Towards Federated Mission Networking in the Tactical Domain

Marianne R. Brannsten, Frank T. Johnsen, Trude H. Bloebaum, Ketil Lund, Norwegian Defence Research Establishment (FFI)

Abstract

NATO is currently working on the Federated Mission Networking (FMN) concept, which will become the foundation for establishing mission networks in the future. The realization of the FMN concept is described in the NATO FMN Implementation Plan (NFIP). The information infrastructure outlined in NFIP today builds on the concept of service-oriented architecture (SOA) in order to achieve interoperability, and bases itself on many of the same standards and specifications as the ones identified through NATO Network Enabled Capabilities (NNEC). The NNEC SOA Baseline [1] identifies a number of Core Enterprise Services (CES) that represent the common functionality needed to build an interoperable service-oriented infrastructure in a federation. A subset of these capabilities includes messaging services, collaboration services, service discovery and security services. It further identifies which standards should be used to realize these core services while ensuring interoperability between the federation members.

This paper looks into each of these foundational core services, and present the challenges related to extending support for these services into the tactical domain and identify potential solutions.

Introduction

NATO is working on the FMN concept to enable efficient establishment of mission networks in the future. FMN consists of three parts; (1) the FMN framework, which serves as a template for how to build mission networks, (2) a number of mission network instances, and (3) a governance structure which oversees both the FMN framework and the specific mission network instances. FMN as a capability will continue to develop over time, and the approved concept[1] uses a spiral approach to the development of FMN.

To realize the FMN concept NATO is working on the NFIP, which is divided into three volumes. Volume I [2] covers the overall concept and governance, Volume II covers the FMN Framework, and Volume III describes the common NATO capabilities. At the time of this writing, the current version of the NFIP is version 3.0, which outlines a spiral approach for FMN Implementation which aims at having an initial capability with limited functionality defined in Spiral 1. The Spiral 1 ambition level is to establish a basic capability, which supports a limited set of mission threads, and enables information exchange down to the deployed headquarters level. Extending the capability to other mission threads and enabling interoperability in the tactical domain is left for future spirals.

The NFIP today consists of many of standards identified in NNEC. Both FMN Spiral 1 and NNEC SOA Baseline focus on interoperability between federation members on the strategic and operational

[1] The Future Mission Network concept was approved by the Military Committee on 16.11.2012, and its name has since changed to Federated Mission Networking.

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2015.7295463

or the request times out. However, it can also be done asynchronously, such that the connection is closed as soon as the request is delivered, and then the response is delivered at some later time, through a callback function. The latter is especially useful when the processing time of the service can be long.

In addition, the request/response pattern can be used for a push-based message delivery pattern, where the data is delivered in the request message, and the recipient only responds with an acknowledgement message.

As opposed to request/response, the publish/subscribe paradigm relieves the client from having to check for new data. Instead, the node simply sends a subscription request to the information provider, asking to be notified whenever new information is available. This has several advantages: The network traffic is reduced, since the client doesn't have to send periodic requests; the server load is reduced, since there are fewer requests to process; and the client will potentially receive new data sooner, although this is dependent on the request frequency in a Request/Response setting (which in turn will affect network and server load). For a given subscription, the notifications are normally always of the same type, independent of the actual information that is delivered (i.e., the payload of the notification). When a client wants to subscribe to a specific type of data, it therefore expresses the type of information it is interested in by including a topic in the subscription request.

Web services

Web services are based on loose coupling between client and server, and instead of having to rely on Application Programming Interfaces (APIs), the focus is on message formats. Thus, a Web service can be used by any platform that supports exchange of messages that conform to the format used by the service interface. Web services often use the XML-based SOAP protocol for information exchange, and are in widespread use on the Internet today, with civil, commercial products and development tools readily available. Both request/response and publish/subscribe are supported.

In a NATO context, there are two general requirements that must be met by any message exchange mechanism, namely interoperability and ability to function in DIL environments.

For publish/subscribe, the use of WS-Notification is specified, including all sub-specifications (WS-BaseNotification, WS-BrokeredNotification and WS-Topics).

Web services in DIL networking environments

Web services in general focus on environments with static networks and abundant data rates, which in a military context typically means strategic, operational, and deployed tactical levels. Consequently, the overhead associated with Web services is not a problem in such environments.

However, in NNEC the challenge is to enable users to exchange information with each other at *all* operational levels. This includes users in the field who may only communicate with others over radio systems with DIL characteristics. Radio systems such as HF or VHF may have a very low data transfer rate, due to the need for long range signals and jamming resistance. In addition, some radio systems suffer from long turn times for directional changes, plus long setup times for connections.

Reducing the traffic generated is thus necessary. This can be done both by the application itself, and by the platform/communication system [4]. Filtering done by the application will typically be based on message content (e.g. only send tracks within a certain radius from the user. On the platform

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2015.7295463

level, filtering will typically be based on criteria like importance of the message, type of data (e.g. text or video), or priority.

In addition, a common way of reducing network traffic is through compression. Although verbose, XML-based messages are compression friendly, and the size can be reduced significantly, even with standard compression mechanisms like gzip [5].

As mentioned above, NATO has chosen the WS-Notification standard for publish/subscribe. This standard is well-suited to strategic networks, but may require some adaptation for deployment in tactical networks. We have attempted to use WS-Notification over tactical broadband radios and our results show that it functions, but that loss of messages must be expected under poor networking conditions. Figure 1 illustrates this using actual radios. On the X-axis the interval 1-100 is the total message count for the first half of both runs from publisher to broker. The interval 101-200 on the X-axis shows the second half of the experiment runs from broker to subscriber. The Y-axis shows the packet count, thus, the fluctuation illustrates poor conditions leading to retransmissions. In good conditions 12 packets constitute a message sent, and at times more packets are sent in retransmission in order to try delivering the packets and other times the message is lost.

We performed two experiments, using Wm600 Kongsberg radios and a network degradation tool (a matrix of attenuators) for emulation of poor link conditions, using NATO Friendly Force Information (NFFI) [6] over WS-Notification. Note that figure 1 shows some fluctuations in traffic, this can be attributed to signal loss and routing changes. If we were to simulate this, instead of using actual hardware, these results would have looked “cleaner”. The scenario is simple; a deployed user periodically reports his position to a broker, which relays the information back to the tactical forward deployed HQ. In the first run (depicted by the blue line), the radios are well within range and fully connected. 100 messages consisting of multiple NFFI messages where sent, and all were received by the HQ. In the second run (depicted by the red line), the conditions are good between publisher and broker, but poor on the link between broker and subscriber (i.e., HQ). HQ only received 85% of the issued messages do to packet loss and the fluctuation in the packet count resulting in retransmissions.

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2015.7295463

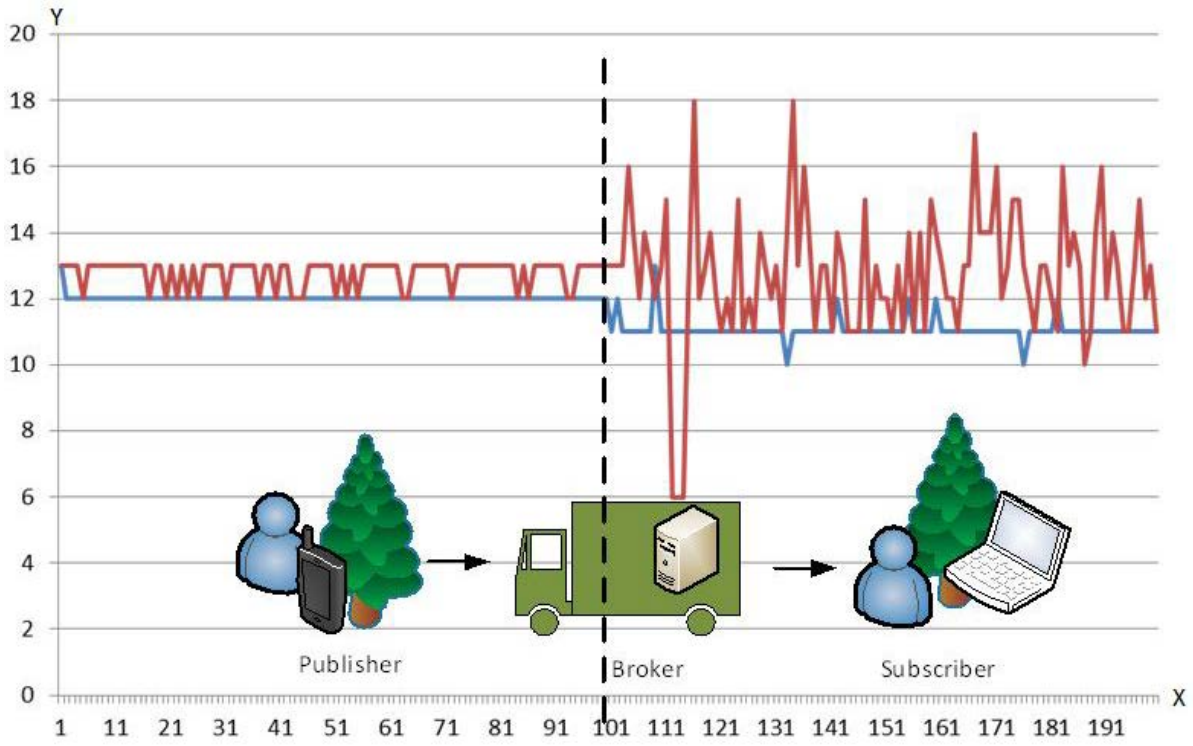

Figure 1 Publish/Subscribe over tactical radio

It should be noted that WS-Notification is a relatively simple standard. In principle, it is a reversed request/response service, in the sense that the server invokes a Web service at the client side when delivering a notification (in other words, it follows the publish/subscribe pattern). In addition, the standard is based on unicast message transmission only, which may have implications in limited capacity networks; even when multiple nodes in the same network want the same information, a WS-Notification broker will send one unicast message to each recipient rather than send one multicast message that reaches all recipients. When subscribers unexpectedly leave the network, permanently or temporarily, WS-Notification is unable to deliver messages to them. NATO has created an add-on to the WS-Notification standard that opens up for caching of messages so that messages can be saved for later delivery [7]. In radio based networks, where the transmission medium is shared, there is a potential for a significant reduction in network load by switching from unicast to multicast. In this case, a reliable multicast mechanism would seem necessary. Note that making such as switch will require further functionality to be implemented into WS-Notification, namely the ability to manage multicast group memberships.

Messaging services as described above enable information exchange between systems. At the next level we need to facilitate collaboration between humans. The following section discusses the parameters for enabling functionality like chat and video conferencing.

Collaboration

Collaboration services are part of the NATO CES, but differ from other services in that they are not pure middleware services as such, but provide functionality directly to the user. Examples of typical collaboration services include audio, video, and chat. The SOA Baseline [1] talks of collaboration

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2015.7295463

The enterprise scenario requires all the participants to belong to the same enterprise, and Figure 3 depicts two enterprises in a federation. The Consumer has a direct trust relationship to the local IdP, and the IdPs of the different enterprises forms a trust relation across enterprise borders. The SP secures a Web resource. When the Consumer, in the remote domain, requests access to the Web resource without an authentication token, the SP redirects the Consumer to acquire one from the local domain's IdP. If the Consumer successfully authenticates to the local domain's IdP, the IdP further requests a token from the remote domain's IdP authorizing access to the Web resource.

Security Overhead in DIL

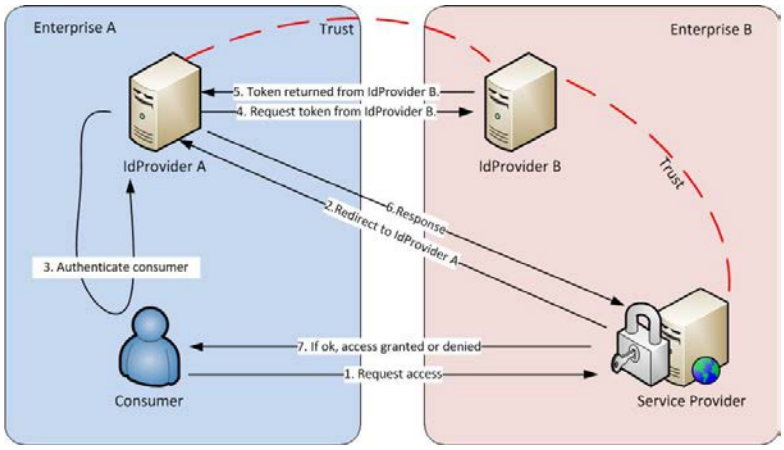

Figure 3 Federated Web authentication

There are two ways of initiating Web authentication, SP-initiated or IdP-initiated. This is defined as to where the user goes first. A user can start by going to SP, getting redirected to IdP, and then directed back after authentication, or the user can go to the IdP first, authenticate and then manually go to the SP to request access.

Table 3 shows the measured results of SP initiated SSO and IdP initiated SSO. The overhead ranges from 5233bytes to 7252bytes. If the user already has a valid token the overhead only diminishes between 165 bytes and 370 bytes. This tells us that the evaluation of how long a token is to be valid is not that important when considering overhead. The result is rather that adding security is costly, but at the same time it is a necessity.

Table 3 Federated Web authentication [12]

Federated SSO	**Network traffic in bytes**		
	Network traffic	***Payload***	***Overhead***
SP-initiated SSO (not logged in)	7459	207	7252
SP-initiated SSO (logged in)	7089	207	6882
IdP-initiated SSO (not logged in)	5505	207	5298
IdP-initiated SSO (logged in)	5340	207	5133

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2015.7295463

There are experimental approaches to supporting SSO in DIL environments with low overhead, an example being [14]. However, interoperability has largely been neglected in such experimental solutions. Hence, further research is necessary in order to bring interoperable SSO to the tactical domain.

Summary

The realization of the FMN concept rests on NATO's work on the NFIP. Future NFIP spirals include work on enabling interoperability in the tactical domain. NNEC also focuses on interoperability and points to SOA and Web services as an enabling technology. CES identified for this enablement are amongst others: messaging, collaboration, discovery and security. These CES were evaluated on the tactical level in this paper. We found that further research is still needed in different areas in pursuit of fully realizing FMN in the tactical domain.

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2015.7295463

References

[1] Consultation, Command and Control Board (C3B). *CORE ENTERPRISE SERVICES STANDARDS RECOMMENDATIONS: THE SOA BASELINE PROFILE VERSION 1.7. Enclosure 1 to AC/322-N(2011)0205*, NATO Unclassified releasable to EAPC/PFP, 11 November 2011.

[2] North Atlantic Council. NFIP Volume I. Approved 29.01.2015

[3] Frank T. Johnsen, Trude Hafsøe, Anders Eggen, Carsten Griwodz, Pål Halvorsen , *Web Services Discovery across Heterogenous Military Networks, IEEE Communications Magazine,* October 2010, pp. 84-90

[4] NATO Science and Technology Organization. *STO-TR-IST-090 - SOA Challenges for Real-Time and Disadvantaged Grids*. STO-TR-IST-090 AC/323(IST-090)TP/520. Final Report of TR-IST-090. ISBN 978-92-837-0195-8. April 2014.

[5] Teixeira, M.A., et al., *New Approaches for XML Data Compression*. In proceedings of International Conference on Web Information Systems and Technologies (WEBIST 2012), pp.233–237., 2012.

[6] NC3B Information Systems SC*, Interim NFFI Standard For Interoperability of FTS*, AC322(SC5)N(2006)0025, 16 (Approved on 16 December 2006)

[7] NCI Agency. TTB Notification Cache V1.1.0. http://tide.act.nato.int/tidepedia/index.php?title=TTB_Notification_Cache_V1.1.0 (Access requires a Tidepedia account), 26 March 2013.

[8] Magnus Skjegstad, Ketil Lund, Espen Skjervold, and Frank T. Johnsen. *Distributed chat in dynamic networks*. IEEE Military Communications Conference (MILCOM) 2011, pp.1651-1657, 7-10 Nov. 2011, Baltimore, MD, USA.

[9] Magnus Skjegstad et.al., *Mist: A Reliable and Delay-Tolerant Publish/Subscribe Solution for Dynamic Networks, New Technologies, Mobility and Security (NTMS), 2012 5th International Conference, 2012*

[10] Eli Gjørven et al., *Towards NNEC – breaking the interaction barrier with collaboration services*, FFI-Report 2014/00943, http://rapporter.ffi.no/rapporter/2014/00943.pdf

[11] Magnus Skjegstad, Frank T. Johnsen, Trude Hafsøe, *An Evaluation of Web Services Discovery Protocols for the Network-Centric Battlefield,* Military Communications and Information Systems Conference (MCC) 2011, Amsterdam, Netherlands, 17-18 October 2011

[12] Marianne R. Brannsten, *Federated Single Sign On in Disconnected Intermittent and Limited (DIL) Networks*, IEEE VTC2015-Spring International Workshop on Service-Oriented Computing (SOC) in Disconnected, Intermittent and Limited (DIL) Networks (SOC-DIL), Glasgow, Scotland, May 2015.

[13] Trude Hafsøe et al., *Using Web Services and XML Security to Increase Agility in an Operational Experiment Featuring Cooperative ESM Operations*, 14th International Command and Control Research and Technology Symposium (ICCRTS), Washington DC, USA, June 2009.

[14] Anders Fongen. *Federated identity management in a tactical multi-domain network.* International Journal on Advances in Systems and Measurements, vol 4, no 3&4, 2011

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2015.7295463

	MARIANNE R. BRANNSTEN (Marianne-rustad.brannsten@ffi.no) is a research scientist at the Norwegian Defence Research Establishment (FFI), engaged in theoretical research and practical development in areas such as distributed systems and Service Oriented Architecture. She received her Master's degree from the University of Oslo (UiO) in 2006, and has been working at FFI since then.
	FRANK T. JOHNSEN (frank-trethan.johnsen@ffi.no) received his Ph.D. from UiO. He started work as a scientist at the Norwegian Defence Research Establishment (FFI) in 2006. At FFI he is currently working within the area of secure pervasive SOA. His research interests include Web Services, Quality of Service, and middleware. He also holds a position as part-time Associate Professor at UiO.
	TRUDE H. BLOEBAUM (trude-hafsoe.bloebaum@ffi.no) is a scientist at the Norwegian Defence Research Establishment (FFI), where she has been working since 2006. Before coming to FFI she worked with content distribution systems at UiO. She received her Cand.scient. degree from UiO. Her research interests are Web Services, Quality of Service, and network protocols.
	KETIL LUND (ketil.lund@ffi.no) is a scientist at the Norwegian Defence Research Establishment (FFI), where he has been working since 2006. His research interests include Service Oriented Architectures, Web Services, Quality of Service, and middleware. At FFI he is currently working within the area of secure pervasive SOA. He received his Ph.D. in informatics from UiO.

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2015.7295463

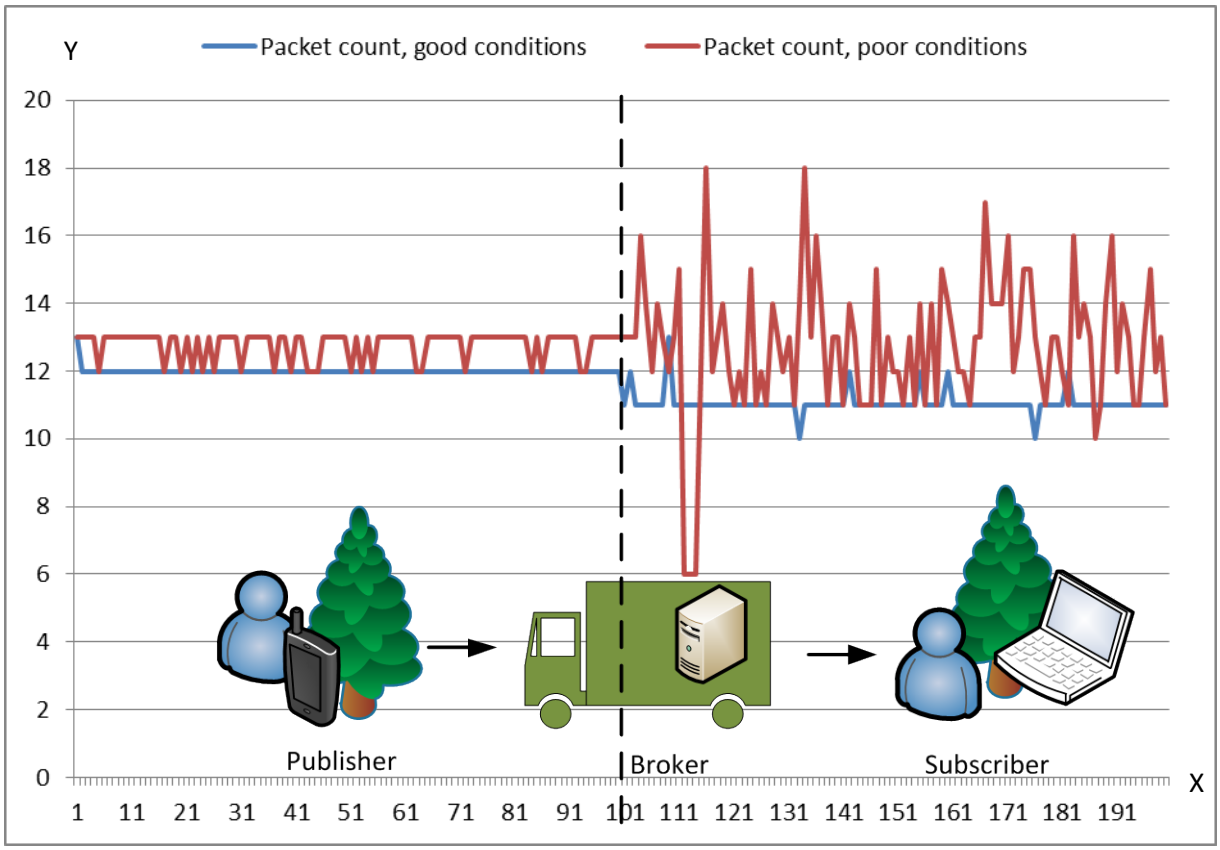

Figure 1 Publish/Subscribe over tactical radio

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2015.7295463

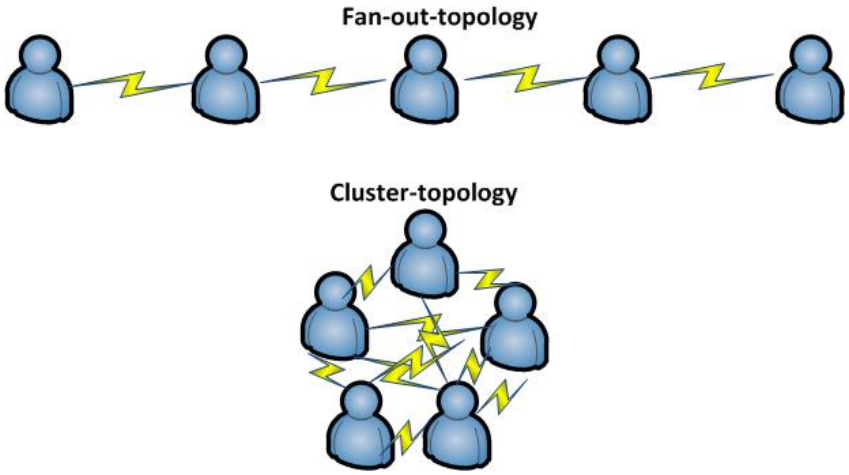

Figure 2 Fan-out-topology vs. cluster-topology

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2015.7295463

Table 1 Current state of collaboration services (adapted from [10]).

	Chat	Audio and video	Data-centric collaboration services
Adaptation to the tactical domain	Solutions are known and tested.	Known solutions work well in the civil domain, but must be tested in the tactical domain. A specific implementation must be explicitly tested for compliance.	New trends in the civil domain barely introduced in the military domain.
Interoperability	Agreement on XMPP, but tactical adaptations and security protocols are not standardized. Requires a gateway between proprietary solution and standardized XMPP to function seamlessly.	Several standards exist, but in practice interoperability is not always achievable.	Well established standards in the civil domain, but these have to be adapted to the tactical domain.
Security	Known mechanisms can be applied, but open issues exist related to tactical adaptations and interoperability.	Interoperability issues related to streaming and many-to-many communication.	No support for classified information. Largely based on network and transport layer security.

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2015.7295463

Table 2 Average bandwidth for cluster- and fan-out- topology (from [11])

Average bandwidth for fan-out-topology				
Protocol	Mist	WS-Discovery	SAM	SLP
Central	0.06 KB/s	14.90 KB/s	0.28 KB/s	7.12 KB/s
Edge	0.05 KB/s	2.28 KB/s	0.02 KB/s	1.05 KB/s
Average bandwidth for cluster-topology				
Protocol	Mist	WS-Discovery	SAM	SLP
Total	0.62 KB/s	27.30 KB/s	0.27 KB/s	12.57 KB/s
Per node	0.05 KB/s	2.27 KB/s	0.02 KB/s	1.05 KB/s
Per query	N/A	27.08 KB/q	N/A	12.59 KB/q
Per query/node	N/A	2.26 KB/q/n	N/A	1.05 KB/q/n

DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2015.7295463

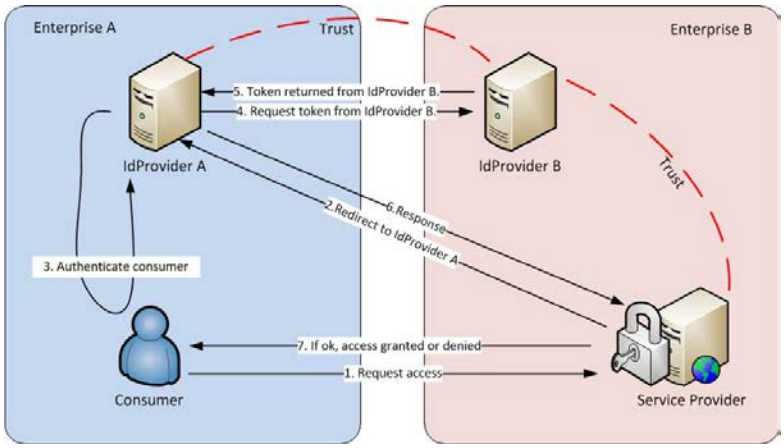

Figure 3 Federated Web authentication

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2015.7295463

Table 3 Federated Web authentication

Federated SSO	Network traffic in bytes		
	Network traffic	*Payload*	*Overhead*
SP-initiated SSO (not logged in)	7459	207	7252
SP-initiated SSO (logged in)	7089	207	6882
IdP-initiated SSO (not logged in)	5505	207	5298
IdP-initiated SSO (logged in)	5340	207	5133

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2015.7295463