Federated Single Sign On in Disconnected, Intermittent and Limited (DIL) Networks

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

***Abstract*—In a military setting resource exchange amongst coalition partners is of great importance. Using SAML2.0 in a Single Sign On scheme in a federated setting can be a solution to Web authentication of Web resources. The problem of adding security in a potentially disconnected, intermittent and limited (DIL) network environment is the security overhead. In this paper tests are performed to measure this overhead, and the results are evaluated.**

Keywords—Single Sign On(SSO); Enterprise; Federation; WS-Federation;SAML2.0

I. INTRODUCTION

In both operations and exercises, NATO needs to connect to coalition partners. FMN (Federated Mission Networking)[8] is defined by NATO to enable information and service exchange amongst coalition participants in such events. This requires interoperability between nations and their often heterogeneous systems. The NATO Network Enabled Capability feasibility study [11] defined Service Oriented Architecture (SOA) implemented using Web services to be a key enabler for interoperability. Available services, applications and Web sites in a military setting often need security solutions, such as Web authentication, granting and denying access appropriately.

When several systems and nations interoperate and share Web resources we move from an enterprise scenario where all participants are in the same security domain to a federated scenario where the different participants establish a ring of trust to manage access security across several enterprises.

In a civil arena there are for the most part stable networking connections with more than enough bandwidth. In a military scenario this might not be the case as we often have to handle Disconnected, Intermittent and Limited (DIL) networking environments. The cost of adding security in such an environment is important to study, as this can influence the usability and stability of the available resources. In this paper we measure the overhead in network traffic when adding Web authentication using a Single Sign On (SSO) security solution, in federated systems, and bringing FMN specifications into DIL networking environments. Note that the experiments described in this paper were performed in a lab environment and not in a live DIL setting.

II. RELATED WORK

Earlier work has shown that it is possible to use Web services in tactical networks [15]. Standards "out of the box" might not handle the additional challenges DIL environments introduce, but by using specialized proxies, the technology could work despite the DIL limitations. This lets us attain the advantages of SOA using Web services on a tactical level. Lund et al. [1] have proved this in their "Delay- and distruption tolerant SOAP proxy". Johnsen et al. [2] have shown that service discovery also can be brought into tactical networks using a discovery protocol translations enabled gateway solution. Both solutions bring Web services to the tactical domain, but none of them are evaluated with use of relevant security standards. The work presented in this paper can by this be viewed as orthogonal and complementary to this earlier work, as this paper focus on the use of relevant security standards in a DIL network.

In the context of exchanging sensor information, earlier studies have measured and evaluated the overhead of SOAP security. In the study by Hafsøe et al. [3], XML signature was used in conjunction with WS-Security to secure the integrity of SOAP messages. Certificates were predistributed in this basic point-to-point communication. The study showed that the SOAP messages increased approximately 2.5 times in size when compared to running with no security. This revealed a potential problem of bringing such solutions into a tactical level and DIL networks, where bandwidth typically is a scarce resource. The work presented in this paper is complementary to this former study as the focus here is on SSO and federated security, another necessary building block to achieve a complete security solution. In this paper the focus is on the Security Assertion Markup Language (SAML) 2.0 standard [13]. For further details about complementary standards, XML signature, XML Encryption, WS-Security and more, take a look at [4].

Any security scheme requires distribution of certificates and revocation lists. This is challenging in DIL environments and is currently an unsolved issue. Research is being performed in this area, see e.g. [7]. In this paper certificates are pre-distributed and assumed valid for the duration of the experiments.

In NATO there is a persistent focus on bringing selected core enterprise services into the tactical level. Existing standards and recommendations mainly target use in networks

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/VTCSpring.2015.7145841

with fixed infrastructure. This is why NATO research groups as IST-090 [5] and IST-118 [6] have focused on SOA and challenges in DIL networks (often described as "disadvantaged grids" in a military context). Common for these two groups is that security has not been in focus, even though security is a core enterprise service. This paper can by this be seen as a concrete input of security to IST-118 and the group's focus on creating recommendations for SOA on the tactical level.

III. Web Authentication

In both civil and military settings Web resources are often in need of access restrictions. Web authentication lets legitimate users authenticate before they are granted access. Often the individual site owner implements a username and password scheme to secure their resources. If the user needs to authenticate at every step it can be troublesome and take up too much time. Remembering several usernames and passwords can hinder efficient work. Therefore the SSO scheme is a good solution. The user signs in once at one place, and is granted a security token giving access to several resources.

SSO is applicable in both enterprise systems and in federated systems. FMN defines how nations are to collaborate in a federation in order to achieve interoperability. Participants contribute with their resources and can use the resources available by the other participants in the federation [8]. Bringing SSO into a federated scenario has its challenges, and when SSO is brought into a DIL environment there are even more challenges.

A. *Single Sign On (SSO)*

SSO is the process of enabling users to authenticate one time and granting them access to the system as long as the authentication is valid.

Traditionally, SSO systems have relied on browser cookies. The cookies store information about the consumer enabling access to a system without having to authenticate every time. The problem with cookies is that they are not suitable for cross domain application as they are never transmitted between Domain Name System (DNS) domains without a proprietary mechanism. There needs to be another solution for both enterprise and federated SSO.

The SSO scheme used in this paper uses a central service handling Web authentication. The authentication participants are a Secure Token Service (STS) and an Identity Provider (IdP). The STS is responsible for distributing security tokens used for accessing Web resources. The IdP is an extension of the STS and is responsible for authenticating incoming requests for access.

The consumers are able to authenticate once and use the available services without new authentication at every step. Also, the consumers are able to sign out once in a Single Sign Out operation, and then not having access to any secure resources before a new "sign in" operation is performed.

SSO is applicable in several settings. The following subchapter describes the enterprise scenario.

B. *Enterprise systems*

The Enterprise scenario involves one or more domains where the participants operating are all members of the same enterprise. There is a direct trust relationship to the entity handling access management. Even if they reside in different domains they all belong to the same enterprise.

You can picture a Web application residing behind a lock operated by the Service Provider (SP), where the IdP and its STS are responsible for providing the tokens and the IdP authenticate the tokens when access is requested. If you do not have the key, it will be provided to you by the STS, as long as you are registered as a valid user in the system and you are able to authenticate yourself by username and password. After the consumer receives the new token this is a valid key until it times out (if the token includes liveness data) or the user logs out in a Single Sign Out operation.

Fig. 1 shows the steps and participants in the enterprise scenario. The consumer requests access to a Web application. The request is redirected to the IdP (the IdProvider in the figure contains both the IdP and the STS) checking if the consumer has privileges to use the resource. If not, the user is prompted to authenticate and if this is OK the IdP tells the Web resource to grant access to the user and the consumer receives a valid security token. This token can be used at a later date by the consumer to access the secure application as long as the timestamp has not expired.

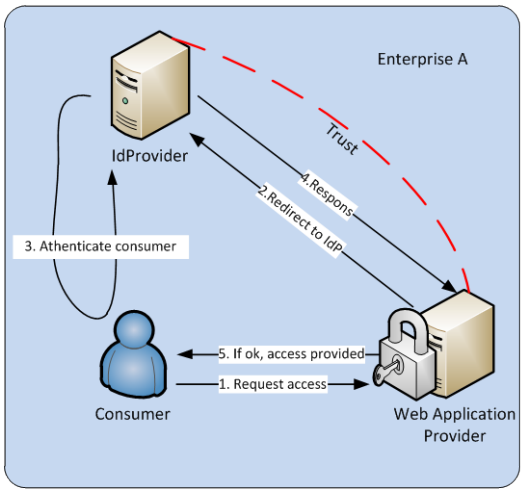

Fig. 1. Enterprise scenario

As mentioned earlier there is a need for interoperability between different heterogeneous systems and there is also a need for easy sharing of resources with other nations in a military setting. This brings us to a federation, where the enterprises of different nations establish trust among them to grant access to Web resources and by this enable collaboration.

C. *Federated systems*

The Federated scenario involves one or more enterprises and potentially several domains. They all have a direct trust relationship to the entity handling access management in their

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/VTCSpring.2015.7145841

enterprise, similar to the enterprise scenario. The federation is established by a ring of trust between the IdPs in the different enterprises.

As Fig.2 shows there are some additional steps in the federated scenario compared with the steps of the enterprise scenario. To the consumer these additional steps will not be noticed. The request is redirected to the consumer's IdP for authentication. When the consumer is approved by its local *IdP A* a request for a security token is sent to *IdP B* by sending the valid token from *Enterprise A*. The two providers trust each other and *IdP B* returns a token valid in *Enterprise B* and the consumer is able to access the Web resource.

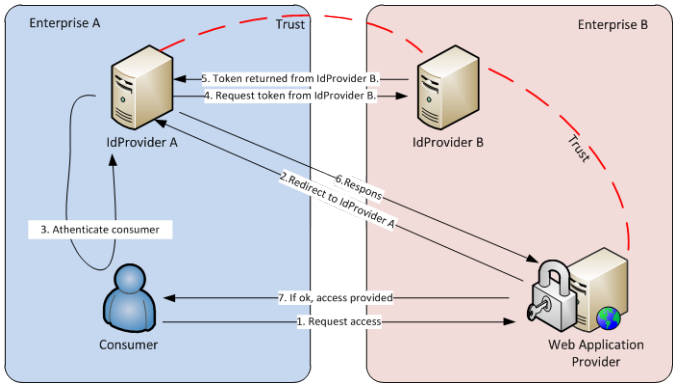

Fig. 2. Federated scenario

D. *Disconnected, Intermittent and Limited (DIL) environments*

Military networks are often challenged with other problems than civil networks. DIL environments are often troubled with disruptive behavior where resources might not always be able to be connected to a network. For example, there may be no network nodes available in the area to connect the mobile device to. The network access is intermittent as the network nodes might move or fail. And the network, if available could have a low capacity hindering efficient communication. DIL environments are often called disadvantaged grids in a military setting. Disadvantaged grids are characterized by low bandwidth, variable throughput, unreliable connectivity, and energy constraints imposed by the wireless communications grid that links the nodes [9]. Given these limitations, standardized solutions must be evaluated and possibly adapted to ensure expected functionality in such an environment.

The impact of the additional steps needed in Web authentication using SSO is measured in section V, and the findings are evaluated in context of the potential challenges in DIL environments. The measurements taken are done in a federated setting as this is the most interesting case in a military setting seeking interoperability and collaboration.

IV. Technical Background

There are several approaches to enable Web authentication and SSO solutions. It is important to follow standards as this increase the potential for success in collaboration with others. The participants do not have to use the same system, but it is of great advantage that they all follow the same standardized interfaces and data formats.

FMN points to WS-Federation as the standard for federation, but tests preformed at the Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX) 2014 [10] showed that there were difficulties utilizing that standard as it is lacking in tool support. SAML 2.0 remedies this with better tool support. Testing performed at CWIX 2014 was mainly of SAML2.0 as the WS-Federation proved to be impossible to test for several participants, and this resulted in the proposal of including SAML2.0 in the FMN joining instructions [8].

In our test lab we use the OpenAM 11.0.2 software for authentication, authorization and federation. OpenAM [12] is an access management system with several possibilities in how authentication is performed. In our setup we enable SSO using SAML2.0 tokens. SAML is defined for exchanging security information between trusted participants

OASIS defines a technical overview of SAML2.0 in [13]. This section gives a quick intro to the different profiles of SAML2.0 and defining the technical background for the tests performed in section V. Listed in the specification there are several profiles defined. The one being used in this paper is the *Web Browser SSO Profile*, which defines how to achieve SSO in a standard Web browser. Further details are discussed below.

A. *Web Browser SSO Profile*

The Web Browser SSO Profile defines how to use SAML for SSO. There are two ways of initiating SSO, either through the Service Provider (SP) or through the IdP.

1) *SP-initiated SSO*

SP-initiated SSO is the case where the consumer initiates SSO by trying to access a protected resource at the SP.

This is the most common scenario. The consumer wants to access a resource and goes directly to the SP. The fact that the resource is secured is something the consumer potentially would find out trying to access the resource. If the consumer does not hold a valid access token SP redirects to the IdP for authentication and would then be prompted for username and password. If the requestor already holds a valid token he is granted access without a new authentication process and could by this not even be aware of the security measures. After authentication, if OK, the IdP returns an OK to the SP who then grants the consumer access.

Fig. 3 shows the details of an SP-initiated request. The figure resembles the enterprise scenario, but takes notice of the fact that the participants are not depicted in any specific

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/VTCSpring.2015.7145841

domain or enterprise. This is simply a description of SSO initiation type. The consumer requests access to a resource. The request is redirected if no valid token is presented by the consumer. The authentication process is started, and if OK, the consumer is granted access.

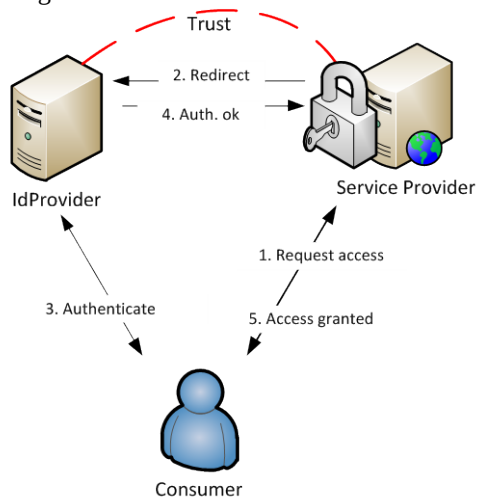

Fig. 3. SP initiated SSO

Another type of SP-initiated SSO is the case where there is an additional step where messages are too long or in need of a digital signature.

2) IdP-initiated SSO

IdP-initiated SSO is where the consumer goes directly to an IdP and requests access to a resource it knows is secured by an SP. The same requirements as for SP-initiated SSO are applied. If the user does not hold a valid security token, one is provided after the requestor authenticates with a username and password. Then access is granted to the desired resource. As for the SP-initiated SSO scenario, Fig. 4 has no domain or enterprise defined. It describes the IdP initiated SSO where the scenario is that the consumer first authenticates to the IdP and then is able to access the resource secured by the service provider.

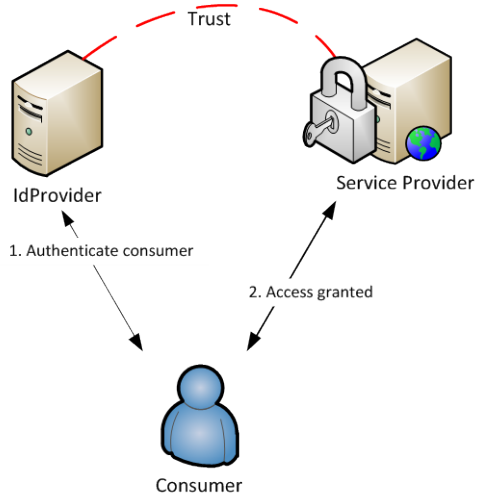

Fig. 4. IdP-initiated SSO

As you can see from Fig.3 and Fig. 4 there are less steps involved in the IdP-initiated SSO, but the SP-initiated SSO described is the more common scenario. In fact, SAML 2.0's SP-initiated SSO offers the exact same functionality as WS-Federation.

V. Testing and Evaluation

All security adds overhead and in DIL environments this overhead can have a big impact on usability. In this chapter we evaluate how much overhead is added by Web authentication using SSO. Both SP-initiated and IdP-initiated SSO in the federated scenarios are measured.

As described earlier, if the consumer already holds a valid token there is no need for the authentication step towards the consumer. This implies that there are less steps, and by this less overhead, in the process if the consumer is already authenticated.

The tests are conducted using Wireshark [14] for capturing payload and overhead. The overhead is defined as all metadata needed to deliver the payload (e.g. HTTP headers). Thus to calculate overhead the size of the payload is deducted from the size of the message exchange (what Wireshark calls a conversation).

A. No authentication

Traffic measured in a setting where there are no additional security measures is as shown in Tab.I.

TABLE I. No Authentication

No Authentication	**Network traffic in bytes**	
	Payload	***Overhead***
	207	594

B. Overhead in the federated scenario

SP-initiated SSO in a federated system is the same as described in Fig. 2. The consumer approaches the SP with the request to access the Web resource and SP redirects to the requestors IdP for authentication, which in turn redirects to the IdP of the SP to obtain a valid token to the requested service.

IdP-initiated SSO in a federated system differs slightly as the consumer goes directly to the Idp and request access.

TABLE II. Federated SSO

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

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/VTCSpring.2015.7145841

Tab. II shows network traffic measured in the experiment. The setting is a federated SSO setting with and without a valid SAML2.0 token. The overhead for all variations are large. The payload is only 270, and the overhead ranges from 5133bytes to 7252bytes. The difference between the requestor having a valid token and not having a valid token is 370bytes for the SP-initiated setting and in the IdP-initiated setting the difference is only 165bytes.

Evaluating these numbers indicates that adding Web authentication security to a federated system in this fashion is costly. But there is a need for easy Web authentication and for making resources more available across enterprise boundaries.

Another security aspect of interest is the timeframe a security token is valid ("liveness" of the tokens). There needs to be an evaluation between security and SSO token liveness. How long should the token be valid? If the token lives forever the risk of a security breach is increasing as time goes by. And if the token has a time to live through liveness data there has to be an evaluation on how long time it should be valid. Too short gives more overhead as the user might have to re-authenticate often and by this adding traffic and overhead. As the numbers in Tab. 2 show, this is not extensive overhead so it is better to define "time to live" in accordance with the increase of security risks with long validity and in compliance with usability for the consumer.

VI. Conclusion and Further Work

Implementing SSO in a federated scenario enables collaboration if the participants all implement a solution that is interoperable with each other. This is why it is important to come to a consensus of the desired technology. SAML 2.0 is supported by several vendors, and has been proposed as a part of the FMN joining instructions.

Bringing SSO to DIL poses problems in terms of overhead, but it would still possibly add value in terms of collaboration with coalition partners, enabling resource, information and service exchange.

The experiment described in this paper was conducted as part of preparations for a larger experiment of Web authentication using SAML2.0 which is to be conducted at CWIX 2015. There the focus is on interoperability rather than limiting overhead.

In addition to CWIX 2015 we at FFI are working on a Web application using fine grained claims based access control, supported by the framework and in key with current FMN specifications.

Acknowledgements

I would like to thank Ketil Lund and other colleagues for their feedback and support. Thanks to the OpenAM team for providing us with access the OpenAM software used in this experiment.

References

[1] Ketil Lund et al., Robust Web Services in Heterogeneous Military Networks, in IEEE Communications magazine, special issue on military communications, October 2010.

[2] Frank T. Johnsen et al., Web Services Discovery across Heterogeneous Military Networks, in IEEE Communications magazine, special issue on military communications, October 2010.

[3] 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.

[4] Nils Agne Nordbotten, XML and Web Services Security Standards, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 3, THIRD QUARTER 2009.

[5] Peter-Paul Meiler et al., An Overview of the Research and Experimentation of IST-090: SOA over Disadvantaged Grids, Military Communications and Information Systems Conference (MCC 2011), Amsterdam, Netherlands, October 2011.

[6] F.T. Johnsen et al., IST-118 – SOA recommendations for Disadvantaged Grids in the Tactical Domain, 18th International Command and Control Research and Technology Symposium (ICCRTS), Alexandria, VA, USA, June 2013.

[7] A. Fongen, "Optimization of a Public Key Infrastructure," *MILITARY COMMUNICATIONS CONFERENCE, 2011 - MILCOM 2011* , vol., no., pp.1440,1447, 7-10 Nov. 2011

[8] ACT, FMN 101- A primer on NATO Federated Mission Networking, https://tide.act.nato.int/tidepedia/index.php?title=FMN_101 (Requires a Tidepedia account)

[9] A. Gibb, H. Fassbender, M. Schmeing, J. Michalak, and J. E.Wieselthier. Information management over disadvantaged grids. Final report of the RTO Information Systems Technology Panel, Task Group IST-030 / RTG-012, RTO-TR-IST-030, 2007.

[10] ACT, Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise 2014 Final Report, 9 September 2014, MCM-0130-2013

[11] P. Bartolomasi, T. Buckman, A. Campbell, J. Grainger, J. Mahaffey, R. Marchand, O. Kruidhof, C. Shawcross, and K. Veum. NATO network enabled capability feasibility study. Version 2.0, October 2005.

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

[13] 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

[14] Wireshark homepage: https://www.wireshark.org/

[15] Trude H. Bloebaum and Ketil Lund, CoNSIS: Demonstration of SOA Interoperability in Heterogeneous Tactical Networks, IEEE *MCC*, Gdansk, Poland, October 2012

Dette er en postprint-versjon / This is a postprint version.

DOI til publisert versjon / DOI to published version: 10.1109/VTCSpring.2015.7145841