innvirker på systemenes ordinære bruk. Dette vil muliggjøre umiddelbar bruk av de modne delene av semantiske teknologier, samt gjøre det mulig å løpende ta i bruk andre deler av teknologiene etter hvert som disse også modnes.

I tillegg til dette bør arbeidet med å følge utviklingen av disse teknologiene fortsette, med særlig vekt på å støtte særskilte militære behov som ikke er dekket av sivil forskning.

2.2.1 Integrasjon av informasjon fra heterogene kilder

Det teknologiske fokuset i utviklingen mot et NbF har så langt vært på hvordan informasjon skal kunne gjøres tilgjengelig. Det er imidlertid en vel så stor utfordring hvordan informasjonen skal behandles videre. En bruker må kunne finne den relevante informasjonen, men må også være i stand til å integrere den med annen informasjon. I tillegg må brukeren være i stand til å nyttiggjøre seg informasjon fra oppdukkende kilder.

Når det gjelder å finne relevant informasjon, har prosjektet fokusert på å identifisere informasjonskilder basert på innholdet i de forskjellige kildene - såkalt information discovery. To forskjellige tilnærminger har vært studert: å representere kildene (1) ved hjelp av autonome agenter og (2) ved hjelp av kildebeskrivelser.

I tilnærming (1) [9] håndteres information discovery i et multi-agent-system [34]. Alle aktørene i informasjonsintegrasjonen (beslutningstakere, informasjonskilder og andre prosesseringsnoder) er representert av enkle agenter. Relevante kilder blir funnet gjennom at beslutningstakerens agent kringkaster informasjonsbehovet som en spørring, mens informasjonskildenes agenter besvarer spørringen dersom de har relevant informasjon.

Tilnærming (2) ([19], kap. 6) ligner løsningen valgt i TIDE transformation baseline [35], og baserer seg på at hver kilde beskriver hvor de befinner seg (IP-adresse) og hva slags informasjon de holder. Kildene kringkaster så denne beskrivelsen i nettverket.

Utfordringen med å integrere informasjonen fra forskjellige kilder forsterkes av at kildene ofte er heterogene - de kan benytte forskjellige kommunikasjonsprotokoller, forskjellige utvekslingsformater og de kan representere informasjonen sin i henhold til forskjellige informasjonsmodeller. Prosjektet har fokusert på heterogeniteten som skyldes forskjellig representasjon av informasjonen, og har studert hvordan bruk av semantiske teknologier kan bidra til å løse denne interoperabilitetsutfordringen. Spesielt har vi studert bruk av ontologier til dette formålet (ontologibasert informasjonsintegrasjon). Ontologier er formelle informasjonsmodeller som kan representere meningen (semantikken) i informasjonsinnholdet, og de kan håndteres separat fra informasjonskildene. Siden de er formelle, legger de også til rette for automatisert resonnering.

Spesielt har prosjektet fokusert på ontologibasert informasjonsintegrasjon der informasjonskildene kan komme og gå. Dette var tema både i SOA-piloten (kapittel 3.1) og eksperimentet prosjektet gjennomførte på CWIX 2012 (kapittel 3.2).

Ontologier lar seg koble sammen. Gjeldende praksis i bruk av ontologier tilsier derfor at man utvikler et antall ontologier av håndterbar størrelse og kobler disse sammen snarere enn å lage få, omfattende ontologier ([36], kap. 8.4) . Da får man imidlertid ofte en situasjon der de forskjellige ontologiene kommer fra urelaterte kilder, for eksempel forskjellige systemleverandører, militære interessegrupper (COI), overordnede standardiseringsinitiativ, osv. Dette fører til et behov for metoder for å avgjøre hvorvidt forskjellige ontologier overlapper hverandre, hvor de i så fall overlapper og hvordan de kan kobles sammen. Slike metoder kalles ontologimathcing [37], og prosjektet har bl.a. sett på såkalt deduktiv ontologimatching [58] for å finne en automatisert metode som både er tilstrekkelig rask og som kan garantere for en tilstrekkelig kvalitet i resultatet.

2.2.2 Støtte til analyse av informasjon

Informasjonsanalyse og analyserelaterte oppgaver er et annet bruksområde der prosjektet mener at semantiske teknologier kan være til stor nytte. Det er generelt akseptert at mennesker er gode til å gjenkjenne kompliserte mønstre. Imidlertid skalerer denne manuelle prosessen meget dårlig når enten datamengden eller antall mønstre øker. Dette resulterer i informasjonsoverlast, noe som igjen øker sannsynligheten for at mønstre blir oversett.

Samtidig som mengden av informasjon relevant for dagens analyseoppgaver øker kraftig i volum og variasjon, øker også kompleksiteten i selve analysejobben. Dette skyldes at dagens etterretningsbehov i felten har utviklet seg fra å hovedsaklig bestå av tradisjonelle fiendtlige posisjoner, meteorologiske data og terrenginformasjon, til også å inkludere sivile kilder fra sivil-militært samarbeid samt informasjon fra åpne kilder.

En analytiker ville tradisjonelt tydd til dybdekunnskap om kildesystemene for å kunne besvare sitt informasjonsbehov, men dette skalerer dårlig sett i lys av dagens nye etterretningsbehov [38]. Det er derfor et behov for automatisert analysestøtte som legger til rette for a) hurtig endrende informasjonsbehov, b) gjenbruk av domenekunnskap, og c) integrasjon av heterogene, oppdukkende og hurtig endrende kilder. Vi mener at semantiske teknologier kan bidra til å løse de ovennevnte utfordringene.

Bruk av semantiske teknologier gjør det også mulig å automatisere oppgaver som integrasjon, klassifisering og utledning av ny informasjon, og prosjektet har utviklet demonstratorer for å eksemplifisere bruk av disse teknologiene for analysestøtte.

I de to eksperimentene SOA-pilot og CWIX 2012 demonsterte vi bruk av semantiske teknologier for gjenkjenning av mønste i store menger høyt varierte data (variasjon i type data). Det ble også lagt til rette for å håndtere hyppig endrende informasjonsbehov og -kilder. Bruksmønsteret vi baserte våre eksperimenter på, og som vi mener ofte vil dukke opp i analyserelaterte oppgaver, innebærer å først stille generelle spørringer for å skape et overblikk over interessante elementer, for så å gjøre et dypdykk og forfølge de mest interessante elementene videre (drill-down, videre spisset informasjonsøkning).

I eksperimentene var analyseontologien som fanget brukerens domene, koblet sammen med og definert ved hjelp av andre ontologier. Bruken av ontologier i denne sammenhengen gjorde det mulig å a) gjennomføre integrasjon uten at analytikeren var avhengig av spesifikk kunnskap om informasjonskildene og b) la analytikeren automatisk nyttiggjøre seg domenespesifikk kunnskap utenfor sitt faglige kunnskapsområde (f.eks. detaljert klassifisering). Analyseontologien fungerte derfor som en abstrakt modell over kildene og andre kunnskapsdomener, og analytikeren kunne bruke denne til å stille spørringer.

2.3 Informasjonssikkerhet

Innen informasjonssikkerhet har prosjektet hatt fokus på løsninger for å gi tilgang til informasjon på tvers av sikkerhetsdomener. Dette er en forutsetning både for å realisere høyere modenhetsgrader av NbF, og for å utnytte den gevinsten tjenesteorientering gir ved å legge til rette for interoperabilitet og interaksjon på tvers av systemer og organisatoriske skiller.

Visjonen er at brukeren kun trenger å forholde seg til ett informasjonsdomene, samtidig som all informasjon er beskyttet i henhold til behov. Realiseringen av en slik løsning er imidlertid en langvarig prosess og synes ikke å være oppnåelig i overskuelig fremtid. Det er derfor stort behov for sikre løsninger som gir mer fleksibilitet enn hva en har i dag.

Prosjektet har adressert flere aspekter av dette. Et aspekt er bruk av guardløsninger for å tillate to-veis informasjonsutveksling mellom sikkerhetsdomener. Et annet aspekt er løsninger for å kunne håndtere flere graderingsnivå på en og samme maskin. Et tredje er tilgangskontroll og identitetshåndtering på tvers av sikkerhetsdomener. Felles for alle områdene er at det er til dels høye krav til tilliten til sikkerheten i løsningene, og dette er også et område det er blitt jobbet med

i prosjektet. Når det gjelder guardløsninger er en for eksempel avhengig av både av å ha tillit til at guarden filterer informasjonen riktig og at sikkerhetsmerkene som angir graderingen er riktige.

Løsningene det har vært jobbet med er i stor grad komplementære. For eksempel vil løsningene det har vært jobbet med innen høy tillit og håndtering av flere graderingsnivå på en og samme maskin også kunne ha en viktig funksjon for å påføre troverdige sikkerhetsmerker for senere bruk i en guard. En observasjon er at for å kunne påføre sikkerhetsmerker som angir informasjonens gradering på en sikker måte, og dermed legge til rette for mer fleksibel informasjonsutveksling, vil det være en fordel i størst mulig grad å tilstrebe at enkeltsystemer opererer på ett enkelt graderingsnivå [25]. Dette legger klart føringer for hvordan en bør tenke arkitektur, men passer godt både med prinsippene for tjenesteorientering og arkitekturen i Multiple Indendent Levels of Security (MILS, ref kapittel 2.3.2).

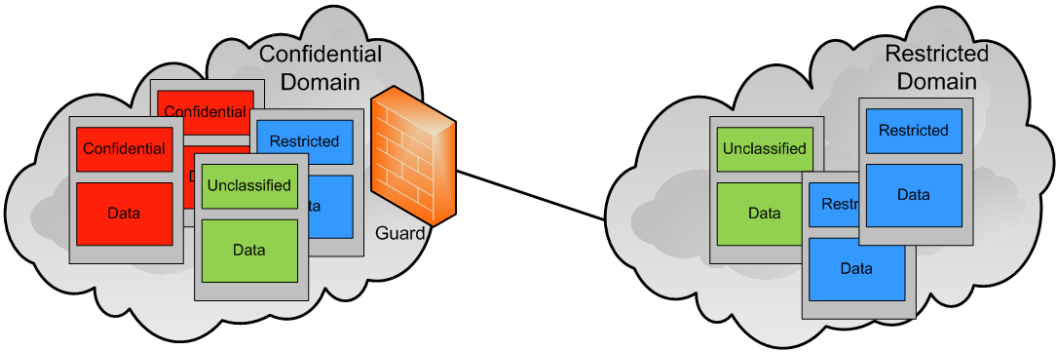
I det følgende gis først en beskrivelse av arbeidet som er utført i prosjektet relatert til guardløsninger. Deretter omtales løsninger med høy tillit og håndtering av flere graderingsnivå på en og samme maskin. Til slutt diskuteres arbeidet relatert til tilgangskontroll og identitetshåndtering.

2.3.1 Guard for sikker informasjonsutveksling mellom domener

En av hovedaktivitetene innenfor sikkerhetsarbeidet i prosjektet har vært utvikling av løsninger som kan muliggjøre informasjonsutveksling mellom sikkerhetsdomener samtidig som kravene til sikkerhet ivaretas. Prosjektet har valgt å fokusere på løsninger for å hindre lekkasje av informasjon fra det høyt graderte domenet til det lavere graderte. I tillegg er det viktig å hindre virus, skadevare (malware) og cyber-angrep fra å kunne flyte fra det lave til det høye domenet, men på grunn av begrensede ressurser valgte prosjektet ikke å fokusere på dette.

For å realisere en slik sikker og automatisk toveis utveksling av informasjon mellom sikkerhetsdomener anbefaler prosjektet at man i større grad tar i bruk objektnivå sikkerhet (Object Level Protection). Prinsipielt vil en da beskytte informasjonsobjekter ut fra det faktiske behovet, og ikke basert på hvilken infrastruktur som lagrer eller behandler objektet. Tre viktige komponenter i objektnivå sikkerhet kan trekkes frem; informasjonsobjektet, metadata og beskyttelsesmekanismer. Metadata brukes til å beskrive forskjellige aspekter ved et informasjonsobjekt, som f.eks. sensitivitet, og bindes til dette ved hjelp av en bindingsmekanisme. Beskyttelsesmekanismer bruker denne metadataen til å gjøre sine beregninger. Avgjørelser kan dermed gjøres ut fra beskyttelsesbehovet til informasjonen, og ikke ut fra hvilken infrastruktur informasjonen er lagret på.

Figur 2.1 viser hvordan objektnivå sikkerhet kan brukes til å realisere en sikker toveis utveksling av informasjon mellom sikkerhetsdomener. Her er sensitiviteten (graderingen) uttrykt som metadata som er bundet til informasjonen. Beskyttelsesmekanismen, i dette tilfellet en guard, bruker da denne metadataen til å avgjøre om informasjon kan frigis eller ikke.



Figur 2.1 Utveksling av informasjon mellom sikkerhetsdomener

Basert på tidligere arbeid har prosjektet publisert forslag til spesifikasjon av XML konfidensialitets-metadata (label) og XML metadata binding [1][2][46]. Disse spesifikasjonene ble tatt frem gjennom en Nato forskningsgruppe og er blitt foreslått som fremtidige Nato standarder for nettopp konfidensialitets-metadata og bindingsmekanisme. Spesifikasjonen ble blant annet inkludert i Natos Core Enterprise Services Framework [81] og i nyeste versjon av NATO Interoperability Standards and Profiles (NISP) [82].

Videre har prosjektet utviklet en demonstrator-guard for sikker utveksling av informasjon fra høyt til lavt sikkerhetsnivå. Denne demonstratoren er et resultat av en iterativ utvikling som startet i tidligere FFI-prosjekter og som dette prosjektet har bygget videre på. Demonstratoren har vært brukt både til å verifisere våre hypoteser og få testet konseptet med bruk av guard for slik utveksling. Guarden har også vært et viktig verktøy for å teste de foreslåtte sikkerhetsmerkene og bindingsmekanismene. Gjennom bruk av guarden har vi kunnet verifisere at disse lar seg implementere, og at det er mulig for en beskyttelsesmekanisme å bruke disse som grunnlag for å kunne ta avgjørelser. Inkludert i demonstratorutviklingen har vi også laget diverse programvare for å produsere konfidensialitetsmerker, samt binde disse til informasjon. Demonstratoren har vært brukt i eksperimenter som SOA-piloten og CoNSIS, omtalt i kapittel 0. Beskrivelse av eksperimentene og resultatene kan finnes i rapportene [16][73]. I tillegg har prosjektet også vært delvis involvert i en CD&E-aktivitet gjennomført av UAV-miljøet ved FFI der guarden ble brukt for sikker overføring av planer fra høyt til lavt sikkerhetsdomene.

Den versjonen av guarden som er tatt frem av prosjektet er kun en demonstrator og er derfor langt unna å kunne sertifiseres og tas i bruk operativt. For å komme et steg nærmere en løsning som kan operasjonaliseres, har prosjektet tatt initiativ til en CD&E-aktivitet. Hovedformålet for denne aktiviteten er å ta frem og teste en sertifiserbar guardløsning for tjenesteorienterte arkitekturer. Aktiviteten vil basere seg på vårt tidligere arbeid med konfidensialitetsmerker og MILS separasjonskjerner (kapittel 2.3.2). Vår hypotese er at det er mulig å lage en slik sertifiserbar guard ved å gjenbruke store deler av de sikkerhetskritiske komponentene til den nye meldingsguarden som tas frem av Forsvaret. Dersom dette er mulig vil en kunne få operasjonalisert en guard for tjenesteorienterte arkitekturer raskere og forhåpentligvis til en lavere kostnad. CD&E-aktiviteten startet i januar 2013 og er planlagt å vare ut dette året.

En slik guard vil også kunne være en viktig komponent i en Information Exchange Gateway, se kapittel 4.5 om planlagte aktiviteter på det.

I løpet av arbeidet i prosjektet med dette temaet har også mulige fremtidige utvidelser blitt identifisert. Kombinasjonen av konseptet Protected Core Networking (PCN) og større satsing på objektnivå sikkerhet, vil gjøre at en flytter sikkerheten nærmere endesystemene. Det vil derfor være naturlig at der en på kort sikt ser for seg å bruke guarder ved nettverksgrenser (i dag er ofte disse synonymt med grenser mellom sikkerhetsdomener). En vil da kunne trenge en løsning for distribuerte beskyttelsesmekanismer.

I tillegg til dette ser en også for seg at måten en lager og behandler sikkerhetsmerker vil endre seg. Dagens sikkerhetsmerker, inkludert den foreslåtte spesifikasjonen av konfidensialitetsmerker, knytter en policy og gradering til data. Dette gir en sterk og lite dynamisk kobling mellom data og policy. En mulig fremtidsvisjon er at metadata bare brukes til å beskrive faktiske karakteristikker om data den er knyttet til. En vil da dynamisk kunne endre hvordan data med forskjellige karakteristikker skal behandles. Hvilken policy som skal brukes kan da også endres basert på variabler som for eksempel miljø og risikovurderinger.

2.3.2 Løsninger med høy tillit og terminal for håndtering av flere sikkerhetsdomener

Prosjektet har arbeidet med løsninger for å kunne realisere sikkerhetsfunksjonalitet med høy grad av tillit. Det er bygd opp god kompetanse om tilgjengelige «high assurance» plattformer, og særlig angående separasjonskjerner basert på Multiple Independent Levels of Security (MILS), og mulige anvendelser av disse i Forsvaret.

Separasjonskjerner legger til rette for å dele opp et system i mindre, verifiserbare komponenter med definerte kommunikasjonskanaler. Foruten å være velegnet for å implementere sikkerhetskritisk funksjonalitet, passer en MILS-arkitektur således godt overens med en modulbasert eller tjenesteorientert tankegang. Støtte for virtualisering legger videre til rette for gjenbruk av eksisterende systemer.

Til tross for at en leverandør har sertifisert en separasjonskjerne til høyt tillitsnivå (Evaluation Assurance Level 6) i USA, er tilgjengeligheten av sertifiserte separasjonskjerner og tilhørende maskinvare foreløpig svært begrenset. Det pågår imidlertid et større EU-prosjekt med målsetting om å sertifisere en MILS separasjonskjerne i Europa. Da sertifiseringer på de høyeste tillitsnivåene er knyttet opp mot spesifikk maskinvare, legger dette begrensninger på anvendelsen av et sertifisert produkt og mer kompleks maskinvare vil ikke være egnet til sertifisering på de høyeste nivåene. For endebrukersystemer vil derfor et noe lavere tillitsnivå (EAL 5) være mer realistisk på kortere sikt, samtidig som dette vil være tilstrekkelig for mange anvendelser.

I denne sammenheng er det i prosjektet blitt tatt frem en prototypeløsning i form av en terminal for håndtering av flere sikkerhetsdomener/graderingsnivå. Denne terminalløsningen muliggjør håndtering av flere graderingsnivå på én og samme PC, hvor hvert graderingsnivå kjører i en separat virtuell maskin. Den foreslåtte løsningen har den fordel at den medfører minimalt med

sikkerhetskritisk funksjonalitet utover det som allerede ligger i separasjonskjernen, og vil derfor relativt enkelt kunne la seg sertifisere gitt en sertifisert/sertifiserbar separasjonskjerne på egnet maskinvare. Designet for løsningen er også overførbart til enheter med berøringsskjerm, for eksempel med tanke bruk på taktisk nivå. Den foreslåtte løsningen er nærmere beskrevet i [15].

Under CoNSIS (kapittel 3.3) ble det også eksperimentert med en lignende løsning for å gi økt tillit til påføringen av sikkerhetsmerker. Sikkerhetsmerkene ble da påført i en egen partisjon uten direkte tilgang til nettverket for å sikre mot at høyere gradert informasjon (tilgjengelig på nettverket) utilsiktet ble påført en for lav gradering og for å gi økt beskyttelse av signeringsnøklene.

Bruk av MILS-arkitekturen for å gi økt tillit til sikkerhetsmerker er diskutert i [25]. En MILS-arkitektur er også tenkt anvendt i den tidligere nevnte CD&E-aktiviteten som skal ta frem en sertifiserbar guardløsning.

2.3.3 Tilgangskontroll og identitetshåndtering i tjenesteorienterte arkitekturer

Identitetshåndtering og tilgangskontroll er viktige elementer for å kunne tillate fleksibel interaksjon på tvers av administrative domener. For å kunne utføre tilgangskontroll er en avhengig av å kjenne tilgangsattributtene til den som forespør, og det er flere standarder som kan benyttes for dette i tjenesteorienterte arkitekturer. Vi har utført en studie av i hvilken grad disse løsningene, som er beregnet for bruk i sivile applikasjoner, er egnet for bruk i militære systemer. Det er spesielt lagt vekt på de arkitektoniske tilnærmingene og de resulterende kommunikasjonsmønstrene, med tanke på innvirkning på tilgjengelighet og tillitsnivå.

Detaljene i studien er gjengitt i [54]. Generelt ble det imidlertid funnet at eksisterende løsninger ikke synes å være direkte anvendbare for mange militære systemer. Spesielt utgjør de ekstra forbindelsesavhengighetene som slike løsninger introduserer, en utfordring når det gjelder tilgjengelighet i en del militære systemer; for eksempel på taktisk nivå, hvor kommunikasjonsavbrudd må påregnes. Videre medfører den overordnede arkitekturen til disse løsningene at utstedertjenestene er svært sikkerhetskritiske, noe som vanskeliggjør replikering av disse nærme brukerne for å bedre tilgjengeligheten. Det er derfor foreslått en alternativ tilnærming for å kunne både bedre tilliten til sikkerheten i slike løsninger og bedre sikre tilgjengeligheten av brukertjenestene.

2.4 Arkitekturarbeidet i Forsvaret

Det faglige grunnlaget for prosjektets arbeid på arkitekturområdet er godt beskrevet i sluttrapporten til FFI-prosjekt 889 Systemarkitektur [30]. For området Information Management (IM) bygget prosjektbeskrivelsen for 1176 på at Forsvaret hadde gjennomført et prosjekt og var i gang med å utarbeide direktiv og retningslinjer som grunnlag for ivaretakelse av roller (og i noen grad også egne stillinger) som såkalte IM'ere.

Det ble tidlig besluttet å innrette aktiviteten på dette området i prosjektet mot å utvikle FFIs evne som faglig støttespiller for Forsvaret, og bidra til fagutvikling gjennom samspill og dialog med relevante miljøer. For å oppnå nytteverdi ble praktisk arbeid gjennom deltakelse i Forsvarets prosesser vurdert som viktigere enn fordypning i teori og metodeverk. Det ble en periode arbeidet for å få til et samarbeid om et CD&E-finansiert eksperiment på IM-området, men forslaget endte opp med å bli nedprioritet fra Forsvarets side. Forsvarets fagråd for Information Management ble etablert, men har ikke møttes siden november 2011.

Sommeren 2011 ble Forsvarssjefens NbF-plan Del 2 [31] gitt ut. Det skjedde også organisatoriske endringer som gjorde at Forsvarets arkitekturråd skulle bli liggende uvirksomt i vel et år. Høsten 2011 tok vi i prosjektet initiativ til en besøksrunde til sentrale miljøer i Forsvaret, i håp om å avdekke arbeid med tiltak som følge av NbF-planen som prosjektet kunne ha en utviklende men praktisk målrettet fagdialog med. Erfaringene fra dette styrket troen på den pragmatiske tilnærmingen for å skape nødvendig utbredelse for arkitekturrelatert tenkning. Arbeidet inspirerte også til en idé om en forenkling av NATO Architecture Framework , en såkalt NAF kjerne, som et teoribidrag til den videre utviklingen av rammeverket. Ideen og arbeidet er beskrevet i [28].

Forsvarets arkitekturråd ble revitalisert mot slutten av 2012, og det gjøres godt og målrettet arkitekturarbeid i flere miljøer. De viktigste miljøene er i FLO/IKT, som har etablert viktige beskrivelser av forholdene rundt alle hovedsystemer som de forvalter, i LOS-programmet, som har fullverdige modeller av Forsvarets forvaltningsløsninger (FIF), samt i Cyberforsvaret som har tatt et ansvar på virksomhetsnivå, og som også er pådriver for arkitekturrådet.

Dette FFI-prosjektet har altså prioritert dialog og deltakelse i Forsvarets arkitekturarbeid. Formålet har vært å øke vår kompetanse til å bidra med verdiskapning. Vår anbefaling vil være å ha et pragmatisk forhold til teori og metodeverk, og heller fokusere på innholdet i beskrivelsene. Beskrivelsene må lages for å utveksle ideer og forståelse mellom mennesker, og en stor del av verdien må skapes gjennom deling og gjenbruk. Det brukes samlet sett forholdsvis sparsomt med ressurser på denne typen arbeid i Forsvaret for tiden, men det er å håpe at praktisk tilnærming og konkretisering som grunnlag for å skape opplevd nytteverdi, vil gi grobunn for økt innsats og flere resultater i tiden som kommer.

I sluttfasen av 1176 er det i samarbeid med nærstående FFI-prosjekter gjennomført en studie av hvordan Natos C3 Classification Taxonomy ser ut til å egne seg for å beskrive arkitekturen i de deler av Forsvarets INI som de berørte prosjektene arbeider med. Resultatet fra dette arbeidet publiseres i [29].

3 Eksperimentering

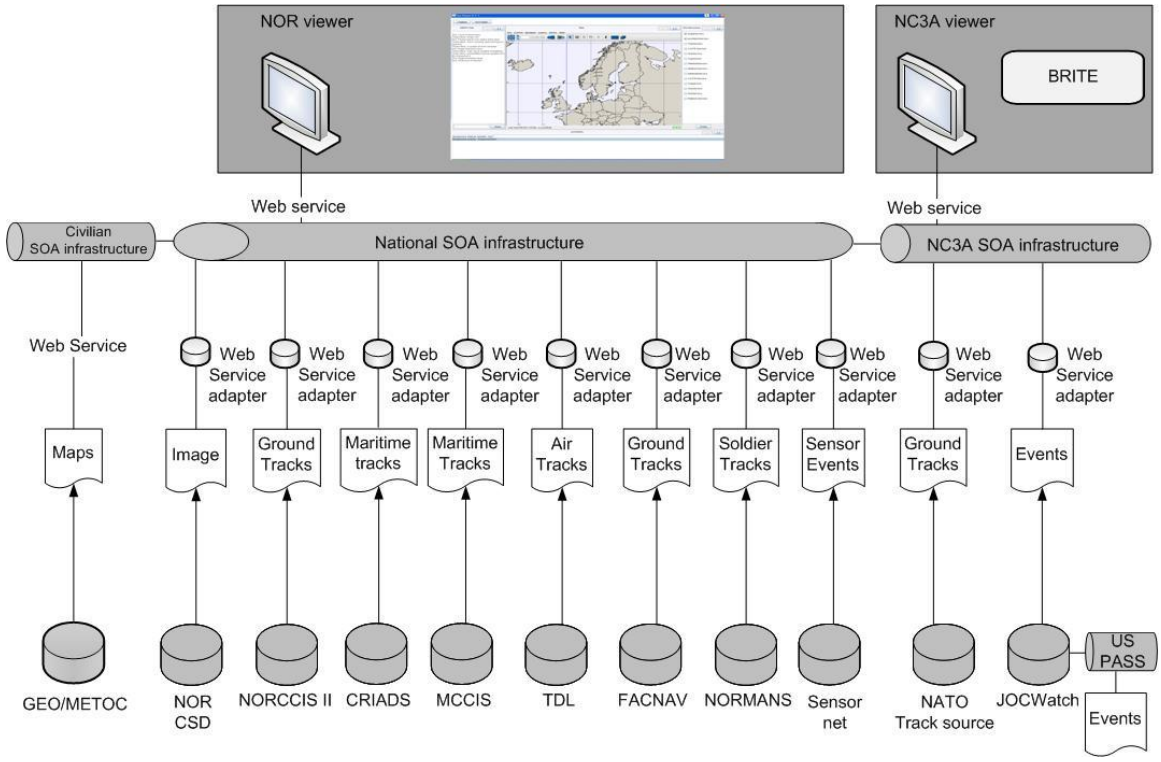
Dette hovedkapitlet beskriver prosjektets bidrag til tre viktige eksperiment-aktiviteter: SOA-piloten, CWIX 2012 og CoNSIS.

3.1 SOA-piloten 2011

SOA-piloten er en eksperimentell demonstrator utviklet av FFI i samarbeid med NC3A (nå NCIA) og ressurser fra Forsvaret. Hensikten var å vise hvordan tjenesteorientering og bruk av en felles SOA-infrastruktur kan bidra til operativ nytte. En rekke eksisterende militære systemer ble inkludert i piloten, noe som økte de tekniske erfaringene i betydelig grad.

Med utgangspunkt i et scenario sentrert rundt en koalisjonsoperasjon ble det utviklet et hendelsesforløp med situasjoner som viste bruk av teknologi som ga operativ nytte. Utvalgte kjernetjenester fra Natos Core Enterprise Services (CES) [75] ble implementert i piloten, og blant disse fikk områdene service discovery og publish/subscribe størst synlighet. En egen visningsmodul (viewer) ble utviklet for å synliggjøre effekten av disse kjernetjenestene.

Figuren under viser hvilke eksisterende militære systemer som ble inkludert i piloten. For hvert av disse systemene ble det bygget et Web services-adapter foran, som gjorde at de enkelte systemene fremsto som tjenesteorienterte informasjonskilder inn mot informasjonsinfrastrukturen.



Figur 3.1 Oversikt over systemer involvert i SOA-piloten

I tillegg ble infrastrukturene fra FFI og NC3A koplet sammen, samt at sivil infrastruktur (internett) ble brukt for å hente kartdata fra Statens Kartverk. Både hos NC3A og FFI ble tjenesteorientert programvare for presentasjon av data brukt, og man sto fritt til å velge blant de ulike informasjonskildene.

Eksperimentene med SOA-infrastrukturen viste at en tjenesteorientert infrastruktur gir en stor fleksibilitet med hensyn på muligheter til å velge og kombinere informasjonskilder. Ved at alle parter fulgte spesifikasjonene fra Natos CES hadde man også mulighet til å velge informasjonskilder på tvers av infrastrukturer.

Som en del av SOA-piloten studerte prosjektet bruk av semantiske teknologier for å hjelpe en beslutningstaker med å oppdage tegn til trusler mot egne styrker i den store mengden tilgjengelig informasjon. Informasjonen kom i dette tilfellet hovedsakelig fra NORCCIS II og Nato-systemet JOCWatch. JOCWatch håndterer innsamling, organisering og distribusjon av innmeldte hendelser. Gjennom å definere trusselkriterier formelt i en ontologi, kunne vi demonstrere hvordan et multiagent-system kunne avsløre en mulig trussel ved bruk av automatisert resonnering. Denne delen av eksperimentet er nærmere beskrevet i [9].

SOA-piloten inkluderte også tre demonstrasjoner av ulike sikkerhetsløsninger for mer effektiv tilgang til informasjon på tvers av sikkerhetsdomener. Den første sikkerhetsløsningen som ble demonstrert var en prototypeløsning for å kunne håndtere flere sikkerhetsdomener på en og samme brukermaskin. Denne løsningen ble i SOA-piloten benyttet for å sammenligne informasjon fra ulike kilder på forskjellig graderingsnivå, samtidig som den ga mulighet til å interagere mot hvert sikkerhetsdomene. Den andre sikkerhetsløsningen som ble demonstrert var en prototype guardløsning for å kunne sluse informasjon mellom sikkerhetsdomener basert på konfidensialitetsmerker som angir informasjonens gradering. I SOA-piloten ble denne løsningen benyttet for å filtrere bort Mission Secret informasjon ved sammenkobling mot et Mission Restricted domene. Disse sikkerhetsløsningene er nærmere beskrevet i sikkerhetskapitlet av denne rapporten. Til slutt ble det også demonstrert bruk av en løsning for føderert identitetshåndtering og tilgangskontroll for å tillate eksterne brukere aksess til tjenester hos NC3A.

SOA-piloten viste imidlertid også at tjenesteorientering av systemer fortrinnsvis bør utføres av de enkelte systemleverandørene, eller andre som kjenner systemene godt fra innsiden. I tillegg så vi at det raskt oppstår et behov for tjenestehåndtering (service management & control), og dette er det viktig å ta i betraktning ved innføring av en tjenesteorientert infrastruktur i Forsvaret.

Resultatene fra piloten ble presentert på et seminar for Forsvaret, 15. og 16. juni 2011. SOA-piloten ble godt mottatt, og ble vurdert som et viktig initiativ som bidrar til NbF-utviklingen i Forsvaret. FFI anbefaler videre eksperimentarbeid i forlengelsen av SOA-piloten. Natos kjernetjenester er den foretrukne tekniske plattformen for dette.

SOA-piloten er dokumentert på et overordnet nivå i [14], mens ytterligere detaljer om henholdsvis tjenestedelen og sikkerhetsdelen av piloten er å finne i [13] og [16].

3.2 CWIX 2012

I samarbeid med NCIA deltok prosjektet med to aktiviteter på Natos CWIX (Coalition Warrior Interoperability eXperiment) 2012: En demonstrator for ontologibasert informasjonsintegrasjon, samt en teknisk utprøving av CoNSIS-eksperimentet som skulle gjennomføres kort tid etter. Den tekniske utprøvingen av CoNSIS ble på CWIX gjennomført med NCIA, som ikke deltok i CoNSIS, som testpartner. Foruten dette var det tekniske innholdet likt det som er beskrevet i kapittel 3.3.

Demonstratoren for ontologibasert inforasjonsintrgrasjon var bygget rundt en komponent som kunne ta en SPARQL-spørring og splitte den opp i mindre spørringer tilpasset de tilgjengelige informasjonskildene. I eksperimentet ble det demonstrert at semantiske teknologier kan bidra til å gi en beslutningstaker et verktøy der han kan uttrykke sitt informasjonsbehov i sitt eget vokabular, mens systemet tar seg av å oversette det til spørringer hver informasjonskilde kan behandle. Eksperimentet er nærmere beskrevet i [19].

3.3 CoNSIS 2012

Coalition Network for Secure Information Sharing (CoNSIS) er er et flernasjonalt samarbeid som er nærmere beskrevet i kapittel 4.2. CoNSIS-samarbeidet gjennomførte et større eksperiment i Greding i Tyskland, i juni 2012. I dette eksperimentet var målet å teste ut interoperabilitet i praksis mellom informasjonsinfrastrukturer i det taktiske domenet. Eksperimentet strakk seg over to uker, og inkluderte et stasjonært hovedkvarter (HQ) og ni biler.

Vårt prosjekt var involvert i arbeidsgruppe 2 og 3. For arbeidsgruppe 2 var målet med CoNSIS-eksperimentet å vise at ved å bruke Web service-standarder, slik de er spesifisert i NNEC Core Enterprise Services (NNEC CES), er tjenestespesifikasjoner (uttrykt i WSDL) tilstrekkelig for å få uavhengig implementerte tjenesteinfrastrukturer til å fungere sammen. Ved å fokusere på interoperabilitet gjennom bruk av standarder, blir det mulig å evaluere både de ulike implementasjonene *og* selve standardene som er benyttet. Dermed blir det mulig å vurdere hvor egnet standardene spesifisert i NNEC CES er for bruk i taktiske (radiobaserte) nettverk.

Arbeidsgruppe 2-delen av CoNSIS-eksperimentet hadde deltakere fra Tyskland og Norge, og besto av et multinasjonalt HQ (med representanter fra både Tyskland og Norge), en tysk konvoi (fire biler) og en norsk konvoi (fire biler). Internt i HQ ble det benyttet vanlig Ethernet, mens det i konvoyene ble brukt to radiotyper, tyske HiMonn og norske Kongsberg WM600. De to konvoiene hadde radioer av begge typer, slik at det var mulig å utveksle informasjon mellom dem, det samme hadde HQ. Konvoiene var i utgangspunktet et stykke fra hverandre, men underveis i eksperimentet ble de slått sammen. Dette innebar flere topologiendringer i nettverket, noe som påvirket forsinkelse og tilgjengelig båndbredde.

Vi fokuserte primært på to kjernetjenester, *service discovery* og *publish/subscribe*. I eksperimentet utgjorde de implementerte kjernetjenestene en infrastruktur for funksjonelle tjenester som tilbød tre typer informasjon: kjøretøyposisjoner, meldingstjeneste («operational messages») og chat. Hver bil rapporterte sin posisjon til lederbilen, som genererte et samlebilde for konvoien og sendte dette til HQ. Her ble samlebildene fra de to konvoiene slått sammen til ett bilde, som så ble distribuert til alle bilene, via lederbilene.

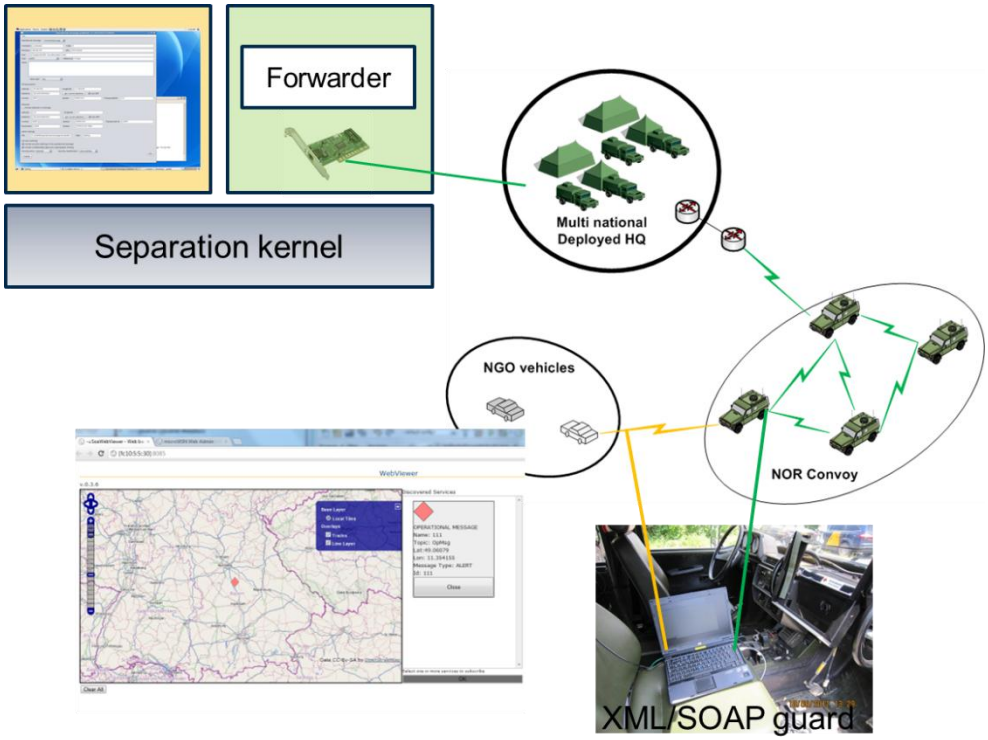
All informasjon ble distribuert med WS-Notification, som er spesifisert i NNEC CES som standarden for publish/subscribe. For alle datatyper gikk denne distribusjonen mellom HQ og alle bilene, med lederbilene som koplingspunktet mellom HQ og konvoiene. I og med at alle tjenester var basert på publish/subscribe var det ikke mulig å skille dem fra hverandre basert på *tjenestetype*. I stedet måtte de skilles basert på hvilken *informasjonstype* de tilbød, og for dette benyttet vi *topics* for å klassifisere de ulike informasjonstypene.

CoNSIS-eksperimentet viste at det er fullt mulig å knytte sammen ulike implementasjoner av tjenesteinfrastrukturer med kun tjenestespesifikasjoner som felles referanse. Dette forutsetter imidlertid at implementasjonene følger standardene fra NNEC CES eksakt, og i noen tilfeller er det også nødvendig med ytterligere spesifikasjoner i form av profiler.

Publish/subscribe er en effektiv metode for distribusjon av informasjon i taktiske nett, da det reduserer nettverkstrafikken noe. Vi brukte WS-Notification, som fungerte bra, men det var nødvendig med båndbreddereduserende tiltak i form av komprimering. Det er også ønskelig å forbedre effektiviteten i informasjonsdistribusjonen ytterligere, for eksempel gjennom bruk av pålitelig multicast. Vi så også behovet for å utvide funksjonaliteten i WS-Notification med mulighet for å sjekke status på abonnementer, samt mellomlagring av tidligere sendte meldinger. Dette er arbeid som pågår i Nato nå.

For service discovery benyttet vi WS-Discovery, som er godt egnet for dynamiske miljøer hvor tjenester kommer og går hele tiden. Eksperimentet viste at WS-Discovery fungerte bra, men viste at det er behov for å spesifisere en profil som muliggjør samtidig bruk både internt i, og på tvers av, subnett.

WS-Discovery ble også brukt til å distribuere topic-informasjon, og fungerte bra til dette. Vi så imidlertid behovet for mer arbeid rundt håndteringen av topics, blant annet slik at alle parter har en felles forståelse av hva de ulike topics betyr og hvordan de er organisert.



Figur 3.2 Eksperiment med informasjonsutveksling på tvers av sikkerhetsdomener

Innenfor CoNSIS arbeidsgruppe 3 utførte prosjektet et eksperiment med informasjonsutveksling på tvers av sikkerhetsdomener, som illustrert i Figur 3.2. Dette eksperimentet benyttet en guardløsning for bruk i tjenesteorienterte arkitekturer for å tillate toveis informasjonsutveksling mellom sikkerhetsdomenene, nærmere bestemt et gradert militært domene og et ugradert domene tilhørende en ikke-statlig organisasjon. Meldinger ble frigitt fra det militære domenet av guarden basert på konfidensialitetsmerker.

Foruten korrekt filtrering i guarden, avhenger en slik løsning av at en kan ha tiltro til konfidensialitetsmerkene. I dette tilfellet ville dette si å være sikker på at gradert informasjon ikke ble merket som ugradert. For å oppnå dette ble det benyttet en løsning basert på en MILS separasjonskjerne, hvor meldingene som skulle sendes gjennom guarden hadde opphav i en separat ugradert partisjon uten direkte tilgang til nettverket.

Eksperimentene i CoNSIS ble presentert på FFI i et heldagsseminar 7.11.2012. Ytterligere detaljer vil bli beskrevet i den internasjonale sluttrapporten fra CoNSIS [73] når den foreligger.

4 Internasjonale aktiviteter

I dette hovedkapitlet omtales prosjektets viktigste internasjonale samarbeidsrelasjoner og samarbeidende aktiviteter.

4.1 Nato kjernetjenester

Sentrale prosjektdeltakere har vært sterkt medvirkende til utgivelsen av dokumentet som anbefaler tekniske standarder for Nato kjernetjenester [75]. Forut for utgivelsen ble det gjennomført et omfattende arbeid i regi av arbeidsgruppen for Core Enterprise Services (CESWG). Den var en av mange organisert under NATO C3 Board (NC3B).

I 2012 ble strukturen med paneler og arbeidsgrupper under NC3B omorganisert. Det gode arbeidet fra CESWG er ment videreført i et såkalt Capability Team med tittelen Information and Integration Services. Arbeidet har så langt lidt under svak fremdrift og lav oppslutning fra nasjonene. FFI har en uttalt ambisjon om å delta i dette arbeidet fremover.

4.2 CoNSIS-samarbeidet

CoNSIS (Coalition Network for Secure Information Sharing) er et flernasjonalt samarbeidsprosjekt basert på en samarbeidsavtale mellom forsvarsministeriene i Frankrike, Tyskland, USA og Norge. Målet med prosjektet har vært å utvikle, implementere, teste og demonstrere teknologier og metoder som skal øke deltakerlandenes evne til å dele informasjon og tjenester på en sikker måte i ad hoc-koalisjoner og mellom sivile og militære kommunikasjonssystemer.

Prosjektet er sterkt knyttet til medlemslandenes arbeid med å innføre nettverksbasert forsvar, og intensjonen har vært å utnytte kommersielle standarder så langt som mulig, for å redusere interoperabilitetsproblemer. Kun der det ikke finnes tilgjengelige løsninger på det åpne markedet har man gjort egen utvikling

Arbeidet i CoNSIS har vært delt inn i fem arbeidsgrupper, hvor hver arbeidsgruppe fokuserer på ulike aspekter ved interoperabilitet. Prosjekt 1176 har vært representert i arbeidsgruppe 2 og 3.

- Arbeidsgruppe 1 har fokusert på hvordan man kan støtte en gjennomgående IP-basert infrastruktur. Målet har vært å demonstrere løsninger som fungerer innenfor de begrensningene som finnes i mobile taktiske nett med dynamiske topologier.
- Arbeidsgruppe 2 har sett på utfordringer knyttet til utveksling av informasjon og tjenester i radiobaserte nettverk. Målet har vært å demonstrere at ved å basere seg på Natos Core Enterprise Services-spesifikasjon kan man oppnå interoperabilitet mellom tjenesteorienterte infrastrukturer.
- Arbeidsgruppe 3 har undersøkt, spesifisert og demonstrert sikkerhetsmekanismer for å understøtte integrasjon og interoperabilitet i heterogene koalisjonsnettverk. Arbeidsgruppen har særlig fokusert på tre områder, sikkerhetsmekanismer i taktiske mobile nett, nettverkstopologier og arkitekturer som er egnet for sorte kjernenett, samt flernivå-sikkerhet uten behov for separate infrastrukturer for hvert sikkerhetsnivå.

- Arbeidsgruppe 4 har sett på mekanismer for automatisk monitorering og drift/forvaltning i koalisjonsnettverk.
- Arbeidsgruppe 5 har utviklet en overordnet eksperimentarkitektur for CoNSIS. Denne arkitekturen har vært førende for hvordan leveransene fra de øvrige arbeidsgruppene har blitt integrert. I tillegg har arbeidsgruppen stått for planlegging og koordinering av selve CoNSIS-samarbeidet

Første del av CoNSIS ble avsluttet med et stort felteksperiment som er nærmere beskrevet i kapittel 3.3. Det arbeides for en videreføring under arbeidstittelen CoNSIS-II.

4.3 Forskningsgruppen IST-090 om SOA i DisGrids

Forskningsgruppens tittel var ”SOA Challenges over disadvantaged grids”, og hovedmålet var å identifisere utfordringer knyttet til det å innføre SOA på det taktiske nivået, inkludert i disadvantaged grids. Gruppen undersøkte ulike tilnærminger til det å implementere SOA. Tyskland demonstrerte sin interimsløsning (teknisk sett ikke SOA, men et steg på veien til å realisere SOA), Spania demonstrerte sin DDS-baserte løsning, og NC3A, Polen, og Norge samarbeidet om å demonstrere bruken av Web services (inkludert interoperabilitet med DDS via et WS-DDS-grensesnitt som Polen utviklet). Norge stilte bl.a. med DSProxy, som implementerer en god del optimaliseringer for Web services og dermed muliggjør bruken av denne teknologien i nettverk med lav båndbredde og hyppige kommunikasjons-avbrudd.

Gruppen identifiserte viktige suksessfaktorer som at når man implementerer SOA er det viktig å basere seg på åpne standarder, og å benytte løsninger som er enkle å deployere og vedlikeholde. Proxy-konseptet ansees som smart, ettersom man da kan benytte standardiserte klienter og tjenester, og implementere optimaliseringer i proxyene for å håndtere kommunikasjonsutfordringene. Web services har kommet lengst med hensyn på standardisering, så denne teknologien bør benyttes der det er mulig. I visse sub-systemer kan det hende man har spesielle tjenestekvalitets- eller tidskrav, og da kan man vurdere å benytte andre teknologier som f.eks. DDS. Det en da må være klar over er at selv om DDS er standardisert, så fungerer ikke standarden i disadvantaged grids. Man må da benytte leverandørspesifikke optimaliseringer, og låser seg på denne måten i praksis til en leverandør.

IST-090 er fullført, og arbeidet som ble utført vil bygges videre på i den nyoppstartede gruppen IST-118 ”SOA Recommendations for Disadvantaged Grids in the Tactical Domain”. FFI vil delta i IST-118 der målet er å benytte kunnskaper fra IST-090 til å arbeide videre mot det vi kaller en taktisk SOA-profil. Profilen skal inneholde et sett med anbefalinger for hvordan man kan realisere gitte kjernetjenester på taktisk nivå. Se også [22] fra første møte.

4.4 Forskningsgruppen IST-094 om semantisk interoperabilitet

Forskningsgruppen IST-094 (Framework for Semantic Interoperability) var en videreføring av IST-075 (Semantic Interoperability), som FFI også deltok i.

Hovedmålet med gruppen var å videreføre ideene fra IST-075 om et rammeverk for semantisk interoperabilitet (Semantic Interoperability Logical Framework – SILF). Formålet med dette rammeverket er å gjøre systemer som ikke er designet for å utveksle informasjon i stand til allikevel å kunne gjøre dette. Arbeidet ble gjort gjennom arbeidsmøter og gjennom å arrangere et Nato-symposium (Semantic and Domain-Based Interoperability) og en tilhørende workshop i Oslo i november 2011.

Utgangspunktet for gruppen er definisjonen for semantisk interoperabilitet slik den ble definert i IST-075: *Semantisk interoperabilitet er to eller flere informasjonssystemers evne til å utveksle informasjon om en spesifikk oppgave slik at meningen av denne informasjonen automatisk blir tolketkorrekt av det mottagende systemet, med hensyn på oppgaven som skal utføres.* [77]

Resultatet fra gruppen var en tydeligere forståelse av hva et slikt rammeverk for semantisk interoperabilitet bør bestå i. Spesielt har gruppen fokusert på håndtering av ontologier, som har en sentral plass i rammeverket, og hvordan man skal representere oppgaver (tasks) slik oppgaver inngår i den ovennevnte definisjonen av semantisk interoperabilitet.

Gruppen ble avsluttet ved utgangen av 2012, og arbeidet videreføres i en ny forskningsgruppe: IST-119 – ”Maturing and Validation of SILF. Feasibility study”, der FFI også deltar. Resultatene fra IST-094 er fanget i sluttrapporten fra gruppen [78].

4.5 Forskningsgruppen IST-114 om sikker informasjonsdeling

IST-114 har tittelen ”Trusted Information Sharing for Partnerships”. Hovedfokuset til denne gruppen er å legge til rette for å kunne utveksle og dele informasjon mellom Nato og partnere. Et fremtidig behov er identifisert for å utveksle mellom systemer på forskjellige sikkerhetsnivåer (NATO Secret, Restricted og Unclassified) og systemer som tilhører internasjonale organisasjoner, ikke-statlige organisasjoner og nasjoner som ikke er medlemmer av Nato.

Konseptet Information Exchange Gateway (IEG) har blitt tatt frem for å kunne realisere slik utveksling. Flere scenarier er definert for IEG som reflekterer forskjellige ambisjonsnivåer, der scenarioene A – C er relativt godt forstått og definert. Gruppen fokuserer på IEG scenario D (utveksling av informasjon fra NATO Secret til ikke statlige aktører o.l.), som er det mest komplekse og kanskje til nå minst definerte og forståtte scenarioet. Krav, design og løsninger for IEG scenario D preges av en høy grad av kompleksitet. Gruppen har delt sitt arbeid inn i tre arbeidspakker:

- **Arbeidspakke 1: Design av IEG Scenario D.** Denne arbeidspakken vil definere operasjonelle krav og design av en IEG scenario D. Leveranser fra denne arbeidspakken vil også inkludere krav til informasjonsutveksling og krav til informasjonssikkerhet.

- **Arbeidspakke 2: Plattformer med høy tillit.** I denne arbeidspakken vil gruppen se på plattformer med høye tillitsnivåer (high assurance) og utvikling av guard-løsning med høy tillit.
- **Arbeidspakke 3: Merking av informasjon.** I denne arbeidspakken vil gruppen jobbe videre med resultatene som ble produsert av den tidligere gruppen IST-068 XML in Cross Domain Security Solutions. Denne gruppen foreslo blant annet spesifikasjoner for konfidensialitetsmerker. Arbeidet i denne gruppen vil blant annet undersøke behovet for og innhold i eventuelle merker for integritet og tilgjengelighet.

Gruppen er bredt sammensatt og ledes av Italia. Den har nasjonale medlemmer fra Norge, Sverige, Storbritannia, Polen, Tyrkia og Tyskland, i tillegg til er Nato-institusjoner som ACT og NCIA representert.

IST-114 ble startet våren 2012 og prosjektet har vært involvert i siden dette. Gruppen avslutter sitt arbeid ved årsskiftet 2014 og 2015 og vår representasjon vil bli videreført av FFI prosjektet 1294 IKT-sikkerhet i Cyberdomenet (ISIC). Gruppen vil levere en avsluttende rapport.

5 Publikasjoner utenfor FFI

Prosjektet har medvirket til tre journalartikler og i alt 27 bidrag til internasjonale konferanser. En oversikt med hovedfokus på bidragenes titler er gjengitt i tabellform nedenfor. For konferansedelen er også tatt med referanser til FFI-reiserapport der det finnes. Ytterligere detaljer, inkludert fullstendig forfatteroversikt, er gjengitt i referanselisten.

Journalartikler:

#	Artikkel	Tidsskrift	Ref
1	Semantic Service Discovery for Interoperability in Tactical Military Networks	The International C2 Journal, Volume 4, Number 1, 2010	[43]
2	Web Services Discovery across Heterogeneous Military Networks	IEEE Communications Magazine, Special Issue on Military Communications, October 2010	[44]
3	Robust Web services in heterogeneous military networks	IEEE Communications Magazine, Special Issue on Military Communications, October 2010	[45]

Konferansebidrag:

#	Tittel	Konferanse	Ref
1	A Proposal for an XML Confidentiality Label Syntax and Binding of Metadata to Data Objects	NATO RTO/IST Panel Symposium, 2010	[46]
2	Semantically Enabled QoS Aware Service Discovery and Orchestration for MANETs	ICCRTS 2010	[47]
3	Experiments with Web Services at Combined Endevour	ICCRTS 2010	[48]
4	IST-090 SOA Challenges for Disadvantaged Grids	ICCRTS 2010	[49]
5	Publish/Subscribe with COTS Web Services across Heterogeneous Networks	8th IEEE ICWS 2010	[50]
6	Enabling Publish/Subscribe with COTS Web Services across Heterogeneous Networks	4th ACT4SOC 2010	[51]
7	Automated QoS-aware Service Selection and Orchestration in Disadvantaged Grids	MCC 2010	[52]
8	Robust and Efficient Service Discovery in Highly Mobile Radio Networks using the MIST Protocol	IEEE MILCOM 2010	[53]
9	Cross-Domain Access Control in a Military SOA	IEEE MILCOM 2010	[54]
10	Service Advertisements in MANETs (SAM): A Decentralized Web Services Discovery Protocol	UbiCoNet, IEEE GLOBECOM 2010	[55]
11	Adapting WS-Discovery for use in tactical networks	ICCRTS 2011	[56][8]
12	Employing Web services between domains with restricted information flows	ICCRTS 2011	[57][8]
13	Towards Ontology Matching Suitable for Information Integration in Time-Critical Situations	ICCRTS 2011	[58][8]
14	An Experimental Evaluation of Web Services Discovery Protocols for Search and Rescue Operations	IEEE IWCMC 2011	[59]
15	An Evaluation of Web Services Discovery Protocols for the Network-Centric Battlefield	MCC 2011	[60][10]
16	An Overview of the Research and Experimentation of IST-090: SOA over Disadvantaged Grids	MCC 2011	[61][10]
17	Integrating Military Systems using Mobile Agents	NATO RTO/IST Panel Symposium, 2011	[62]
18	Integrating Wireless Sensor Networks in the NATO Network Enabled Capability using Web Services	IEEE MILCOM 2011	[63]
19	Distributed Chat in Dynamic Networks	IEEE MILCOM 2011	[64]
20	Cross-layer Quality of Service Based Admission Control for Web Services	IEEE HeterWMN 2011	[65]
21	An Emulated Test Framework for Service Discovery and MANET Research based on ns-3	5th IFIP NTMS 2012	[66][18]
22	Mist: A Reliable and Delay-Tolerant Publish/Subscribe Solution for Dynamic Networks	5th IFIP NTMS 2012	[67][18]
23	Towards operational agility using service oriented integration of prototype and legacy systems	ICCRTS 2012	[68][27]
24	Topic Discovery for Publish/Subscribe Web Services	The 8th IWCMC 2012	[69][21]
25	SOA over disadvantaged grids experiment and demonstrator	IEEE MCC 2012	[70]
26	Bandwidth optimizations for standards-based publish/subscribe in disadvantaged grids	IEEE MILCOM 2012	[71]
27	Role-based Quality of Service for Web Services	IEEE HeterWMN 2012	[72]

6 Andre bidrag

Med en innretning fokusert mot de muliggjørende elementer i fremtidens INI, har prosjektet hatt hovedvekt på kombinasjonen av teoretiske studier og praktisk utprøving av tilgjengelige teknologiske løsninger. I tillegg til de aktiviteter og resultater som er beskrevet i foregående kapitler, fortjener følgende øvrige bidrag å trekkes frem:

- Prosjektet har gjennom hele arbeidet hatt en nær relasjon til Forsvarets prosjekt 8009 – Modernisering av kjernetjenester. Det har vært enighet om å legge til rette for avtapninger av løsninger, og prosjektet har siden høsten 2012 deltatt i 14-daglige arbeidsmøter med utviklingsmiljøet for SOA-infrastruktur i 8009.
- Prosjektet har deltatt i arbeidet med å utvikle prosjektideen for det planlagte leveranseprosjektet ”Tilgjengeliggjøring av sensorinformasjon for beslutningsstøtte” (8156)
- Prosjektets fagmiljø var en bidragsyter til FFIs vurdering av fremtidig innretning av investeringsporteføljen på området NbF og INI, ref [79]
- En prosjektmedarbeider deltok i gruppen fra FFI som vurderte mulige tekniske løsninger for beskyttet kommunikasjon mellom offentlige etater på oppdrag fra Barentswatch, ref [80]

Flere studenter har fått veiledning frem mot master- eller bacheloroppgaver gjennom prosjektets fagmiljø. Oppgaveresultatene har bidratt positivt til prosjektets arbeid, det samme har sommerstudentene vi har hatt. Se eksempler på gode resultater i [4][11][20][72].

Et viktig mål med prosjektet har vært kompetansebygging. Det innebærer deltakelse på kurs og konferanser, også i noen tilfeller uten at vi har egne forskningsresultater som skal presenteres. Et sett reiserapporter fra slik kompetanse- og relasjonsbyggende deltakelse er [3][6][12][17].

Prosjektet har i 2013 gitt viktige bidrag til å få etablert en såkalt ”INI-lab” ved FFI. Hensikten er å fasilitere utprøving av INI-relaterte løsninger (kommunikasjon, kjernetjenester, sikkerhetsløsninger) i kombinasjon med utvalgte mer brukerorienterte prosjektmiljøer, som det finnes mange av på FFI.

I tillegg til at dette gir gode muligheter til eksperimentell bruk av prosjektets kjernetjenester i mer operativt orienterte løsninger, vil INI-lab være en velegnet arena for samordning av eksperiment-innsats fra ulike FFI-miljøer, eksempelvis som en forberedelse til deltakelse på Forsvarets øvelser. For det videre arbeid innenfor SOA og semantiske teknologier vil det være viktig å holde fokus på relevante militære anvendelser av de teknologiske løsninger som forskningen resulterer i.

Referanser

[1] Eggen Anders, Haakseth Raymond, Oudkerk Sander (NC3A), Thummel Andreas (NC3A), "XML Confidentiality Label Syntax – a proposal for a NATO specification", FFI-rapport 2010/00961

[2] Eggen Anders, Haakseth Raymond, Oudkerk Sander (NC3A), Thummel Andreas (NC3A), "Binding of Metadata to Data Objects – a proposal for a NATO specification", FFI-rapport 2010/00962

[3] Halvorsen Jonas, Semantic Technology Conference 2010, FFI-reiserapport 2010/01561

[4] Berg Peter, Hansen Bjørn Jervell, "Algoritme for ontologimatching", FFI-notat 2010/01607

[5] Johnsen Frank T., "NATO RTO/IST-090 meeting in October 2010 in Madrid, Spain", FFI-reiserapport 2010/02137

[6] Rustad Marianne, "Semantic Days 2010 - Stavanger 31. mai - 2. juni 2010", FFI-reiserapport 2010/02199

[7] Johnsen Frank T., "Pervasive Web Services Discovery and Invocation in Military Networks", FFI-rapport 2011/00257

[8] Johnsen Frank T., Hafsøe Trude, Hansen Bjørn J., "16th Command and Control Resarch and Technology Conference, Quebec City Canada, 21-23.06.11, FFI-reiserapport 2011/01389

[9] Halvorsen Jonas, Hansen Bjørn Jervell: "Integrating military systems using semantic web technologies and lightweight agents", FFI-notat 2011/01851

[10] Johnsen Frank T. , Hafsøe Trude: "NATO RTO/IST-090 final meeting and demo at MCC 2011", FFI-reiserapport 2011/01936

[11] Nordmoen Jørgen, Johnsen Frank T., Skjegstad Magnus, Bloebaum Trude H., "Using ns-3 to evaluate mobile nodes running web services discovery protocols", FFI-notat 2011/02173

[12] Hansen Bjørn Jervell, Halvorsen Jonas: "International Semantic Web Conference 2011", FFI-reiserapport 2011/02215

[13] Lund Ketil, Johnsen Frank T., Bloebaum Trude H., Skjervold Espen: "SOA Pilot 2011 - service infrastructure", FFI-rapport 2011/02235

[14] Rasmussen Rolf, Hansen Bjørn Jervell: "Experiment report – SOA Pilot 2011", FFI-rapport 2011/02407

[15] Nordbotten Nils Agne, Gjertsen Tor "Towards a certifiable MILS based workstation", FFI-rapport 2012/00049

[16] Haakseth Raymond, "SOA Pilot 2011: Demonstrating secure exchange of information between security domains", FFI-rapport 2012/00117

[17] Johnsen Frank T: "Traffic monitoring and analysis workshop & passive and active measurement conference 2012", FFI-reiserapport 2012/00620

[18] Johnsen Frank T., "The 5th international conference on new technologies, mobility and security (NTMS 2012)", FFI-reiserapport 2012/01145

[19] Hansen Bjørn Jervell, Halvorsen Jonas, Stolpe Audun, "Information integration experiment at NATO CWIX 2012", FFI-rapport 2012/01543

[20] Nordmoen Jørgen, Johnsen Frank T., Bloebaum Trude H., "Towards a framework for automated protocol evaluation in MANETs using ns-3", FFI-notat 2012/01574

[21] Johnsen Frank T., “The eighth IEEE International Wireless Communications and Mobile Computing Conference (IWCMC 2012)”, FFI-reiserapport 2012/01827
[22] Johnsen Frank T., Bloebaum Trude H., “NATO IST-118 SOA recommendations for disadvantaged grids kick-off meeting”, FFI-reiserapport 2012/02233
[23] Johnsen Frank T., Bloebaum Trude H., Brannsten Marianne R., “Quality aspects of Web services”, FFI-rapport 2012/02494
[24] Gjørven Eli, Stolpe Audun, “On the roles and synergies of the service oriented architecture- and the semantic technologies paradigms in an NNEC context”, FFI-notat 2013/00131
[25] Gjertsen Tor, “Concept for Trusted Binding of Metadata to Data”, FFI-rapport 2013/00547
[26] Lund Ketil, Bloebaum Trude H., Johnsen Frank T., ”Enterprise Service Bus: definisjon og bruksområder”, FFI-rapport 2013/00441
[27] Reitan Bård K, Johnsen Frank T, Darisiro Ramin, ”17th ICCRTS - International Command and Control Research and Technology Symposium, 19-21 juni 2012, Fairfax/Washington DC, USA”, FFI-reiserapport 2013/00615
[28] Hansbø Morten, Jørgensen Håvard D., Rasmussen Rolf, ”Arkitekturarbeid i Forsvaret med forenklet bruk av NATO Architecture Framework (NAF)”, FFI-rapport 2013/01069
[29] Bloebaum Trude H. et al, ”Architecture for the Norwegian Defence Information Infrastructure (INI) – Remarks for the INI Laboratory at the Norwegian Defence Research Establishment”, FFI-rapport 2013/01729
[30] Hansbø Morten, Skogstad Arne, ”889 Systemarkitektur - erfaringer og anbefalinger”, FFI-rapport 2010/01158
[31] Sunde, ”Forsvarssjefens plan for utvikling av et nettverksbasert forsvar. Del II – Plan”, 2011
[32] US DoD Deputy Chief Management Officer, “Use of End-to-End (E2E) Business Models and Ontology in DoD Business Architectures. Memorandum for secretaries of the military departments”, 2011
[33] US DoD Deputy Chief Management Officer, “Same mission, new vision. The future of the DoD Business Enterprise Architecture”, 2012
[34] Wooldridge, “An introduction to MultiAgent Systems”. Second Edition. Wiley, 2009
[35] NATO ACT, “TIDE Transformational Baseline 3.0”, 2009
[36] Hitzler, Krötzsch, Rudolph, “Foundations of Semantic Web Technologies”. CRC Press, 2009
[37] Euzenat, Shvaiko, “Ontology Matching”. Springer, 2009
[38] Smith, Barry et. al, “Ontology for the Intelligence Analyst”, CrossTalk: The Journal of Defense Software Engineering, November/December 2012,18-25.
[39] Garshol, Borge, “Hafslund Sesam - an archive on semantics”. Proceedings of the 10th Extended Semantic Web Conference (ESWC), 2013
[40] Pierce, Booth, Ogbuji, Deaton, Blackstone, Lenat, “SemanticDB: A Semantic Web Infrastructure for Clinical Research and Quality Reporting”. Current Bioinformatics, 2012
[41] Briggs, Sahoo, Raghavendra, Appavu, Anwar, “Resource description framework application development in DB2 10 for Linux, UNIX, and Windows”, 2012

[42] Oracle, “Oracle Database. Semantic Technologies Developer's Guide 11g Release 2 (11.2)”, 2010

[43] Frank T. Johnsen, Marianne Rustad, Trude Hafsøe, Anders Eggen, Tommy Gagnes, ”Semantic Service Discovery for Interoperability in Tactical Military Networks”, The International C2 Journal, Volume 4, Number 1, 2010

[44] Frank T. Johnsen, Trude Hafsøe, Anders Eggen, Carsten Griwodz, Pål Halvorsen, ”Web Services Discovery across Heterogeneous Military Networks”, IEEE Communications Magazine, Special Issue on Military Communications, October 2010

[45] Ketil Lund, Espen Skjervold, Frank T. Johnsen, Trude Hafsøe, Anders Eggen, ”Robust Web services in heterogeneous military networks”, IEEE Communications Magazine, Special Issue on Military Communications, October 2010

[46] Sander Oudkerk (NC3A) , Anders Eggen (FFI), Raymond Haakseth (FFI), Ian Bryant (UK MOD), ”A Proposal for an XML Confidentiality Label Syntax and Binding of Metadata to Data Objects”, NATO RTO/IST Panel Symposium (IST-091) Information Assurance and Cyber Defence, Antalya Turkey, April 2010.

[47] Trude Hafsøe. Frank T. Johnsen, Marianne Rustad, ”Semantically Enabled QoS Aware Service Discovery and Orchestration for MANETs”, 15th International Command and Control Research and Technology Symposium (ICCRTS), Santa Monica, CA, USA, June 2010

[48] Frank T. Johnsen, Trude Hafsøe, ”Experiments with Web Services at Combined Endevour”, 15th International Command and Control Research and Technology Symposium (ICCRTS), Santa Monica, CA, USA, June 2010

[49] Annunziata, Francesca; Ardic, Burcu; Denis, Xavier; Fletcher, Graham; Hafsøe, Trude; Hernández Novo, Ignacio; Jansen, Norman; Johnsen, Frank Trethan; Meiler, Peter-Paul; Owens, Ian; Sasioglu, Betül; Sliwa, Joanna; Stavnstrup, Jens; Tokuz, Akif, ”IST-090 SOA Challenges for Disadvantaged Grids”, 15th International Command and Control Research and Technology Symposium (ICCRTS), Los Angeles, CA, USA, June 2010.

[50] Espen Skjervold, Trude Hafsøe, Frank T. Johnsen, Ketil Lund, ”Publish/Subscribe with COTS Web Services across Heterogeneous Networks”, 8th IEEE International Conference on Web Services (ICWS), Miami, FL, USA, July 2010

[51] Espen Skjervold, Trude Hafsøe, Frank T. Johnsen, Ketil Lund, ”Enabling Publish/Subscribe with COTS Web Services across Heterogeneous Networks”, 4th International Workshop on Architectures, Concepts and Technologies for Service Oriented Computing (ACT4SOC) 2010, held in conjunction with 5th International Conference on Software and Data Technologies (ICSOFT), Athens, Greece, July 2010

[52] Trude Hafsøe, Frank T. Johnsen, Marianne Rustad, ”Automated QoS-aware Service Selection and Orchestration in Disadvantaged Grids”, Military Communications and Information Systems Conference (MCC), Wroclaw Poland, September 2010

[53] Magnus Skjegstad, Frank T. Johnsen, Trude Hafsøe, Ketil Lund, ”Robust and Efficient Service Discovery in Highly Mobile Radio Networks using the MIST Protocol”, IEEE Military Communications Conference (MILCOM), San Jose, CA, USA, October 2010

[54] Nils Agne Nordbotten, ”Cross-Domain Access Control in a Military SOA”, IEEE Military Conference on Communications (MILCOM), San Jose, CA, USA, October 2010.

[55] Frank T. Johnsen, Trude Hafsøe, ”Service Advertisements in MANETs (SAM): A Decentralized Web Services Discovery Protocol ”, Workshop on Ubiquitous Computing and Networks (UbiCoNet), IEEE Global Communications Conference (GLOBECOM), Miami ,FL, USA, December 2010

[56] Frank T. Johnsen, Trude Hafsøe, ”Adapting WS-Discovery for use in tactical networks”, 16th ICCRTS, June 2011

[57] Trude Hafsøe, Frank T. Johnsen, ”Employing Web services between domains with restricted information flows”, 16th ICCRTS, June 2011

[58] Bjørn Jervell Hansen, ”Towards Ontology Matching Suitable for Information Integration in Time-Critical Situations”, 16th International Command and Control Research and Technology Symposium (ICCRTS), Québec City, Canada, June 2011

[59] M. Skjegstad, F.T. Johnsen, T. Hafsøe, ”An Experimental Evaluation of Web Services Discovery Protocols for Search and Rescue Operations”, IEEE IWCMC 2011, Istanbul, Turkey, July 5-8, 2011.

[60] Magnus Skjegstad, Frank T. Johnsen, Trude Hafsøe, ”An Evaluation of Web Services Discovery Protocols for the Network-Centric Battlefield”, MCC 2011, Amsterdam, Netherlands, 17-18 October 2011

[61] Peter-Paul Meiler, Francesca Annunziata, Burcu Ardic, Christoph Barz, Graham Fletcher, Trude Hafsøe, Novo Ignacio Hernández, Norman Jansen, Frank T. Johnsen, Daniel Marco-Mompel, Jonas Martin, Ian Owens, Betül Sasioglu, Léon Schenkels, Joanna Śliwa, Jens Stavnstrup, Akif Tokuz, ”An Overview of the Research and Experimentation of IST-090: SOA over Disadvantaged Grids”, MCC 2011, Amsterdam, Netherlands, 17-18 October 2011

[62] Jonas Halvorsen, Bjørn Jervell Hansen, ”Integrating Military Systems using Mobile Agents”, Symposium (IST-101/RSY-024) Semantic and Domain-Based Interoperability, Oslo, Norway, November 2011

[63] Joakim Flathagen and Frank T. Johnsen, ”Integrating Wireless Sensor Networks in the NATO Network Enabled Capability using Web Services”, IEEE MILCOM 2011, Baltimore, MD, USA, November 7-10 2011

[64] Magnus Skjegstad, Ketil Lund, Espen Skjervold, and Frank T. Johnsen, ”Distributed Chat in Dynamic Networks”, IEEE MILCOM 2011, Baltimore, MD, USA, November 7-10 2011

[65] Frank T. Johnsen, Trude Hafsøe, Mariann Hauge, Øyvind Kolbu, ”Cross-layer Quality of Service Based Admission Control for Web Services”, IEEE HeterWMN 2011, Houston, TX, USA, December 9 2011

[66] Magnus Skjegstad, Frank T. Johnsen, Jørgen Nordmoen, ”An Emulated Test Framework for Service Discovery and MANET Research based on ns-3”, 5th IFIP International Conference on New Technologies, Mobility and Security (NTMS) 2012, Istanbul, Turkey, 7-10 May 2012

[67] Magnus Skjegstad, Frank T. Johnsen, Trude H. Bloebaum, Torleiv Maseng, ”Mist: A Reliable and Delay-Tolerant Publish/Subscribe Solution for Dynamic Networks”, 5th IFIP International Conference on New Technologies, Mobility and Security (NTMS) 2012, Istanbul, Turkey, 7-10 May 2012

[68] Frank T. Johnsen, Trude H. Bloebaum, Ketil Lund, Espen Skjervold, ”Towards operational agility using service oriented integration of prototype and legacy systems”, ICCRTS 2012, Fairfax, VA, USA, June 19-21 2012

[69] Frank T. Johnsen, Trude H. Bloebaum, ”Topic Discovery for Publish/Subscribe Web Services”, The 8th International Wireless Communications and Mobile Computing Conference (IWCMC 2012), Limassol, Cyprus, August 27-31 2012

[70] Frank T. Johnsen, Trude H. Bloebaum, Léon Schenkels, Rui Fiske, Marc van Zelm, Vincenzo de Sortis, Aad van der Zanden, Joanna Śliwa, and Przemysław Caban, ”SOA over disadvantaged grids experiment and demonstrator”, Military Communications and Information Systems Conference (MCC) 2012, Gdańsk, Poland, 8-9 October, 2012

[71] Espen Skjervold, Ketil Lund, Trude H. Bloebaum, and Frank T. Johnsen, ”Bandwidth optimizations for standards-based publish/subscribe in disadvantaged grids”, IEEE MILCOM 2012, Orlando, FL, USA, October 29 - November 1, 2012

[72] Frank T. Johnsen, Trude H. Bloebaum, Jørgen Nordmoen, Jan A. S. Bremnes, Stig Tore Johanessen, Magnus L. Kirø, Ola Martin T. Støvneng, and Håvard Tørresen, ”Role-based Quality of Service for Web Services”, IEEE HeterWMN 2012, Anaheim, CA, USA, 3 December 2012

[73] CoNSIS, ” Coalition Networks for Secure Information Sharing - Final Report” (under utgivelse, bidrag fra Task 1 til 5 foreligger)

[74] EPIM ReportingHub: http://www.reportinghub.org/erh/menu/about-erh

[75] NATO CESWG, ”Core Enterprise Services Standards Recommendations - The SOA Baseline Profile version 1.7”, dated 11.11.2011

[76] NC3A, ”NATO Network Enabled Capability Feasibility Study,Volume 1, Version 2.0”, 2005.

[77] Bacchelli, Boury-Brisset, Isenor, Kuehne, Martinez Reif, Miles, Mojtahedzadeh, Poell, Rasmussen, Uzunali, Wunder, “Semantic Interoperability”, NATO RTO Technical Report, 2009

[78] Ford, Kuehne, Hansen, Hanz, Last, Nogalski, Mojtahedzadeh, Tuncer, Wunder, “Framework for Semantic Interoperability”, NATO RTO Technical Report, 2012

[79] Winjum Eli, Bentstuen Ole Ingar, Eggen Anders, Lund Ketil, Macdonald Robert H., Nordbotten Nils Agne, Rasmussen Rolf, Reitan Bård, Voldhaug Jan Erik, “Forslag til innretting av perspektivplan materiell (PPM) for programområde NbF-systemer”, FFI-rapport 2012/02075 (unntatt offentlighet)

[80] Hagen Janne Merete, Fongen Anders, Gjørven Eli, Libæk Bjørnar, ”Studie for BarentsWatch om løsninger for beskyttet kommunikasjon mellom etater”, FFI-rapport 2013/00697 (unntatt offentlighet)

[81] NATO CESWG, ”Core Enterprise Services Framework V1.2”, 2009

[82] NATO IP CaT, ”NATO Interoperability Standards and Profiles”, ADatP-34(G) dated 08.03.2013; http://nhqc3s.nato.int/architecture/_docs/NISP/index.html

Forkortelser

ACT	Allied Command Transformation
C3	Consultation, Command and Control (NATO-kontekst)
CD&E	Concept Develompent and Experimentation
CES	Core Enterprise Services
CESWG	CES Working Group
COI	Community of Interest
CoNSIS	Coalition Network for Secure Information Sharing
COTS	Commercial off-the-shelf
CWIX	Coaltion Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise
DDS	Data Distribution Service
DoD	Department of Defence
EAL	Evaluation Assurance Level
ebXML	electronic business using XML
ESB	Enterprise Service Bus
FIF	Felles integrert forvaltningssystem
FLO	Forsvarets logistikkorganisasjon
FLO/IKT	FLOs avdeling for Informasjons- og kommunikasjonsteknologi
HQ	Headquarter
HTTP	Hypertext Transfer Protocol
IEG	Information Exchange Gateway
IM	Information Management
INI	Forsvarets informasjonsinfrastruktur
IP	Internet Protocol
ISIC	IKT-sikkerhet i Cyberdomenet
IST	Information Systems Technology
MANET	Mobile adhoc-nett
MILS	Multiple Indendent Levels of Security
NAF	NATO Architecture Framework
NATO	North Atlantic Treaty Organization
NbF	Nettverksbasert forsvar
NC3A	NATO C3 Agency
NC3B	NATO C3 Board
NCIA	NATO Communications and Information Agency
NEC	Network Enabled Capabilty (ref NbF)
NISP	NATO Interoperability Standards and Profiles
NNEC	NATO NEC
OASIS	Organization for the Advancement of Structured Information STandards
PCN	Protected Core Network
QoS	Quality of Service

RTO	Research and Technology Organization
SD	Service discovery
SILF	Semantic Interoperability Logical Framework
SOA	Service-oriented architectures
SPARQL	SPARQL Protocol And RDF Query Language
TCP	Transmission Control Protocol
TIDE	Technology for Information, Decision and Execution
UAV	Unmanned Aerial Vehicle
UDDI	Universal Description, Discovery and Integration
US	United States
W3C	World Wide Web Consortium
WS	Web service
WSDL	Web Service Description Language
XML	eXtensible Markup Language