FFI-RAPPORT

16/02459

CWIX 2016 core services experimentation

–

Trude H. Bloebaum,
Frank T. Johnsen,
Ketil Lund

CWIX 2016 core services experimentation

Trude H. Bloebaum,
Frank T. Johnsen,
Ketil Lund

Norwegian Defence Research Establishment (FFI) 6 March 2017

Keywords

Tjenesteorientert arkitektur
Kjernetjenester
Federated Mission Networking (FMN)

FFI-rapport

FFI-RAPPORT 16/02459

Prosjektnummer

1277

ISBN

P: 978-82-464-2881-9
E: 978-82-464-2882-6

Approved by

Bjørn Jervell Hansen, *Research Manager*
Anders Eggen, *Director*

Summary

This report covers the experiments conducted by the participants in the Service Oriented Architecture (SOA) focus area at CWIX 2016. This report gives a brief overview of the full set of SOA-related experimentation at CWIX 2016, with particular focus on the experiment series that the Norwegian Defence Research Establishment (FFI) participated in. The main findings from the experiment series where FFI did not participate are included because they provide valuable insight into the use of SOA foundational services in a federation.

At CWIX 2016, FFI collaborated with the NATO Communication and Information Agency (NCIA) and partner nations in experiments where the main goal was development and verification of Federated Mission Networking (FMN)-related interoperability specifications for central infrastructure services. In particular, we participated in two experiment series related to information sharing using the request/response and publish/subscribe messaging patterns.

Within request/response messaging, FFI took part in testing the new Web Services Messaging Protocol (WSMP), which is designed to be a transport and querying protocol for friendly force tracking independent of the XML data format being used.

NATO has selected the WS-Notification standard for subscription services, and FFI participated in experiments designed to help verify subscription services specifications. In particular, we tested advanced functionality which has not been tested at CWIX before.

In retrospect, this year's CWIX was very successful. We were able to test aspects of several different core services, and uncovered limitations of the frameworks that were in use. This shows that CWIX is a valuable arena, not only for nations to test their own systems, but also to be able to influence the development of specifications that will be included in FMN. This makes CWIX a very important experimentation venue for FFI and Norway.

Sammendrag

Denne rapporten dekker eksperimentene som ble gjennomført av deltakerne innen fokusområdet for tjenesteorientert arkitektur (SOA) under CWIX 2016, og gir en oversikt over resultatene fra alle disse eksperimentene. Forsvarets forskningsinstitutt (FFI) deltok i noen av testseriene og disse testene beskrives i detalj. Hovedresultatene fra de testseriene der FFI ikke deltok er også gjengitt, da disse resultatene gir viktig kunnskap om bruk av SOA i føderasjoner.

På CWIX 2016 samarbeidet FFI med NATO Communication and Information Agency (NCIA) og partnernasjoner i eksperimenter der målet var utvikling og verifisering av Federated Mission Networking (FMN)-relaterte interoperabilitetsspesifikasjoner for sentrale infrastrukturtjenester. Rent konkret deltok FFI i to eksperimentserier tilknyttet informasjonsutveksling med henholdsvis request/response-meldingsutveksling og abonnementsbasert meldingsutveksling.

Innenfor temaet request/response-meldingsutveksling deltok FFI i testingen av den nye Web Service Messaging Protocol (WSMP), som er designet til å være en transport- og spørreprotokoll for utveksling av XML-data for posisjonering av vennlige styrker.

Nato har valgt standarden WS-Notification for abonnementstjenester, og FFI deltok i eksperimenter for å verifisere Nato FMN-relaterte spesifikasjoner for abonnementstjenester. Det ble fokusert på avanserte temaer som ikke tidligere har vært testet på CWIX.

Avslutningsvis vil vi understreke at vi mener årets CWIX var svært vellykket: Vi var i stand til å teste aspekter ved flere ulike kjernetjenester og avdekket begrensninger ved rammeverkene som var i bruk. Dette viser at CWIX er en verdifull arena, ikke bare for å teste egne systemer, men også for å kunne påvirke utviklingen av spesifikasjoner som vil inngå i FMN. Dette gjør CWIX til en svært viktig arena for FFI og Norge.

Content

1 Introduction

The Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX) is an interoperability testing event arranged by NATO Allied Command Transformation (ACT). The event is hosted annually, most recently at the Joint Forces Training Center (JFTC) in Bydgoszcz, Poland.

CWIX is a federated multi-functional test environment, and a wide spectrum of technical interoperability topics are addressed during the planning and execution of CWIX. The aim of CWIX is to improve the technical interoperability within the NATO alliance in a timely and cost effective manner by testing systems, finding solutions for interoperability shortfalls, experimenting with alternative approaches, and exploring emerging technologies. CWIX is a key tool in the process of addressing the technical shortfalls of systems before they are operationally deployed, thus reducing risk, resource requirements, and system failures in theatre.

The activities at CWIX range from explorative testing of emerging standards and profiles, through experimentation with new interoperability solutions and examination of the technical interoperability of systems, to interoperability exercises for operational users. More recently, it has taken on an important role as testing arena for early Federated Mission Networking (FMN)-related experiments, where nations can test their FMN capabilities for interoperability prior to the formal FMN validation and verification process.

The different activities at CWIX are organized in focus areas. Each focus area functions both as a meeting ground for CWIX participants with common interests, and as a coordination point for the testing performed in that focus area's field of expertise.

This report focuses on the activities in the Service Oriented Architecture (SOA) focus area, which is responsible for the SOA-related testing at CWIX. SOA is a paradigm for how to build highly interoperable distributed systems, and is within NATO recognized as a key enabler for building federated systems. Both the NATO Network Enabled Capability (NNEC) and FMN visions rely on the SOA paradigm for the technical integration of software components (services and applications) and federation of systems.

The primary concern of the SOA focus area is the common enabling layer of services, called SOA platform services in the C3 Taxonomy [1]. These services provide basic building blocks to support execution, monitoring, and control of other functional services, information sharing, and security in a SOA environment.

In 2016, FFI participated in a subset of the test series that were performed in the SOA focus area. Chapter 2 gives the background and motivation for the FFI participation, Chapter 3 summarizes the SOA focus area results for the tests FFI did not participate in, while Chapters 4 and 5 give further details on the tests FFI was involved in. Chapter 6 concludes this report.

2 FFI participation at CWIX 2016

The Information and Integration Services research program at FFI has participated in testing events at CWIX for a number of years, primarily in order to support the work on developing core services specifications for FMN. This work has so far been done primarily by the Technology for Information, Decision and Execution (TIDE) Technology Track, in which FFI participates. This community develops and improves profiles for how to use a number of core services standards in a federation context.

CWIX, and the SOA focus area in particular, is the primary testing arena for the TIDE Technology Track. During the experimentation at CWIX, valuable feedback on how well the specifications and profiles function as interoperability enablers is captured. This feedback is processed by the TIDE Technology community, which uses this information to improve the specifications and profiles. When the profiles, normally after multiple iterations of testing at CWIX, reach a high degree of maturity, they are passed on to the FMN community for potential inclusion in future FMN spiral specifications. The interactions between these two communities are illustrated in Figure 2.1.

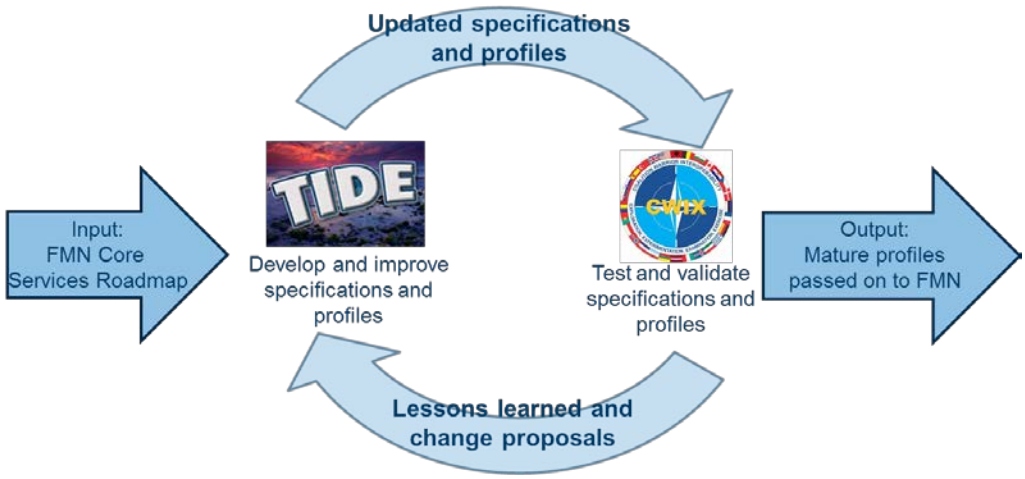


Figure 2.1 Interactions between the TIDE Technology Track and the CWIX SOA focus area

During CWIX 2016 there were multiple different test series performed within the SOA focus area, most of them focusing on supporting the profiling work for FMN. FFI participated in a subset of these tests. The tests in which FFI did not take part are summarized in Chapter 3, while the two test series FFI participated in, namely request/response messaging using the Web Service Messaging Protocol (WSMP) and advanced use of publish/subscribe, are described in detail in Chapters 4 and 5 respectively.

In addition to supporting the process described above, the FFI participation at CWIX also supported testing related to other activities relevant to FFI. These activities, and the purpose of the testing done at CWIX to support these activities, are described further in the following sections.

2.1 Coalition Network for Secure Information Sharing (CoNSIS II)

The Coalition Network for Secure Information Sharing II (CoNSIS II) is a multinational collaboration project which, amongst other topics, is looking into supporting Web services technology at the tactical level [2]. Current activities within this topic is focused on supporting publish/subscribe in tactical networks, and also looking into ensuring that information recipients that suffer from connection disruptions are able to retrieve the information that they have missed out on while disconnected. This requires the use of the more advanced features of publish/subscribe, which is what FFI focused on in support of CoNSIS II at CWIX this year. This activity is described in detail in Chapter 5.

In addition to the CoNSIS II-related testing done within the SOA focus area, there were some additional CoNSIS II-related activities in the Communications focus area as well. Within this focus area, Fraunhofer FKIE from Germany showcased some of their CoNSIS II contributions.

CWIX 2016 was the first year of the Communications focus area, and only Fraunhofer FKIE participated in this focus area, using a proof-of-concept prototype of software defined radios. The prototype was set up with a Flexible IP (FLIP)[1] waveform developed by Fraunhofer FKIE. In addition, they used Dynamic Link Exchange Protocol (DLEP)[2] for exchange of network information between radios and routers.

Although networking and communication so far has not been a subject in CWIX, there are two factors that indicate that this will become an important focus area:

- FMN is currently (spiral 1 and 2) only concerned with fixed networking. However, future FMN spirals will have to take mobility into account, and the services included in FMN must be able to function over radio networks. Being able to test interoperability with realistic networking conditions is very valuable to the other functional areas, and it is therefore important to have test facilities that enable such testing.

- Software Defined Networking (SDN) is very rapidly gaining momentum and should be investigated also in a military (NATO) context.

These aspects imply that the communications focus area will be important both for doing testing on network technology as such (both radio and fixed networks) and for providing realistic networking conditions for other focus areas. This, in turn, means that the focus area will probably have to handle both own experimental activities, and providing networking services for other focus areas.

Some possible candidates for testing within the focus area are interoperability for the Optimized Link State Routing Protocol Version 2 (OLSRv2) [3] and DLEP, interoperability between

[1] Flexible IP waveform: An, experimental waveform for tactical environments, designed to work together with software-defined networks
[2] Dynamic Link Exchange Protocol: A mechanism used by the routing protocol for exchanging information with the radio, in order to do better routing decisions

radios and routers, and testing of legacy modes for existing radios. Also, a possible future coalition waveform is a relevant area for this focus area.

2.2 NATO RTG/STO IST-118

IST-118 is a NATO research task group working under the IST panel. The full name and topic of IST-118 is “SOA recommendations for disadvantaged grids in the tactical domain”. The focus of this group is thus to provide recommendations on how one can support the various core services required in a service-oriented system when the system is deployed in the tactical domain. An important aspect of making such recommendations is to ensure that the tactical optimizations the group recommends do not compromise the interoperability with other nations. In order to ensure that this interoperability is retained, the same software components that are used in IST-118 were tested for interoperability at CWIX 2016. For further information about IST-118 and its results, see [4].

2.3 EP1667 SMART – Pervasive common situational awareness at the individual soldier level

“EP1667 SMART – Pervasive common situational awareness at the individual soldier level” is a Norwegian national Concept Development & Experimentation (CD&E) activity. Every year the Norwegian Armed Forces executes a number of such activities, and one of the activities being performed in 2016 was EP1667 SMART. The purpose of this activity was to investigate whether commercial smart technology, primarily smart phones, can be used as a cheap and powerful platform for situational awareness for units that have little to no technological support tools available today [5].

One aspect of the testing performed in EP1667 SMART was done in order to ensure that the technical solutions used in the demonstrator would be able to exchange information with both the Norwegian defense information infrastructure and with NATO. The national interoperability was tested at national labs, while the NATO interoperability was tested at CWIX 2016 as part of the FFI experimentation on request/response message exchange, as described in Chapter 4.

3 SOA focus area summary

The SOA focus area encompasses a number of different activities, and there are tests being performed within a number of different topic areas. This chapter summarizes the main findings from the topic areas in which Norway did not participate, and is a summary of the information found in the CWIX 2016 SOA Final Report [6]. Information about the two test series Norway participated in can be found in the next two chapters of this report.

3.1 Public Key Infrastructure (PKI)

The SOA focus area (FA) has been working on testing PKI interoperability for several years, and that testing continued this year, in conjunction with the FMN focus area. This year, NATO deployed an instance of the NATO PKI, which allowed NATO systems to use NATO certificates. The testing of certificates, which was based on the current FMN Spiral 1 specifications for digital certificates, was generally successful, with server certificates being trusted for secure information exchange without issues on the client side.

One notable success, was the testing of asymmetric trust models between NATO and the German “DEU Mission PKI”. The NATO PKI trusted the DEU Mission PKI using trust lists, while the DEU PKI trusted the NATO PKI using cross-certification. This demonstrated that partners do not need to adopt the same trust model in both directions to achieve interoperability.

3.2 Labeling

NATO is currently working on two STANAGs related to confidentiality labeling of information, namely STANAG 4774 for the labeling syntax and STANAG 4778 for the binding profiles. Both of these were tested extensively in both the SOA focus area and the Data Centric focus area. The work in the SOA focus area complemented the work done in the Data Centric focus area, which was not so focused on testing the individual binding profiles. Note that while not all participants in the SOA focus area tested all of the binding profiles, all the binding profiles were tested successfully between at least two partners.

The SOA FA Test partners had agreed that they would provide data labeling to support information sharing test cases with NIEM over WSMP (see Chapter 4 for more information on the unsecured version of these tests). STANAG 4778 specifies a number of different binding profiles to support different data formats, applications and information exchanges.

For NIEM over WSMP there are three viable binding profiles from STANAG 4778 that could have been used:

1. Encapsulating XML Binding;
2. SOAP Binding; or,
3. Detached XML Binding (WSMP).

Claiming conformance to STANAG 4774 alone, or to both STANAG 4774 and STANAG 4778 in conjunction, is not enough for interoperable information exchange with labeled information. It is also necessary to specify the STANAG 4778 binding profile(s) that are to be supported in the information exchange. In this particular case, the recommendation would be to use the detached XML binding in the WSMP element.

Note that FFI did participate as an information consumer in one of the labeling tests, as the partners performing the main testing wanted to see if the labeled information they were sharing could be parsed correctly by a partner that did not have a labeling capacity at CWIX 2016. FFI was able to correctly interpret information that had either a detached or SOAP binding, while encapsulating XML bindings failed. This was due to the fact that the encapsulated XML binding changes the format of the data payload in a way that makes it difficult to parse without understanding the label syntax.

3.3 Securing Web Services

In addition to adding labeling to the information, it is also important to protect the services themselves. The TIDE community has developed specifications for both end-user authentication towards Web applications (so-called Web authentication or single sign-on (SSO)), and for security between Web services and clients (called Web services security (WSS)). Both of these specifications have been tested at previous CWIX exercises, with FFI participating in the tests of SSO in 2014 and 2015.

The SSO testing was concluded in 2015, as an agreement was reached on how to support this aspect of securing services. WSS continues to be a challenging topic, but the tests performed at CWIX 2016 were ultimately successful. The main interoperability issue that was identified, national implementation issues aside, was the use of SHA-1 as the signature algorithm. While the use of SHA-1 has been retired across NATO and in most nations, some participants were still using SHA-1. It was noted that a primary source of this issue was that the WS-SecurityPolicy standard lacks support for expressing that SHA-2 should be used. The current TIDE specification for WSS mandates the use of SHA-2, but also recommends the use of WS-SecurityPolicy without addressing how the use of SHA-2 should be supported. Solving this issue is straight forward technically, but requires agreement between all partners, and the issue was therefore forwarded to the TIDE community for potential inclusion into their specification work.

In addition to looking into security for SOAP Web services, CWIX 2016 included, for the first time, tests related to securing RESTful Web services. These tests proved to be more straightforward, with the two available implementations working more or less out of the box. The specification used as a basis for the REST security tests will be forwarded as a recommendation to the FMN community, but it will also be subject to further testing at CWIX 2017 to ensure that it can be verified by more than two partners.

Two further security related topics were discussed, but not tested, at CWIX 2016. The first of these two topics is end-to-end (E2E) authentication. The SSO specification mandates how an end user should authenticate to a Web application such as a portal, while the WSS specification covers service-to-service security, such as for instance a portal using back-end services. This is illustrated in Figure 3.1.

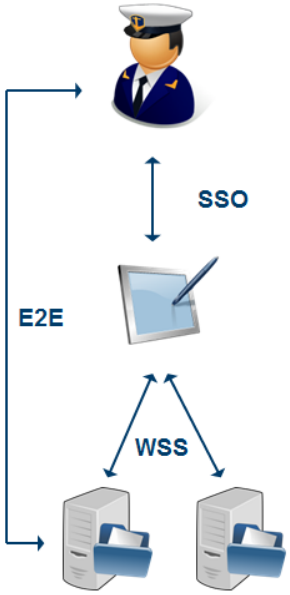


Figure 3.1 Securing service interactions end-to-end requires bridging between the mechanisms used for Web authentication (SSO) and Web services security (WSS)

Supporting both SSO and WSS does however not give E2E authentication on their own, as there is no relaying of identity information between the two. If SSO and WSS are used stand-alone in our portal example, the portal would know who the end user is, but the portal would use its own identity when using the back-end services. This means that the back-end services would only know that the request came from the portal, but not which end user the request was on behalf of.

In order for the back-end services to get the identity of the actual user, there is a need to relay that information through the portal. This means that one has to support authentication with multiple identity tokens, one representing the portal, and a delegated token representing the end user. This challenge was discussed, and suggested as a topic for further testing next CWIX.

The second security topic that was discussed at CWIX was security for publish/subscribe services. Securing such services is challenging, due to the disconnected nature of this information exchange messaging pattern. As information consumers in a publish/subscribe system does not need to know the identity of the information producer, one cannot simply utilize the same mechanisms as for standard request/response communication. Securing publish/subscribe services remains an open research question, and it was decided that this topic should be taken in for discussion during the next TIDE Sprint event.

4 Request/response message exchange

The exchange of messages in a request/response manner is the most fundamental building block of SOA environments, and being interoperable at this level is a requirement before one can support more complex interaction such as publish/subscribe, or support value-added functionality such as security and information labeling. As such, request/response messaging has been tested in the SOA focus area since it was first established, but there continues to be new developments in this area that warrants continued testing. This chapter describes the request/response-based testing performed at CWIX 2016.

4.1 Technical background

The Friendly Force Tracking (FFT) focus area at CWIX has, for the last few CWIX cycles, worked on the follow-on to the successful NATO Friendly Force Information (NFFI) standard. As part of this work, they have identified the need for a protocol for friendly force information that is able to carry, in a uniform manner, positional information formatted using different eXtensible Markup Language (XML) data formats. The protocol should also support querying for information, including the use of format specific queries. Additionally, the transport mechanism should support both request/response message exchanges and publish/subscribe message exchanges. As a response to this need, NATO has developed WSMP, which supports all of these features.

4.2 CWIX 2016 test focus

During CWIX 2016, the SOA focus area did a number of tests using the request/response mechanism of WSMP, called WSMP-RR. While the protocol itself is being developed by the FFT community, it is based on the core services specifications for SOAP messaging and publish/subscribe messaging. These two specifications fall within the responsibility of the SOA focus area, making it a topic of interest for this community as well. Additionally, some members of the SOA focus area are looking into different data formats, and WSMP-RR appeared to be a good mechanism for exchanging multiple data formats at the same time and testing mediation services which translate between these data formats.

In addition to the testing of WSMP-RR, the SOA focus area also looked into two other mechanisms for exchanging information in a request/response manner. These two mechanisms were REST and WebSockets. Both of these technologies have become common in use both in the civilian sector and within some communities of interest within NATO. Most of the testing done with these two protocols was performed in collaboration with the Modeling & Simulation focus area.

4.3 FFI's technical solution

One of the key principles of SOA is that functionality should be broken down into smaller, autonomous services, which can then be re-used when building other applications that require parts of the same functionality. As part of the FFI CWIX participation, we decided to use a multi-format track store where we applied this principle: storage, format mediation and protocol handling were implemented as separate functionality. This made it easier to expand the software with support for new data formats and transport protocols.

The main components of the multi-format track store are shown in Figure 4.1. Incoming requests was handled by the appropriate handler for the protocol the message arrived over. The protocols supported by the multi-format track store were:

- WSMP-RR as a carrier for both NFFI-formatted data and data formatted according to the US National Information Exchange Model (NIEM)
- NFFI over the TCP-based interface (IP2) of the NFFI-standard. This interface was used when importing information from the Norwegian C2IS, NORCCIS.
- A REST-based interface for synchronizing information with the Android-based demonstrator developed in EP1667 SMART. This interface supported the operations and data format described in [7].

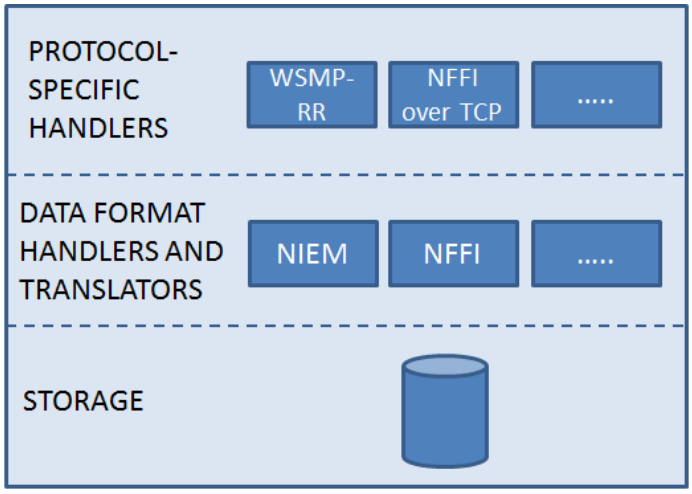


Figure 4.1 Main components of the multi-format track store

If the incoming message contained new data to be added to the track store, the protocol-specific handler would extract the information from the message, identify the data format, and pass the data on to the matching data handler. The data handler would ensure that the data was translated to all other formats, and the information would be passed on to the storage function which would save the data in all formats. This translate-on-arrival approach was chosen as we expect queries for information to be more common than the arrival of new information.

Incoming requests for information (queries) would be handled somewhat differently depending on the protocol it arrived over and the requested data format. This was due to the fact that not all protocols support the same query expressions. For NFFI over TCP and for the synchronizing with the EP1667 SMART solution, the most recent data for the entire available data set was exchanged every time.

For requests arriving over WSMP (so-called WSMP Read request), the request would include a filter expression. The only supported filter type at CWIX was the NIEM filter, which allows you to query by battle dimension (surface, sub-surface, ground and air), by time, and by geographical location. Our track store supported this filter type, so requests would be answered with a response matching the query filter. A request for NFFI over WSMP-RR, on the other hand, would give a response containing the most recent data for all units in the track store, since filters are not supported for NFFI.

The implementation of the track store was done as a student project, and more details on this project can be found in [8].

4.4 Main outcomes

The WSMP-RR testing done within the SOA focus area showed that the protocol can be used successfully both for querying, and for transferring, data on multiple different formats. By specifying the response format in the query, the same services can be used to support multiple formats.

There are some issues related to these multi-format exchanges; for each new format, a document specifying how data of that format should be included into each of WSMP-RRs operations is required, and the format specific filter must be formally described and implemented.

Also note that the following observation from CWIX 2015 [9] still holds true:

> *The primary finding from the data format testing was related to the use of the XML constructs xs:Any and/or substitutionGroups in XML schemas. These constructs function as extensibility points in the schemas, which allows for multiple levels of abstraction in the message exchange, i.e., allowing the same message wrapper and filtering mechanism to be applied to multiple different data formats. There is one significant downside to the use of such extensibility points in schemas, namely that many of the tools used for auto-generating classes from schemas are unable to handle this properly. This means that supporting such schemas require more manual implementation work, which in turn may increase development time and cost.*

For REST and WebSockets it was determined that achieving interoperability with these Web technologies is fairly straight forward, but some profiling work should be done ahead of next year's CWIX to ensure that more partners are able to bring compatible solutions.

5 Publish/subscribe message exchange

The basic publish/subscribe message exchange has been tested within the SOA focus area at CWIX for the past few years [9] [10], and we know from those tests that the basic exchange can be supported in an interoperable manner. This year, testing was focused primarily on the more advanced topics within publish/subscribe. Note that securing publish/subscribe message exchanges has not been addressed yet, and remains a topic for future profiling and testing work.

5.1 Technical background

In order to support the publish/subscribe messaging pattern, NATO has pointed to the WS-Notification family of standards. This standard supports both the direct and the brokered publish/subscribe patterns, as illustrated in Figure 5.1.

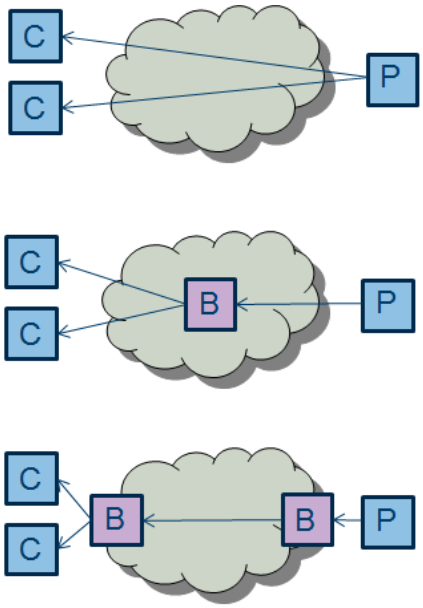


Figure 5.1 The different publish/subscribe topologies supported by WS-Notification, with direct message exchange at the top, single brokered exchange in the center and a multi-broker topology at the bottom

The direct message exchange, in which the information producers communication directly with the information consumers require both producer and consumer systems to support the publish/subscribe pattern and protocol. In addition, this direct exchange of information typically means that multiple copies of the same information are sent all the way from the producer to the consumer. At CWIX 2016, this type of message exchange was utilized by the Multilateral Interoperabilty Programme (MIP) focus area, which was testing transporting MIPs next generation message set, called the MIP 4 Information Exchange Specifications (IES), in this manner (see [11] for more detail on these tests). This testing was co-located with the SOA focus

area, but the tests were performed separately from the brokered publish/subscribe tests FFI participated in.

Brokered publish/subscribe involves introducing one or more intermediary nodes, which offload the information producers from such tasks as managing subscriptions and disseminating notifications. These brokers can be deployed in a number of different ways, ranging from a single broker deployment to a mesh of interconnected brokers. The current NATO profiles from publish/subscribe services, such as the Service Interface Profile (SIP) included in the NATO Interoperability Standards and Profiles (NISP), do not mandate a given deployment strategy.

In a publish/subscribe message exchange, there is also a need for sharing information about *interests.* When a subscription is created, the broker needs to know what type of information the consumer is interested in receiving. This can either be done by providing a set of keywords, called *topics,* which is checked against the message metadata every time a new message arrives at the broker. The other option is to use a *content* filter, which is a filter expression that is applied to the content of the message. In this latter case, the broker needs to understand the filter, read the entire message, and apply the filter to that message.

5.2 CWIX 2016 test focus

Within the SOA focus area, there were four participants that indicated interest for performing publish/subscribe testing at CWIX 2016. Of these four capabilities one (France), had to cancel their participation, while the NATO Communications and Information Agency (NCIA) opted to only test publish/subscribe in the context of the FFT focus area, which only used the basic subscription from WS-Notification. This left Norway (represented by FFI) and Germany (represented by IABG) as the two remaining partners for testing the advanced features of the standard. There were two such advanced topics discussed, namely *publisher registration* and the use of so-called *pull points*.

5.2.1 Publisher registration

One of the optional features of the WS-Notification standard is publisher registration, in which a producer can register its intent to publish information on a given topic with the broker. At CWIX 2016, the main publish/subscribe test focus was on trying this optional feature for the first time. The reason behind this test series was that the publisher registration feature can be used in order to ensure that only approved publishers are allowed to push information to the broker. By requiring that all publishers register in advance, particularly if this is combined with authentication of the publishers, this will function as a first step towards protecting the broker infrastructure against attacks such as Denial of Service attacks.

In addition to using the publisher registration as a security enabler, publisher registration can also be used to alleviate an identified issue in multi-broker topologies. During testing with WS-Notification during earlier years at CWIX, interoperability was achieved using brokers. There were, however, some challenges identified related to multi-broker topologies. The main

challenge is that information about which topics were available at each broker would have to be shared out of band, as this is not supported by the WS-Notification standard. This problem also exists in direct and single broker topologies, but there it can be mitigated if the producers and broker expose an overview of the topics they support using a WS-Resource compliant endpoint. In multi-broker topologies, consumers might connect to a different broker than the one that offers the information the consumer is interested in, leading to a need to share topic information between brokers.

In the latest version of the TIDE specifications for publish/subscribe, supporting publisher registration is mandatory [12], primarily due to its role as a security enabler. This aspect of the profile had yet to be verified through testing before CWIX 2016, and was the reason for why this was chosen as a test topic for the SOA focus area.

5.2.2 Pull points

One challenge related to the use of the publish/subscribe messaging pattern in general, is that consumers that either join the message exchange late, or are temporarily disconnected, might miss out on information they need. Being able to retrieve messages after the information has been disseminated was identified as a needed extra feature shortly after testing with WS-Notification started some years ago. As a response to this requirement, the NCIA created a specification for a notification cache. While this notification cache specification did function in conjunction with the WS-Notification standard, support for this feature would require the broker to have functionality beyond what is described in the WS-Notification standard.

During the TIDE Technology Track discussion on the topic, it was suggested that one should, instead of having a separate notification cache, try to solve the same challenge by creating a profile for the WS-Notification pull point interface. Pull points are an optional feature of WS-Notification that enables consumers to request a broker to store information on the consumer's behalf, so that the consumer can retrieve this information later at its own convenience.

For pull points to be a viable option to a notification cache, it must be possible to achieve interoperability between different implementations of the pull point feature. Due to this, investigating pull point interoperability was put on the short list for topics to be covered at CWIX 2016.

5.3 FFI's technical solution

WS-Notification has been a standard since 2006, but support for the standard in commercially available brokers is low. There are some brokers available that support parts of the standard, but the support in those products tends to be either partial or for an older version of the standard.

The software used to test WS-Notification at previous CWIX exercises has been either national, proprietary software, or proprietary extensions built on top of the partial implementations that are openly available. In previous years, FFI has used two different nationally developed

prototype implementations, the most recent being WS-Nu [13], but neither of these supports the full standard. Therefore, it was decided that Norway would use industry funding from CoNSIS II to acquire a more complete implementation of the WS-Notification broker specification [2]. This broker was delivered shortly before CWIX 2016, and was used, along with some FFI-developed testing tools, at this year's CWIX.

In CoNSIS II there have been discussions on how the usage of publisher registration as a means to spread topic information will impact the performance of the brokers. As CoNSIS II focuses on tactical application of services, the network traffic generated is of particular concern. As discussed in [9], there is an issue related to the use of content filters. Publisher registration can be used to spread information about which topics a broker supports. Including support for content filters in all brokers is more challenging, and leads to more complicated broker implementations. In order to limit the complexity of the brokers, one suggested solution is to always forward content filters all the way to the original producer of the information, and process them there. By doing so, the total number of messages that have to traverse the network path from producer to the consumers would increase. While doing this in a fixed network infrastructure has little impact on the overall performance of the system, doing this in a tactical network has a potential risk of overloading the limited networking resource available.

Due to the above described issue, it was agreed that the CoNSIS II members wanted to start investigating the impact of this feature. There was also an agreement that one should start investigating if pull points can be used be used by nodes reconnecting after a temporary disconnection. This required both Germany and Norway (the main partners doing SOA-related testing in CoNSIS II) to have interoperable implementations of WS-Notification supporting registration, topic filtering in the brokers and pull points. The previously used FFI prototype implementations did not support these features, but with our new broker acquired through the CoNSIS II funding, we were now able to do this testing.

In addition to the CoNSIS II developed broker, FFI also utilized a self-developed mechanism for bridging between different publish/subscribe protocols [14]. This protocol federation mechanism was used within our own FFI capability, and was not exposed directly to our partner. The reason for still bringing it to CWIX was that we wanted to confirm that its WS-Notification capabilities were compatible with our partners, which we did indirectly through the WS-Notification tests already taking place. This protocol bridging mechanism has been used to support the activities in IST-118, and is planned to be used in the IST-118 follow-on, IST-150 [15], research task group as well.

5.4 Main outcomes

As previously mentioned, FFI's main testing partner on the topic of advanced publish/subscribe was Germany represented by IABG. Like FFI, they have their own implementation of a service oriented reference system which supports the advanced publish/subscribe features.

Due to the fact that both FFI and IABG had made considerable changes to their respective broker implementations, we first re-tested the basic subscription message exchange. This allowed us to iron out a few implementation bugs and achieve interoperability between the implementations. There was one minor issue related to the handling of the end-time for subscriptions in the FFI broker that was not fixed on-site, but a work-around was identified to allow testing to continue. This issue was rectified shortly after CWIX 2016.

After having confirmed that the new implementations were still compatible with respect to the basic subscription exchange, we tested publisher registration. During the CWIX 2016 planning process, it was agreed that testing the publisher registration process should be done by following the steps listed in Table 5.1.

Number	Description	Expected Result
1	The subscriber sends a subscription request to the broker	The broker receives the subscription request
2	The broker processes the subscription request	The brokers understands the request, including the filter
3	The broker returns a subscription reference to the subscriber	The subscriber receives the response message
4	The publisher publishes to the broker without registering	The publishing fails, and the message is not distributed
5	The publisher registers with the broker	The registration is successfully processed by the broker
6	The publisher publishes to the broker	The notification message is accepted by the broker
7	The broker sends matching notifications to the consumer	The consumer receives notifications
8	The consumer checks the received notification(s)	The consumer has received the correct notification(s)

Table 5.1 Steps in the advanced publish/subscribe tests

Successful completion of the first three steps means that a subscription has been created on behalf of a consumer. This is done first, so that the consumer can be used to verify if the broker behaves correctly.

After the subscription has been created, the publisher attempts to publish without registration. The broker should at this point be configured to only accept messages from registered publishers, and will thus not forward the message to the consumer.

Finally, the publisher registers and then publishes the same message again. In this case, the message is accepted by the broker and forwarded to the consumer.

There were two such tests performed, one with FFI's broker handling the registration and one with the IABG broker handling the registration. When FFI provided the broker, all the steps completed successfully as long as we used the work-around mentioned above to handle the minor subscription end time issue. When the tests were repeated with the IABG broker, there was an issue in step 4, as the message sent from an unregistered publisher still arrived at the consumer. This was due to the IABG broker supporting both registered publishers and unregistered publishers at the same time, and it was not possible to configure it to reject messages from unregistered sources. Despite this issue, it was concluded that publisher registration is a viable method for sharing topic information between brokers as long as all brokers re-register with their partner brokers when their set of provided topics changes.

With respect to testing pull points, there was no test process agreed on during the CWIX planning stage as it was unclear at that time whether there would be at least two pull point implementations available. At the time of the exercise execution, it was discovered that both the IABG and FFI brokers had support for this feature, so some informal tests were done to check for interoperability. The technical implementations proved to be interoperable, but, as expected, the WS-Notification pull point specification does not provide enough guidance on what the broker behavior should be (which of the stored messages should be sent when a consumer pulls for data etc.). It was agreed that a pull point profile is needed, and IABG took on the responsibility to create the first draft for such a profile. This profile will, when ready, be brought into the TIDE Technology community for discussions.

6 Summary

This report has described the activities of the SOA focus area at CWIX 2016. Both the NNEC and FMN visions rely on the SOA paradigm for the technical integration of services and federation of systems, and together with TIDE, this focus area plays a vital role in the work towards these visions. FFI has participated in the SOA focus area over a number of years, and this year, we have focused on request/response- and publish/subscribe messaging.

Request/response messaging is the most fundamental building block of SOA environments, and interoperability at this level is equally fundamental. Although a mature area, new developments warrant continued testing within the area, and FFI contributed through testing of WSMP-RR. We used our own multi-format track store for exchanging NIEM and NFFI messages. The results showed that the WSMP-RR protocol can be used successfully with multiple different formats and, by specifying the response format in the query, the same services can be used to provide multiple data formats.

Publish/subscribe messaging has also been a central subject of the SOA focus area for a number of years, but it is still less mature than request/response. FFI's participation within this subject focused on two topics, namely publisher registration and the use of so-called pull points. FFI participated with a new WS-Notification broker, developed within the CoNSIS II cooperation, which supported both these topics.

Publisher registration is considered a promising mechanism both for security and for disseminating information about available topics to subscribe to. Norway (represented by FFI) tested such registration together with Germany (represented by IABG), and our broker successfully handled publisher registration both as a provider and as a consumer.

Pull points have emerged as a requirement, due to the need for being able to retrieve messages at a later point in time after the information has been published (e.g., a consumer arriving late or having been disconnected). No testing of pull points was formally planned for at CWIX this year, but some informal tests were done between FFI and IABG to check for interoperability. The implementations proved to be interoperable, but more work is needed with respect to broker behavior.

CWIX continues to play an important role for work being done on core services, and it is still the primary venue for interoperability testing of NATO's core services specifications. CWIX also provides an excellent opportunity to influence the specifications being developed by TIDE, before they are handed over to the FMN community. Therefore, FFI plans on a continued presence at the coming CWIX 2017 exercise.

References

[1] C4ISR Technology & Human Factors (THF) Branch, Allied Command Transformation (ACT), *The C3 Taxonomy*, Technical report, 2016. Document generated from the ACT Enterprise Mapping Wiki on November 2016.

[2] Coalition Network for Secure Information Sharing II, *Task 2 Final Report*, Technical Report, 2017 [to appear]

[3] T. Clausen, P. Jaquet and U. Herberg, *The Optimized Link State Routing Protocol Version 2*, RFC 7181, April 2014

[4] T.H. Bloebaum, F.T. Johnsen, P-P.Meiler (editors), *SOA Recommendations for disadvantaged grids in the tactical domain*, Final Report of IST-118, final draft submitted to NATO STO CSO on 15.12.16

[5] Frank T. Johnsen, Trude H. Bloebaum, Marianne R. Brannsten, Ketil Lund, Federico Mancini og Bård K. Reitan, *Bakgrunn for og innretning av støtten til EP1667 "SMART"* (in Norwegian), FFI-Report 2016/00848, Exempt from public disclosure

[6] NATO Allied Command Transformation, *Focus Area Final Report, CWIX 2016, SOA*, Enclosure 15 to the CWIX 2016 Final Report, September 2016

[7] Frank T. Johnsen, Marianne R. Brannsten, Espen Gudmundsen, Kari Helene Bekkelund and Magnus Brurås, *Første brukertest i EP1667 "SMART"* (in Norwegian), FFI-Report 2016/01524, Exempt from public disclosure

[8] E. Fosse, A. Borud, S. Grøneng, F. Gausland, S. Georgiev, M. McMillan, *Interoperable NATO Track Entry Log*, Technical Report, FFI reference number 16/01186, May 30, 2016

[9] T.H. Bloebaum, F.T. Johnsen, M.R. Brannsten, *CWIX 2015 core service experimentation*, FFI-Report 2015/01334

[10] T.H. Bloebaum, F.T. Johnsen, *CWIX 2014 core service experimentation*, FFI-Report 2014/01510

[11] NATO Allied Command Transformation, *Focus Area Final Report, CWIX 2016, MIP*, Enclosure 11 to the CWIX 2016 Final Report, September 2016

[12] NATO Allied Command Transformation, *TIDE Transformational Baseline 4.0*, available (access to TidePedia requires an account) at https://tide.act.nato.int/tidepedia/index.php/TIDE_Transformational_Baseline_v4.0

[13] Tormod Haugland (NTNU), Inge E. Halsaunet (NTNU), Frank T. Johnsen and Trude H. Bloebaum, WS-Nu – open source WS-Notification broker documentation, FFI-note 2015/01250

[14] E. Bertelsen, G. Berthling-Hansen, C. Duvholt, E. Hov, E. Morch, A.H. Weisethaunet, *OKSE 2.0 Protocol Mediator,* Technical Report, FFI reference number 2016/01171, May 30, 2016

[15] Frank T. Johnsen and Trude H. Bloebaum, *IST-150 NATO Core Services profiling for Hybrid Tactical Networks kick-off meeting,* FFI-travel report 2016/02169

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

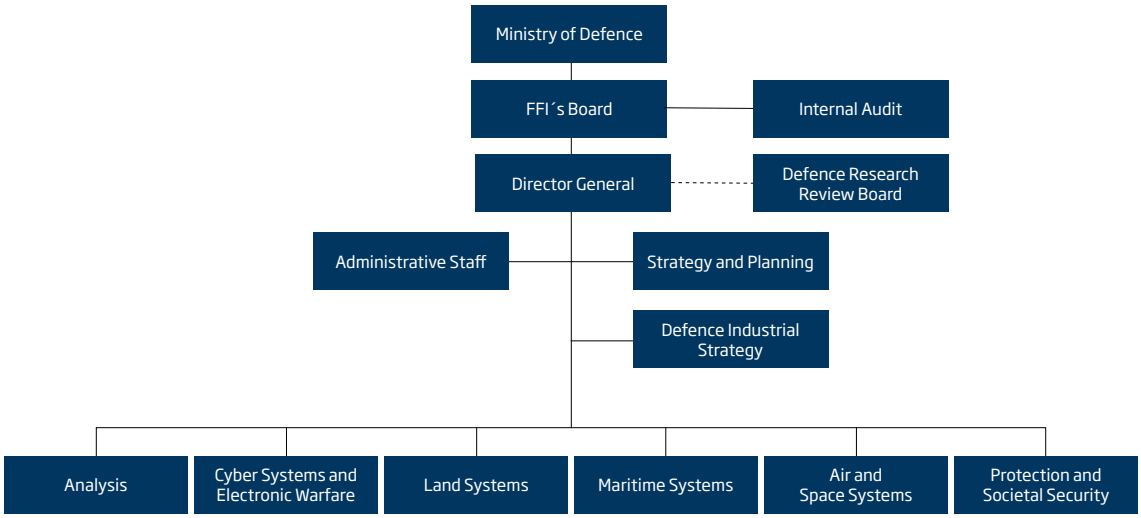
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment