Information Assurance in Federated Identity Management: Experimentations and Issues *

Gail-Joon Ahn[1], Dongwan Shin[1], and Seng-Phil Hong[2]

[1] University of North Carolina at Charlotte, Charlotte, NC 28232, USA
{gahn,doshin}@uncc.edu
[2] Information and Communications University, Taejon, Korea
philhong@icu.ac.kr

Abstract. Identity management has been recently considered to be a viable solution for simplifying user management across enterprise applications. When users interact with services on the Internet, they often tailor the services in some way for their personal use through their personalized accounts and preferences. The network identity of each user is the global set of such attributes constituting the various accounts. In this paper, we investigate two well-known federated identity management (FIM) solutions, *Microsoft Passport* and *Liberty Alliance*, attempting to identify information assurance (IA) requirements in FIM. In particular, this paper focuses on principal IA requirements for Web Services that plays an integral role in enriching identity federation and management. We also discuss our experimental analysis of those models.

1 Introduction

Surveys and polling data confirm that the Internet is now a prime vehicle for business, community, and personal interactions. The notion of identity is the important component of this vehicle. Identity management (IM) has been recently considered to be a viable solution for simplifying user management across enterprise applications. As enterprises have changed their business operation paradigm from brick-and-mortar to click-and-mortar, they have embraced a variety of enterprise applications for streamlining business operations such as emailing systems, customer relationship management systems, enterprise resource planning systems, supply chain management systems, and so on. However, a non-trivial problem has been compounded by this reinforcing line of enterprise applications, *the problem of managing user profiles.* The addition of such applications has proved to be subject to bringing in a new database for storing user profiles, and it was quite costly and complex to manage all those profiles, which were often redundant. Considering business-to-business environments, where a set of users consists of not only their employees or customers but also those of

* The work of Gail-J. Ahn and Dongwan Shin was supported by the grants from Bank of America through e-Business Technology Institute at the University of North Carolina at Charlotte.

X. Zhou et al. (Eds.): WISE 2004, LNCS 3306, pp. 78–89, 2004.

their partners, this problem became even worse. As a set of underlying technologies and processes overarching the creation, maintenance, and termination of user identities, IM has attempted to resolve such issues.

Furthermore, the prevalence of business alliances or coalitions necessitates the further evolution of IM, so called federated identity management (FIM). The main motivation of FIM is to enhance user convenience and privacy as well as to decentralize user management tasks through the federation of identities among business partners. As a consequence, a cost-effective and interoperable technology is strongly required in the process of federation. Web Services (WS) can be as a good candidate for such requirement as it has served to provide the standard way to enable the communication and composition of various enterprise applications over distributed and heterogeneous networks.

Since identity federation is likely to go along with the exchange of sensitive user information in a highly insecure online environment, security and privacy issues with such exchange of information are key concerns in FIM. In this paper, we describe a comparative study of FIM to investigate how to ensure information assurance (IA) for identity federation. We first discuss key benefits of FIM and how WS can play an integral role in enriching IM through federation. Then, we investigate two well-known FIM solutions, *Liberty Alliance* [HW03] and *Microsoft Passport* [tr103], attempting to identify IA requirements in FIM. In addition, we describe our experimental study on those models.

The rest of this paper is organized as follows. Section 2 overviews three approaches involved in IM, along with the prior research works related to our work. Section 3 describes FIM, particularly, Liberty and Passport in detail. Section 4 discusses the role of WS in federating identities in the two models. Section 5 articulates IA requirements for FIM followed by the experimentation details in Section 6. Section 7 concludes this paper.

2 Identity Management and Related Works

In this section, we start with the discussion of IM approaches. We categorize IM approaches into the following three styles: *isolated IM*, *centralized FIM*, and *distributed FIM*. Thereafter, we discuss the core components of WS architectures.

The isolated IM model is the most conservative of the three approaches. Each business forms its own identity management domain (IMD) and has its own way of maintaining the identities of users including employees, customers, and partners. Hence, this model is simple to implement and has a tight control over user profiles. However, it is hard to achieve user convenience with this model since different IMDs are likely to have different authentication processes or mechanisms for their users and corresponding authentication policies may vary between players.

The centralized FIM model has a single identity provider (IDP) that brokers trust to other participating members or service providers (SP) in a Circle of Trust (CoT). IDP being a sole authenticator has a centralized control over the identity management task, providing easy access to all SP domains with simplicity of management and control. The drawback of this approach is a single point of failure within a CoT infrastructure in case that IDP fails to provide authentication service. User convenience can be also achieved partially in that the single sign-on (SSO) for users is only effective within SPs which belong to the same CoT.

The distributed FIM model provides a frictionless IM solution by forming a federation and making authentication a distributed task. Every member agrees to trust user identities *vouched for* by other members of the federation. This helps users maintain their segregated identities, making them portable across autonomous policy domains. It also facilitates SSO and trust, thereby allowing businesses to share the identity management cost with its partners. Microsoft Passport is based on the centralized FIM model, while Liberty Alliance aims to be the distributed FIM model.

Earlier works related to user identity management were mostly focused on a user-centric approach [DPR99], where users have control over IM functions. A simple idea of managing user identities is described in [Cha85]. They proposed the use of personal card computers to handle all payments of a user, thereby ensuring the privacy and security of the user's identity on the Web. Hagel and Singer [HS99] discussed the concept of *infomediaries* where users have to trust and rely on a third party to aggregate their information and perform IM tasks on their behalf while protecting the privacy of their information. The Novell digitalme technology [Cra] allows users to create various identity cards that can be shared on the Internet according to users' preferences. Users can control both what information is stored in each card and conditions under which it may be shared.

3 Federated Identity Management

In this section, we discuss FIM in general, Liberty Alliance and Microsoft Passport in particular. Federated identity gives the ability to securely recognize and leverage user identities owned by trusted organizations within or across CoTs, and identity federation allows organizations to securely share confidential user identities with trusted ones, without requiring users to re-enter their name and password when they access their network resources. Additionally, identity federation provides the ability to optionally and securely share user information such as their profiles or other data between various trusted applications which is subject to user consent and organizational requirements.

Two well-known FIM solutions, Liberty Alliance and Microsoft Passport have fundamentally the same goal of managing web-based identification and authentication. Both enable organizations to build IM systems that can be federated across many disparate sources. Therefore, each user can have a single network identity that provides SSO to the web sites that have implemented either or both of the systems.

3.1 Liberty Alliance

Liberty Alliance is a consortium of more than 150 companies working together towards developing an open, interoperable standard for FIM. It is aimed towards realizing the notion of a cohesive, tangible network identity, which can facilitate SSO and frictionless business operations. It is a distributed FIM model, relying on the notion of IDP and SP, as we discussed earlier. IDP is responsible for carrying out identity federation. Authentication messages or authentication requests are passed between IDP and SP. IDP and SP in Liberty Alliance Model actually facilitate WS to discover service locations and handle incoming messages from other IDP and SP.

3.2 Microsoft Passport

Microsoft Passport provides authentication services for Passport-enabled sites called participating sites. It was initially released as a service and not an open specification and precedes Liberty Alliance by at least a year. It is the underlying authentication system of Microsoft Hotmail and Microsoft Network, and it is integrated for use in Windows XP. A centralized Passport server is the only IDP in Passport model and contains users' authentication credentials and the associated unique global identifier called Passport Unique Identifier (PUID). Passport is an example of a centralized FIM model. Unlike Liberty Alliance, cookies play a major role in Passport architecture where Passport server stores and reads identity information in the form of session and browser cookies stored securely at a client side.

4 Role of Web Services in FIM

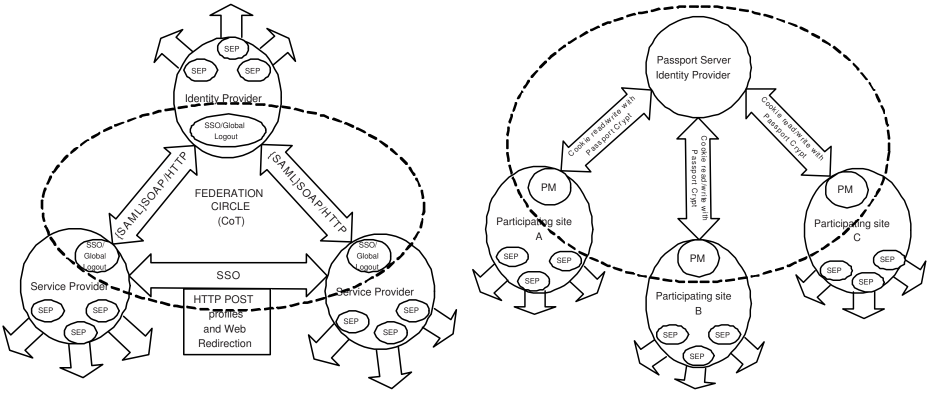
In this section, we describe the role of WS in identity federation. Identity federation usually involves three actors: IDP, SP, and users. IDP in a CoT performs the task of authentication and SP relies on IDP for authentication information of a user before granting the user access to its services. Identity federation occurs with the user's consent to federate his local identity at SP with his identity at IDP which further facilitates SSO. In this process of federation, WS architecture has four key components: consumer, SOAP, WSDL and UDDI and provides SOAP/HTTP-based standard communication vehicles among the providers [tr201]. SP can discover IDP either statically or by querying a UDDI registry. Afterwards, SP communicates with IDP by reading its WSDL from UDDI, whereby SP can exchange authentication request/response through service endpoints (SEP) specified in WSDL.

4.1 Web Services in Liberty Alliance

In Liberty Alliance, each CoT has one or more providers using SOAP/HTTP based communication channels for exchanging authentication-related information between WS endpoints. Both SP and IDP follow agreed-upon schema for federation and SSO. Security Assertion Markup Language (SAML) [HBM02] is an essential component in this process for the purpose of asserting authentication status of users between the providers. A federated sign-in at IDP would provide users with a valid session that is respected by all the SPs in its CoT. Figure 1(a) shows the WS-enabled FIM architecture for Liberty Alliance which hosts two WS components, SSO Login and Global Logout.

Federation requires a user to opt-in by providing consent for mapping his identities at IDP and SP. As a result, both IDP and SP store a *pseudonym* as a name identifier for the user. Pseudonyms are used by IDP later when the user requests an SSO. IDP vouches for SAML-based user authentication request from SP by providing SAML-based authentication response.

Global Logout WS endpoints, also called Single Logout endpoints, receive and process logout events from SP and IDP. Typically, when a user logs out from one provider, the user's SSO session which is active at the rest of providers is invalidated by sending a message to these WS endpoints. The user agent accesses Global Logout WS at IDP and indicates that all SPs, which the IDP has provided authentication for during the current session, must be notified of the session termination. Then, the user agent receives an HTTP response from IDP that confirms the completion of a global logout.



(a) Liberty Alliance model

(b) Passport model

Fig. 1. FIM Models

4.2 Web Services in Microsoft Passport

Figure 1(b) shows the Passport architecture with WS endpoints. There are WS components that make up Passport authentication service and involve the implementation of the authentication service [tr103]. The primary WS component for Passport authentication model is Login Service.

As implied by its name, Login WS is mainly in charge of the user authentication service. For instance, a user logging in to any Passport-enabled site is automatically authenticated by all other Passport-enabled sites, thereby enabling SSO. Subsequent sites receive the authentication status of the user from Login WS through a Component Configuration Document (CCD). CCD is an XML document used by Passport to facilitate the synchronization of the user's authentication status in participating sites.

5 Experimentations for Information Assurance: Metrics and Details

In this section, we describe our experimentations and results. Our goal is to measure the performance of the two models of federated identity management, particularly focusing on authentication issue which is a critical component to maintain information assurance. To measure the performance of $LibertyAlliance$ and $MicrosoftPassport$ models, we developed a set of tools to generate and monitor loads. The performance for various key operations or services–such as federation of identities and SSO–are measured for the generated workload.

To identify those key operations, we first introduce an imaginary company, called *MegaBank*. Then we attempt to have *MegaBank* play one of the following three roles as shown in Figure 1: a) MegaBank as Identity Provider, b)MegaBank as Service Provider with single third-party Identity Provider, and c)MegaBank as Service Provider with two third-party Identity Providers. There are various unpredictable factors such as the delay from user's end, which prevent us from producing a workload that is exactly similar to the real life traffic. Moreover, the workloads that we are using may differ over the scenarios depending upon the role played by the MegaBank in various scenarios. [1]

Finally we develop metrics that are used to evaluate the performance of a system. The comparison and analysis of the systems can be done by comparing the values obtained for these measured metrics. Therefore, metrics can be termed as the key points that reflect the impact of the changes in system state. We have identified certain metrics for measuring the performance of the two FIM Models. These metrics are common for both models. The measurement of these metrics is performed by applying monitors at various locations in the systems. Those monitors are embedded in the codes as software modules. A typical dialog that

[1] Workload can be categorized into test workload and real workload. Real workload is observed on a system being used for normal operations. Test workload denotes any workload used in performance studies.

occurs between the communicating parties in each FIM model consists of various time factors. The dialog between a service provider and identity provider may consist of different time factors as follows:

- *Communication Time,* $Tc_{[from,to]}$: The time an entity takes to send a request to another entity and get a response back from that entity. $Tc_{[from,to]}$ denotes where "from" is the entity at which the time is measured and "to" is the entity which sends back a response to the request made by a "from" entity. The response sent back by the "to" entity completes the communication cycle.
- *Data Access Time,* Td_{at}: The time that a service provider or an identity provider takes to retrieve a user's information or attributes from the local storage for the purpose of authentication is called the Data Access time. In Td_{at}, "at" signifies the entity at which data access time is measured. The data access time may vary depending upon the type or directory servers and data access mechanism employed.
- *Message Processing Time,* Tm_{at}: The time taken by the entities to process the message received. In Tm_{at}, "at" denotes the entity or the communicating party at which message processing time is measured.
- *Request Redirect Time,* $Tr_{[sp1,sp2]}$: The time required for redirecting a service request from one service provider to another service provider. $Tr_{[sp1,sp2]}$ denotes the time between the source service provider $sp1$ and the destination service provider $sp2$.

This section describes additional metrics, their significance, and the composition. By composition, we mean that one or more of these metrics may be composite. They may contain one or more of the time factors and the actual measurement of these time factors may depend upon the case scenario. The steps for measuring these metrics are different for Liberty Alliance and Microsoft Passport because of the differences in their architecture. Though there are a number of sub-factors that we can measure, we have limited our scope to the most important, required and relevant factors to the scope of our research.

- *Local Login Time/Service Provider Authentication Time,* A_{sp}: A_{sp} is the time taken by a principal to get authenticated at the Service Provider. This time neither facilitates federation nor SSO. The measurement of this metric is important in situations where one wants to measure the data access time at the Service Provider.
- *Identity Provider Authentication Time,* A_i: When a principal chooses to logon using the identity providers credentials, the service provider directs the principal to the identity provider site, which is one time process, when the principal signs in for the first time. A_i is the time taken by a principal to get authenticated just after when he signs in at the identity providers' site. In other words, it is obtained from Td_{sp}
- *Federation Time,* $F_{i,sp}$: For attempting a single sign-on, a principal is required to federate her/his identity at the service provider with its identity at the Identity provider. $F_{i,sp}$ consists of A_i and $Tc_{[sp,idp]}$the communication time, data access time and the message processing time.

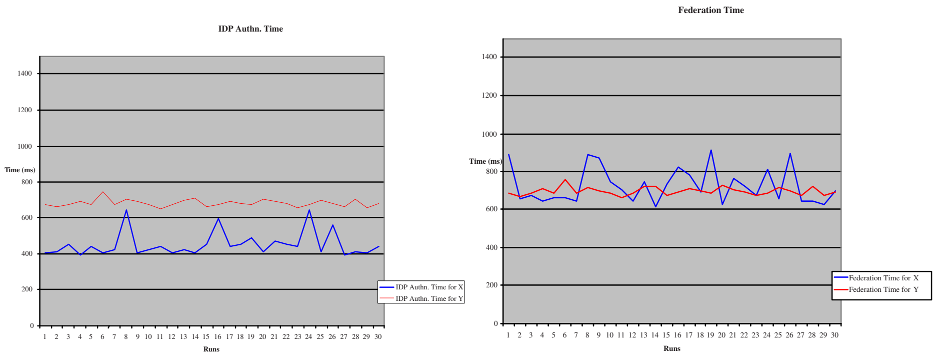
- *Single Sign-On Time,* $S_{[idp,sp]}$: Once principal's identities at various service providers are federated with her/his identity at the identity provider, s/he can access the resources at any of the service providers without re-logging within a common authentication context. This is a very important metric and is the most crucial in studying the performance of the two systems. $S_{[idp,sp]}$ consists of the communication time, the message processing time and the data access time including A_i, $Tc_{[sp1,idp]}$, $Tc_{[sp2,idp]}$ and $Tr_{[sp1,sp2]}$.

Figure 2 shows our experimentation results on authentication and federation issues based on the aforementioned metrics.

As we mentioned earlier, our experimental analysis represents a proportion or a sample of the population that may exist in the real life for both the models. Moreover, the factors that affect the performance of the system may vary with location and deployments across enterprise applications. In such cases, definitive statements cannot be made about the characteristics of all systems, but a probabilistic statement about the range in which the characteristics of most systems would fit can be made. Therefore, we have adopted a statistical approach for performance evaluation. Rather than making any directive statement about the superiority or inferiority of one of the two models, we are summarizing the results based on their characteristics. We have adopted a statistical approach whereby we can state with a certain amount of confidence that the values of the proposed metrics can lies within a specified range. Moreover, we can compare these confidence intervals (CIs) for various metrics with respect to the two models. We use the method to calculate the CIs for unpaired observations. The brief steps for calculating the CIs that we used in this work are as follows:

1. We first calculate the sample mean X_{lam} and X_{pm} for Liberty and Passport, where n is the number of observations.
   $$X_{lam} = \frac{1}{n}\sum_{i=1}^{n} X_i,\ X_{pm} = \frac{1}{n}\sum_{i=1}^{n} X_i$$
2. Next, we derive the sample standard deviations S_{lam} and S_{pm} and it gives us the standard deviation S of the mean difference.
   $$S = \sqrt{\left(\frac{S_{lam}^2}{n} + \frac{S_{pm}^2}{n}\right)}$$
3. Using the standard deviation, we compute the effective number of degrees of freedom V.
   $$V = \left\lfloor \frac{(\frac{S_{lam}^2}{n} + \frac{S_{pm}^2}{n})^2}{\frac{1}{(n+1)}(\frac{S_{lam}^2}{n})^2 + \frac{1}{(n+1)}(\frac{S_{pm}^2}{n})^2} \right\rceil$$
4. Finally we identify the confidence interval CI for the mean that can be used to determine the performance characteristics.
   $$CI = (X_{lam} - X_{pm}) \pm t_{[1-\frac{a}{2},v]}S$$

Unfortunately our results are not permitted to be available in public but we briefly describe lessons learned from this work. Our analysis demonstrated the followings: a) FIM leads us to consider several trade-offs between security and



(a) IDP authentication time

(b) Federation Time

Fig. 2. Experimentation Results

system overheads; b) organizational roles in FIM are very important to identify additional requirements related to performance factors; and c) it gives us an idea on which system and workload parameters mostly affect the performance of FIM models in given case scenarios. We believe this work can be helpful to IA practitioners for designing the enhanced FIM architectures.

6 Information Assurance Issues in FIM

As an effort to identify principal IA requirements for FIM, we discuss security and privacy concerns relevant to WS in FIM in this section. We also describe how Liberty Alliance and Microsoft Passport deal with these concerns to fulfill such requirements in their architectures.

6.1 Security Concerns in FIM

Security concerns in FIM can be observed from the perspective of the general objectives of information security: availability, integrity, and confidentiality. In addition, authorization is also an important aspect to be considered in that controlled access to federated identity information is strongly required.

The *availability* of information in FIM models concerns system reliability and timely delivery of information. In FIM models, the availability of information can be ensured by not only having a common protocol or mechanism for communicating authentication and other information between parties but also securing communication channels and messages. Channel security can be achieved using protocols like TLS1.0/SSL3.0 or other protocols like IPsec with security characteristics that are equivalent to TLS or SSL. However, these protocols can only provide security at the transport level and not at the message level. Liberty specifications strongly recommend TLS/SSL with well-known cipher suites [Wat03] for channel security. More details has been discussed in [SSA03].

Message security is important in FIM for preventing attackers and intermediaries from tampering the messages that are in transit. Improper message security generates concerns like identity theft, false authentication, and unauthorized use of resources. Web Services Security (WSS) [IBM02] tries to address these issues by providing security extensions such as digital signature and encryption to SOAP messages. Signing a SOAP payload using XML Digital Signature [ERB$^+$02] ensures the integrity of the message. The sender can sign a SOAP message with his private key. The receiver can then verify the signature with the sender's public key to see if the message has been modified. In WS architecture, public key infrastructure (PKI) can be leveraged to have organizations sign security assertions instead of issuing certificates. Liberty Alliance specifications recommend XML Digital Signature and Encryption [IDS02] for encrypting a complete SOAP message or a part of the SOAP message to maintain the *integrity* and *confidentiality* of its contents. Microsoft Passport takes an approach to encrypting cookies for securing data contained within them. Cookies store sensitive information like user profiles that can be securely accessed by authorized parties.

FIM requires communicating parties to provide controlled access of information to legitimate users. *Authorization* deals with what information a user or an application has access to or which operations a user or an application can perform. Proper authorization mechanisms are necessary in WS communication especially when the communication endpoint is across multiple hops. Liberty specifications recommend a permission-based attribute sharing mechanism, which enables users to specify authorization policies on their information that they want to share. Similarly, Microsoft Passport allows users to have their choices regarding the information they want to share with participating sites.

6.2 Privacy Concerns in FIM

Privacy is a growing concern with FIM models due to the voluminous exchange of sensitive information that occur across enterprises. Securing communication channels and encrypting messages may help preserve the privacy of relevant information only up to some extent. The security concerns that we discussed in the previous section are obviously applicable to privacy as well. In WS-enabled FIM where the receiver of a message may not be its ultimate destination, improper security measures may result in unauthorized access of user's personal information which leads to violation of privacy.

Protection of user identities and personal information can be achieved by using the principle of pseudonymity. Obfuscating message payloads can also preserve their privacy by making them accessible only by authorized parties having proper credentials or keys [MPB03]. Privacy enhancing technologies like Platform for Privacy Preference (P3P) [CCL$^+$02] provide a solution for point-to-point privacy protection based on user preferences. However, such solutions do not scale for a more open, interoperable WS architecture.

Liberty's SAML implementation uses pseudonyms constructed using pseudorandom values that have no discernable correspondence with users' identifiers at IDP or SP. The pseudonym has a meaning only in the context of the relationship between the two communicating parties. The intent is to create a non-public pseudonym so as to contravene the linkability to users' identities or activities, thereby maintaining the privacy.

Organizations using FIM models is required to follow four key principles of fair information practices which are discussed in [tr102]:

- *Notice*: Users should receive prior notice of the information practices.
- *Choice*: Users have a choice to specify what information will be used and the purpose for which the information is collected.
- *Access*: Users should be able to access and modify their personal information as and when needed.
- *Security*: Users should be assured that the organizational system is capable of securing their personal information.

Liberty specifications have recently proposed an approach to sharing user attributes on the basis of user's permission. The specifications also provide a set of guidelines that will help businesses adhere to these principles. Microsoft Passport's approach to online privacy is also based on adherence to these aforementioned principles.

7 Conclusion and Future Works

Information security and privacy issues are the key concerns in FIM because identity federation requires the exchange of sensitive user information in a highly insecure and open network. In this paper, we discussed two well-known FIM solutions, Microsoft Passport and Liberty Alliance and how WS can play an integral role in FIM. In addition, we have identified certain metrics that are crucial when considering a FIM model. These metrics are composite metrics which may consist of measuring one or more of the time factors. Also, we identified and discussed core IA requirements in FIM focusing on WS-relevant issues. We believe our work can be leveraged by the research and industry communities working on issues in identity management.

Our future work will focus on a privacy attribute management framework within Liberty Alliance which can provide users with a high level of confidence in the privacy of their personal data. Developing IA metrics for FIM is another issue that we intend to work on in the near future. It is generally believed that no single perfect set of IA metrics can be applied to all systems. Thus, we would attempt to investigate IA metrics specifically designed for FIM systems.

References

[CCL$^+$02] Lorrie Cranor, Lorrie Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, and Joseph Reagle. The platform for privacy preferences 1.0 (p3p1.0) specification. Technical report, www.w3.org/TR/2002/REC-P3P-20020416/, 2002.

[Cha85] David Chaum. Security without identification: Card computers to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985.

[Cra] Lorrie Faith Cranor. Agents of choice: Tools that facilitate notice and choice about web site data practices.

[DPR99] Herbert Damker, Ulrich Pordesch, and Martin Reichenbach. Personal reach ability and security management - negotiation of multilateral security. In *Proceedings of Multilateral Security in Communications*, Stuttgart, Germany, 1999.

[ERB$^+$02] D. Eastlake, J. Reagle, J. Boyer, B. Fox, and E. Simon. XML - signature syntax and processing. Technical report, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/, 2002.

[HBM02] Phillip Hallam-Baker and Eve Maler. Assertions and protocols for OASIS SAML. Technical report, http://www.oasis-open.org/committees/security/docs/cs-sstc-core-01.pdf, 2002.

[HS99] John Hegel and Marc Singer, editors. *Net Worth: Shaping Market When Customers Make the Rule*. Harvard Business School Press, 1999.

[HW03] Jeff Hodges and Tom Watson. Liberty architecture overview v 1.2-03. Technical report, http://www.sourceid.org/docs/sso/liberty-architecture-overview-v1.1.pdf, 2003.

[IBM02] IBM. Web services security (WSS) specifications 1.0.05. Technical report, http://www-106.ibm.com/developerworks/webservices/library/ws-secure/, 2002.

[IDS02] Takeshi Imamura, Blair Dillaway, and Ed Simon. XML encryption syntax and processing. Technical report, http://www.w3.org/TR/2002/CR-xmlenc-core-20020304/, 2002.

[MPB03] Marco Casassa Mont, Siani Pearson, and Pete Bramhall. Towards accountable management of identity and privacy: Sticky policies and enforceable tracing services. Technical report, http://www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf, 2003.

[SSA03] Prasad Shenoy, Dongwan Shin, and Gail-Joon Ahn. Towards IA-Aware web services for federated identity management. In *Proceedings of IASTED International Conference on Communication, Network, and Information Security*, pages 10–15, New York, USA, December 2003.

[tr102] Federal Trade Commission. online profiling - a report to congress, part 2. Technical report, http://www.ftc.gov/os/2000/07/onlineprofiling.htm, 2002.

[tr103] Mircrosoft Corporations. Microsoft .Net Passport Review Guide. Technical report, http://www.microsoft.com/net/services/passport/review_guide.asp, 2003.

[tr201] W3C note: Web services description language (WSDL) v 1.1. Technical report, http://www.w3.org/TR/wsdl12/, 2001.

[Wat03] Tom Watson. Liberty ID-FF implementation guidlines v 1.2.02. Technical report, Liberty Alliance Project, 2003.