FFI-rapport 2014/01510

CWIX 2014 core enterprise services experimentation

Trude H. Bloebaum and Frank T. Johnsen

FFI Forsvarets forskningsinstitutt

CWIX 2014 core enterprise services experimentation

Trude H. Bloebaum and Frank T. Johnsen

Norwegian Defence Research Establishment (FFI)

14 November 2014

FFI-rapport 2014/01510

1277

P: ISBN 978-82-464-2460-6
E: ISBN 978-82-464-2461-3

Keywords

CWIX

Eksperimentering

Tjenesteorientert arkitektur

Kjernetjenester

Approved by

Rolf Rasmussen	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 2014. FFI participated in a subset of these experiments, as a preparation for a larger experiment planned for CWIX 2015. This report gives a brief overview of the full set of SOA-related experimentation at CWIX 2014, with particular focus on the experiment series 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 because they form the basis for the planned activities for CWIX 2015, where FFI plans to participate in a broader set of experiments.

At CWIX 2014, FFI collaborated with 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; one related to the publish/subscribe core enterprise service (CES), and one related to the security CES. For the latter 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 specification for NATO FMN Implementation Plan (NFIP) Appendix S-10, which deals with subscription services. In addition, the tests were used as a basis for developing joining instructions for this CES. FFI participated with NATO Friendly Force Information (NFFI) as the test application for the publish/subscribe CES. However, there is currently a drive in NATO towards new, improved information exchange formats. Thus, for next CWIX, FFI plans to participate with a selection of the next generation of NATO-specifications for blue force tracking (BFT) and Common Operational Picture (COP)-exchange.

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, our experiments showed that the tooling support for WS-Federation was inadequate. A competing specification, SAML 2.0, offers similar functionality. For that standard tooling support is better, and several experiments using this solution were completed successfully. As a consequence, a proposal was made that there is a need to include SAML 2.0 in the NFIP. This result illustrates how important it is to participate actively in experimentally oriented venues for interoperability testing, such as CWIX. Thus, FFI wants to further develop and test SOA security solutions at CWIX next year as well.

In retrospect this year's CWIX was very successful. We were able to test aspects of two different CES, 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 we have a desire to participate at CWIX also in 2015.

Sammendrag

Denne rapporten dekker eksperimentene som ble gjennomført av deltagerne innen fokusområdet for tjenesteorienterte arkitekturer (SOA) under CWIX 2014, 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 utgjør grunnlaget for aktivitetene på CWIX 2015, der FFI planlegger å delta i et større antall tester.

På CWIX 2014 samarbeidet FFI med 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; én knyttet til kjernetjenesten (CES) for abonnementstjenester (publish/subscribe), og én relatert til kjernetjenesten for sikkerhet. For sistnevnte fokuserte vi hovedsakelig på aspekter ved føderterte identiteter.

NATO har valgt standarden WS-Notification for abonnementstjenester, og FFI deltok i eksperimenter for å verifisere NATO FMN implementeringsplan (NFIP) Vedlegg S-10, som omhandler med abonnementstjenesten. Disse testene ble også brukt som grunnlag for å utvikle instruksjoner for hvordan man skal sette opp en slik tjeneste i FMN. FFI deltok med NATO Friendly Force informasjon (NFFI) som testapplikasjon for abonnementstjenesten. For tiden er det et driv i NATO mot nye, forbedrede informasjonsutvekslingsformater. Ved neste CWIX planlegger FFI derfor å delta med et utvalg av den neste generasjonen av NATO-spesifikasjoner for blåprikk (BFT) og situasjonsbilde (COP)-utveksling.

En av de viktigste ideene i FMN er at en 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. Våre eksperimenter viste at verktøystøtten for WS-Federation generelt var mangelfull. Videre fant vi at den konkurrerende spesifikasjonen - SAML 2.0 - som tilbyr tilsvarende funksjonalitet var bedre støttet i verktøyene. Dermed ble relativt sett mange flere eksperimenter som benyttet denne løsningen fullført. Dette vakte stor oppsikt i SOA-fokusområdet, og bunnet ut i et forslag om at det er nødvendig å inkludere SAML 2.0 i kommende versjoner av NFIP. Dette ble avdekket gjennom eksperimentering, og viser hvor viktig det er å delta aktivt i en slik løsningsorientert arena som CWIX er. Naturlig nok ønsker FFI å gjenta suksessen og teste SOA sikkerhetsløsninger på CWIX neste år også.

Avslutningsvis vil vi understreke at vi mener årets CWIX var svært vellykket: Vi var i stand til å teste aspekter ved to ulike CES, 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 vi planlegger å delta på CWIX også i 2015.

Contents

1 Introduction

The NATO Coalition Warrior Interoperability eXperiment (CWIX) is an annual NATO Military Committee approved event designed to bring about continuous improvement in interoperability for the NATO alliance. The NATO CWIX program focuses primarily on testing and improving the interoperability of NATO and national Command and Control (C2) systems. In addition to bilateral technical testing, NATO CWIX provides a venue to conduct technical testing of fielded, developmental and experimental systems in the context of a coalition scenario.

This document describes the experiments conducted by the participants in the Service-Oriented Architecture (SOA) Focus Area at CWIX 2014. FFI participated in a subset of these experiments, as a preparation for a larger experiment planned for CWIX 2015. This report gives a brief overview of the full set of SOA-related experimentation at CWIX 2014, with particular focus on the experiment series 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 also included because they form the basis for the planned activities for CWIX 2015, where FFI plans to participate in a broader set of experiments.

At CWIX 2014, FFI collaborated with the NATO Communications 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. FFIs research into SOA deployment focuses on standards and interoperability profiles that can be building blocks in establishing an interoperable and end-to-end information infrastructure. The establishment of such an infrastructure is an area of priority to the Norwegian Armed Forces. Our focus was to collaborate with NCIA and partner nations in the SOA Focus Area, where the main goal was development and verification of FMN-related interoperability specifications for central infrastructure services. In particular we participated in two experiment series; one related to publish/subscribe, and one related to security. For the latter we mainly focused on issues related to federated identities.

The remainder of this document is organized as follows: In Section 2 we discuss the technical background for our experiments. Section 3 covers preparations and pre-testing leading up to our CWIX participation. The actual experiment series and results from CWIX are summarized in Section 4, whereas Section 5 concludes the report.

2 Technical background

The core concept of NATO Network Enabled Capabilities (NNEC) is seamless information exchange between different components in the military structure and even civilian organizations. In other words, information should be provided in a timely fashion to those who are best situated to use it. In addition, the concept of ad-hoc organization is highlighted as another key attribute of NNEC. This should provide a more agile organization capable of reducing time needed for planning and deployment.

FMN builds on the findings and experiences from the NNEC effort, and relies on many of the same concepts and technologies. SOA is a principle that has proved promising for providing the flexibility needed both under the NNEC concept, and for FMN.

From the "Reference Model for Service Oriented Architecture" [4] we can define SOA as "*an architecture for making resources available in a way that they may be found and utilized by parties who don't need to be aware of them in advance*". In this section we explore SOA concepts and selected services that are relevant for both FMN and for our CWIX participation.

2.1 Core Enterprise Services (CES)

In order to realize network enabled capabilities, interoperability is a main concern. Interconnecting heterogeneous systems, both legacy and new systems, implies a transition from stove-pipe systems with little focus on information sharing, to systems with standardized interfaces and data formats. As a consequence, the SOA paradigm has become a key factor and an important initiative both in NATO and nationally. SOA helps making processes interoperable, and enables a much easier exchange of information. The foundation for a common situational awareness is increased information sharing, and this requires a strategy for making information visible, available, accessible, and understandable.

NATO Core Enterprise Services (CES) [3] are defined as "*technical services that facilitate other service and data providers to deliver content and value to end users. They can be thought of as the enablers used by other services [...] They are independent of business process and context, and are ubiquitous.*"

CES encompass many different functionality aspects. At CWIX 2014 FFI mainly focused on two: publish/subscribe and security.

2.2 Publish/Subscribe

Publish/subscribe is a well-known communication pattern for event-driven, asynchronous communication. The pattern is particularly well suited in situations where information is produced at irregular intervals. Simply speaking, publish/subscribe means that you will only receive the information that you have subscribed to. This concept utilizes a combination of push and pull. As opposed to a general push mechanism there are benefits in that you may select

(subscribe) to the information sent to you, and when using pure pull principles you are not able to notify listeners when events occur.

WS-Notification [5] is an OASIS standard defining publish/subscribe for Web services. It is the standard chosen by NATO for implementing the publish/subscribe CES. There are three parts in the specification:

WS-BaseNotification[6], which defines standard message exchanges that allow one service to subscribe and unsubscribe to another, and to receive notification messages from that service.

WS-BrokeredNotification [7] defines the interface for notification intermediaries. A notification broker is an intermediary that decouples the publishers of notification messages from the consumers of those messages; among other things, this allows publication of messages through a chain of proxies.

The WS-Topics specification [8] defines topic–based filtering using an XML model to organize and categorize classes of events into "Topics". It enables users of WS-BaseNotification or WS-BrokeredNotification to specify the types of events in which they are interested. In summary, the specifications standardize the syntax and semantics of the message exchanges that establish and manage subscriptions and the message exchanges that distribute information to subscribers.

2.3 Security

Security encompasses a plethora of standards and functional aspects. Here we present the subset relevant for the web authentication testing at CWIX 2014, i.e., the WS-Federation and SAML 2.0 standards as well as the intended use related to federated identities, the so-called enterprise and federated scenarios.

2.3.1 WS-Federation and SAML 2.0

The Security Assertion Markup Language (SAML) [9] and Web Services Federation (WS-Federation) [10] protocols are very similar but also incompatible. SAML and WS-Federation both allow users that have already logged into one application to access another application without logging in again, so-called single-sign on (SSO). Both standards achieve this by allowing clients to present proof that the users are who they say they are. They both support single sign-out and they both support metadata to exchange SSO information between parties. Further, both standards support building large, complex federations involving different domains in a sophisticated web of trust. One of the most used features of either standard is the set of "passive" features that allows SSO between web sites. The FMN Web Authentication specification uses this feature of WS-Federation to protect Web Applications. Both standards also support securing SOAP Web services through an "active" feature set.

WS-Federation is primarily a Microsoft initiative. SAML is an older specification that is well supported by many different identity management vendors. Today many vendors, including

Microsoft, are moving towards supporting both standards. For example, Microsoft's Active Directory Federation Services (ADFS) come with support for both WS-Federation and SAML.

Both standards leverage SAML security tokens to carry credentials, but there ends their similarity. The protocols are inherently incompatible otherwise. That being said, either standard can be employed in order to implement the different scenarios below, but then you would implement a scenario using either WS-Federation or SAML, you cannot easily interconnect the two without some additional software to perform the bridging.

Central terms include federation, security token service, and identity provider:

- A federation is a collection of realms/domains that have established trust. Federated systems can interoperate across organizational and technical boundaries.
- A Security Token Service (STS) is a Web service that issues security tokens. An STS makes assertions based on evidence that it trusts, which in turn can be provided as proof to whoever trusts the STS. Commonly, these assertions are SAML tokens.
- An Identity Provider (IdP) is an entity that acts as an authentication service to end requestors. It can be a separate service, or an extension of a basic STS.

2.3.2 Enterprise scenario

Web Authentication relies on the establishment of trust between the provider of the web application and the IdP. This trust can be established either directly or indirectly. When the trust is established directly, the provider hosting the application directly trusts the IdP. This direct trust relationship is what we call the enterprise scenario, as it represents a common way of establishing trust between entities belonging to the same enterprise, as shown in Figure 2.1. In this scenario all the entities involved in the authentication belong to the same administrative domain, and are likely to be owned by the same enterprise. This fact makes it feasible to use such a set-up, since one enterprise is likely to have one IdP serving the entire enterprise. In addition, the enterprise is likely to implement the same security policies throughout their infrastructure, making the administrative overhead of an enterprise scenario set-up manageable.

In the enterprise scenario trust is established initially when the system is set up, either by manually distributing and configuring certificates, or by leveraging a public key infrastructure (PKI). Regardless of the method chosen, trust is cryptographically ensured in subsequent use of the system by verifying digital signatures submitted with access requests.

Let us explore what happens when a consumer attempts to access a protected resource (we assume access is made to a web application, i.e., using the so-called passive mode). First, the consumer in domain A requests access to a resource, e.g., a web application, also in domain A. The server providing the application, the so-called *relying party*, inspects the incoming request and finds that it is lacking an appropriate security token (i.e., a SAML token). At this point, the request redirects the consumer back to domain A's IdP. Now the consumer needs to be authenticated, e.g., present a username/password to the IdP. At this point the user is authenticated

to the IdP of domain A, and a security token is generated (by the corresponding STS) and the consumer's request is redirected back to the web application provider. At this point the application provider can verify that the submitted token is valid, and that the claims[1] it represents show that the user is authorized to access this resource. Given proper authorization, access is granted to the resource. Otherwise access is denied.

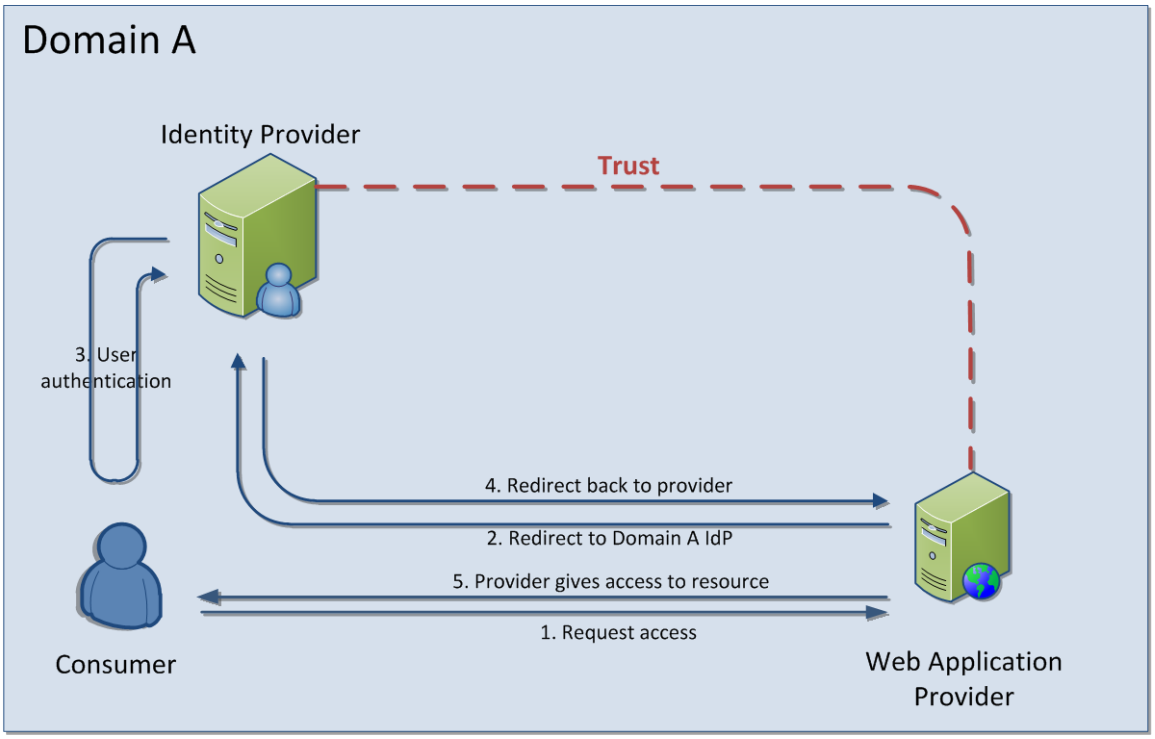

Figure 2.1 Enterprise scenario within one domain

The enterprise scenario is most commonly used within one security domain, but the same configuration of the trust relationship can also be used across domain borders, as illustrated in Figure 2.2. While this set-up is possible, it has a few shortcomings. The message exchanges after trust has been established are the same as when this configuration is used within a single domain. However, since the involved entities are now in different domains, a number of these messages must cross domain boundaries, and thus become subject to any cross-domain communication policies that might be in place.

In addition, using the enterprise scenario set-up for a Web Application Provider that needs to handle requests originating from multiple different domains leads to additional overhead for that provider. The provider will have to have a direct trust relationship with the IdP from each partner domain, and it needs to be able to determine which partner's IdP to re-direct to for each consumer. The issue of determining which domain a consumer belongs to, often called *home realm discovery*, is not unique to the enterprise scenario. It arises whenever multiple trust

[1] You can use claims to implement role-based access control (RBAC). Roles are claims, but claims can contain more information than just role membership. So, claims-based security is a more fine-grained mechanism than RBAC. For an introduction to claims-based identity and access control, see [11].

relationships exist and an entity needs to perform a redirect to an IdP. What is unique to the enterprise scenario is that each individual Web Application Provider needs to be able to handle this issue, rather than being able to delegate the handling of home realm discovery to a third party.

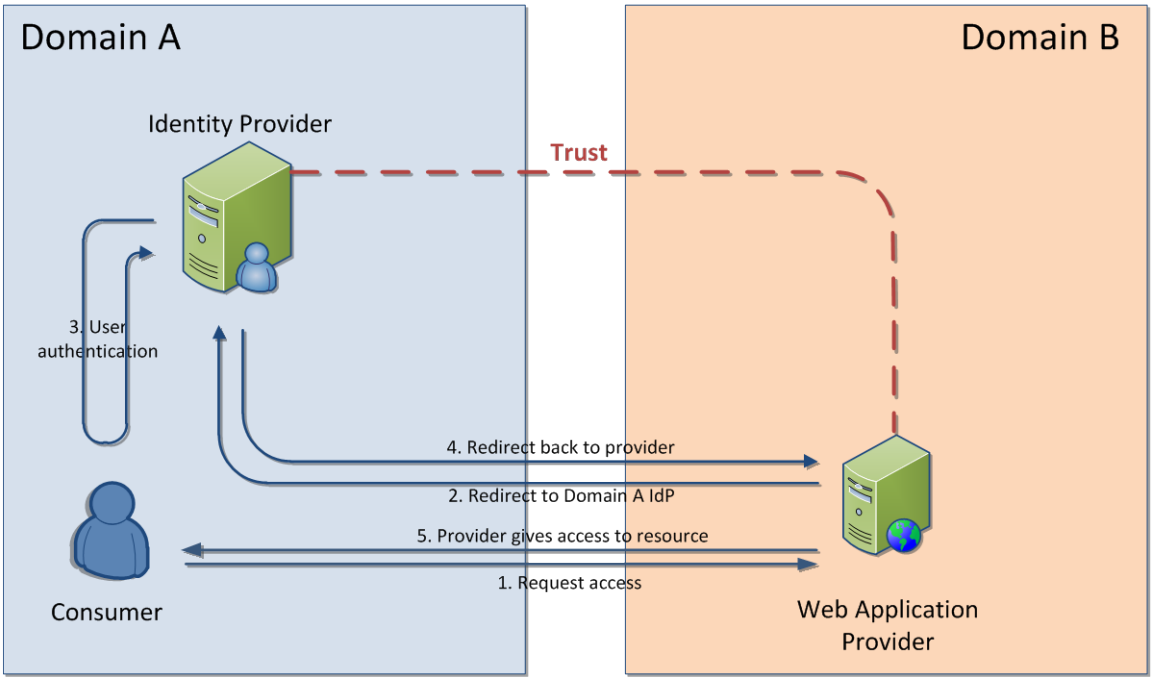

Figure 2.2 Enterprise scenario involving two domains

2.3.3 Federated scenario

The indirect establishment of trust is technically more challenging that the enterprise scenario. In this case the web application provider trusts an IdP in its own domain, and trust to other domains is established by this local IdP trusting the IdPs in the partner domain, as shown in Figure 2.3. This approach, which we call the federated scenario, is preferable to the enterprise scenario when multiple domains are involved as it leads to less administrative overhead. There is less configuration involved in setting up the transitive trust relationships, rather than configuring direct trust between all involved parties.

Here, trust is established directly between consumers and their corresponding IdPs, and directly between the IdPs (i.e., STSes) of the two domains. Finally, trust is established between the application provider and the IdP (i.e., STS) in its own domain.

We have two domains, A and B. Let us explore what happens when a consumer from domain A attempts to access a protected web application in domain B (using passive mode). First, the consumer in domain A requests access to the web application in domain B. The relying party inspects the incoming request and finds that it is lacking an appropriate security token. Now, the request redirects the consumer back to domain A's IdP, because the consumer needs to go through the authentication process. At this point the user is authenticated to the IdP of domain A,

and a security token is generated (by domain A's STS). This token is sent to the STS in domain B, which, because it trusts the STS in domain A, issues a token valid in domain B based on information from the domain A token. Finally, the consumer's request is redirected back to the web application provider. At this point the application provider can verify that the submitted token indeed originates from domain B. Further, it can check whether the claims the token represents prove that the user is authorized to access the resource, and grant or deny access accordingly.

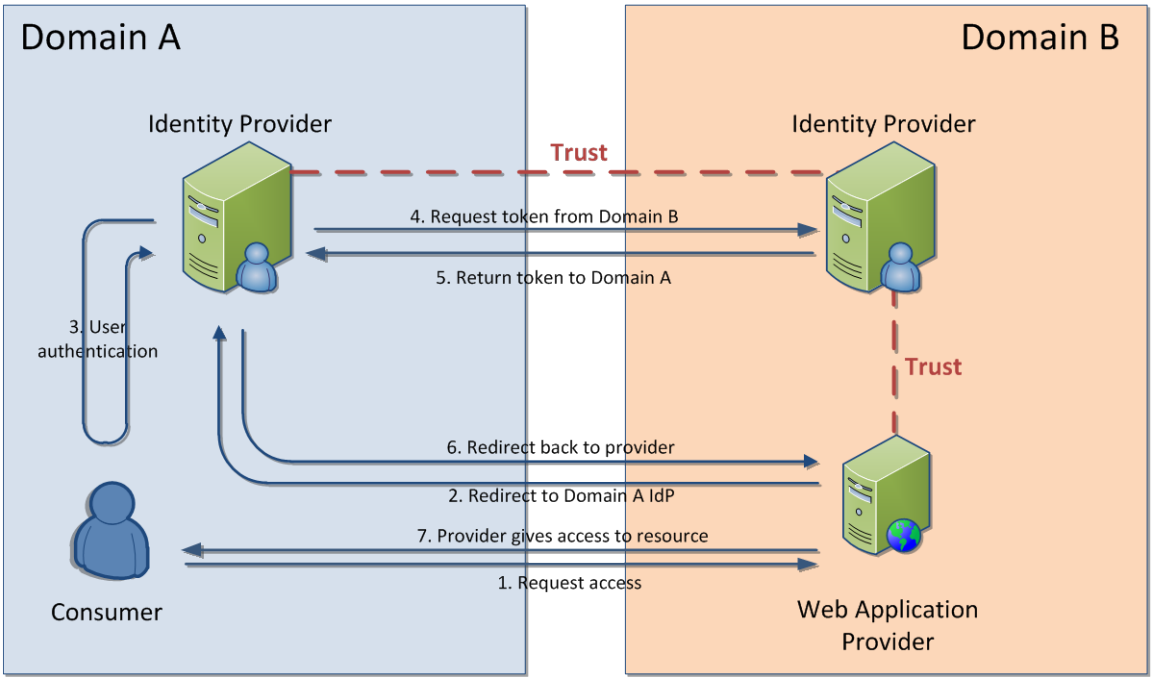

Figure 2.3 Federated scenario

3 Pre-testing

CWIX trials are intended to follow a tight, pre-planned schedule. Thus, pre-testing of software performed prior to actual participation with the aim of ironing out bugs in the software is advisable, as it ensures that one can make the most of the time for actual testing allotted at CWIX. In this section we present our pre-testing efforts.

3.1 Pre-testing at TIDE Sprint, Madrid, Spain

The Technology for Information, Decision and Execution Superiority (TIDE) is Allied Command Transformation (ACT)'s think-tank for information, decision and execution superiority in conjunction with its program of work regarding C4ISR, technology, and human factors. TIDE Sprints are arranged twice a year, with the spring event usually being hosted in Europe, and the autumn event being hosted in Virginia Beach, USA. The TIDE Sprints have a dual focus; they are both a venue for hands-on experimentation and a symposium where topics such as BFT and SOA are discussed. The TIDE Sprints have no formal mandate within NATO, but they have emerged as a venue with short turnover regarding experimentation and fielding of new ideas, as well as finalizing and recommending new specifications through the so-called TIDE Transformational Baseline. Recently the TIDE community has been focusing increasingly on FMN, and the TIDE Sprints are emerging as a potential venue for validating FMN specifications. In this respect the TIDE community and participating in TIDE Sprints can be beneficial for FFI as well.

The 2014 autumn TIDE Sprint was arranged from 31 March to 4 April 2014 at Hotel Husa Charmatin, Calle de Agustín de Foxá, 28036 Madrid, Spain. FFI participated at the event focusing on CWIX pre-testing. There, our main partner was Poland, since we had already started planning with them through our joint participation in the NATO CSO/IST-118 group "SOA recommendations for disadvantaged grids in the tactical domain". Both FFI and Poland showed up with a solution based on what turned out to be the exact same open source framework, i.e., Apache Fediz version 1.1.0. Apache Fediz implements the WS-Federation standard, which is specified in the NATO FMN Implementation Plan (NFIP) [2] for use in securing web applications.

During the three days of experimentation at the TIDE Sprint we got quite far along the way testing with Poland, successfully invoking their service while using an identity provided by the FFI domain (i.e., the federated scenario). We focused on the federated scenario, since Fediz comes "out of the box" configured as a demo pre-configured with two realms (REALMA and REALMB) set up in an enterprise scenario (i.e., with direct trust between the two STSes). During our testing we discovered that several parameters that needed to be configured in Fediz (related to realms, to name one example) were not configurable through the supplied configuration files but actually had to be changed in the actual code. This was very time consuming to remedy, and we did not achieve this fully at this event. Hence, we continued working on this in our lab at FFI later, before bringing the software to the next test venue described below.

3.2 Pre-testing workshop at NCIA, The Hague, Netherlands

The NFIP is published by ACT, and the NCIA in The Hague have contributed to writing many of the technical FMN specifications. Therefore, the NCIA can be seen as the authoritative source regarding these specifications and their validation, making them a much sought-after partner for testing. FFI joined the NCIA for an FFI-funded two day workshop in May 2014 for CWIX pre-testing at NCIA's facilities in The Hague, Netherlands. There, we tested our Fediz-based software with what can be considered the main WS-Federation reference implementation (i.e., Microsoft's ADFS v2.0). Yet again we focused on the most advanced of the two scenarios; the federated scenario. The outcome of the workshop was that we discovered that Fediz, unlike other Apache projects, was very immature. Our tests using NCIA's ADFS solution and our Fediz solution showed poor usability and lacking standards compliancy on Fediz's part.

Following the workshop our test partner advised against continued use of Fediz due to the numerous problems we encountered, and suggested that we should instead look into a different open source solution for CWIX. We considered different options, and found that of the true open source and freely available frameworks that also seemed to be in use in practice OpenAM seemed to be a viable alternative to Fediz, as it claimed support for major standards like WS-Federation, WS-Trust, and SAML 2.0. Based on the advice from the NCIA we chose to abandon Fediz at this point and opt for OpenAM 11.0 instead. This meant, however, that due to this course of action we went to CWIX with a largely new and untested system on our part. This did lead to some difficulties, as we discuss further below. In retrospect, though, we think the advice was sound and are glad that we changed frameworks.

4 CWIX 2014

CWIX is a very large experimentation arena, and because of this, testing is logically organized by dividing the experimentation into *Focus Areas*. In the planning stages for CWIX participation, these Focus Areas form a venue where interested parties within a topic area can meet and discuss potential experiment collaboration and further plan their CWIX participation. During the main CWIX experiments, known as CWIX Execution, the Focus Areas have their own physical space were test partners can be co-located outside their national areas. These areas are venues not only for experiments and discussions, but also for informing interested visitors about the activities conducted within that Focus Area. Examples of such Focus Areas are the Friendly Force Tracking (FFT) Focus Area, the Cyber Focus Area and the SOA Focus Area.

When participating at CWIX, each partner nation has a National Lead, which is responsible for managing and coordinating the nation's participation at the event. The nation's participation is further divided into *capabilities*, where each capability handles its own experiment participation (such as establishing test partnerships, test case management and experiment scheduling). During CWIX 2014 Norway, led by National Lead Maj Leif Oskar Kjellgren, participated with four capabilities. One of these capabilities, named SecSOA, consisted of researchers from FFI that were participating in the SOA Focus Area experimentation. This report covers the SecSOA effort at CWIX 2014.

The SOA Focus Area conducted a number of tests focusing on three main topics, namely *Information Sharing*, *Federated Identity and Access Management*, and *Messaging Services*.

Within the *Information Sharing* topic, the main focus was on National Information Exchange Model (NIEM) message exchange, where multiple nations were involved with testing independent implementations of a set of three NIEM message types developed by the US test partner, TIES CWP. In addition to NIEM, there were some additional tests performed using other data types, more specifically the Alternate Development and Exchange Method (ADEM) and NFFI.

A second activity related to information sharing was XML Labeling, where NIEM messages were labeled using labels according a NATO technical specification. This specification is undergoing the process of becoming a NATO STANAG.

The *Federated Identity and Access Management* topic was divided into two test series, one focusing on web authentication, and one focusing on securing Web services.

The *Messaging Services* topic looked at WS-Notification and its use as the common standard for publish/subscribe message exchange.

FFI participated in a subset of these experiments, as a preparation for a larger experiment planned for CWIX 2015. In this Chapter we give a brief overview of the full set of SOA-related experimentation at CWIX 2014, with particular focus on the experiment series FFI participated

in, including details experiment execution and results. The main findings from the experiment series where FFI did not participate are included because they form the basis for the planned activities for CWIX 2015, where FFI plans to participate in a broader set of experiments.

The Norwegian participation in the SOA Focus Area was limited to two of the above listed topics. The majority of the test cases that the SecSOA capability participated in were on the topic of Web Authentication, while the remaining test cases focused on testing the interoperability of different implementations of WS-Notification using NFFI data as the notification payload.

4.1 Information Sharing

During the experiments at CWIX 2014 information was shared between partners using a number of data formats. Some of these formats (such as NFFI) were only used as the payload format while conducting other tests. There were however specific tests exploring the interoperability of independent implementations of the two formats NIEM and ADEM, the first of which was tested both plain and with XML Labeling added to the messages.

The Norwegian SecSOA capability did not participate in any of these tests this year, but plan to participate in some of follow-on tests next year.

4.1.1 NIEM Testing

NIEM consists of two main elements: The NIEM Core contains a number of pre-defined information types for common entities, such as persons. The NIEM Domains are domain specific information models that extend the NIEM Core (and information from other NIEM Domains) in order to create an Information Exchange Package (IEP) that determines how data is supposed to be formatted within that domain.

For the experiments at CWIX 2014, US TIES CWP developed an IEP for sharing (a subset of) tactical data. The IEP contained three message types that were tested during the experiments at CWIX 2014. These message types allowed for the exchange of air tracks, friendly ground positions reports and observed positions reports.

NIEM does not specify how messages are to be exchanged, and NIEM data can thus be delivered using a number for different message exchange patterns and protocols. During CWIX 2014 the NIEM data was primarily exchanged using the SIP 3 specification developed used by the FFT Focus Area.

During testing, all the partners participating in these tests were able to exchange and correctly process all three of the NIEM message types that were tested.

4.1.2 ADEM Testing

ADEM, created within the Multilateral Interoperability Program (MIP) community, is an alternate method to the MIP Data Exchange Model (DEM) for exchanging C2 and current situation

information to mission partners. It uses the semantics of the Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM), but implements only the C2 and current situation subsets of the full model.

During CWIX 2014, ADEM formatted messages were exchanged between independent implementations of the specification (NCIA and Germany were the main test partners) using several different message exchange mechanisms, including both request/response and publish/subscribe.

4.1.3 XML Labeling

The XML Labeling experiments at CWIX 2014 consisted of NIEM messages that were labeled with a confidentiality label. The main use case that was tested was where the confidentiality label was directly embedded into the NIEM message structure, and all the involved partners were able to create, bind, share and process these exchanged labels.

Furthermore, some partners also tested adding the confidentiality label into the transport envelope (more specifically into the SOAP Header) rather than into the payload of the message.

4.2 Federated Identity and Access Management

The *Federated Identity and Access Management* topic can be further divided into two main sub-topics, *web authentication* and *Web services security*. The SecSOA capability participated in the experiments covering the first of these two sub-topics this year, and plans to participate in both areas next year.

4.2.1 Web Authentication

The purpose of the Web Authentication testing at CWIX was to help test and verify the specification and joining instructions developed for use in FMN. The NFIP contains a specification of how Web Authentication should be done within the alliance. The current version (at the time of writing) of the NFIP called for the use of the WS-Federation protocol to be used. However, the competing SAML 2.0 protocol has taken on the role as the protocol favored by most commercial SOA support software.

To ensure that the findings from the Web Authentication testing at CWIX 2014 were as complete as possible, the participants in the SOA Focus Area decided to test both the WS-Federation and the SAML 2.0 protocols in both the enterprise and federated scenarios. This led to four Web Authentication test scenarios, which were named SSO1 through SSO4 as listed below:

- SSO1: Web Single Sign-On using WS-Federation in an enterprise scenario
- SSO2: Web Single Sign-On using the SAML 2.0 protocol in an enterprise scenario
- SSO3: Web Single Sign-On using WS-Federation in a federated scenario
- SSO4: Web Single Sign-On using the SAML 2.0 protocol in a federated scenario

There were a number of partners participating in the web authentication experiments at CWIX 2014, but most partners only participated in a subset of test scenarios, depending on which protocol was supported by the framework(s) their software was built upon. SecSOA planned to participate in the tests that were using WS-Federation, and test with all the test partners that were supporting this protocol. These partners were:

- NATO Centre for Maritime Research and Experimentation (CMRE), which participated with the FaaS capability
- NATO Modeling & Simulation Centre of Excellence (MSCOE), which participated with the SGA capability
- NATO ACT, which participated with the THINC capability

During our initial CWIX planning we had, as discussed in Section 2 on pre-testing, based our software on Apache Fediz. This software suite supports only WS-Federation, hence our commitment to the SSO1 and SSO3 test series. However, as we discovered during pre-testing, Fediz was an immature product with several standard compliancy issues. Hence, we switched to the OpenAM framework instead. This framework is primarily SAML 2.0 based, but it does claim to offer support for other protocols as well, including WS-Federation. This let us engage in the SSO2 and SSO4 test series as well, together with two of the partners that supported the SAML 2.0 protocol. These partners were:

- NATO CMRE, which participated with the FaaS capability
- NCIA, which participated with the IETV-FMN MNE capability

The completed web authentication test cases with SecSOA as a participant are listed in Table 4.1. In addition to these test cases eight test cases were not tested due issues discovered during testing. We encountered what turned out to be several bugs and shortcomings in OpenAM 11.0, which kept us from completing the tests involving WS-Federation. Detailed descriptions of each of the completed web authentication test cases where SecSOA participated are available through the CWIX Test Case Tool[2].

Test case ID	Provider(s)	Consumer(s)	Short description	Status
3125	IETV-FMN MNE	SecSOA	SSO2	Limited Success
3128	THINC	SecSOA	SSO4	Success
3132	THINC	SecSOA	SSO2	Success

Table 4.1 Web authentication test cases with SecSOA as a participant

Due to issues with the framework that we were unable to resolve during our participation at CWIX, we were able to take part in SSO2 and SSO4 tests, but only as data consumers, not providers.

[2] The CWIX Test Case Tool is found at http://portal.cwix.act.nato.int. Access to this portal requires a user account and password.

For test scenario SSO2, the overall goal was to achieve Web SSO using the SAML 2.0 protocol in an enterprise scenario, that is, the trust and message flow is done as described for the enterprise scenario (see Section 2.3.2).

Here, a provider offers a Web application accessible via a browser. The IdP is used to authenticate users in the provider domain. The consumer provides the IdP used to authenticate users in the consumer's domain. The interaction between the Web application, the provider's IdP and the consumer's IdP exchange SAML Security Token based on the SAML 2.0 protocol.

For the SSO2 series of tests, the main success criterion was that the user authenticated in the consumer domain should be able to obtain access to a protected Web application in the provider domain. Achieving this criterion ensured that the test was flagged a "limited success". We achieved this result with the partner IETV-FMN MNE as data provider.

The additional success criteria for SSO2 were 1) that the user authenticated in the consumer domain was denied access, and 2) that the level of access to the protected Web application should depend on the user account characteristics. If these additional criteria were met then the test was flagged as a "success". We achieved this result with the partner NATO THINC as data provider.

Following the SSO2 tests we took part in a test according to the SSO4 test scenario, that is, Web SSO using the SAML 2.0 protocol in a federated scenario. Here, a provider offers a Web application accessible via a browser, and the IdP is used to authenticate users in the provider domain. The consumer provides an IdP used to authenticate users in the consumer domain. Trust and message flow is done as described for the federated scenario (see Section 2.3.3). Interaction between the Web application, the provider's IdP and the consumer's IdP were used to exchange SAML Security Token is based on SAML 2.0 protocol.

For the SSO4 series of tests the success criteria were 1) that the user authenticated in the consumer domain should be able to obtain access to the protected Web application in the provider domain, 2) that the user authenticated in the consumer domain is denied access, 3) that the level of access to the protected Web Application depends on the user characteristics. Meeting all the criteria meant that the test was flagged a "success". We achieved this result with the partner NATO THINC as data provider.

Our experiments showed that the tooling support for WS-Federation was inadequate, and that many of the tests were not possible to complete for many partners. The competing specification, SAML 2.0, offers similar functionality. Here is tooling support apparently is better, and several experiments using this solution were completed successfully. As a consequence, a proposal was made that there is a need to include SAML 2.0 in the FMN joining instructions.

4.2.2 Web service security

The current version of the NFIP does not contain a specification for how to secure Web services, despite Web services being identified as a core enabler for building federated information

infrastructures such as the FMN. The currently most mature interoperability specification for Web services security is a Service Interoperability Profile (SIP) written by the NCIA, which has been tested and verified through the TIDE community. In addition, the US has developed their own NCES Profile for Web service security.

The goal of the Web service security testing at CWIX 2014 was to gain further experience with the standards, as described in the Web service security specifications mentioned above, and thus be able to provide recommendations for new FMN joining instructions on this topic.

The test performed on this topic showed that it is possible to achieve interoperability between the independent implementations of SOAP Web service security. Configuration is however complex, and there were several interoperability issues that arose during the experiments. The participants were able to overcome these issues, and show that supporting Web service security is a complex topic, but that it is possible to achieve interoperability.

The Norwegian delegation, represented by the SecSOA capability did not participate in these experiments. This topic is planned to be investigated further during CWIX 2015, and FFI intends to take part in this test series then.

4.3 Messaging services

The data formats tested under the *Information Sharing* topic can be transported across the network in a variety of different ways. Within the *Messaging Services* topic the SOA Focus Area continued the evaluation of the open standard WS-Notification as the preferred mechanism for publish/subscribe message exchange. Both NFIP Appendix S-10 and the TIDE-verified NCIA Publish/Subscribe SIP point to this standard.

Test case ID	Provider(s)	Consumer(s)	Short description	Status
422	LabeledRuDi	THINC SecSOA	WS-Notification subscription and notification	Limited Success
483	LabeledRuDi	SecSOA	Secure WS-Notification	Not Tested
3069	SecSOA	LabeledRuDi	WS-Notification subscription and notification	Success

Table 4.2 Messaging services test cases with SecSOA as a participant

WS-Notification was tested as a carrier for multiple different data formats. SecSOA participated in the tests where NFFI was used as the payload data format while other partners tested the same standard using other data formats. Germany, represented by the LabeledRuDi capability, was SecSOA's primary test partner in performing the three test cases listed in Table 4.2. These two partners have successfully done publish/subscribe with WS-Notification between their two

domains previously [1]. However, Germany has re-implemented WS-Notification within their RuDi software, and it was therefore necessary to re-test in order to discover any new interoperability issues.

Based on the results from the experiments, the SOA Focus Area participants were able to show that it is possible to achieve interoperability based on the FMN joining instructions for publish/subscribe services. There was one small issue discovered related to compatibility between the brokered and non-brokered configurations of WS-Notification. Due to the fact that WS-Notification defines two separate port types, one for each configuration, interoperability can only be achieved if all participants support both these port types.

Test cases 422 and 3069 were executed as planned. In the first of these two test cases, SecSOA functioned as consumer, while we functioned as the provider in the latter test case. The testing with FFI as the provider completed successfully, despite a minor issue with namespace prefixing in the German solution. Conversely, in the other test, LabeledRudi made a subscription to SecSOA, and finally proceeded to unsubscribe. This test was flagged as a “limited success”, due to SecSOA not properly confirming that the unsubscribe message had been received.

Test case 483 was not executed and is therefore set as “Not Tested”. The reason for this is that this test case requires Web services security to be applied. SecSOA had only committed to Web authentication based tests, and did not support this necessary functionality. Thus, this can be considered for testing next year instead.

Further details about all the messaging service test cases are available through the CWIX Test Case Tool.

5 Conclusion

Below we summarize the most important findings from the two major test series FFI participated in at CWIX 2014, along with our overall observations regarding this experimentally inclined venue.

5.1 Test series: federated identity and access management

The idea 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. Establishing an infrastructure that support such a federated identity will be an important building block when participating in a federated scenario such as FMN. The NFIP Appendix S12 states that you can use the standard WS-Federation to achieve this. However, our experiments showed that the tooling support for WS-Federation was inadequate, and that many of the tests were not possible to complete for many partners. A competing specification, SAML 2.0, offers similar functionality. Here is tooling support apparently is better, and several experiments using this solution were completed successfully. As a consequence, a proposal was made that there is a need to include SAML 2.0 in the FMN joining instructions. This result was surprising for many people participating in the SOA focus area, and shows how important it is to participate actively in such an experimentally oriented venue for interoperability testing that CWIX is. Thus, FFI wants to further develop and test SOA security solutions at CWIX next year as well.

5.2 Test series: messaging services

We participated with NATO Friendly Force Information (NFFI) as the test application for the publish/subscribe CES. Our test partner, Germany, supported a similar subscription service, and we were able to use it. Such services form building blocks that in the long term can be used to achieve situational awareness as a whole. For next CWIX FFI plans to participate with a selection of the next generation of NATO-specifications for blue force tracking (BFT) and COP-exchange. In addition to experimentation with NATO specifications we want to attempt interoperability with the U.S. Army project TIES, which is in the process of implementing the National Information Exchange Model (NIEM). NIEM is an American standard and approach to information exchange. It is in widespread use in the United States, and has also been submitted to NATO as an option for use in coalitions. It is therefore important to gain experience with this approach, as it may become important in the context of FMN in the future.

Finally, it should be noted that NATO has selected the standard WS-Notification for subscription services, and it was the one we used. This was included as part of efforts to verify joining instructions for NFIP Appendix S-10, which deals with subscription services.

5.3 Overall observations

In general this year's CWIX was a success because we were able to test aspects of two different CES, 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. Important partner nations participate with their domain experts. This often leads 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. This makes CWIX a very important venue for the project, and we have a desire to participate also in 2015. The plan is to continue work in the above test areas, as well as to include security labeling.

References

[1] Trude H. Bloebaum and Ketil Lund, "CoNSIS: Demonstration of SOA Interoperability in Heterogeneous Tactical Networks", 2012 Military Communications and Information Systems Conference (MCC), Gdansk, Poland, 8-9 Oct 2012

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

[3] NATO Core Enterprise Services Standards Recommendation, The SOA Baseline Profile, Version 1.7, Jan 2012

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

[5] OASIS WS-Notification (2006) TC http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsn

[6] OASIS, WS-BaseNotification 1.3 OASIS Standard, approved October 1st 2006 http://docs.oasis-open.org/wsn/wsn-ws_base_notification-1.3-spec-os.pdf

[7] OASIS, WS-BrokeredNotification 1.3 OASIS Standard, approved October 1st 2006 http://docs.oasis-open.org/wsn/wsn-ws_brokered_notification-1.3-spec-os.pdf

[8] OASIS, WS-Topics 1.3 OASIS Standard, approved October 1st 2006 http://docs.oasis-open.org/wsn/wsn-ws_topics-1.3-spec-os.pdf

[9] OASIS Security Services TC, Security Assertion Markup Language (SAML) v2.0, approved March 2005

[10] OASIS, Web Services Federation Language (WS-Federation) v1.2, approved May 22nd 2009

[11] Microsoft Developer Network. A guide to claims-based identity and access control (2nd edition). http://msdn.microsoft.com/en-us/library/ff359101.aspx,September 2011.