MACQUARIE UNIVERSITY

INVESTIGATING LIBERTY ALLIANCE AND SHIBBOLETH INTEGRATION

ITEC809 – PROJECT PROPOSAL

Nishen Naidoo
30396468
nishen.naidoo@mq.edu.au
Supervisor: Steve Cassidy (steve.cassidy@mq.edu.au)

DOCUMENT CONTROL

Author(s):	**Nishen Naidoo**
Release Version:	**1.0**
Status:	**Final**
Revision:	**70**

Version	Date	Purpose	Amended by
0.1	2009-08-15	Initial draft	Nishen Naidoo
0.2	2009-08-19	Summary completed	Nishen Naidoo
1.0	2009-08-21	Final release for submission	Nishen Naidoo

TABLE OF CONTENTS

1 SUMMARY

The current state of identity management solutions has seen significant strides being made towards federation in order to reduce the amount and the management complexity of private user information that is distributed across the internet. There are currently three separate frameworks for Federated Identity Management (FIM): WS-Federation, Shibboleth and Liberty Alliance. However, multiple frameworks can add complexity and cost to users, Identity Providers (IdPs) and Service Providers (SPs). It would be far simpler for users, IdPs and SPs if communication across FIM frameworks was possible. Given that the fundamental technologies used by both Shibboleth and Liberty Alliance are the same, it would seem that integration should be possible. This project aims to investigate both these frameworks and determine if, how and where integration can occur.

2 PROJECT DESCRIPTION

2.1 BACKGROUND INFORMATION

As more businesses begin operating online, it is becoming necessary for end users to maintain multiple identities at multiple locations. It is often the case that a user manages a digital identity for each service that they use. This means that each service provider (SP) used maintains a copy of a set of credentials and profile information for a particular user. Bhargav-Spantzel (2006) discusses this model and explains it as the 'silo' model and states that it is the most common form of identity management today. He argues that this form of management is cumbersome for the end user, although its predominant position is due to it being the simplest model for managing identity. However, with simplicity comes the inability to adapt to changing and growing requirements, and with the average user exposed to over 25 online accounts and typing 8 passwords a day, ‘password fatigue’ is becoming more of an issue (Dhamija and Dusseault 2008).

As the requirements for online identities and identity management change with the growth of online activity, management techniques need to evolve as well. Some of the growing requirements around identity management relate to privacy and are driven by legislation (Hansen et al. 2008). The US, Canada and the EU are all being pressured into data protection legislation with regards to financial and medical data (Peyton et al. 2007) and are examining FIM as a mechanism for dealing with these requirements.

So what is FIM?

> *A Federated Identity Architecture (FIA) is a group of organisations that have built trust relationships among each other in order to exchange digital identity information in a safe way, preserving the integrity and confidentiality (privacy) of the user personal information. The FIA basically involves Identity Providers (IdP) and*

> *Service Providers in a structure of trust by means of secured communication channels and business agreements. (Fragoso-Rodriguez et al. 2006)*

To explain with an example, let us examine 'John' who is a student at 'Alpha Tech University' (ATU). ATU is John's IdP. ATU has a trust relationship with 'Random House Publishers' (RHP) to allow their postgraduate students access to certain academic publications. RHP has similar trust relationships with many universities and other organisations around the world. When John attempts to access a resource at RHP over the web, he is prompted to select his IdP. He is then forwarded to the IdP (which in this instance would be ATU), where he is challenged for his credentials. On providing his credentials he is authenticated, has an authentication token added to his web session (stating where and when he was authenticated and a transparent ID) and returned to where the transaction originated – RHP. On returning, RHP is able to identify that John has in fact been authenticated at ATU, even though RHP has no idea about who John is. Using the transparent ID (to preserve John's privacy/anonymity), RHP can send a request to ATU asking for specific attributes about the user. Provided John is amenable to the requested attributes being divulged, ATU can release these attributes to RHP (e.g. an attribute stating whether John is a postgraduate student or an undergraduate student). Based on the attributes returned, RHP can then make an authorisation decision as to whether to allow John access to the resource he requested. In this case, as John is a postgraduate student, he is granted access and provided with the full text of the publication (Cantor 2005).

ATU, RHP and the other connected organisations form what is called a Federation in Shibboleth and a Circle of Trust (CoT) in Liberty Alliance. While the terminology seems quite different, the high level interactions are very similar between both frameworks and both are supported by similar underlying technologies.

2.2 AIMS, SIGNIFICANCE AND EXPECTED OUTCOMES

The purpose of this project is an investigation into both the Shibboleth and Liberty Alliance federation frameworks in order to identify integration opportunities. Currently, members of each framework are isolated from other frameworks. While in many cases this does not present a problem, consider the following scenario:

I am a student at a university. The university is part of a Shibboleth federation and is therefore also my IdP. I wish to book a study trip abroad through an online travel agency that offers a special discount to students. The travel agency has trust relationships with several universities that it services, including my own, and is therefore part of the Shibboleth federation. Through the authentication and attribute sharing process the travel agency is able to identify that I am in fact a student and thus entitled to the student discount. As part of the package, the travel agency is also able to book a car for me when I arrive at my destination. The care hire service however, is part of a Liberty Alliance CoT. In order for the travel agency to book the car on my behalf, it also has to be a member of the

Liberty Alliance CoT and therefore has to support two frameworks. If I were to then want to book some additional tours from a tourism company independent of the travel agency, and the tourism company is part of a Liberty Alliance CoT, I will then be forced to create an identity within that CoT exposing my personal information to yet another set of organisations.

The example, while simplistic, can be applied to many potential real world scenarios and highlights some core issues with multiple frameworks:

- A service provider might be required to operate under multiple frameworks adding cost and complexity to their service.
- A user accessing multiple frameworks will have to have multiple identities and distributed personal data.
- Identity Providers could potentially have clients requiring access to services in both frameworks.

Another point to note that was raised in the literature review for this project is that each of these frameworks tends to target particular domains, namely the business and education sectors, and the designs for these frameworks are greatly influenced by domain specific assumptions. However, as a user belonging to both these domains I should not have to duplicate my identity across two silos that share a significant amount of the same information and, in doing so, violate one of the primary directives of FIM. After all, I am still the same person whether student, client or customer.

It would seem that in order to avoid some of these issues, a Shibboleth IdP that is able to integrate into a Liberty Alliance CoT (or vice versa) could potentially reduce the identity management complexity for users, IdPs and SPs and more fully realise the FIM ideal.

To this purpose the project will involve the investigation of both frameworks and identifying their profiles, protocols, underlying technologies, transport mechanisms and vocabularies. Once these are identified and contrasted, it should be possible to identify differences and possible integration models that might be able to be applied.

The outcome of this project will be a report that includes:

a) a literature review (including FIM overview)
b) analysis of the Shibboleth framework
c) analysis of the Liberty Alliance framework
d) discussion of models and technologies that might be used to bridge the frameworks

3 RESEARCH METHODOLOGY AND PLAN

3.1 METHODOLOGY

The objective here is to investigate and identify a set of technologies that can be implemented to integrate two federation frameworks.

Preliminary research has identified that the underlying protocol used for communication between IdPs and SPs for both frameworks is SAML (Security Assertion Markup Language). This is the ground level communication that we will be working towards integrating, but we first have to develop a more holistic overview of the communication profiles of each of the frameworks.

The profiles in question dictate the sequences of interactions between the three primary nodes of the framework: the SP, IdP and User. In addition to these, Shibboleth has a fourth component called the WAYF. The WAYF is the "Where Are You From?" component that can be a link between Users, SPs and IdPs, but is not compulsory.

Understanding these profiles is critical to finding points where these frameworks can integrate and understanding the protocols and vocabularies involved is crucial to enabling communication between these frameworks once they are connected.

3.2 TASK PLAN

Task	Description	W04	W05	W06	W07	W08	W09	W10	W11	W12	W13	W14	W15
1	Shibboleth Analysis												
2	Liberty Alliance Analysis												
3	Investigate Technologies												
4	Model Generation												
5	Report Outline												
6	Report Writing												
7	Presentation Design												

3.2.1 TASK 1 – SHIBBOLETH ANALYSIS

This task will involve breaking down the Shibboleth framework specifications and technologies and understanding the components, communication profiles and protocols that are used. It will involve reading through several specification documents and research papers and obtaining both a holistic and detailed understanding of the framework.

3.2.2 TASK 2 – LIBERTY ALLIANCE ANALYSIS

As above, this task will involve breaking down the Liberty Alliance framework specifications and technologies and understanding the components, communication profiles and protocols that are used. As the analysis on the Shibboleth framework should be complete, it will possible to start identifying the specific differences in the frameworks. This task will also involve reading through specification documents and research papers.

3.2.3 TASK 3 – INVESTIGATE TECHNOLOGIES

By this stage we should have a thorough understanding of both the frameworks and can start identifying the points where we can insert technologies that will enable integration, and the technologies themselves. Ideally we would be able to identify methods of integration that do not require alterations to the frameworks themselves. This might initially indicate some kind of middleware solution.

3.2.4 TASK 4 – MODEL GENERATION

Once we've identified the technologies we can start documenting the possible solution models. This will most likely involve generation of diagrams (UML and sequence) that describe the communication profiles involved in cross federation communication.

3.2.5 TASK 5 – REPORT OUTLINE

At this stage we should be nearing the end of the investigatory phase of the project and enough information should have been obtained to be able to develop a report outline. This is a deliverable for the course. This task can run in tandem with the model generation.

3.2.6 TASK 6 – REPORT WRITING

We have hopefully completed the research phase of the project and can start preparing the final report deliverable. The report will encapsulate the process that has occurred through tasks 1 – 5.

3.2.7 TASK 7 – PRESENTATION DESIGN

As part of the project the presentation is a deliverable. This task can run in tandem with task 6 as they are complimentary. The presentation will cover the findings that were made throughout the project.

4 REFERENCES

1. Bhargav-Spantzel, A., Camenisch, J., Gross, T., Sommer, D., (2006) “User centricity: a taxonomy and open issues.” Proceedings of the second ACM workshop on Digital identity management, Alexandria, Virginia, USA: ACM, pp. 1-10
2. Cantor, S., ed. (2005) “Shibboleth Architecture Protocols and Profiles,” Internet2 Middleware Initiative URL: http://shibboleth.internet2.edu/docs/internet2-mace-shibboletharch-protocols-200509.pdf (accessed at 20 May 2008)
3. Dhamija, R., Dusseault, L., (2008) “The Seven Flaws of Identity Management: Usability and Security Challenges.” Security & Privacy, IEEE Vol. 6, Iss. 2 pp. 24-29
4. Fragoso-Rodriguez, U., Laurent-Maknavicius M., Incera-Dieguez J., (2006) “Federated Identity Architectures.” Proceedings of the 1st Mexican Conference on Informatics Security 2006 URL: http://www-lor.int-evry.fr/~maknavic/articles/mlaurent-mcis06.pdf (accessed on 15 May 2008)
5. Hansen, M., Schwartz, A., Cooper, A., (2008) “Privacy and Identity Management.” Security & Privacy, IEEE Vol. 6, Iss. 2 pp. 38-45
6. Peyton, L., Hu, J., Doshi, C., Seguin, P., (2007) “Addressing Privacy in a Federated Identity Management Network for EHealth.” Management of eBusiness, 2007. WCMeB 2007. Eighth World Congress on the