Experiment report: “SOA – Cross Domain and Disadvantaged Grids” – NATO CWID 2007

Raymond Haakseth, Tommy Gagnes, Dinko Hadzic, Trude Hafsøe, Frank Trethan Johnsen, Ketil Lund and Bård Karsten Reitan

Norwegian Defence Research Establishment (FFI)

26.11.2007

FFI-rapport 2007/02301

1086

ISBN 978-82-464-1272-6

Keywords

Nettverksbasert forsvar

Tjenesteorientert arkitektur

Webtjenester

Eksperimentering

Informasjonssikkerhet

Semantisk teknologi

Lynmeldinger

Approved by

Anders Eggen	Project manager
Vidar S. Andersen	Director

Sammendrag

Våren 2007 deltok til sammen tre prosjekter fra FFI på øvelsen NATO Coalition Warrior Interoperability Demonstration (CWID) på Jørstadmoen. Deltagelsen var samlet under ett forsøk med navnet ”SOA – Cross Domain and Disadvantaged Grids”. Prosjektene som deltok fra FFI var: 1086 – Sikker gjennomgående SOA, 1085 – SEMANTINI og 1084 – SINETT. Førstnevnte prosjekt var toneangivende, mens de to andre spilte mindre, men viktige, roller.

CWID er en multilateral øvelse som har som hovedformål å teste interoperabilitet mellom forskjellige nasjoners systemer. Det er først og fremst operative systemer som skal delta i NATO Response Force (NRF) og Combined Joint Task Force (CJTF) som testes. Det legges i tillegg stor vekt på eksperimentering for kartlegging av fremtidige behov, slik som NATO Network Enabled Capability (NNEC). For årets utgave av CWID var dette også trukket frem som et av tre hovedmål, med spesielt fokus på tjenesteorienterte arkitekturer (SOA).

Felles for alle prosjektene som deltok fra FFI er fokus på Nettverksbasert Forsvar (NbF) og alle har som overordnet målsetning å støtte utviklingen av et fremtidig NbF. Siden NbF er den norske ekvivalenten til NNEC passet de tre prosjektenes aktiviteter godt inn i målsetningen for CWID. Totalt ble det utført fire eksperimenter under FFI forsøket, og prosjekt 1086 – Sikker gjennomgående SOA utførte to av disse. Det første eksperimentet så på løsninger for automatisk toveis informasjonsutveksling mellom sikkerhetsdomener ved å bruke sikkerhetsmerking og filtrering. Bruk av SOA, og da spesielt Web Services, på lavere taktisk nivå var tema for det andre eksperimentet utført av prosjektet. Hovedtemaet her var effektiv representasjon og utveksling av informasjon. Prosjekt 1085 – SEMANTINI brukte CWID til å eksperimentere med semantisk informasjonsintegrasjon, og hovedtemaet for dette eksperimentet var integrering av informasjon fra heterogene kilder ved hjelp av semantisk teknologi. Utforskning av nye måter å interagere med tjenester på var fokuset for prosjekt 1084 – SINETT, og det ble demonstrert bruk av lynmeldinger (instant messaging) for å kommunisere med tjenester i ett nettverk.

Dette dokumentet oppsummerer alle aktivitetene og eksperimentene utført av FFI på CWID 2007. Inkluderer i denne oppsummeringen er beskrivelse av problemstillinger og hypoteser, gjennomføring og resultater. Mer detaljerte tekniske beskrivelser vil bli tilgjengelig gjennom en serie av ”FFI-notat”.

English summary

During the spring of 2007, three FFI projects participated at the NATO Coalition Warrior Interoperability Demonstration (CWID) at Jørstadmoen, Lillehammer. The participation was gathered under a trial named “SOA – Cross Domain and Disadvantaged Grids”. The following projects participated from FFI; 1086 – Secure and Pervasive SOA, 1085 – SEMANTINI, and 1084 – SINETT.

CWID is an annual event targeted at improving interoperability between C4I systems of NATO, NATO nations and partner nations. Its main objective is ensuring interoperability of systems to be deployed in NATO Response Force (NRF) and Combined Joint Task Force (CJTF). In addition, the need to perform experimentation in order to uncover future requirements is recognised. This year one of three overall goals defined for CWID was NATO Network Enabled Capability (NNEC), and especially the use of Service Oriented Architectures (SOA).

The common denominator for the three FFI projects participating at CWID this year is Network Based Defence (NBD) and providing support for the development of the future information infrastructure. NBD may be regarded as the Norwegian equivalent of NNEC, therefore established activities within the projects fit well into the CWID objective. A total of four different experiments were performed under the FFI trial. Project 1086 – Secure and Pervasive SOA conducted two experiments. First, in order to achieve automatic information exchange between security domains one experiment tested the use of trusted security labels and filtering. In the second experiment, service enabling of the lower tactical levels was demonstrated, with focus on efficient representation and exchange mechanisms for information in disadvantaged grid environments. Semantic information integration was the focus of the experiment performed by project 1085 – SEMANTINI. This experiment involved translation between heterogeneous data models using semantic technology. Finally, the project 1084 – SINETT experimented with instant messaging as a human interface to services as part of exploring new ways of interacting with services.

This document summarises the activities and experiments performed by FFI at CWID 2007. This includes problem descriptions and hypotheses, execution of the experiments and results gained during CWID. While this document provides a high-level view of the experiments, a series of ‘FFI-notat’ will be published covering the technical details.

Contents

1 Introduction

In the spring of 2007, FFI participated at NATO CWID 2007 with a trial named "SOA – Cross Domain and Disadvantaged Grids". This document describes the activities conducted in preparation to, and during CWID. This includes a description of the technological goals defined and the results gained. The participation by FFI at NATO CWID 2007 may be regarded as a follow-up from the participation at NATO CWID 2006 by the FFI project "889 – NBF Beslutningsstøtte" [1]. For CWID 2007 the FFI delegation involved participation from three projects, namely project "1086 – Secure and Pervasive SOA", project "1085 – SEMANTINI" and project "1084 – SINETT". The first of the above mentioned projects was the main contributor, while the other two played minor parts. In total, four different experiments were performed by the FFI trial. This document provides an overview of these, while a series of documents in the form of 'FFI-notat' were produced for more in-depth technical documentation of the experiments [2-4].

This document is structured as follows; Section 2 gives an overall description of NATO CWID and gives a more explicit description of the focus areas defined for this year. In Section 3, we provide the overall description of the FFI experiment, including goals and overall demonstrator description.

Section 4 gives further details on the technological goals. This includes an overview of the theory and technological architecture used to support the goal. The results of the experiments derived from the technological goals are provided in Section 5.

In conjunction with our participation at NATO CWID 2007, the projects involved organized a series of seminars; these are described in Section 6. Finally, this document is rounded off with the overall conclusions in Section 7.

2 NATO CWID 2007

NATO Coalition Warrior Interoperability Demonstration (CWID) is an annual event targeted at improving interoperability between NATO and national C4I systems. The event is approved by the NATO Military Committee, and supported by the Allied Command Transformation (ACT). CWID is also the successor of the Joint Warrior Interoperability Demonstration (JWID). The main site for NATO CWID this year was Camp Jørstadmoen outside Lillehammer, Norway. Camp Jørstadmoen has played this role since 2004, and will also be the designated site for at least NATO CWID 2008. In addition to the NATO CWID, there is also a UK CWID and a US CWID. For the rest of the document, when the term CWID is used it implicitly refers to NATO CWID.

The prime focus of CWID is testing of interoperability between operational systems to be used in NATO Response Force (NRF) and Combined Joint Task Force (CJTF). In addition, CWID is used as an arena for testing and experimenting to support the future development of the capabilities of the alliance. This is also reflected in the types of trials defined for CWID, namely

Interoperability Trials and Interoperability Experiments. It should be noted that, since the nature of our work is experimental and the main section of contributions tend to focus on shorter term interoperability goals, it is advantageous to have potential test partners identified early in the process.

For CWID 2007 three overall goals and objectives were defined. The first goal was "NRF Test and Validation", targeted at performing testing for certification and interoperability of systems required for NRF 11 and 12. The second goal defined was, "NATO Network Enabled Capability", where testing was conducted in support of the future NNEC. This included management of information, enabling of automatic discovery, and integration technologies to provide loose coupling between systems. This goal also incorporated tests and experimentation with web-based Service Oriented Architecture (SOA). The third and final goal defined for CWID 2007, "Current NATO Operations", was designed to test and verify the interoperability between systems used in current NATO operations.

NATO CWID 2007 gathered approximately 1300 participants from 16 nations and NATO agencies. A total of 133 trials were registered, of which about 95 were completed and did participate. The Norwegian delegation counted six trials in total. As for test cases, approximately 1400 were registered in total, and the status of these varies from "not-tested" to "success". The sheer number of participants and test cases goes to show the importance of CWID as an arena for ensuring interoperability between the systems of different nations and agencies.

3 Trial Description

Common to the three FFI projects participating is the focus on Network Based Defence (NBD), or Network Enabled Capability (NEC), and the overall goal is to support the development of the future NEC[1]. Giving a short and commonly agreed upon definition of NEC is virtually impossible. We use this working definition presented by the ACT at the 2006 Network Enabled Capability Conference; "*NNEC is the Alliance's ability to federate the various components of the operational environment, from the strategic level (including NATO HQ) down to the tactical levels, through a networking and information infrastructure (NII)*". The concept of NEC is revolved around the need for seamless information exchange between different components in the military structure and even civilian organisations, both governmental and commercial. In other words, information should be provided in a timely fashion to those who are best situated to use it. In addition, the concept of ad-hoc organisation is highlighted as another key attribute of NEC. This should provide a more agile organisation capable of reducing time needed for planning and deployment.

Current C2 systems are often not designed to provide the type of flexibility outlined for NEC. Service Oriented Architecture (SOA) is an architectural principle that has proved promising for

[1] NEC is more or less the equivalent of the Norwegian NBD, and since this experiment was conducted in a NATO setting we will use the term NEC for the remainder of this document.

providing the needed flexibility. From the "Reference Model for Service Oriented Architecture" [5] we can define SOA as *an architecture for making resources available in a way that they may be found and utilized by parties who don't need to be aware of them in advance.* We believe that the SOA principle is very much suited for use in the future implementation of NEC, a fact that is also recognized by NATO NEC Feasibility Study [6]. As a consequence of this the trial carried out by FFI at CWID 2007 focused on the use of SOA in a NEC setting. This also coincides with Objective 2 defined by ACT for CWID 2007, see Section 2. Web Services is at the moment the preferred technology for implementing SOA, and as such this also formed the basis of our experimentation.

In order to be able to realise NEC, there are numerous challenges that must be overcome. While the FFI contribution to NATO CWID 2006 had a broader scope, this year's experiment was more focused in depth at a couple of challenges inherently present when talking about NEC, and the implementation of SOA. This approach was chosen in order to have a more manageable scope for the experimentation. The first challenge identified was enabling secure exchange of information between security domains. This includes trusted release of information to domains implementing a different security policy. The second challenge identified was service-enabling of the lower tactical levels to facilitate information sharing. Lower tactical levels are often characterised by scarceness of resources like network capacity, often denoted Disadvantaged Grids. Since Web Services technology is not originally designed for these kinds of environments, we need to find techniques suitable for reducing e.g. bandwidth usage. During CWID the two experiments mentioned above were carried out by the FFI project "1086 – Secure and Pervasive SOA".

In addition, semantic interoperability was the subject of an experiment carried out by the FFI project "1085 – SEMANTINI". The focus of this experiment was primarily on translation between data models using semantic technologies. Using an instant messaging application as an interface to services was an additional experiment that was performed by the FFI project "1084 – SINETT" as a part of the FFI trial during CWID 2007. More detailed information on these technical objectives, as well as the challenges and the solutions proposed by this experiment can be found in section 4.

3.1 Partners

The main testing partners for the FFI trial during CWID was the NATO Consultation, Command and Control Agency (NC3A) trial "Cross-Domain Web Services (CDWS)" and the Norwegian trial "NOR Blue Force Situation Awareness/NFFI (NOR BFSA/NFFI)". In addition, the FFI trial also cooperated and exchanged data with other partners like the French "T-BMS" trial and the Norwegian "NEC CCIS" trial.

3.2 Scenario

The focus of the FFI CWID trial was primarily technological, and as such it was decided that an extensive operational scenario was not needed, and a limited scenario was used instead. This scenario involved Blue Force Tracking, from the tactical level to the strategic, and between

different security domains. The general overview of this scenario can be found in Figure 3.1. Blue force tracking information can be generated at the tactical level and exchanged with higher level systems, within one security domain (e.g. Security Domain A). This information can then be exchanged to other partners, in other security domains, by the use of XML Guards.

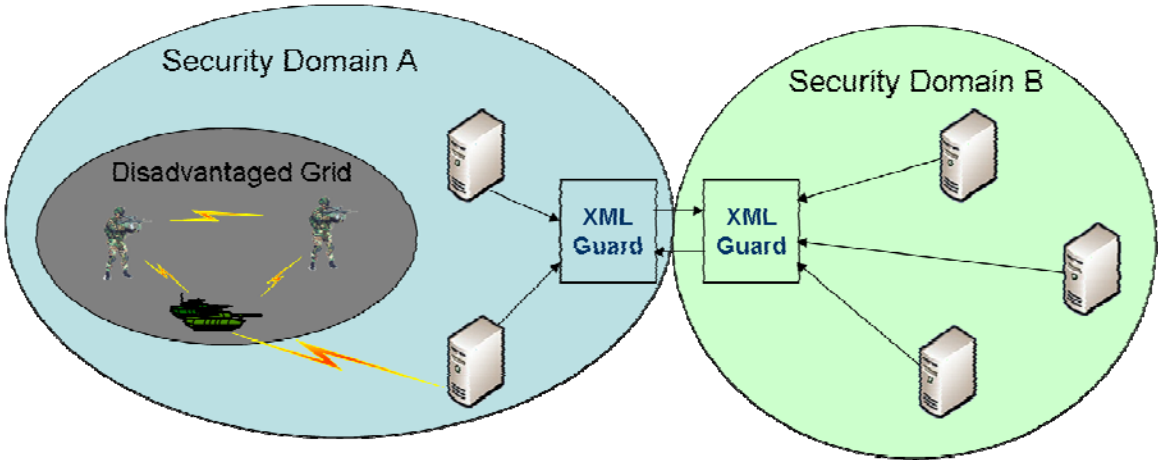

Figure 3.1 Generic demonstrator scenario

We recognise the fact that this scenario was very limited; however it served its purpose for our needs and requirements. It should be pointed out that since we had a technological and experimental focus, participating in the official scenario was never an option. However, we used fragments of this scenario, like the given geographical area and blue force tracking. By doing this we were positioned to receive information from other sources than those pre-planned.

3.3 Demonstrator description

As described above, and detailed in section 4, four different experiments were conducted in the FFI trial at CWID. All four experiments used a common demonstrator developed in-house. This section gives a brief overview of this demonstrator, and its use at CWID.

The common demonstrator is developed for experimenting with promising technologies for the future NEC in general and in particular for distributed picture compilation and situational awareness. The main principle behind the demonstrator design is flexibility and a stabile core. The high-level demonstrator design is shown in Figure 3.2.

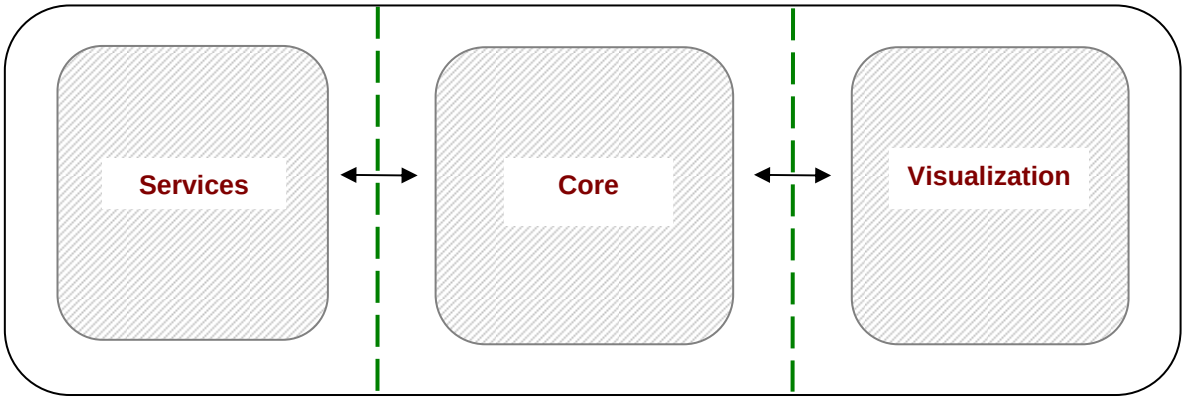

Figure 3.2 High-level demonstrator design

The demonstrator design consists of three logical layers. The core layer is implemented using the Java Messaging Service (JMS) and handles shared functionality. This includes general functionality for picture compilation, such as storage of tracks and functionality for data format translation. In addition, JMS provides the infrastructure for internal asynchronous messaging between functional components, using message stores and queues. Services communicate with the core using predefined message formats. For more detailed information about the design and implementation of the core, please consult [7;8].

The visualization layer contains functionality to display, for instance, tracks to the user. This layer may be viewed as a highly specialised service in the context of the demonstrator design. As such, it is recognised as an extra layer in the design. For the CWID 07 demonstrator we used Maria from Teleplan for visualisation, and an interface was developed for communication with the core. We also used Maria for simulating tracks and provided these tracks to the core for further distribution.

The service layer typically contains stand-alone applications used for performing a specialised task or service. Any type of application can, in the context of the demonstrator, be defined as a service as long as it conforms to the specified interface of the core layer. For CWID 07, the service layer consisted of NFFI-related services [9]. NFFI is a proposed NATO standard for exchanging blue force information. NFFI IP3 was used as a basis for our experimentation at CWID. We implemented the request/response web service for delivering tracks to external partners, and an NFFI client for retrieving tracks from external partners. These were both deployed within the service layer of the demonstrator. In principle, an identical implementation was used for all experiments. However, special purpose adaptations tailored for the different experiments were implemented when necessary. These will be further explained in section 4.

Together the three layers of the demonstrator explained above form what we have denoted an “FFI node”. Several of these nodes were deployed during CWID. In Figure 3.3 the standard deployment of the FFI demonstrator to the CWID WAN, including FFI nodes and necessary hardware, is shown. Additional FFI nodes were deployed during CWID to enable internal testing and debugging, but these are not shown. Nodes from test partners, that is, NC3A and the NORCCIS-II system, are also shown in the figure. The communication patterns between the

participating nodes are also outlined, showing how information flows between the involved partners. The figure provides two views; one from the disadvantaged grids and one from the cross domain web services experiment respectively. The two experiments were independent of each other when it comes to deployment. However, as the figure shows, they could be interconnected when needed. This figure is not complete, but gives a good impression of how the experiments were set up from a network perspective. The other experiments used the shown setup, or parts of it. We did also communicate with other partners not mentioned here, but the general idea of how partners were connected is shown.

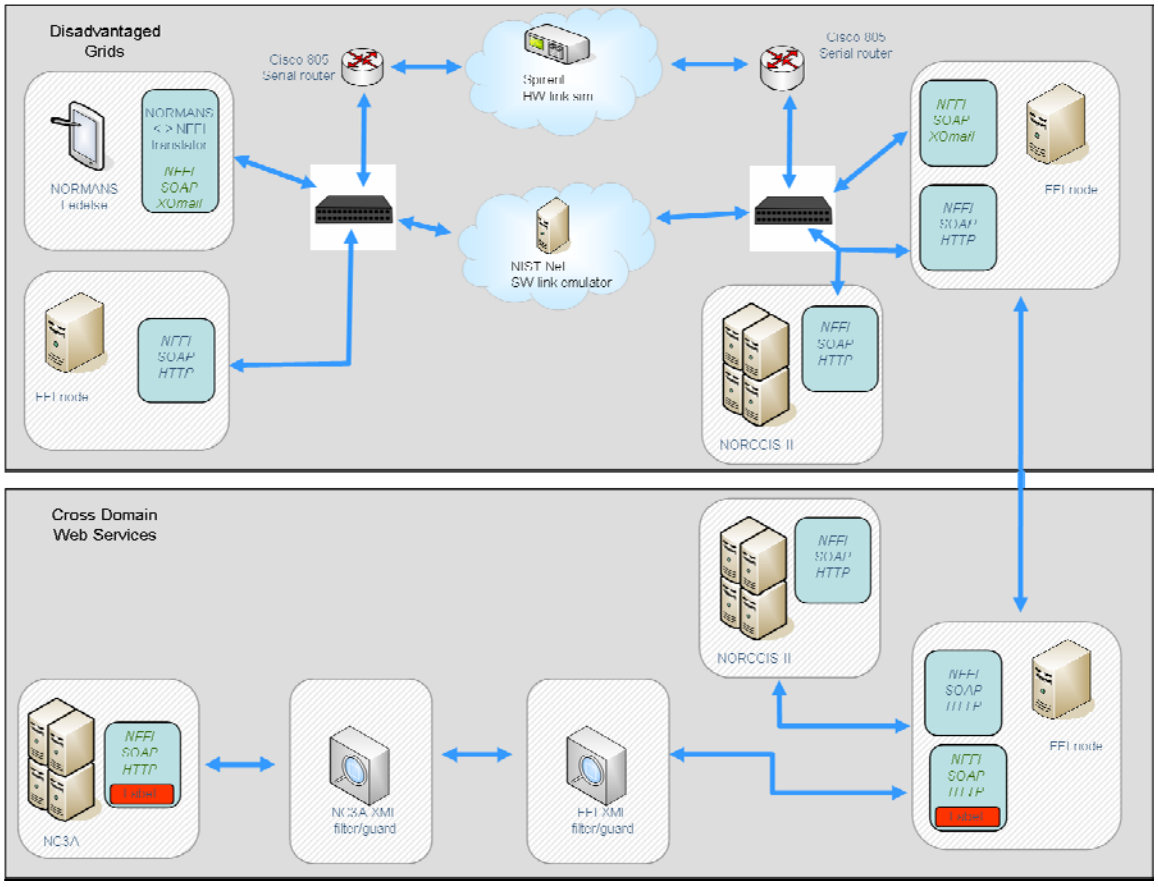

Figure 3.3 Deployment of the FFI Demonstrator at CWID 2007

3.4 Test Cases

The unit of measurement for success on CWID is test cases and the status of these. In order to track these test cases the CWID organisation provides a centralised tool, in which the participants can register test cases and update with results as tests are performed. Test cases are performed between identified partners, and these partners should be from different nations. In the end, partners of a test case recommend status and the total test case is evaluated by the CWID organisation.

The FFI trial produced four test cases and was also involved in six other test cases as a partner. All these test cases were performed by the Cross Domain Web Services experiment. This was the

only experiment producing official test cases, due to the fact that it was the only one of our contributions that had partners from other nations. The results from these test cases are described in section 5.1. The other experiments used CWID as an arena for national testing and experimentation, and it was thus decided not to register these as test cases. Nevertheless, tests and experiments were performed and these are described in this document in Section 4, together with the results in section 5.

3.5 Resource Usage

Considerable resources, both human and other, were used by FFI both in the pre-phase of, and during the execution of CWID 2007. In total, approximately ten persons were involved on an on-and-off basis during this work. The pre-phase included administrative work like participating at conferences, establishing partner relationships, security documentation, and hardware inventory and participation registration, which at times was quite time consuming. However, the process of designing, implementing and testing the demonstrator represented the main use of human resources during the CWID preparations.

During execution, approximately the same number of human resources was used, i.e. 10 persons on and off for the four weeks of CWID. Other types of resources used during the CWID execution included computer hardware. The demonstrator setup included in total 14 desktop or laptop computers, a hardware link simulator, routers and of course peripherals like monitors. All in all the deployment of the demonstrator became quite complex and resource demanding.

4 Technological Objectives

This section takes a more in-depth look at the four technological objectives defined by FFI for the CWID ’07 participation, and describes the experimentation performed within each of these. For the results from this experimentation, please refer to Section 5.

4.1 Cross Domain Web Services

One of the important principles of NEC is making information available to the user who needs it when she needs it. The current situation is quite different due to several factors, one being that the use of physically and administratively divided security domains constitutes considerable obstacles for information sharing. Often the only means of information exchange is a manual review and release process, including air gaps and swivel chair operators. This process is time-consuming and hence not in-line with the NEC vision of automated information exchange. The separation of security domains is of course adopted to prevent the potential leak of classified information to non-authorised networks and users. However, there is a real requirement to be able to perform such information exchange in a timely and secure fashion both in current operations and in the future NEC. In the long term vision the use of object level security and end-to-end security measures are believed to be one possible solution. However, in order to achieve this in a short to mid-term, automatic two-way exchange of information between security domains is needed, and this trial has used a combination of XML labels and XML enabled guards to show one possible

solution. The overall technological objectives for the Cross Domain Web Services experimentation at CWID can be summarised as follows:

- Investigate automatic mechanisms for secure information exchange between security domains.
- Implement and validate the usability of our proposed XML label, the mechanisms for binding label and data, and the filtering of information based on these labels.
- Identify areas in need of further research and development.

Our primary partner for these tests has been the NATO-CDWS trial of NC3A, but data has also been included from the French TBMS trial and the NORCCIS-II system.

There are numerous definitions of a security domain, but for our work we define it as *"A collection of entities to which applies a single security policy executed by a single authority"*. As a consequence of this we define a Cross Domain Solution (CDS) in the following way: *"A Cross-Domain Solution (CDS) allows the export and import of information and services between two or more security domains in accordance with domain security policies"*.

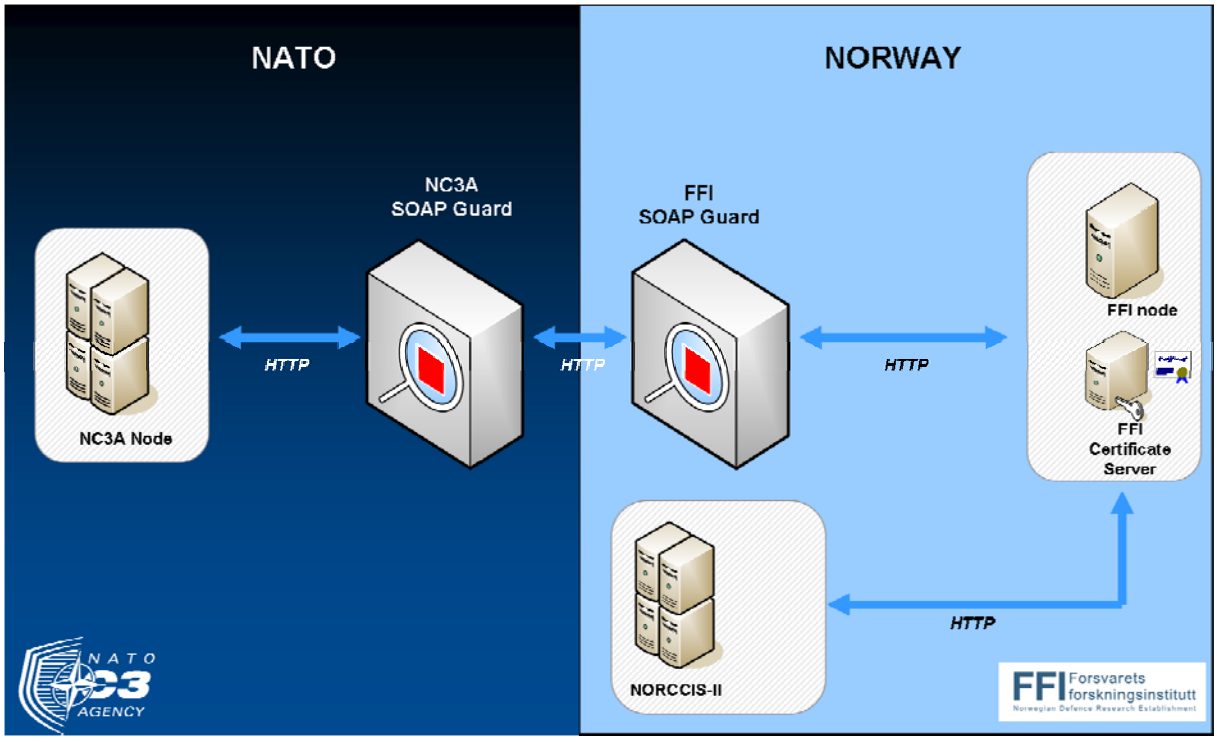

Figure 4.1 Cross Domain Web Services using XML labels, signatures and guards

The overall experiment setup can be found in Figure 4.1. This figure depicts two separate simulated security domains; one is not necessarily defined as of higher classification than the other but each domain has its own policy for exchanging data with the other. The security domain denoted "NATO" was during the experimentation administered by the NC3A, and the other denoted "Norway" was administered by FFI. The policy is implemented in the guards in order to protect the respective domain from information leakage. Release decision at the guard is based on the defined policy and the labels associated with the data to be released. Any information not in-

line with the policy will be removed by the guard; this also includes unmarked information objects. One example of a policy scenario used at CWID is that release of information under NATO POLICY, classified as NATO RESTRICTED or lower can be released to the other domain. However, information marked with a national policy, hence also national classification, cannot be released from the Norwegian domain. Labels are applied to the data in question by the FFI Node in the Norwegian domain. Information can be provided by other nodes within the Norwegian domain, for instance NORCCIS-II as can be seen in the figure, but the actual labelling will be performed at the FFI Node based on some predefined attributes. These attributes will be explained below. All information forwarded to the guard must be digitally signed, if not the guard will reject it. In this experiment, the labels were removed by the guard before the information objects were forwarded.

The label used in this experiment is a generic XML label defined by FFI for describing security metadata about a given information object. The label used during CWID 07 was highly influenced by the IETF S/MIME ESS [10] security label. Attributes used to describe security features of a given information object include; Security Policy Identifier, Security Classification, Privacy Mark and Security Categories. The first two are mandatory fields that provide a unique way of identifying which policy to treat this object under, and what the classification is according to this policy. The last two attributes are optional, but may be used to provide additional information. As an example, the Security Categories field provide finer granularity by adding statements like “National Eyes Only” and “Releasable to Nation X”.

In order to be able to trust the label, it needs to be associated with the information object in a trusted way. To achieve this, XML Digital Signature (XMLDSIG) [11] is used to provide a cryptographic binding. In addition, this ensures the integrity and provides authentication. Several information objects can be bound to one instance of the label, that is, information objects that share common security attributes. This is useful when, for example, only given paragraphs of one document are classified. The label, although specified in XML, can be used to mark virtually any information object. The only requirements are that the information object can be referenced in a unique way and that it can be processed by XMLDSIG for the binding. It should also be mentioned that this label was only used in the Norwegian domain. NC3A implemented another XML label that they had defined. These label proposals are similar but differ, especially on how binding is performed.

The main focus of this experiment was Web Services technology and how the XML label outlined above could be used to provide security metadata about the content of SOAP messages. The solution chosen for this experiment was to include the label and binding information in the SOAP header. It is important to note that one SOAP message can have multiple labels included, labelling different elements. This enables us to transport SOAP messages where the content is of different sensitivity. Also, one label may point to different elements within a SOAP message. This eliminates the need to have multiple labels for elements with identical sensitivity. As mentioned above, we used NFFI as a case-study for our experiments and we thus labelled NFFI information transported by Web Services. The NFFI specification used in this experiment also

features the possibility for adding security metadata to different child elements of what is called a track element, with similar attributes as found in our label. This label is highly specialised for the NFFI data model, and is not very generic. This stands in contrast to the proposed label above, so using this label for release decisions would involve the design and specification of an NFFI-aware guard solution. To make matters worse specialised guards would have to be designed for every other data model or protocol that includes a security label, or security metadata of some sort. This is obviously not a very scalable solution for Cross Domain information exchange. In addition, the NFFI label internal marking is not bound to the data it labels by, for instance, a digital signature; the trust level provided by this label may thus be discussed. The solution chosen for this experiment is to translate the NFFI specific label to our proposed generic XML label at the producer and consumer side. This eliminates the need to have one guard implementation for each proprietary label format available. The FFI node depicted in Figure 4.1 is responsible for the labelling of SOAP messages. This includes both NFFI service replies, in other words providing NFFI data to external consumers, and the labelling of requests bound for external producers. Requests may also contain classified information and must thus be subject to labelling, binding and filtering at the guard. NFFI tracks may be produced by the FFI node in two ways; either tracks received from external sources, or internally produced tracks. Tracks produced by the FFI node itself are labelled by a given internal policy. Tracks received from external sources, for example the NORCCIS-II node, must have the NFFI label fields set; these are used in the translation process outlined above. Any tracks without NFFI labels will receive the value UNMARKED. Data in the SOAP body and the label in the SOAP header are then digitally signed by the FFI node.

Due to implementation specific details of our internal data format we were only able to preserve one label for each track. This is in contrast to the NFFI specification where sub-elements within a track can be labelled individually. We thus implemented an algorithm for max label generation from NFFI labels, such that the resulting label for the NFFI track equalled the highest label found within the track. By doing this we ensured that no information got a lower classification than anticipated, in order to avoid releasing information that was not supposed to be released. This implies that some information that could have been released never was, due to the max label generation. From an information exchange perspective this is not acceptable, but as mentioned this simplification was only due to implementation ease and is not important for the experiment results. It should also be mentioned that all other mechanisms, labelling process, verification, and filtering, are independent of this, and should thus also support finer granularity labelling.

The FFI SOAP guard, depicted in Figure 4.1, receives or intercepts all outward bound SOAP messages via HTTP and TCP. Upon receiving a message the guard will verify the signature, compare the label against its release policy and remove information, NFFI track elements in this case, not allowed to leave the domain. The signature is verified in order to ensure that the integrity of the message and the authentication of the issuer are correct and to verify the binding between labels and data. If the signature is invalid, the whole message is discarded by the guard. On the other hand, if the signature is valid the labels of the message are compared to the given policy to render a release decision. For CWID the guard implemented a simplified policy which

included an instance of the XML label. The labels contained in the SOAP message were compared to the label configured in the guard, and release was approved if the SOAP labels were assessed to be of lower classification. Messages with no label, or labels with value UNMARKED, were removed together with the associated data since the guard has no way of knowing the potential sensitivity of the information. The final step performed by the guard before releasing SOAP messages is filtering; elements that are associated with labels not suitable for release are removed. This may cause the whole message to be discarded or forwarded. If the message contains more than one part, and some parts are associated with a label indication that they are not releasable, these parts may be removed before the message is forwarded. The guard also strips the generic XML label from the message and removes the signature before forwarding it to the other domain.

The focus of the experiment has been cross-domain web services, limiting our scope to the SOAP protocol. A natural extension would of course be to include other protocols, as long as they can be labelled with the defined XML label. In addition, during CWID our guard has only been configured to verify signatures and filter outgoing messages for releasability. The guard can also be used to perform sanity check on information arriving at the guard, including virus scans and other types of validation. Due to the limited scope of this experiment, other areas like security infrastructure (for instance certificate and key distribution) were not prioritised. Simple solutions were used in order to not loose focus on the objectives at hand.

For further details the interested reader is referred to [2], which goes more in-depth on the design and implementation.

4.2 Disadvantaged Grids

Web Services is today the preferred way of realizing SOA, and its widespread use implies large benefits with respect to interoperability. However, Web Services is a resource demanding technology, and this is a considerable challenge when service enabling the lower tactical levels, where resources are scarce. Such networks, collectively called *disadvantaged grids*, are wireless networks characterized by low bandwidth, high delay, and frequent service disruptions, and they represent an environment that is very different from what Web Services technology is designed for.

Because of the interoperability benefits of using Web Services, we want to extend its use as far out on the tactical level as possible. In order to achieve this, we need to optimize the data communication in all areas possible. *Figure 4.2* shows the different layers that are involved when systems are communicating. We focus on the application and transport layers (the upper layers) in our work on using Web Services over disadvantaged grids.

We have tested different data models in order to achieve an efficient information representation. This year at CWID we have been using XML-encoded NFFI, which is a relatively compact format. On the Web Services layer, we have used different types of compression, in order to reduce the size of the SOAP messages that are passed between the systems. In particular, we have

focused on Efficient XML from Agile Delta, which has proven to achieve high compression ratios.

Web Services normally use HTTP over TCP/IP for sending SOAP messages. However, this is not suited in a disadvantaged grids environment, and we have therefore replaced the entire communication stack with XOmail, a STANAG 4406 [12] compliant military message handling system (MMHS). The tactical profiles of this system are designed for use in disadvantaged grids, and are therefore well suited as transport for SOAP messages.

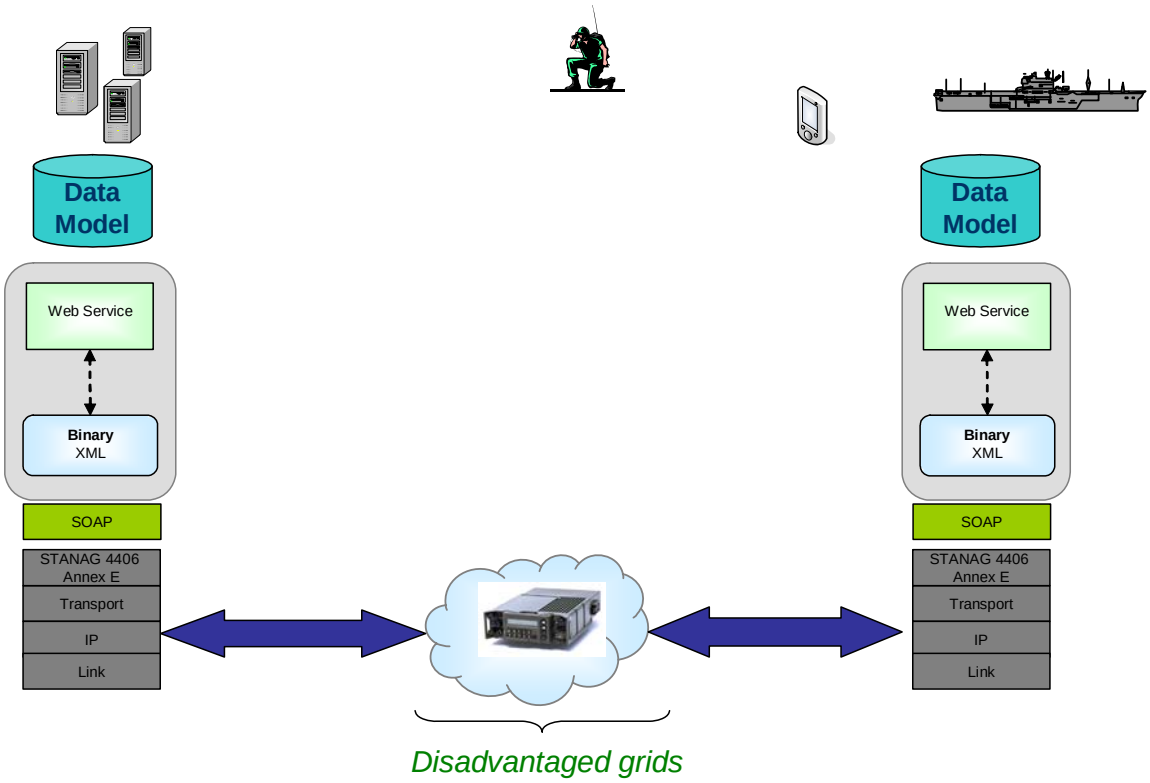

Figure 4.2 Communication between systems

We have also experimented with content filtering as an additional means of reducing overhead. When performing track filtering for a blue force tracking application, the content filter needs to know which track information is relevant to the recipient. For a tactical user with a limited area of operations, one possible type of filtering is geographical track filtering. The simplest form of geographical track filtering is using a fixed zone filter to remove all tracks that are outside the unit's area of operation. Such a filter is shown in the left image of Figure 4.3, where the circle marks the tactical unit's area of operation. Tracks inside this circle are transmitted to the unit, while track outside it are not.

Geographical filtering can also be used in combination with a second content filter type that reduces the frequency of track reports. A zone ring filter, shown in the right image in Figure 4.3, is similar to the fixed zone filter in that it uses distance as its filter metric. It is, however, optimized to allow for more frequent updates of tracks that are closer to the client than those that

are further away. Tracks inside the inner circle are transmitted with a higher frequency than tracks in the other two circles, while tracks outside the outer circle are never sent to the tactical unit.

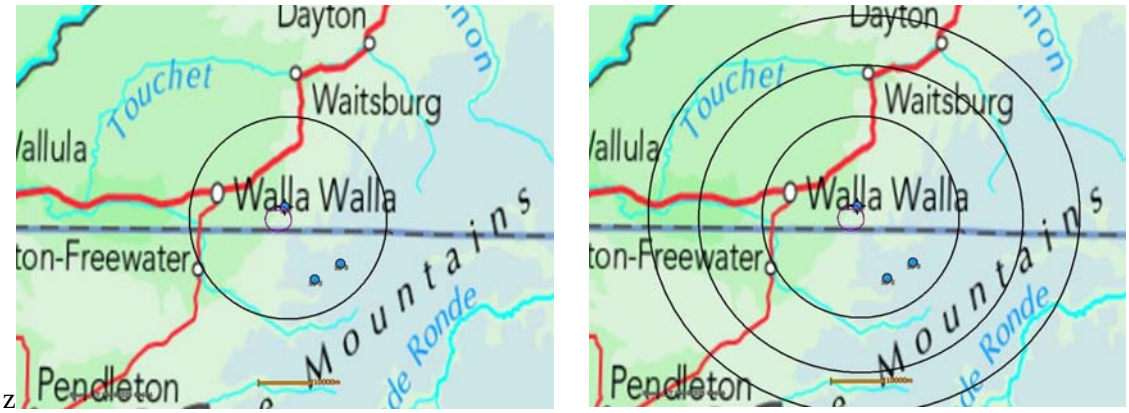

Figure 4.3 Content filtering – Fixed zone filter (left) and zone ring filter (right)

The context of the experiment is picture compilation, and we demonstrate how track information flows from the tactical level and up to the strategic level. The tactical level is represented by a handheld blue force tracking system, NORMANS Advanced. The software has been modified to use Web Services over XOmail rather than the proprietary NORMANS protocol. In order to achieve a controlled environment, (and also because radio equipment was prohibited inside the CWID building) we used an emulated tactical network for this communication.

For further details about the experiment setup, execution and results see the technical documentation in [3].

4.3 Semantic Information Integration

The FFI project SEMANTINI (Semantic Services in the Information Infrastructure) is tasked with investigating whether semantic technology has any potential for the Norwegian Defence. We saw CWID as an arena for demonstrating and discussing semantic technology, as well as exchanging knowledge with other nations' participants. Semantic technology is currently emerging as new way to build systems, and semantic information integration is envisioned as a better way to integrate information from heterogeneous data sources. For a broader introduction to semantic technology, refer to [13].

The main idea of semantic information integration is to solve semantic mismatch between different formats and systems at the semantic level. By exposing the semantic models (ontologies) to the systems, one can define mappings between these ontologies. Since ontologies are formal models based on logic, it is possible to use automatic reasoning tools on these models to execute mappings. This can be used to integrate information from heterogeneous sources

automatically (based on the specified mappings). The result is a model-driven way to resolve semantic mismatch, which introduces a (logical) hub-spoke structure at the semantic level.

By doing information integration in this centralized or federated way, proponents of semantic technology claim that it is possible to approach linear growth in the number of integrations that must be carried out. This contrasts vastly with the current worst-case scenario of exponential growth in such integrations, since it is based on a decentralized (point-to-point) integration structure. The exponential growth in integrations is commonly known as the n^2-problem, which is roughly the maximum number of integrations that are needed for n systems. With the semantic information integration model, it is claimed that only n integrations are needed at best.

The hypothetical benefits of semantic information integration are therefore clearly interesting, since the Norwegian Defence, just like any large organization, suffers from many different systems that should ideally share more information between them. Additionally, new and existing collaboration partners could often be provided with more or better information. The semantic approach is claimed to make information more adaptable, better supporting evolving and changing requirements for information-sharing.

From a military point of view, the ability to make information more adaptable to change is in line with the vision described in the NATO NEC Feasibility Study [6], where SOA is the vision. The NC3A is also researching this topic, and has produced some interesting work (see e.g. [14]). Further, a NATO Research and Technology Organization (RTO) group on “Semantic Interoperability” (IST-075) with Norway as one of the participants has recently started up.

The technological objectives for the Semantic Information Integration part of the bigger FFI effort at CWID had the following technological objectives:

1. Overall purpose: Explore semantic technology and tools.
2. Experiment with ontology creation, mapping, and reasoning in the context of semantic information integration.
3. Gain experience with semantic information integration and assess the potential benefits of this approach for the Norwegian Defence.

To be able to experiment with semantic information integration, we identified the translator component in the FFI demonstrator as a suitable place to insert semantics-based solutions.
As mentioned [8], the translator is a general interface which takes an input and delivers an output, and masks the actual implementation. There already existed special-purpose traditional implementations (using Java code in this example) of the translator, which translated between the Nato Friendly Force Information (NFFI) [9] format and the internal XML-format. We decided to make a semantic version of this component, called SemanticTranslator.

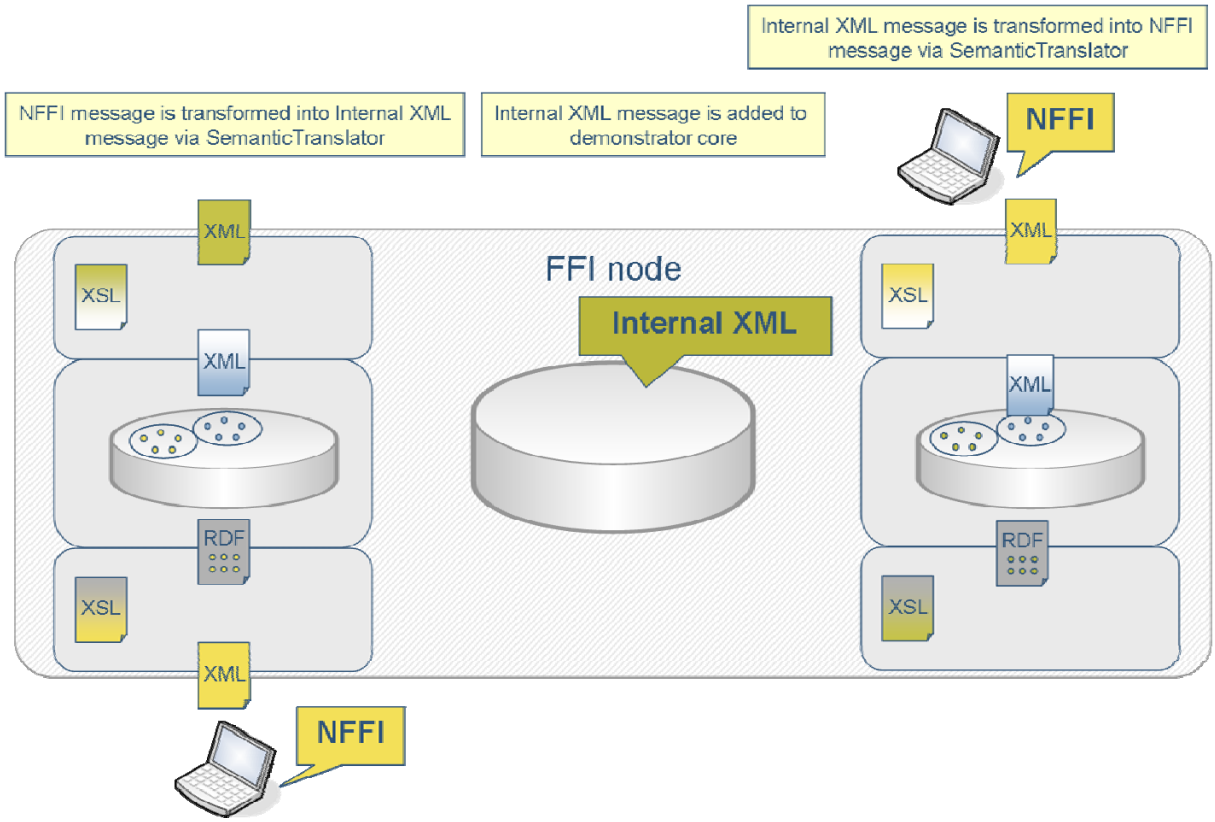

Figure 4.4 Two SemanticTranslator instances used in an FFI-node

An FFI-node is illustrated in Figure 4.4. There are two SemanticTranslator instances running in this scenario, one to the left and one to the right. The flow of data goes from bottom left and up, via the cylindrical shaped database, to the bottom right and up. The main thing to notice is that with incoming information, we go from the NFFI format to the internal XML format before the information is stored. Next, when information is to be exported, the same process is reversed.

Figure 4.5 shows a more detailed view of what is happening inside the SemanticTranslator. When an NFFI message arrives at the bottom, it is validated before it is transformed into Resource Description Framework (RDF) [15] triples containing instance data according to the NFFI ontology we have created. Next, these triples is added to a knowledge base, where hybrid reasoning is used to execute the mappings we have defined between a generic ontology and the NFFI ontology (both specified using Web Ontology language (OWL) [16]). Executing the mappings infers new instance data triples according to the generic ontology. Therefore, when a query is posed on the generic ontology (using the SPARQL Query Language for RDF [17]), the newly inferred triples are returned. Finally, the query results are converted to the internal XML representation. For more technical details on this experiment, please refer to [4].

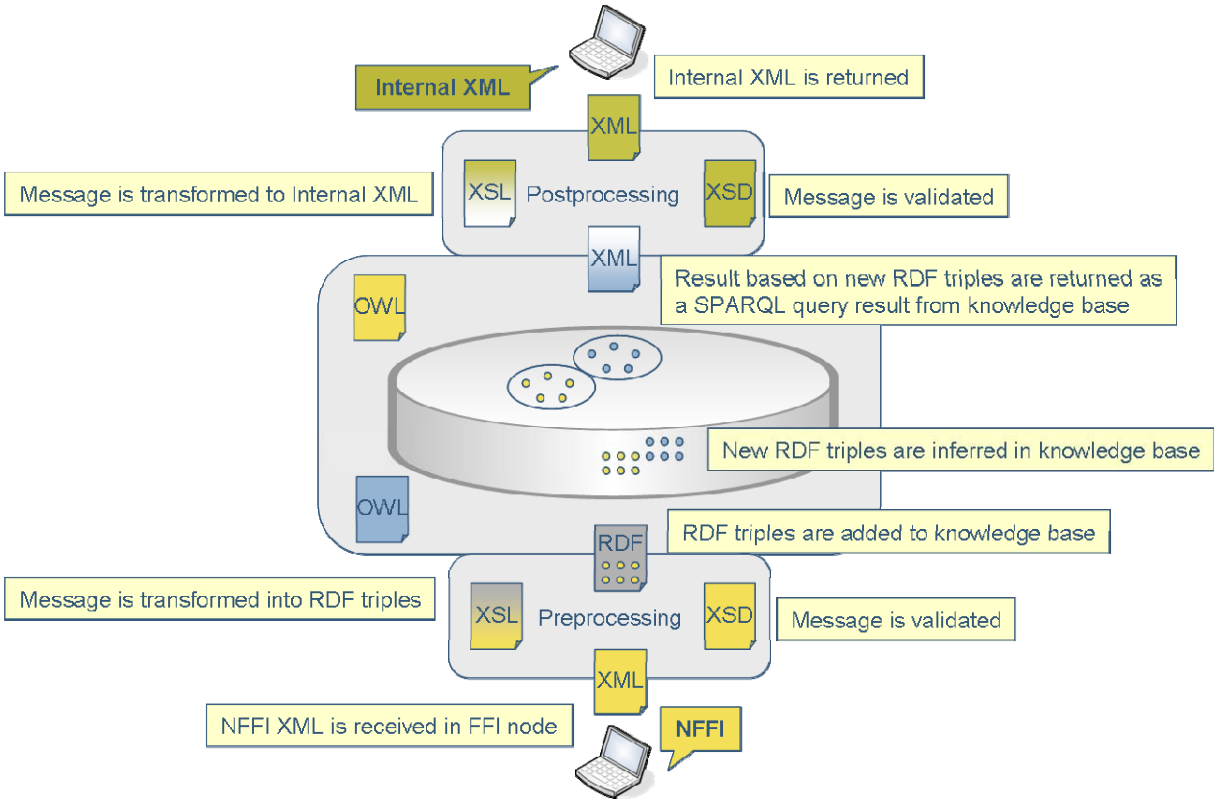

Figure 4.5 A more detailed view of the translation process

4.4 Instant Messaging

Instant Messaging (IM) is primarily considered a technology for unstructured communication between people. One of the main advantages of IM technology is its low resource (bandwidth and processing) demands. It is one of few technologies that may be available throughout the organisation to constitute a ubiquitous network. In many situations, simply being networked, and the availability of a service, no matter how primitive, is more important than being provided with a rich user interface. For this reason, we have explored the possibilities of giving services an IM user interface. Such IM services are often called IM-bots. An IM-bot is simply an automated chat client and the user experiences the interaction with the service as a conversation with another client.

The CWID experiments with Instant Messaging (IM) were performed by the FFI-project SINETT, which focuses on exploring emerging and future network collaboration technologies in a military context. This experiment had a limited technical scope, and was performed internally in the FFI test-bed without communicating with other participating systems at CWID 2007. Nevertheless, the IM experiment was important in order to explore our concept and to verify the applicability of the XMPP standards in this context.

In order to realize the automated chat client, we developed an IM-bot for collecting observations. The experiment test-bed is illustrated in Figure 4.6. Using the demonstrator terminology, our application runs as a *service* that communicates with the demonstrator core. The core itself

functions as a central repository for military tracks, and it is responsible for data format translations and visualizing the tracks using Teleplan Maria. Maria is a commercial map application that also supports military symbols. In this experiment, the IM-bot adds new tracks to the *Track Store*, which are further visualized as APP6 military symbols in Maria.

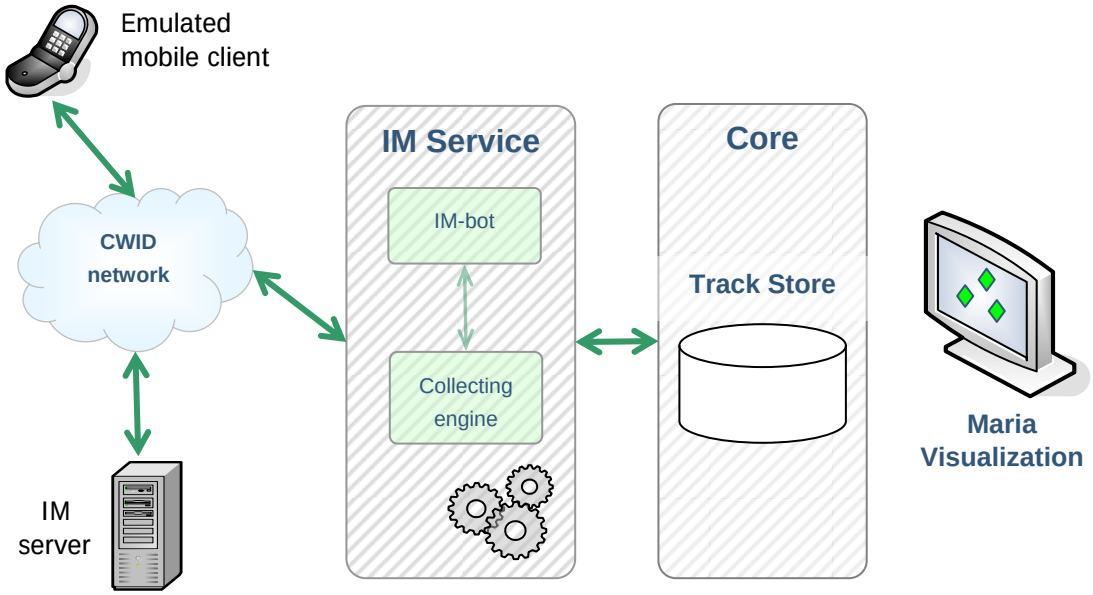

Figure 4.6 IM experiment architecture

The mobile client was realized using an emulated mobile phone, due to restrictions for using real mobile devices inside the CWID area. The emulated phone runs an ordinary XMPP (Extensible Messaging and Presence Protocol) client implemented in Java ME, without any extensions or modifications. Seen from the perspective of the person using the mobile phone, he or she performs an ordinary IM conversation with the remote side, as if it were a human being, when in fact it is the IM-bot software application.

XMPP[1] is an open and extensible protocol for IM and presence information. XMPP is based on XML and standardized by IETF. The core protocol has later been extended with features such as Voice over IP (VoIP) and file transfer. XMPP is based on the Jabber IM protocol developed by the open source community, and although XMPP is the official name, the name Jabber is still often being used. In our experiment, we have used XMPP over TCP. However, the protocol is independent of the underlying transport layer.

[1] http://www.xmpp.org

Figure 4.7 IM client on an emulated mobile phone in dialog with the IM-bot

The underlying scenario for the IM experiment is a deployed soldier carrying a mobile device with limited computing and networking resources and without capability to run specialized applications. The soldier makes an observation he would like to report.

The purpose of our IM-bot was to collect necessary information about observations, and pass it on to the command and control information system using a standardized data format. The collection engine of the IM-bot was not fully implemented, and only a few possible observations were available. Still, below (Figure 4.8) is an example of a possible dialog between the IM-bot and a user that would like to register a hostile brigade engineering vehicle seen 600 meters north of his current position.

```
im-bot> Register observation. Where?
user> 600m N
im-bot> Affiliation: (1) Hostile, (2) Nautral, (3) Friend?
user> 1
im-bot> Battle dimension: (1) Ground, (2) Air, (3) Sea?
user> 1
im-bot> Function: (1) Unit (2) Equipment (3) Installation?
user> 2
im-bot> Equipment: (1) Weapon, (2) Vehicle, (3) Sensor, (4) Special?
user> 2
im-bot> Vehicle: (1) Armored, (2) Utility, (3) Engineer?
user> 3
im-bot> Engineer vehicle: (1) Bridge, (2) Earthmover, (3) Constuction, (4) Mine
laying, (5) Mine Clearing?
user> 1
im-bot> A hostile bridge engineering vehicle is registered at 46.04, -118.17
```

Figure 4.8 Example of a dialog with the IM-bot

Instant Messaging is a technology with low resource demands and is therefore a technology that may become widely available in military networks. Also, an IM client is a general application and available on most platforms. In our experiment we have shown how a service in general, and an observation reporting service in particular, may be accessed through a standard IM network using only a general IM client on the client side.

5 Experiment Results

This section presents the results from the FFI participation at CWID 2007. The overall results have been more than satisfactory. This Interoperability Experiment has explored the use of SOA over disadvantaged grids; the use of XML security solutions has been demonstrated in a cross-domain setting; and semantic information integration and instant messaging have been shown. The results from the experiments derived from the four technological goals defined in Section 4 are presented in the subsections below.

5.1 Cross Domain Web Services

Having implemented, tested and experimented with Cross Domain Web Services at CWID 2007, we feel that we have gained more experience in the field of cross domain information exchange, and that the overall experiment has been a success. Given the experimental nature of our system, we did of course run into some problems and needed to do some last minute bug fixing and tweaks. But in the end we had the opportunity to complete all pre-planned tests with the identified

partners. Measured against the technological objectives listed in section 4.1, we feel that the return from our participation has been good.

The first objective stated for this experiment was to investigate automatic mechanisms for secure information exchange between security domains. Our solution featured the combination of trusted labelling of information and guards for release control. The solution worked and we believe that this is a viable solution to enable information sharing between security domains in a short to mid term. It should be noted though, that the system being used at CWID is only a demonstrator and as a consequence no parts of it have been evaluated or certified. This is the case for the concept, design, and implementation of the mechanisms featured here. Perhaps the most important and difficult task here is to be able to provide a high enough trust level in the process of producing the label and the process of binding the label and data. If such trust levels are provided, the implementation and certification of a guard solution should be easier. It is our opinion that, in the longer term, the release decision should be made on the basis of the user privileges, and not like today were physical security domain boundaries constitute the release decision. This will be more in-line with the overall aim of providing information object level security.

The second identified technological objective was to implement and validate the usability of the proposed XML label, which included the mechanisms for binding the label and data, and the filtering of this information. This objective was tested by the implementation of the label, labelling mechanisms and the filtering provided by the guard. Overall, we will characterise this objective as fulfilled and the experimentation as a success. The label proved to be versatile enough for our scenarios, and we were able to express our policies within the range of attributes defined by the label. However, the scenarios used in this experiment were limited and there is a need to discuss if the attributes featured in the label are those that are needed in the future. The binding of label and data is vital to provide trust and thus being able to perform release decisions or access control. The binding mechanism featured in this experiment uses digital signatures, which provides integrity and authentication, and forms a good basis for future development. Especially the ability to reuse and bind the same instance of the label to different information objects of the same classification, proved valuable. There are some issues with using XMLDSIG that need to be solved, especially the use of potentially unsafe transformations.

Filtering of information based on the label was performed by the guard, and worked as expected. Performance is an issue often faced when security features are introduced, both with respect to time usage and bandwidth consumption. We did not do any formal measurements and analysis of these factors as this was not within the scope of our experimentation. Nevertheless, a review of the messages sent did reveal some trends. Dependent on the type of information labelled the ratio between label information and payload became smaller when increasing message size, since the amount of label information was almost constant. The reason for this was the nature of the NFFI messages used, which often contained tracks with only a few different classifications, and the fact that one label is used to reference all information items with equal classification. As a consequence, the number of labels is more or less constant when increasing the size of the NFFI message by adding more tracks. Due to our scope during this experiment the usage of

computational resources, i.e. time consumption, was not surveyed any further. It is too early to come to a conclusion on the performance penalty endured by introducing these security measures, and this needs to be investigated further.

Several areas were identified as being in need of further research effort, thus fulfilling the last objective identified. Some of these have already been identified in the previous paragraphs. These include trust in the process of binding labels and data, attributes needed in the label and to survey potential performance issues. A natural extension to performance monitoring is placing these mechanisms in a more challenging environment, for example in a disadvantaged grid. Another natural extension to the CWID experiment is the development of a more extensive architecture for cross domain information exchange. This would include subjects like; dynamic policy management and cross domain exchange of identity management information, privilege management information and security tokens. All in all this experiment confirmed the design and ideas behind it as viable and provided us with a stable foundation for further development and experimentation.

In addition to the technological goals provided above, the experiment was also measured against official test cases, albeit provided by ourselves. The experiment produced four such test cases. For future reference the official numbers of these in the CWID test case tool[1] are 483, 1656, 1657 and 1658. These were all variants of testing the use of XML guards and XML Labelling in combination with SOAP for cross domain exchange of Web Services. Variation included the use of single guards and cascading guards, input from other nations and switching the role of producer and consumer between partners. We also participated in test cases in a supportive role for our partners, most notably the NC3A. In the official test case tool these are numbered 371, 1181, 1346, 1370 and 1375. In addition, we exported land tracks from our system to the Norwegian NEC CCIS system which is documented in test case number 1702.

5.2 Disadvantaged Grids

The most important result we got was that the interoperability demonstration worked: The SOA-enabled NORMANS software communicated flawlessly over an emulated disadvantaged grid with the local HQ using NFFI. We did not have any background traffic over the disadvantaged grid; the entire channel was exclusively available to our application. Thus, we have proved that under similar circumstances SOA implemented using Web Services may be used at the tactical level provided certain measures are used:

- One must reduce the information overhead by using compression and an efficient information representation. We found that Agile Delta's Efficient XML (EFX) with its internal compression enabled yielded the best overall results, and we therefore used this approach in our demonstrator.
- Using a tactical transport protocol facilitates Web Services communication in environments where the usual HTTP over TCP/IP protocol suite breaks. By using the tactical protocols as implemented in XOmail we gained the additional benefit of store-

[1] http://cwid.act.nato.int/ (requires username and password)

and-forward, a property that is essential in a communication environment with frequent disconnections.

5.2.1 Compression results

We tested several combinations of lossless compression methods: We used a generic compression method that can be used on any document, GZIP, and we evaluated two XML specific compression methods, namely EFX and XMLPPM. EFX can be used in one of two modes of operation; *generic* and *schema specific* compression. The generic option can compress any valid XML document without knowledge of the schema. The schema specific option needs to have access to the XML schema when it performs compression and decompression, thereby sacrificing generality for a very slight increase in compression rate. We used the generic option in our experiments enabling us to compare EFX directly to XMLPPM (which provides only non-schema specific XML compression). When evaluating the efficiency of the algorithms we only looked at compression results and not resource use during compression (memory and CPU usage). The reason for this is that for our intended use in disadvantaged grids, the bandwidth is the limiting resource, thus making the compression ratio the most important metric. Our tests (see Figure 5.1) showed that EFX with its built in GZIP compression enabled (called *efxz* in the figure) was the most efficient under these circumstances. As a consequence, we used EFX with compression enabled in all our disadvantaged grid experiments at CWID.

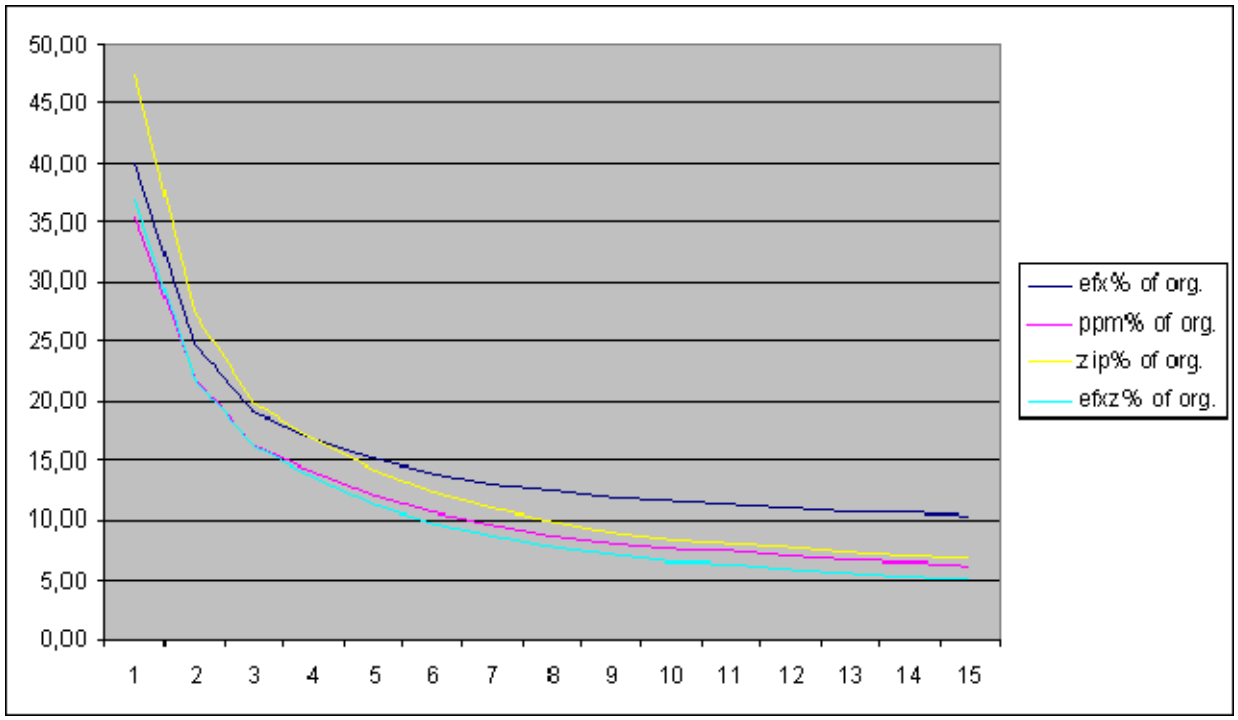

Figure 5.1 Graph showing the document size in percent of original size after NFFI compression. The Y-axis shows resulting document size in percent, whereas the X-axis shows the number of NFFI tracks within the document

It should be noted that the achievable compression rate is dependent on the input data. The NFFI documents used in our experiments did not have any optional fields in the contained tracks. This may improve the compression results somewhat, since the tracks in the documents become more uniform, and thereby more compression-friendly. For more details on this, see [3].

5.2.2 Content filtering

In addition to the removal of optional fields in the NFFI message mentioned above, we also experimented with filtering of whole tracks. The idea behind this filter was to stop unnecessary information from being sent (for example tracks outside the unit's range) and thus to save bandwidth. By preventing irrelevant data from being sent, more frequent updates of the relevant information are made possible. Using such filtering is especially useful in disadvantaged grids where bandwidth is scarce. For further details about filtering, see [3].

5.2.3 Use of tactical transport protocols

STANAG 4406 ed. 2 (S4406) [12] is a NATO standard for MMHS and defines three protocol profiles adapted to different communication networks. Systems compatible with the S4406 standard have been and are being implemented widely by the NATO nations and by the NATO organization.

The original connection-oriented protocol stack defined in S4406 Annex C was developed for strategic high data rate networks, and is not suitable for channels with low data rate and high delays. The protocol profiles TMI-1 and TMI-4 have therefore been developed for use over disadvantaged grids. With the inclusion of these protocol profiles in Annex E of S4406, a common baseline protocol solution exists that opens for the use of MMHS in both the strategic and tactical environments. In the MMHS implementation we use (XOmail); TMI-1 is called "TMI" while TMI-4 is referred to as "DMP". We tried both protocols in our experiments at CWID, and found (as expected) that DMP has less overhead than TMI. Figure 5.2 shows the difference in latency for TMI and DMP under the same network conditions, in this case an emulated 2.4 Kbps link. The NORMANS unit reports less information (it only reports its own position) to the HQ than the HQ sends to it (all relevant tracks in its area), leading to the asymmetry between the two. For further information, see [3].

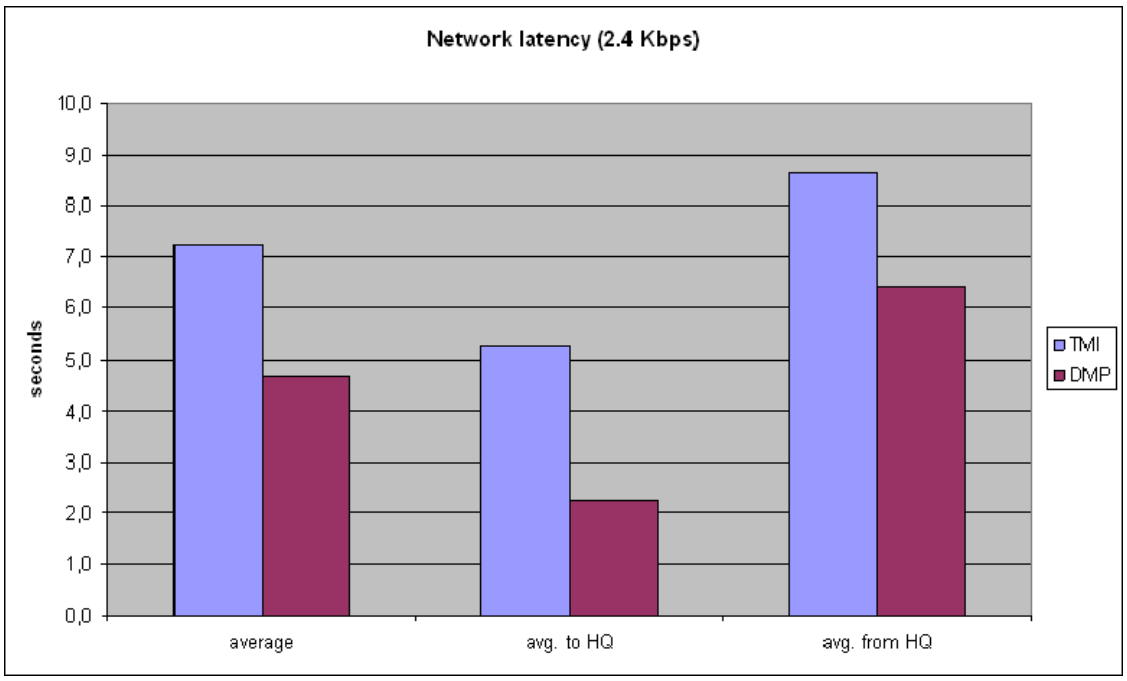

Figure 5.2 Message transmission delays

5.3 Semantic Information Integration

The results of the semantic information integration experiment were quite satisfactory. We have used various tools and technologies for creating ontologies and mappings between them and to build a prototype semantic middleware component called SemanticTranslator. This prototype uses hybrid reasoning to execute mappings between ontologies and is completely model-independent, meaning that the same infrastructure could be used for other models. There is not a single line of format-specific Java code in the translator. Instead, translation is done declaratively using transformations, mappings, and reasoning. In our experiment, we did not measure performance specifically, but it was still evident that semantic translation only is viable on complete XML documents, and not individual XML elements due to performance issues with current tools. For further information please refer to [4].

The Norwegian Defence is faced with challenging information integration tasks and new information sharing and information availability needs. We think the concept of semantic information integration has the potential to help overcome these challenges in the long term. However, lack of technological maturity, performance, and best practices means that deployment of such solutions lies somewhat further into the future.

5.4 Instant Messaging

Instant Messaging is a technology with low resource demands and is therefore a technology that may become widely available in military networks. Also, an IM client is a general application and available on most platforms. Although the IM experiment had a limited technical scope, we have shown how services in general, and an observation reporting service in particular, may be

accessed through a standard IM network using only a general IM client on the client side. Using IM to access services in a military context is a promising concept, and should be investigated further. Also, the open standard XMPP has shown to be flexible and applicable due to its interoperability and platform independency.

6 Seminar

In addition to the experiments performed at CWID, we also arranged three half-day seminars for invited guests. The background for these seminars is that we wanted to show how our activities within the three projects fit into an operational context, and how they support the development towards network-based defence.

Our activities within the projects are inherently difficult to visualize; the resources needed to create a live demonstration of the mechanisms we use, would by no means stand in proportion to the effect gained (if possible at all). Therefore, as an alternative, these seminars gave us an opportunity to provide an in-depth description of the experiments. In addition, the seminars allowed us to present part of the theoretical background for the experiments, and as such provide some knowledge transfer.

Each seminar consisted of four parts, a common introduction, and then one section for each of the participating projects. The introduction provided some background on NATO CWID, why we participate, how we work within the projects, as well as a short introduction to each of the participating projects.

The presentation of the project “Secure Pervasive SOA” consisted of a short introduction to NATO NEC FS, and then a brief overview of the situation today. Next, we explained the principles we build our activities on (SOA, Web Services, proxy servers, etc), and finally we gave a comprehensive presentation of the experiments we performed at CWID.

In the presentation of the project SEMANTINI (Semantic interoperability), we put a strong emphasize on explaining semantic technologies, as this is a field that is relatively unknown to most people. In addition, we described how such technologies may fit into a military context, and we presented the experiment performed at CWID.

While the first two project presentations had a strong technical focus, the presentation of the SINETT project focused on describing current development and trends in Internet technology, and what possibilities these create for military collaboration. One of the main purposes of this presentation was to give the audience some insight into these trends, and thereby inspire them to start thinking about the new possibilities that arise. In addition, we also provided a comprehensive description of the experiment performed at CWID.

After the presentations, the participants had the opportunity to visit the Norwegian room at CWID and see the different experiments we performed. In addition, there was an opportunity to sit in on

a presentation from Sun Microsystems on their solution for multi-level security called SNAP (Secure Network Access Platform).

On average there were 12 participants on each seminar, including people from the Norwegian Defence Logistics Organisation (FLO/ IKT), Norwegian National Security Authority (NSM), Norwegian Defence CIS Centre (FK KKIS), Ministry of Defence, and Norwegian Defence Security Agency (FSA). The presentations triggered several questions from the participants, and responses after the presentations indicated that they were well satisfied with the seminars. In addition, a number of the seminar participants requested us to send the presentations on email.

We consider the seminars as very successful, and a valuable way of providing an in-depth presentation of our research activities to a relevant audience. It is our opinion that by giving these seminars, we presented our activities as CWID in a much better way than what we would have achieved through ordinary demonstrations.

7 Conclusion

The experimentation performed by FFI at CWID 2007 was all in all successful and proved the usefulness and applicability of a service oriented approach when designing the future information infrastructure. The experiments, although only going into depth at given subjects, showed the usefulness of making military resources available as services and that this might help integrate today's stove pipe systems, and in the long run also replace them. One important piece of the SOA puzzle that has not been within the scope of this experiment is service discovery. Due to its importance to the overall architecture, this will be part of future work.

The CWID experimentation was based on the use of a simple scenario and had more or less a pure technological focus. Due to the lack of a real scenario and environment our results and conclusion are only based on lab experience and should thus be treated as such. We recognise that our technology focus comes with the danger of not having the end-user and user requirements highlighted. However, for this experiment we did not specify any user requirements to test our technology. Nevertheless, the results gained do not seem to be in conflict with user requirements.

The cross domain Web Services experiment outlined a possible solution for exchanging information in a secure and trusted way between security domains. The experiment confirmed our hypothesis that the use of labelling of information at the object level is of the utmost importance in order to achieve an automated and trusted process. Although, this experiment was successful it is still a long way to go before this can be put into operational systems. Issues that need to be further elaborated include e.g. trusted bindings of labels and also the specification of what metadata is needed.

Through the disadvantaged grids experiment we showed, based on a lab environment testing, that it is viable to implement an SOA using Web Services also at some lower tactical levels. Through a series of optimization steps the bandwidth consuming XML representation is reduced to a

format and size suitable for transmission on a disadvantaged grid type of network. Furthermore, the reduction is performed using a technology that is currently envisaged to be the open standard for Binary XML. This eliminates the need to use proprietary technologies, and thus reducing the risk of producing new stovepipe systems or communication channels. We also tested more efficient transport protocols than HTTP/TCP by using the MMHS system to convey SOAP messages. The results from this experiment are promising and the work will be continued and expanded on.

The semantic information integration experiment represented a first cut into the cutting edge of semantic technologies for us. The experiment has to some extent shown the great potential for these types of technologies when integrating data from heterogeneous sources. The experiment results support our hypothesis that these technologies can greatly help in the massive task of data integration. However, the lack of technological maturity, performance, and best practices results in the need for further research and development. FFI will continue its work on these topics.

The main focus of the instant messaging experiment was exploring new ways of interacting with services. It showed how instant messaging, a technology normally used for unstructured communication, can be used as a low resource (bandwidth and processing) alternative. The results from this experiment, although limited, are promising and the work will be continued.

As a final remark it should also be mentioned that execution of these experiments at CWID has been of great benefit and a valuable experience for the whole crew. CWID is a good arena for doing such experiments and provides an environment for valuable exchange of ideas with other participants. In general, CWID has confirmed our belief that the technologies experimented with during CWID has great potential to become vital enablers of the future NEC information infrastructure. However, more research is needed and we recommend that these issues are pursued further.

References

[1] R. Rasmussen, A. Eggen, D. Hadzic, O.-E. Hedenstad, R. Haakseth, and K. Lund, "Experiment report: "Secure SOA supporting NEC" - NATO CWID 2006," FFI rapport 2006/00325 (U), 2006.

[2] R. Haakseth and M. Andreassen (Thales Norway), "NATO CWID 2007 Cross Domain Web Services Experiments," FFI-notat 2007/02302 (U), 2007.

[3] F. T. Johnsen, T. Hafsøe, and K. Lund, "NATO CWID 2007 Disadvantaged Grids experiments," FFI notat 2007/02063 (U), 2007.

[4] T. Gagnes, "Semantic Information Integration - an Experimental Tranlsation Service at NATO CWID 2007, Norwegian Defence Research Establishment (FFI) Note 2007/02920," 2007.

[5] OASIS, "Reference Model for Service Oriented Architecture 1.0," 2006.

[6] P. Bartolomasi, T. Buckman, A. Campell, J. Grainger, J. Mahaffey, R. Marchand, O. Kruidhof, C. Shawcross, and K. Veum, "NATO Network Enabled Capability Feasibility Study, Version 2.0," 2005.

[7] D. Hadzic and K. Lund, "Design guidelines for a new distributed picture compilation demonstrator," FFI notat 2007/00179 (U), 2007.

[8] D. Hadzic, K. Rose, K. Lund, and T. Gagnes, "An Extensible and Modular Software Test-Bed for Distributed Communication and Picture Compilation - Technical Documentation," FFI notat 2007/01968 (U), 2007.

[9] R. Malewicz, "NATO Friendly Force Information (NFFI) (version 1.2) Interface Protocol Definition IP3, NC3A Working Document," 2006.

[10] P. Hoffman, "RFC 2634: Enhanced Security Service for S/MIME,".

[11] World Wide Web Consortium, "XML-Signature Syntax and Processing," 2002.

[12] STANAG 4406, "Military Message Handling System, Edition 2," 2005.

[13] B. J. Hansen, T. Gagnes, R. Rasmussen, M. Rustad, and G. Sletten, "Semantic Technologies, Norwegian Defence Research Establishment (FFI) Report," 2007.

[14] V. Rodriguez-Herola, D. Cadamuro, D. Clarke, I. Karakas, and A. Tucker, "NNEC Semnatic Interoperability, NC3A Technical Note 1131," 2006.

[15] World Wide Web Consortium, "RDF Primer," 2004.

[16] D. McGuinness, "OWL Web Ontology Language Overview," 2004.

[17] World Wide Web Consortium, "SPARQL Query Language for RDF, W3C Working Draft," 2005.

Appendix A Acronyms and Abbreviations

ACT	Allied Command Transformation
CDS	Cross Domain Solution
CJTF	Combined Joint Task Force
CWID	Coalition Warrior Interoperability Demonstration
EFX	Efficient XML
FFI	Norwegian Defence Research Establishment
IETF	Internet Engineering Task Force
IM	Instant Messaging
JMS	Java Messaging Service
MMHS	Military Message Handling System
NBD	Network Based Defence
NC3A	NATO Consultation, Command and Control Agency
NEC	Network Enabled Capability
NFFI	NATO Friendly Force Identifier
NNEC	NATO Network Enabled Capability
NORCCIS	Norwegian Command and Control Information System
NRF	NATO Response Force
OWL	Web Ontology Language
RDF	Resource Description Framework
SOA	Service Oriented Architecture
XML	eXtensible Markup Language
XMLDSIG	XML Digital Signature
XMPP	Extensible Messaging and Presence Protocol