FFI-rapport 2015/01334

CWIX 2015 core service experimentation

Trude H. Bloebaum, Frank T. Johnsen and Marianne R. Brannsten

FFI Forsvarets forskningsinstitutt

FFI-rapport 2015/01334

CWIX 2015 core service experimentation

Trude H. Bloebaum, Frank T. Johnsen and Marianne R. Brannsten

Norwegian Defence Research Establishment (FFI)

19 October 2015

FFI-rapport 2015/01334

1277

P: ISBN 978-82-464-2580-0
E: ISBN 978-82-464-2581-7

Keywords

Eksperimentelle metoder

Tjenesteorientert arkitektur

Kjernetjenester

Federated Mission Networking (FMN)

Approved by

Bjørn Jervell Hansen	Project Manager
Anders Eggen	Director

English summary

This report covers the experiments conducted by the participants in the Service Oriented Architecture (SOA) Focus Area at CWIX 2015 and gives a brief overview of the full set of SOA-related experimentation. The report has particular focus on the experiment series that FFI participated in, including details related to pre-testing, experiment execution and results. The main findings from the experiment series where FFI did not participate are included in the report because they provide valuable insight into the use of SOA foundational service in a federation.

At CWIX 2015, FFI collaborated with 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 three experiment series; two related to information sharing using the request/response and publish/subscribe messaging patterns, and one related to security. For the latter experiment series we mainly focused on issues related to federated identities.

NATO has selected the standard WS-Notification for subscription services, and FFI participated in experiments designed to help verify the subscription services specification from the NATO FMN Implementation Plan (NFIP).

One of the core ideas in FMN is that one should be able to use the national identity (e.g., login to the system) in the federation, regardless of whether it is for use in a designated national system, a NATO system, or a system that is offered from a NATO nation. NFIP appendix S-12 points to the WS-Federation standard for this functionality. However, experiments performed at CWIX both in 2014 and 2015 have shown that it is easier to achieve interoperable authentication with the SAML 2.0 protocol. The NFIP should be updated to reflect this finding.

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 deltagerne innen fokusområdet for tjenesteorientert arkitektur (SOA) under CWIX 2015, og gir en oversikt over resultatene fra alle disse eksperimentene. FFI deltok i noen av testseriene, og disse testene beskrives i mer detalj, inkludert informasjon om innledende testing, gjennomføring og resultater. 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 2015 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 tre eksperimentserier: to tilknyttet informasjonsutveksling med henholdsvis request/response meldingsutveksling og abonnementsbasert meldingsutveksling, og én relatert til kjernetjenesten for sikkerhet. For sistnevnte eksperimentserie fokuserte vi hovedsakelig på aspekter ved fødererte identiteter.

Nato har valgt standarden WS-Notification for abonnementstjenester, og FFI deltok i eksperimenter for å verifisere spesifikasjonen for abonnementstjenester fra NATO FMN implementeringsplan (NFIP). Disse testene ble også brukt som grunnlag for å utvikle instruksjoner for hvordan man skal sette opp en slik tjeneste i FMN.

En av de viktigste ideene i FMN er at man skal være i stand til å bruke sin nasjonale identitet (f.eks. ved pålogging) i føderasjonen, uavhengig av om det er til bruk i et eget nasjonalt system, et Nato-system eller et system som tilbys fra en Nato-nasjon. NFIP-vedlegg S-12 forklarer hvordan man kan bruke standarden WS-Federation for å oppnå dette. Eksperimenter foretatt på CWIX både i 2014 og i år viser at det er enklere å oppnå interoperabilitet med SAML 2.0-protokollen. Anbefalingen fra fokusområdet for SOA er at NFIP oppdateres til å gå inn for SAML 2.0 som protokoll for web-autentisering.

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.

Contents

1 Introduction

The Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX) is a large annual NATO-hosted interoperability testing event. CWIX gathers different stakeholders from NATO and the nations, and functions as a federated multi-functional test environment, and there is a wide spectrum of technical interoperability topics 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. In a highly federated multi-national environment, it is important to improve communication and collaboration between all stakeholders in order to meet common goals and objectives. CWIX is a key tool in the process of addressing the technical shortfalls of systems before they are operational 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, through to interoperability exercises for operational users. 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.

The report focuses on the activities in the Service Oriented Architecture (SOA) Foundation focus area (referred to as the SOA focus area in this report), 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 the Federated Mission Networking (FMN) visions rely on the SOA paradigm for the integration of software components (services and applications) and federation of systems.

The SOA focus area's primary concern 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 SOA environment. The SOA focus area was built around the group of participants providing their own implementations of SOA platform services, but also successfully engaged several partners from other CWIX focus areas that were willing to apply proposed solutions in operational systems.

1.1 Standardization and profiling

One of the basic principles from the SOA paradigm is that information exchange between parties should be based on open, agreed upon and available standards. The reason for this is that the use of such standards is the first step towards achieving interoperability. The use of the standards alone is however not sufficient to ensure interoperability, as many standards have optional features, several alternative solutions for a problem, ambiguities, and other shortcomings.

Profiling of the standards is the next step towards interoperability, as profiles provide guidance on how to use both single standards and combinations of standards. The WS-I Basic Profile 2.0 [2] is one example of such a profile for Web services, which is the technology most commonly used to realize SOA.

In addition to these technology-specific profiles, there is also a need for specifications and profiles that describe how to build and interconnect the services and systems of the nations that wish to participate in the common NATO federated information infrastructure as described by the NATO FMN Implementation Plan (NFIP) [3]. The current version of the NFIP includes specifications for some of the foundational SOA services, but not all. The TIDE Transformational Baseline (TTB) [4] also describes a handful of foundational SOA services, while some aspects of SOA-related topics are covered by NATO Standardization Agreements (STANAGs).

The work done by the SOA focus area centers around the testing, verification and further development of the SOA foundation specifications, with the NFIP, the TTB, and STANAGs 4774 and 4778 being the primary point of focus during this year’s event. During the execution of CWIX 2015, the partners gained experience with the specifications and profiles. In addition, a number of valuable lessons were learnt, and these will be fed back to the appropriate groups for incorporation into the next versions of these important documents.

1.2 Test series

The testing performed by the participants in the SOA focus area was divided into a set of test topics, and each topic had a related series of tests that were to be performed during the CWIX execution. The total number of test topics in the SOA focus area was six, with FFI participating in three of these test series. In this section we introduce all the different test series, and summarize the goals and results of the test series that FFI did not participate in. The tests performed by FFI are the main focus of this report, and the goals and results of these test series are covered in greater detail in the following chapters.

1.2.1 Information sharing

The information sharing topic at CWIX is a broad topic, covering different aspects of information sharing. The involved test partners focus on different aspects; some partners have their main interest in data formats, while others focus primarily on the data exchange mechanisms. The FFI participation at CWIX 2015 focused on the testing and verification of the two message exchange patterns request/response and publish/subscribe. Chapters 2 and 3 present these tests in more detail.

As for the data format testing, the data format being tested was the National Information Exchange Model (NIEM). The US partner, along with the NCIA, was experimenting to gain experience with making and using their own NIEM Information Exchange Package Documentation (IEPD). 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.

1.2.2 Public key infrastructure

Public key infrastructure (PKI) is a term used to describe an infrastructure that supports the creation, management, distribution, verification, and revocation of the digital certificates based on public/private key pairs. These certificates are used to establish trust relationships between partners. The current version of the NFIP includes a specification which describes how to achieve interoperability between the PKI solutions of the different partners. At CWIX 2015, the testing and verification of this specification was delegated from the FMN focus area to the SOA focus area.

The NFIP PKI specification allows for trust to be established in two different ways, either through mutual trust or through cross-certification (for a detailed explanation of these two methods for establishing trust, refer to appendix S-10 of the NFIP). During CWIX 2015 the mutual trust tests were successful for most partners, and it was concluded that this should remain as the recommended approach for FMN. Some test partners also has successes with cross-certification, but this proved to be a more complex scenario that generated several issues. Information about these issues will, together with the experiences the test partners had with using the FMN Template form for PKI, be used to generate change proposals for the FMN specification where needed.

1.2.3 Web authentication

The Web authentication test series is also referred to as Single Sign-On (SSO), and is a part of the SOA focus area investigations into federated identity and access management. FFI participated in these tests, which are further discussed in Chapter 4.

1.2.4 Web service security

The Web service security test series (WSS) is the second topic that falls into the federated identity and access management category. This test series relies on many of the same standards, technologies and frameworks as the web authentication tests, but in WSS these technologies are used to secure the interactions between Web services rather than between the user and a service front-end.

In this test series the primary goal was to provide recommendations for the next version of the TTB specification for Web service security. This topic is a likely candidate for inclusion in future versions of the NFIP, and the goal is that the TTB specification can serve as a well-tested basis for a future NFIP Web service security specification.

There exists several different profiles for how to secure a Web service, and the WSS test series included test for all three basic profiles:

- Security based on the X.509 certificates (WSS1)
- Security based on the Net-Centric Enterprise Services (NCES) [5] profile (WSS2)
- Security based on the Security Assertion Markup Language (SAML) 2.0 token (WSS3)

All three profiles were successfully tested by more than one partner, using heterogeneous implementations of the profiles. The WSS3 tests were most widely supported and also the most successful. Based on this there was a clear majority opinion that using the SAML 2.0 token profile is the preferable approach in the future.

1.2.5 XML labeling

At CWIX 2015 there were two focus areas that were looking into the usage of confidentiality labels to mark data. Both focus areas looked into using the current version of the proposed STANAGs for the confidentiality label syntax (STANAG 4774) and the binding profiles for this label (STANAG 4778), but applied these for different purposes. The Data-Centric focus area primarily applied labels to email and chat services, while the SOA focus area looked at labeling in the context of SOAP and XML message exchanges.

An NCIA-provided NATO Metadata Binding Service (NMBS) was used by multiple partners to verify their labels, which proved to be a useful tool during testing. Further tests with both embedded labels and with SOAP-header labels were successfully tested by some partners through the use of heterogeneous implementations.

It was concluded that there is a need for further testing of XML labeling in the future, particularly once the two STANAGs have been finalized and agreed upon.

1.2.6 Service management and control

Service management and control (SMC) was a new topic for the SOA focus area, which meant that only a few participants actively participated in the test series. However, the main test partners, which were France and NCIA, successfully demonstrated both hub-and-spoke style and peer-to-peer style exchange of monitoring data.

Most of the other SOA focus area test partners participated in the SMC testing by allowing the main test partners to monitor the availability of their services. This information was used to populate the Communication Information System Common Operational Picture (CIS COP) service, provided by France, with data. The CIS COP was demonstrated to both participants and visitors and was well received, and it was concluded that SMC should be a topic for the SOA focus area at future events as well.

1.3 Test partners

The SOA focus area has been performing tests at CWIX for several years, and the number of nations and organizations participating in the focus area as test partners this year was higher than earlier years. In addition, the SOA focus area presentations during the CWIX visitor days were well visited, and included representatives from several nations that are currently not participating in the focus area.

The participating nations and organizations structured their participation in the SOA focus area in different manners. Some partners participated with multiple different capabilities, some partners had one capability responsible for all the SOA related tests, while others performed their SOA tests as a part of a larger national capability. The CWIX 2015 SOA focus area main participants were the following:

- NATO Allied Command Transformation (ACT) functioned as both the focus area lead and a test partner for a number of tests.
- The NCIA participated in the SOA focus area with multiple capabilities, and were involved in most of the test cases performed by the group.
- The NATO Modeling and Simulation Center of Excellence (M&S CoE) participated in multiple test series, with a main focus on the security related tests.
- Germany was represented by Industrieanlagen-Betriebsgesellschaft mbH (IABG), which participated with the capability RuDi-OpenCOP.
- Norway was represented by FFI with the SecSOA capability.
- The US was represented by Tactical Infrastructure Enterprise Services Coalition Warfare Program (TIES CWP), which was one of the main test partners in the data format testing.
- Finland had two capabilities participating in the SOA focus area, FIN-LION and FINACCIS3 SOA.
- France participated with two capabilities: JACENT Tactical Infrastructure Enterprise Services (JACENT-TIES) and Business- Systéme d´Information des Armées (Business-SIA).
- Poland participated in the SOA focus area tests as a part of their larger national Polish Mission Network (PMN) capability.

In addition to the partners listed here, a few capabilities from other focus areas took part in a few of the SOA focus area test cases, but none of these partnered with FFI for our test cases.

2 Request/Response Messaging

These tests were included to validate information exchange aspects of the messaging core service (namely the request/response communication pattern). As such, these tests included only unsecured clients and services, since the focus was on the exchange mechanism itself. In order to test the exchange mechanism, one needs something to exchange. From the point of view of the SOA focus area, the actual data being transmitted is of little importance as we aim to validate the middleware functionality. Hence, the Service Interoperability Profile 3 (SIP3) protocol with NIEM data was chosen for these tests as several test partners could support this.

2.1 Technical background

In order to fully understand the contents of the request/response test series at CWIX, the reader needs to have a basic understanding of what SIP3 and NIEM are. These two constructs are discussed further below.

2.1.1 SIP3

SIP3 is a container format for blue force tracking data. It originated along with the NATO Friendly Force Information (NFFI) format, and up to and including SIP3 v1.1 it was tightly coupled with NFFI. Version 1.1 described how a client should access the NFFI service, and provided constructs for compressing the data to reduce communication overhead, as well as filtering opportunities to better control the actual data transmitted (e.g., time filters to avoid old messages and geographical filters to limit information exchange to the area of interest). This protocol turned out to be very useful in practice, so much in fact that the NCIA decided to decouple NFFI from SIP3 starting with the most recent SIP3 v1.2. The generalization in version 1.2 implies that any XML-based data format can be exchanged with the protocol. This was the approach taken in the SOA focus area for CWIX, as we used SIP3 v1.2 with NIEM as the data format.

2.1.2 NIEM

NIEM is USA's national XML-based model for expressing all data modeling needs of the U.S. Government. It has been used for years in the USA, with the Department of Defense being among the last to adopt the model. USA now has a nation-wide approach to data modeling which implies that they should always consider using NIEM for any data modeling task, and other options can be used only if NIEM can be proven to be unsuitable for the task at hand. Hence, it can be seen as a holistic approach to USA's national need for information exchange. NIEM is now a successful and proven approach in USA, and because of this it has also been suggested for use by NATO. Some see NIEM as a contender to and replacement for MIP's JC3IEDM, while others see it as a supplement. In the SOA focus area we did not (and still do not) engage in that debate. We merely chose NIEM as an example data format for testing middleware, as mentioned above.

At CWIX 2015 there were two separate test series involving SIP3 and NIEM. One was called IS1a, the other was called IS1b. IS1a consisted of three NIEM-based message types: Ground unit positions (called "PosRep"), air unit positions (called "AirTrk"), and general observations and their positions (called “ObsPos”). To participate in the tests one had to support SIP3 and at least one of the NIEM-based data formats. Most nations, Norway included, opted for the “PosRep”, which in a broad sense is just NFFI data formatted according to NIEM rules. IS1b was NCIA’s take at combining the three separate messages from IS1a into a single unified message. Implementing and testing IS1b would not shed any new light on the middleware services, so FFI took part only in the IS1a tests using SIP3 with “PosRep” NIEM messages.

2.2 Pre-testing

“COPS”, short for “Common Operational Picture Secured”, is a prototype implementation by students from the Oslo and Akershus University College of Applied Sciences (HiOA) of a front- and backend system implementing basic situational awareness aspects (in short, blue force tracking). The backend supports SIP3 using both NFFI and NIEM PosRep, and our intentions for CWIX 2015 was to leverage the backend in the IS1a tests and the entire system in the SSO tests. COPS is fully documented in FFI note 2015/01306.

ACT arranges a bi-annual venue for the further development of interoperability called Technology for Information, Decision and Execution superiority (TIDE). In spring 2015 TIDE was arranged in Berlin, and FFI participated there with the COPS prototype. There, several flaws were identified in the SIP3 implementation (particularly related to filter handling). The main test partner was NCIA, and the tests were deemed a partial success (see TIDEPEDIA for further details [6]). Following TIDE these issues were resolved in preparation for CWIX.

2.3 CWIX tests

FFI participated in the IS1a tests, which in short encompassed a SIP3/NIEM client and a SIP3/NIEM Web service.

2.3.1 Execution

At CWIX we relied on virtual machines containing all necessary software. For the IS1a tests we started the COPS backend which contained our SIP3/NIEM service. However, as it turned out the NIEM schemas for use in the tests had been updated a couple of weeks before CWIX. COPS implemented an older and incompatible version. Hence, the service we brought could not be used for the tests. Furthermore, we were unable to successfully launch the COPS front-end which would provide access to the NIEM client (see more on COPS issues in Chapter 4 on SSO). Due to the inherent complexity of COPS, we ended up building a stand-alone SIP3/NIEM service and client for the sake of the IS1a tests. The service/client pair was built using standard Java development tools.

2.3.2 Results

All our IS1a tests were successful, both when we acted as a service provider and as a service consumer. Our approach required an online available service definition to work (i.e., the WSDL had to be accessible across the network). Neither FINACCIS3 nor M&S COE provided such an interface, but by using a workaround on our side (i.e., deploying a SIP3/NIEM WSDL using their service endpoint on our Web server and then pointing our client to that description) we could still consume their services. It should be noted that while current specifications and best practices dictate that a WSDL should be made available, there is no requirement that it should be available over HTTP which our framework expected. Hence, employing such a workaround may be necessary for some client software.

When issuing a SIP3 request, the requestor specifies which data format it wants the response message formatted according to. The SIP3 specification says that a request for an unsupported response dialect should be replied to with an error message. Some of the implementations at this year's experiment violated this by returning the requested information using whichever data format the service supported.

An additional observation was that the different implementations of the SIP3/NIEM services in use during testing would respond differently to receiving requests containing an empty filter. Some implementations of the service would respond with their full data set, while others returned an empty response. Neither the SIP3 documentation nor the NIEM IS1a Information Exchange Package Documentation (IEPD) specified what the correct behavior should be. Future versions of the NIEM IS1a IEPD should be expanded to resolve this issue.

3 Publish/Subscribe Messaging

Publish/subscribe is an event-based messaging pattern, where information consumers can subscribe to the information they are interested in, and receive notifications when new information matching their interests becomes available. This messaging pattern has shown great promise for use in military networks, and specifications for how to implement this pattern exist in both the NFIP and the TTB.

3.1 Technical background

In order to better understand the challenges related to the CWIX test series for publish/subscribe a short technology introduction is required. The open standard WS-Notification (WS-N) [7] is the technical basis for both the NFIP and TTB specifications of how to implement publish/subscribe in the NATO federation. These two specifications are similar, but not identical.

3.1.1 Publish/subscribe fundamentals

There are two important features of publish/subscribe systems that have a big impact on how one can realize event-based messaging in a federation, namely the difference between direct and brokered publish/subscribe, and the difference between topic and content-based filtering of information.

The message exchanges in a publish/subscribe system can either be done directly or via one or more intermediaries, called brokers. In the direct message exchange case the information consumer subscribes to a specific information source, and this information source sends its notification directly to each of its subscribers. In the brokered case, however, the information consumer and information source do not communicate directly. Both use the broker as an intermediary, and it is the broker's task to maintain subscription information and to ensure that the correct information is delivered to the recipients. This leads to a very loose coupling between the information source and the information consumer, which in turn generates a number of challenges in a federated scenario.

The second important distinction in publish/subscribe systems, is the difference between topic-based and content-based information filtering. When an information consumer subscribes to some type of information, it needs to somehow specify which type of information it is interested in. This can be done by having the consumer specify a number of categories or information types it wants to receive, and this is then matched against keywords that the information source labels its information with. In publish/subscribe systems the use of such keywords for message filtering is called topic-based publish/subscribe.

The alternative approach to topics is using content-based publish/subscribe. In this case the information is not labeled with keywords/topics, but the filter is instead applied to the message content itself. Topic and content filtering can also be combined, with content filtering then being applied to any information matching the requested topic.

3.1.2 WS-Notification

WS-N is a family of three related standards, namely WS-BaseNotification, WS-BrokeredNotification and WS-Topics. Together these three standards specify how to realize the publish/subscribe messaging pattern for Web services. This standard has been tested for military purposes in several previous experiments, and it has been proven that it is possible to achieve technical interoperability using this standard. There are however a number of open issues related to the use of the standard in different federated topologies.

3.1.3 WS-Nu and the OKSE broker

WS-Nu, documented in full in FFI note 2015/01250, is a standalone implementation of the WS-N standard, and implements both the direct and brokered message exchanges from the standard. The OKSE broker, see FFI note 2015/01325 for details, is an open source implementation of a publish/subscribe federation mechanism capable of translating between the WS-N and the Advanced Message Queuing Protocol (AMQP)[8]. At CWIX 2015 these two implementations were used by FFI to support the transport of NIEM messages using the publish/subscribe messaging pattern.

3.2 CWIX tests

The main purpose of the publish/subscribe testing at CWIX 2015 was to investigate the use of the WS-N standard, using the mesh topology as described in the NFIP. In this topology configuration, each network participant provides one WS-N broker which functions as a WS-N gateway or proxy for all the information sources and consumers in that participant's network.

Note that all publish/subscribe tests were performed with unsecured services, as publish/subscribe security is an unsolved problem that would need to be addressed in the future.

3.2.1 Execution

Norway took part in the publish/subscribe test series using WS-Nu and the OKSE broker as the publish/subscribe system. This enabled us to take part in WS-N tests with the other partners that provided WS-N brokers in their networks. In addition, we were able to test the bridging between the WS-N and AMQP protocols by publishing information internally using AMQP, and translating the notification message to WS-N before sharing it with our partners.

3.2.2 Results

We successfully managed to set up a mesh topology federation of WS-N brokers together with our partners, and we managed to configure the subscriptions in such a way that the information consumers on both sides of the federation received all published information that matched their subscriptions. Configuring a mesh topology in this manner did however reveal some challenges related to brokered publish/subscribe, in particular in scenarios where multiple brokers are involved in the message exchange. Each broker would have a number of information sources using it, but the other brokers in the federation would have no way of knowing which information topics those sources offered. There exists several possible ways of working around this issue, but it remains a challenge to find a solution that works well in a full scale deployed systems. At CWIX 2015 we were able to work around the issue by manually configuring subscriptions between brokers, a solution that works in a small scale test network.

An alternative solution would be to always share all notification between all brokers (which in effect means that all brokers subscribe to all possible information), but this is likely to lead to a high traffic load in the backbone network.

A third solution that was suggested during the experiments was to use the optional publisher registration feature of the WS-N standard to propagate information between brokers, but this solution remains untested. This solution seems promising, but it raises a number of issues that must be resolved before such a solution can be realized. These challenges include the fact that the publisher registration feature of the standards is optional, and may thus not be supported by all implementations. In addition, there are several issues related to the handling of content filters. While publisher registration can be the basis for successfully handling topic filtering in a federation, content filters would still have to either be handled by the original information sources, or broker/consumers would have to be extended with additional logic to handle such filters. A consequence of handling content filters at the brokers would be that the brokers would have to understand the data formats involved in the message exchange. It was agreed that while WS-N is a good technical basis for publish/subscribe in a federation, further experiments and work on the specifications is required to resolve the identified issues.

4 Web Authentication

There is often a need to restrict access to Web resources. Users authenticate themselves before they are granted access to the resource. To eliminate several authentication processes, the SSO scheme is a good solution. The user authenticates once and is given access to potentially several resources for a set time period using a security token.

SSO is applicable in both enterprise systems and in federated systems. The enterprise scenario involves one or more domains where the participants operating are all members of the same enterprise. They all have a direct trust relationship to the entity handling access management. In the federated scenario there are one or more enterprises. They all have a direct trust relationship to the entity handling access management in their enterprise, similar to the enterprise scenario, but a federation is established in a ring of trust between the different enterprises.

4.1 Technical background

At CWIX 2014 (see FFI report 2014/01510) we pursued the enterprise scenario (that is, using direct trust between all identity providers) using a product called OpenAM. At CWIX 2014, WS-Federation was the main SSO protocol being tested, and SAML 2.0 was added as an afterthought. However, in 2014 it became apparent that SAML 2.0 had much better tool support than WS-Federation and, even though only WS-Federation is currently in the NFIP, it was noted that SAML 2.0 should be added. Hence, for CWIX 2015 our goal was to achieve the more complex federated scenario (i.e., transitive trust between involved parties) using the SAML 2.0 protocol.

4.1.1 Federated scenario

In order to support collaboration between nations, a scheme for allowing access to partners' Web resources is important. Traditionally, SSO has relied on browser cookies to store information. The problem with this is that the solution is not applicable in scenarios where resources are located in different Domain Name System (DNS) domains as cookies are not transmitted between them. Instead of using a proprietary mechanism for transmitting the cookies, we use a central service handling the Web authentication and SSO. Participants in this setup are a Security Token Service (STS) responsible for issuing security tokens as part of a claims-based identity system, an Identity Provider (IdP) responsible for authenticating incoming requests, and a Service Provider (SP) responsible for protecting the Web applications.

Figure 4.1 shows the federated scenario where there is more than one enterprise and where the consumer has a direct trust relationship to its own IdP, and where the IdPs themselves form a "ring-of-trust" crossing enterprise borders. This enables the consumer to request and get access to Web resources located in other enterprises and not even noticing any difference between getting access directly from its enterprise IdP.

The consumer requests access to a Web application and is redirected to the IdP, the consumer is authenticated and the IdP requests a token from the appropriate IdP, residing in the "ring-of-trust" in order to grant the consumer access. The token is then used by the consumer to get access to the resource.

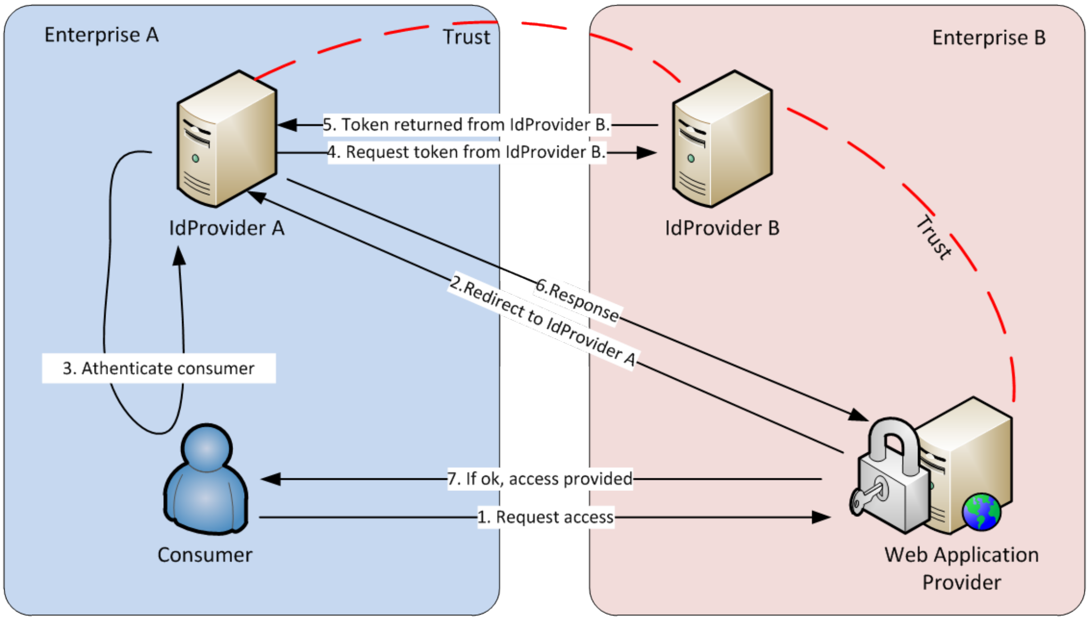

Figure 4.1 Federated scenario

The authentication process results in a security token the consumer can use for a limited time to get access to Web resources residing in other enterprises. In our work we have focused on using SAML tokens for security.

4.1.2 SAML 2.0

In order to achieve SSO in a federated scenario we use the SAML 2.0 tokens to enforce security. SAML is a standard developed and maintained by the Organization for the Advancement of Structured Information Standards (OASIS). The tokens are assertions added to communications expressing trustworthy security information that works across different DNS domains. The standard defines how to create, request, communicate, and use these SAML assertions.

The tokens are described in a technical overview in [9]. The overview lists several profiles, and the Web Browser SSO Profile describes how to achieve SSO in a standard Web browser.

4.1.3 OpenAM

At CWIX 2015 we used OpenAM 11.0.2. It is a product that was developed many years ago by Sun for authentication, authorization, and federation. At the time it was called OpenSSO and was an open source product. When Sun was acquired by Oracle, the company Forgerock created a branch of the OpenSSO source code and rebranded it as “OpenAM”. Since then, Forgerock has continued to develop the solution, but has turned its focus on multi-protocol SSO support. Hence, OpenAM [10] is an access management system with several possibilities in how authentication is performed. In our setup we enable SSO using SAML2.0 tokens.

Using OpenAM to support the federated scenario proved difficult as the software did not work as well as we hoped. To enable the use of several IdPs, we had to incorporate an IdP Proxy allowing the user to choose the appropriate IdP. In Figure 4.2 the OpenAM solution is shown, where the IdP Proxy is an additional point of complexity and a potential single point of failure.

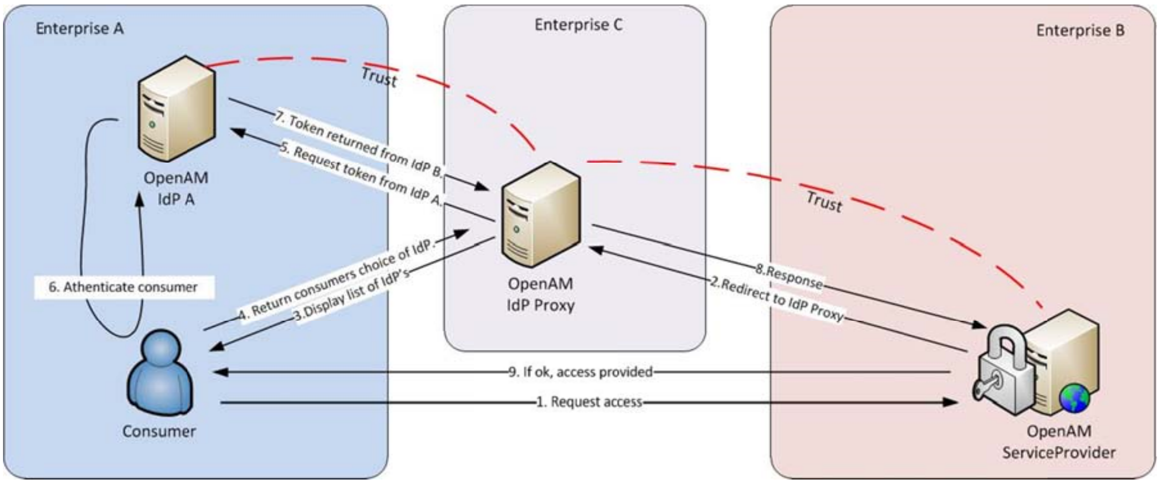

Figure 4.2 Federated scenario using the OpenAM IdP Proxy

Another point worth noting about OpenAM is that the STS functionality is hidden within the product, so only the IdP is exposed. This functions well for achieving SSO, but it means that since the STS is not exposed as a Web service we cannot use OpenAM as a component in achieving Web services security. As a consequence, we did not attempt to participate in the WSS tests this year. The product used to include a proprietary workaround for WSS called Web services agents back when it was owned by Sun, but these are now outdated and seemingly not being maintained anymore by Forgerock.

4.2 Pre-testing

As part of our preparations we arranged a two-day testing workshop at the NCIA where the aim was to achieve the federated scenario between our OpenAM installation and their Active Directory Federation Services (ADFS) 3.0 installation. For the complete results and recommendations following pre-testing, see the FFI travel report 2014/02302. In summary, our most important findings were: 1) When attempting to configure the software in a federation, the first issue we encountered was that ADFS refused to be configured towards using our IdP since it was running on http and not https. Hence, we had to set up https on our IdP. 2) Once https was in place we were able to configure the federation. At this point it was discovered that our certificate (we used the same for both the IdP and the https connection) had 1024 bits, but the NCIA recommended 2048. Thus, we created a new certificate with the appropriate number of bits before starting our tests. At this point the tests were successful one way, that is, using our IdP to authenticate our user and then use that identity for invoking the NCIA Web application. 3) Tests the other way around, i.e., using NCIA's IdP to authenticate and invoke FFI's application were unsuccessful. This issue was not resolved during the workshop, so we focused on elaborate tests with our IdP and NCIA's application. Thus, looking into how to properly get the entire federation going was top priority for follow-up work. The work performed on our side following the workshop, along with the complete description of our OpenAM configuration as it was deployed prior to going to CWIX, is available in FFI note 2015/01328.

4.3 CWIX tests

At CWIX 2015 the SSO tests related to the above mentioned enterprise scenario were cancelled. The reason for this was that the enterprise scenario was not deemed a realistic use case in a NATO federation. Hence, this year's CWIX had two main SSO test cases for the federated scenario: One using the WS-Federation protocol, the other using the SAML 2.0 protocol.

4.3.1 Execution

Norway took part in the SAML 2.0 federated scenario tests. Here, our goal was to both consume our partners' secure services (i.e., access their secured applications) as well as provide our own secure application for our partners to use. Regarding the latter part of the test case, that is, us providing a secure application, we ran into deployment issues. Our aim was to use the previously mentioned COPS frontend as our secure application. However, for reasons unknown, the software did not transition well from our lab and into deployment at CWIX. Thus, we spent a considerable amount of time attempting to recompile the software and redeploy it in the CWIX test arena, since our virtual machine did not work properly after being moved. We managed to get the COPS backend going, which basically was the data store being used for visualization by the frontend. However, the frontend posed a series of problems: First, it was inaccessible and exhibited erratic behavior through the default browser which was Firefox. We managed to work around this by switching to Chrome, and in addition manually providing a user location in the browser. Without such a location set (or location services enabled and an active Internet connection available) the COPS frontend does not work. However, further issues arose following this as well causing us to abandon COPS after a few fruitless days of debugging. We obtained OIOSAML instead [11] and deployed its demo application in our Tomcat application server.

4.3.2 Results

Our main test partners were ACT and NCIA. We were successful in accessing both ACT and NCIA's secure applications. Hence, we successfully achieved federation using SAML 2.0 between our OpenAM IdP and their WSO2 5.0- and ADFS 3.0-protected applications, respectively. The other way around, Norway providing a secure application, was unsuccessful. This was due to a couple of things; first, that the application we had set up prior to departure didn't work anymore at CWIX, and that we were unable to get OpenAM to forward the appropriate attributes from its proxy instance to our deployed OIOSAML replacement application. The latter meant that even though a request made its way all the way from a partner to our SAML 2.0 proxy and onwards to the application, the request did not contain the proper attributes in the final hop of this communication. So, for all intents and purposes OIOSAML denied the requester access since the proper attributes were missing. We were unable to resolve this issue during the timespan of CWIX.

In general, though, the SAML 2.0 tests were overall more successful for the participants than the WS-Federation tests were. This led to the NCIA making a note of a recommendation that WS-Federation should be removed from the NFIP in the next spiral and be replaced by SAML 2.0.

5 Summary

Below we summarize the most important findings from the three major test series FFI participated in at CWIX 2015, along with our overall observations regarding this experimentally inclined venue.

5.1 Main findings

All the test series performed by the SOA focus area at CWIX this year have generated valuable input both for the further development of the NATO FMN and TTB specifications, and for ensuring that national systems are interoperable with the systems of partner nations.

The request/response messaging tests were successfully completed by all the partners that took part in the testing of this specification. There were some minor issues when using SIP3 as a container for NIEM data, but these are easily rectified with better documentation. Additionally, the partners that were interested in the NIEM data format captured some lessons learned for later iterations of their IEPDs.

The publish/subscribe tests using WS-N showed that the standard can be used to achieve technical interoperability between partners. Some important issues with respect to how the standard should be deployed in a federation were identified, and a proposal was made for this to be tested further both during the TIDE mini-sprint events and during CWIX next year.

As for the Web authentication test series, the experiment results confirmed the initial finding from last year, which indicated that SAML 2.0 is better suited as a federation SSO protocol than WS-Federation. A change proposal for the NFIP specification on this topic will be forthcoming.

Furthermore, we gained additional experience with OpenAM as a framework. As continued use of OpenAM for SSO would require a second framework for supporting WSS anyway, we will look into changing it for a different framework for future experiments. The limitations we uncovered, in addition to the fact that licensing for OpenAM is prohibitively expensive, further supports this decision.

5.2 CWIX as a test arena

In general this year's CWIX was a success because 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 future iterations of the NFIP. Important partner nations participate with their domain experts, which often leads to rapid development and achieving interoperability faster than you would normally be able to. For FFI it was especially positive that so many nations were participating in the SOA focus area.

We aim to further contribute to the development and refinement of core service specifications, particularly through the important venues TIDE (creating and updating specifications) and CWIX (validating said specifications). In light of this, we should focus especially on further developments within publish/subscribe and security. Here, we should aim to be active test partners providing WS-Notification services and also secure Web services (WSS test series) at CWIX 2016.

6 Abbreviations

ACT	Allied Command Transformation
ADFS	Active Directory Federation Services
AMQP	Advanced Message Queuing Protocol
CIS COP	Communication Information System Common Operational Picture
COP	Common Operational Picture
CWIX	Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise
FMN	Federated Mission Networking
IABG	Industrieanlagen-Betriebsgesellschaft mbH
IdP	Identity Provider
IEPD	Information Exchange Package Documentation
M&S CoE	Modeling and Simulation Center of Excellence
NCES	Net-Centric Enterprise Services
NCIA	NATO Communication and Information Agency
NFFI	NATO Friendly Force Information
NFIP	NATO FMN Implementation Plan
NIEM	National Information Exchange Model
NMBS	NATO Metadata Binding Service
NNEC	NATO Network Enabled Capability
OASIS	Organization for the Advancement of Structured Information Standards
PKI	Public Key Infrastructure
PMN	Polish Mission Network
SAML	Security Assertion Markup Language
SIA	Systéme d´Information des Armées
SIP3	Service Interoperability Profile 3
SMC	Service management and control
SOA	Service Oriented Architecture
SP	Service Provider
SSO	Single Sign-On
STANAG	Standardization Agreement
STS	Security Token Service

TIDE	Tactical Information Data Exchange
TIES	Tactical Infrastructure Enterprise Services
TIES CWP	Tactical Infrastructure Enterprise Services Coalition Warfare Program
TTB	TIDE Transformational Baseline
WSS	Web Service Security

References

[1] C4ISR Technology & Human Factors (THF) Branch, Allied Command Transformation (ACT), *The C3 Classification Taxonomy*, Technical report, 2012. Document generated from the ACT Enterprise Mapping Wiki on November 2012

[2] The Web Services-Interoperability Organization (WS-I), *Basic Profile Version 2.0* , November 2010. Available at http://ws-i.org/profiles/basicprofile-2.0-2010-11-09.html

[3] *NATO FMN Implementation Plan v3.0*, approved by the NATO Military Committee August 6th, 2014

[4] NATO ACT, *TIDE Transformational Baseline 4.0*, available at https://tide.act.nato.int/tidepedia/index.php/TIDE_Transformational_Baseline_v4.0 (requires an account)

[5] National Security Agency/ Defense Information Systems Agency, *Net-Centric Enterprise Services (NCES) Profile of Web Service Security: Simple Object Access Protocol (SOAP)Message Security (WSSE)*, May 2008

[6] TIDEPEDIA (requires an account), Berlin mini-Sprint request/response testing results. https://tide.act.nato.int/tidepedia/index.php?title=TIDE_mini-Sprint_%2822-24_Apr_2015%29_-_NFFI_and_NIEM_Data_Exchange_Testing

[7] OASIS, Web services Notification TC, http://www.oasisopen.org/committees/tc_home.php?wg_abbrev=wsn

[8] Oasis, “Advanced Message Queuing Protocol (AMQP) Version 1.0“, 29 October 2012

[9] OASIS, Security Assertion Markup Language(SAML) V2.0 Technical Overview, Committee Draft 02, 25 March 2008, http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0-cd-02.pdf

[10] Forgerock, OpenAM, http://forgerock.com/products/open-identity-stack/openam/

[11] OIOSAML. A Servlet-compliant SAML Service Provider for use in a SAML federation. https://svn.softwareborsen.dk/oiosaml.java/sp/trunk/docs/intro.html