# Enhancing Consumer Privacy in the Liberty Alliance Identity Federation and Web Services Frameworks

Mansour Alsaleh, Carlisle Adams
*School of Information Technology and Engineering (SITE), University of Ottawa*
{malsaleh, cadams}@site.uottawa.ca

**Abstract.** Internet usage has been growing significantly, and the issue of online privacy has become a correspondingly greater concern. Several recent surveys show that users' concern about the privacy of their personal information reduces their use of electronic businesses and Internet services; furthermore, many users choose to provide false data in order to protect their real identities. Identity federation aims to assemble an identity virtually from a user's personal information stored across several distinct identity management systems. Liberty Alliance is one of the most recognized projects in developing an open standard for federated network identity. While one of the key objectives of the Liberty Alliance is to enable consumers to protect the privacy and security of their network identity information, this paper identifies and analyzes possible privacy breaches within the Liberty identity Federation Framework and Liberty identity Web Services Framework. Proposals for improvement in both these frameworks are discussed.

## 1 Introduction

Privacy is of particular concern to Internet users. Collecting personal information without users' awareness, sharing personal information between businesses without users' consent, using personal information for purposes other than stated, and the inability to access, change, or delete personal information, are among the main privacy concerns for many users. In 2003, industry watchdog Gartner Group predicted that by 2006, the first barrier to electronic business and commerce will be user concerns over information privacy [9]. A March 2000 Business-Week/Harris Poll shows that 86% of users want a Web site to obtain opt-in consent before collecting user name, address, phone number, or financial information. The same poll shows that 88% of users support opt-in as the standard before a Web site shares personal information with others [6]. A Pew Internet & American Life Project survey in 2000 found that 54% of Internet users believe that Web site tracking of users is harmful and invasive to user privacy; 24% of users reported giving false information to a Web site and 20% gave alternative or secondary e-mail addresses to Web sites [8].

Users maintain many separate accounts on different Internet businesses and services. Web sites almost always keep a profile for each visitor; this profile will contain more Personally Identifiable Information (PII) when the user registers his/her

information (otherwise, the Web site may identify the user by other means such as a browser cookie, or an IP address). Users usually need distinct authentication credentials (e.g. user name and a password) to access their profiles. Managing user profiles is a costly process for both users and service providers. Identity federation enables users to link, assemble and control an identity virtually from separate accounts where a user can control sharing of his/her identity attributes between service providers. Identity federation defines mechanisms for enterprises to share identity information between domains. These mechanisms include single sign-on (SSO), authorization, identity mapping and account linking, and directory services. The SSO mechanism reduces redundant logons whereby a user can login once with a member of a federate group and gain access to resources of multiple members among the group without signing-on again. In addition to fewer redundant logons, identity federation has the advantages of reducing the administrative costs of user profiles for service providers and keeping more accurate and up-to-date information about users [22].

One of the early identity federation frameworks is Microsoft's Passport. It deploys a centralized framework where there is just one identity provider (Microsoft). Any time a user logs into a Passport-participating site, the site is immediately able to access the information in the user's Passport account. Users' privacy concerns (users have no privacy with respect to the identity provider which is Microsoft) and the concept of a single trusted third party led to limited adoption of this architecture [12]. Microsoft carried out a significant upgrade to Passport and changed the service name to Windows Live ID. The new service overcomes the limitation of not supporting multiple identity management by utilizing a new Microsoft model, InfoCard, which is an identity selector that enables users to manage and exchange their digital identities [5]. InfoCard supports more than one identity provider (not just Microsoft) and the identity provider can be the user machine itself. One major drawback of InfoCard is that users lose their digital identities when using a different machine (unless the user uses an external security token such as a smartcard).

Set up at the instigation of Sun Microsystems in 2001, the Liberty Alliance is a consortium of technology vendors and consumer-facing enterprises formed to develop an open standard for federated network identity. The Liberty Alliance project is based on the concept of enabling users to connect multiple sets of personal information which exist across several e-commerce providers into a single easy-to-manage federated identity. This allows for the convenience of an SSO mechanism as well as easier administration of personal information across multiple service providers [15, 26]. Liberty Alliance is one of the most prominent federated identity standard proposals.

Although one of the key objectives of Liberty Alliance is to enable consumers to protect the privacy and security of their network identity information, the multidiscipline specifications Liberty covers make it vulnerable to a variety of privacy breaches. In this paper, we identify and analyze possible privacy breaches within the Liberty Identity Federation Framework and the Liberty Identity Web Services Framework. The main focus will be on identifying privacy concerns that are not discussed at all, or in much depth in Liberty specifications or Liberty privacy and security documentations. We believe that enhancing consumer privacy in these frameworks will increase consumer trust in using Liberty-enabled providers' services and thus will lead to greater adoption of Liberty standards. Our goal is that this paper helps to complement

the current Liberty security and privacy documents by addressing possible privacy breaches and proposals for improvement.

The remainder of the paper is structured as follows. In the next section, we discuss related work. This is followed by a brief introduction to the Liberty Alliance project in 3.1. In particular, in section 3.2, we illustrate the concept of identity federation and SSO through a simple user case scenario. In section 4, we discuss some of the privacy requirements in identity federation systems and we highlight best privacy practices. In section 5.1, we give a detailed user case scenario that integrates the usage of both the Liberty Identity Federation Framework (ID-FF) and the Liberty Identity Web Services Framework (ID-WSF). In Section 5.2 we then identify and analyze possible privacy breaches within the different transactions of the given scenario and discuss proposals for improvement. We propose three new services that can merge with the current Liberty ID-FF and ID-WSF frameworks in section 5.3. We conclude by summarizing our recommendations to enhance consumer privacy within the Liberty frameworks.

## 2 Related Work

In addition to specification documents, Liberty Alliance has published several non-normative documents pertaining to security and privacy in their multi-level specifications. In [24], the author addressed some privacy laws, privacy and security fair information practices, and implementation guidance for organizations using the Liberty Alliance specifications. In particular, [7, 14] provided an overview of the security and privacy issues in ID-WSF technology and briefly explained potential security and privacy ramifications of the technology used in ID-WSF. The authors in [16] investigated the topic of identity theft in Liberty Alliance Project and showed how a cross-organizational and a vendor-neutral method of approaching the problem can work where piecemeal approaches will not. Varney and Sheckler [25] gave guidelines to assist businesses deploying Liberty-enabled solutions by identifying and addressing certain privacy and security issues that arise in business-to-consumer applications. The authors in [1] provided a high-level example of how to manage privacy preferences within Liberty Alliance's ID-WSF framework.

Recently, some academic publications have discussed the security and privacy in the Liberty Alliance project. Pfitzmann [19] evaluated the privacy of the Liberty Alliance phase 1 specifications that concern the browser single sign-on protocol. Later, an update for this paper evaluated the privacy on the same part of the Liberty project but for phase 2 of the specifications. The majority of the privacy concerns in this paper are about the user giving clear consents for transactions that happen between the different providers. A non-technical overview in [17] showed some scenarios by which federated identity management can actually help address certain aspects of the identity theft problem. The paper pointed out that federated identity management connects together previously isolated collections of identity information, which might be perceived as contributing to the identity theft problem because it exacerbates the ramifications of any successful attack. The concern is that if one of the user identity provider accounts is compromised, then all the related service provider federated accounts will

be compromised as well. The paper then suggested new mechanisms against identity theft in these scenarios, mainly in the authentication part. The authors in [4] proposed a flexible and privacy-preserving approach that allowed a user to establish a unique identifier and then proceed to establish other complex identity attributes in a federation. A solution to the problem of identity theft based on cryptographic techniques was presented.

Ahn and Lam [2] investigated the privacy issues in federated identity management focusing on the Liberty Alliance project. The authors discussed the privacy requirements using business scenarios. They proposed a privacy preferences expression language that uses the user preferences language PREP as a basis. The paper did not give any user interface proposal that could be used to store his/her preferences in the suggested customized PREP language. Easy-to-use and clear user interface that give the user full control in specifying privacy preferences for his/her personal information seems to be a significant challenge. The authors in [3] identified information assurance requirements in federated identity management. The paper briefly discussed privacy concerns in federated identity management with the Liberty Alliance project. A security model for authentication and access control for federated systems is described in [23]. The model supports single sign-on for users, a high level of autonomy for database custodians, and low maintenance overhead. The paper is concerned with securing read-only access to sensitive data as it is transmitted and delivered as part of federated database projects. A short survey of privacy issues within current browser-based attribute-exchange protocols is given in [21]; moreover, this paper presented design decisions that are mandatory to fulfill the privacy requirements. Pfitzmann and Waidner [20] gave an overview of the security and privacy properties desirable for the zero-footprint and browser-stateless constraints. The paper proposed a new protocol for browser-based attribute-exchange with better privacy and scalability. The privacy policies for attributes exchange are discussed in detail. In [11], the author first discussed the shortcomings of the existing Attribute Release Policies (ARP). XACML was then recommended as a suitable base language for ARPs. The proposed architecture suggested the integration of XACML ARPs into SAML-based identity providers and it specified the policy evaluation workflows. Gross [10] went through a security analysis of the SAML single sign-on browser profile, revealing several security flaws in the Liberty Alliance specification of this profile. Countermeasures and solutions to these attacks are proposed.

In this paper, we look at the Liberty ID-FF and ID-WSF and identify potential privacy breaches that were not discussed at all, or in much depth in the above work.

## 3 Overview of Liberty Alliance Project

In section 3.1 we give a brief introduction to the Liberty Alliance project. In section 3.2, we provide a simple user case scenario that illustrates the concept of identity federation and SSO.

### 3.1 Liberty Alliance Project

The Liberty Alliance project objective is to create open, technical specifications that enable SSO mechanism through federated network identification using emerging network access devices, and to support a permission-based attribute sharing framework to enable users' control over the use and disclosure of their personal information. The Liberty Alliance project has obtained support from over 150 well known businesses and organizations in the last few years and they were involved in the development of the specifications. The Liberty architecture consists of a multi-level specification set that has three major components. First is the Liberty ID-FF which defines a framework for federating identities and a mechanism for SSO using a federated identity. ID-FF allows a user with multiple accounts at different Liberty-enabled (LE) sites to link these accounts for future SSO. The second component is the Liberty ID-WSF which defines a framework for Web services that allows providers to share users' identities in a permission-based mode. ID-WSF offers features like Permission Based Attribute Sharing, Identity Service Discovery (to discover identity and attribute providers), and Interaction Service (a mechanism to obtain permissions from a user). The third is the Liberty Identity Service Interface Specifications (ID-SIS) that defines service interfaces for each identity-based Web service so that providers can exchange different parts of identity interoperably. These might include services such as registration, contact book, calendar, geo-location, or alerts [13-15, 26]. The privacy analysis in this paper is for the Liberty ID-FF version 1.2 and ID-WSF version 2.0. The Security Assertion Markup Language (SAML) version 2.0, an OASIS Standard, includes many new features derived from the Liberty ID-FF v1.2 specification that were contributed to the OASIS Security Services TC. Some new key features are the following: the use of pseudonyms, attribute profiles for attribute exchange, single logout, common domain cookie for identity provider discovery, and metadata for expressing SAML configuration. The new added features in SAML V2.0 enable SSO and Identity federation mechanisms. Therefore, SAML V2.0 can supersede the Liberty ID-FF V1.2 [18].

### 3.2 Liberty Use Case Scenario

Identity federation and SSO are the two main features offered by the Liberty Alliance project (ID-FF in particular). To best describe these features, we will go through the following use case scenario. In this scenario, a sales employee (SE) in a hardware company (compABC) goes to a business exhibition in a different province to promote compABC's new product. SE needs to book a hotel room, so she checks her favorite hotels-search Web site (hotserABC) to find a good hotel deal that is close from the exhibition location. hotserABC identifies SE after she logs in using her credentials (e.g., user name and a password). All that is required is to choose the hotel and specify the booking date where hotserABC will locate her profile and book the room. Moreover, SE gives her consent to hotserABC to introduce her to some members of the affinity group (e.g., car rental Web site). hotserABC is an LE Web site and it is SE's identity provider (IdP) in this scenario. At a later time, she clicks on a car rental company (carrntABC) that is a member of the affinity group (or the circle of trust, CoT).

carrntABC, which is SE's service provider (SP), will recognize that the visitor is an LE user and that hotserABC is the visitor's IdP. SE may have a local account with carrntABC and in this case, she will typically login to carrntABC. carrntABC will offer to federate her local identity with her IdP, hotserABC, where she gives her consent to federate.

Identity federation between the two Web sites will enable the use of an SSO mechanism. If SE logs in to hotserABC and then visits carrntABC (while the Web session is still valid with hotserABC), she will not need to login to carrntABC. In fact, carrntABC will get authentication assertions from her IdP (either through browser redirect or a back-channel) that SE has been already authenticated with the IdP. When SE logs out from hotserABC, the authentication status (logout notice) is sent by hotserABC to carrntABC and all other SPs within the CoT where SE identity federation occurs with her IdP (and which were visited within the same Web session). Furthermore, Identity federation will enable the IdP and SP to exchange SE's personal information attributes upon her permission. For example, carrntABC will get SE's geographical information and perhaps her credit card number from hotserABC in order to conduct the car rental transaction. Identity federation does not imply that IdP will expose user identity by sharing user's identifiable attributes with the SP. The user IdP always shares a unique pseudonym with the SP to identify the user. This unique pseudonym is valid just between these two providers and means nothing to any other provider in the CoT. Therefore, if the user wants to conceal her identity from the SP, her IdP can provide authentication status (and maybe authorization information as well) to the SP by using this unique pseudonym that will refer to the user and preserve her anonymity. In this case, the SP still gets some non-identifiable attributes about the user (e.g., time zone information for better customization). SE can eliminate linkage between her accounts at an identity provider and a service provider, such that the identity provider no longer provides user identity to the service provider, and the service provider no longer accepts user identity from the identity provider. This process is called defederation. Within the same CoT, the user can have multiple identities linked to one or more identity providers. The user can choose which IdP to federate with when she visits a SP. A more detailed scenario will be provided in section 5.1 that will show the ID-WSF key features and will reveal more underlying layers.

## 4 Privacy Requirements in Identity Federation

Identity federation architectures have many components that need to satisfy user privacy concerns. The Liberty Alliance project takes into consideration different fair information practices; in particular, the Organization for Economic Co-operation and Development (OECD) and the Online Privacy Alliance (OPA) guidelines. Using these guidelines, Liberty offers the following set of fair information practices [24]:

- **Notice:** Consumer-facing LE Providers should provide to the user clear notice of who is collecting the information, what information they collect, how they collect it, how they provide choice, access, security, quality, relevance and timeliness to

users, whether they disclose the information collected to other entities, and whether other entities are collecting information through them.

- **Choice:** Consumer-facing LE Providers should offer users choices, to the extent appropriate given the circumstances, regarding what PII is collected and how the PII is used beyond the use for which the information was provided. In addition, consumer facing LE Providers should allow users to review, verify, or update consents previously given or denied.
- **User Access to PII:** Consumer-facing LE Providers that maintain PII should offer, consistent with and as required by relevant law, a user reasonable access to view the non-proprietary PII that it collects from the user or maintains about him.
- **Complaint Resolution:** LE Providers should offer a complaint resolution mechanism for users who believe their PII has been mishandled.
- **Relevance:** LE Providers should use PII for the purpose for which it was collected, or the purposes about which the user has consented.
- **Quality:** Consumer-facing LE Providers that collect and maintain PII should permit users a reasonable opportunity to provide corrections to the PII that is stored by such entities.
- **Timeliness:** LE Providers should retain PII only so long as is necessary or requested and consistent with a retention policy accepted by the user.
- **Security:** LE Providers should take reasonable steps to protect and provide an adequate level of security for PII.

## 5 Privacy Analysis of Liberty ID-FF and ID-WSF

In this section we present a detailed use case scenario, and identify possible privacy breaches within the different transactions of the scenario and discuss proposals for improvement.

### 5.1 Use Case Scenario using Liberty ID-FF and ID-WSF

In this section, we will use a more detailed scenario than the one given in Section 3.2 to show typical message flow between the different parties. The scenario will integrate the usage of both the Liberty ID-FF and ID-WSF. In this scenario, a user (usrABC) deals with an online payment Web site, payABC, that keeps some of the user attributes (e.g., name, address, credit card information, and so on). Several e-commerce Web sites have business relationships with payABC and they are within the same CoT. usrABC wants a cell phone, so she subscribes first with a wireless service provider and then she can buy a cell phone. Therefore she will visit a phone service provider (phnABC) to sign a wireless service contract. Next, usrABC will visit an online electronics store (eleABC) to buy a cell phone that is compatible with phnABC service. The typical sequence diagram for the identity federation process between the identity provider and the service providers is depicted in Figure 1.

In this scenario, it is assumed that identity federation has occurred between phnABC and payABC, and between eleABC and payABC. Thus, there are business relationships between these Web sites and they are in the same CoT. In step 1, the user visits the phnABC Web site where she is redirected to the payABC Web site since she has not been authenticated (step 2.a and 2.b). payABC will authenticate the user by asking her to provide her credentials in case she has not yet been authenticated. Then, payABC as usrABC's IdP redirects her back to the SP1 Web site (phnABC) with an artifact that points to the corresponding authentication assertion. phABC will use the artifact and send a back-channel Get SAML Assertion message to the IdP in step 4.a. The IdP (payABC) replies with the corresponding SAML authentication assertion in step 4.b that indicates that the user is authenticated.

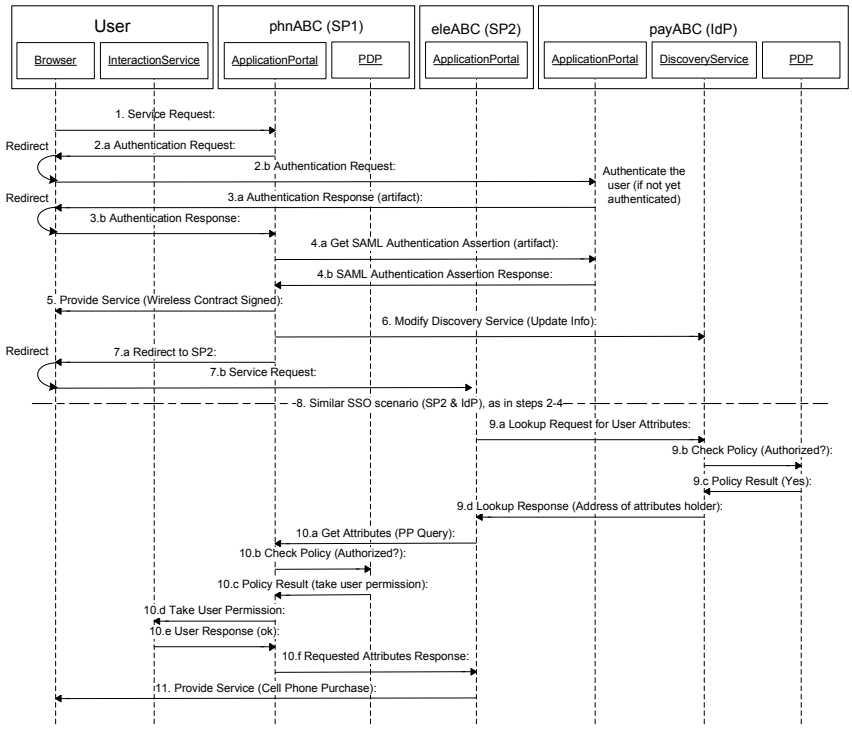


**Fig. 1.** User case scenario typical sequence flow using the Liberty ID-FF and ID-WSF.

Next, the user will be informed of the SSO confirmation and in step 5, chooses her wireless plan. The SP1 (phnABC) needs some basic information about the user (e.g., name, address, or credit card information) in order to complete the wireless contract. In this case, phnABC either: (a) asks the user for her personal information which is then provided (e.g., by completing a form); (b) has an old profile of the user (local

account) and asks the user for any needed updates; or (c) checks with the discovery service (which is hosted by the IdP in this example) and receives the needed information from the corresponding Attribute Provider (which is the IdP). The way of obtaining user's information is both a design choice and user choice. SP1 maintains the user's attributes (e.g., wireless service type, SIM card compatibility) and is able to act as an Attribute Provider. By being requested by usrABC or by asking permission from the user (either immediately via a Web form if the user is still connected to the Web site, or via the Interaction Service), SP1 registers its resource offering to the Discovery Service (DS). This process is performed by sending an ID-WSF Discovery Service Modify message as in step 6.

Now, since the user needs a cell phone to use the wireless service, phnABC offers the user links to online electronic stores to order the needed device. These stores are expected to have business relationships with phnABC, and most likely they are within the same CoT. The user picks eleABC and she is directed to their Web site in step 7. Note that the user has the choice to visit different electronic stores and it is not necessary to be redirected from phnABC. In step 8, the user is authenticated by her IdP (payABC) using the SSO mechanism in a similar way as steps 2 to 4. After authentication confirmation, the user gets service from SP2. eleABC needs to know more about the user wireless service to offer her the sales promotions on the compatible devices (which are cell phones). SP2 does not maintain user attributes. Therefore, at the request of the user, SP2 tries to retrieve the user's attributes from other Web sites. This process is achieved by sending the ID-WSF Query message (lookup request) to DS in step 9.a. Note that SP2 uses ResourceOffering of DS, which it received from IdP with the ID-FF AuthnResponse (i.e., ResourceOffering of DS is embedded in the ID-FF AuthnResponse that was exchanged earlier). In step 9.b, the IdP acts as a Policy Enforcement Point (PEP) and sends a request to the Policy Decision Point (PDP) to find out whether SP2 is authorized to get information about the attribute provider possessing the user attributes (e.g. WSDL for the desired service). The access policy set by the user in the IdP PDP allows this in step 9.c. In this scenario, the IdP is both a PEP and a PDP. It is possible that the PDP service is hosted by another service or identity provider within the same CoT. In step 9.d, the DS responds to SP2 with an ID-WSF Discovery Service QueryResponse in which ResourceOfferings (by SP1) that match with specified ResourceID and ServiceType are embedded. SP2 receives SP1's ResourceOffering, and sends an ID-SIS Personal Profile Query message to SP1 in step 10.a (Get Attributes), to receive the necessary attributes of the user. This message is defined in the ID-WSF Data Service Template specification. SP1 checks its local policy by sending an authorization request to the hosted PDP service as in step 10.b (SP1 is both a PEP and a PDP). Since the user never gave permission for SP2, there is no permit or deny policy result. Therefore, SP1 requires the user permission first, if she is available online. SP1 sends a request for user permission in step 10.d to the Interaction Service (IS). IS is often a user agent that enables providers to interact with the owner of a resource to obtain his/her consent for particular resource exposure. After the user gives consent in step 10.e, SP1 responds to SP2 with an ID-SIS Personal Profile QueryResponse message in which the user's attributes (e.g., SIM type) are embedded (step 10.f). The user will then be able to see the sales promotions on compatible cell phones and purchase the one she likes. Likewise, SP2 can obtain

needed user information (e.g., name, address, or credit card information) by requesting the user IdP or contacting the user SP1.

In general, service providers can register some of the user's attributes with the user DS upon his/her permission/request. For instance, browsing or shopping preferences may be kept at the SP. In the Liberty Alliance project, steps 2, 3, 4, and 8 are defined by the Liberty ID-FF specification; steps 6, 9, 10.b, 10.c, 10.d, and 10.e are defined by the Liberty ID-WSF specification; and steps 10.a and 10.f are defined by the Liberty ID-SIS specification. However, the PDP services are outside the scope of Liberty.

### 5.2 Possible Privacy Breaches: Identification, Analysis, and Proposals

We now identify and analyze possible privacy breaches and concerns within the Liberty ID-FF and ID-WSF frameworks throughout the scenario presented in 5.1. Moreover, we propose several improvements to the frameworks to enhance consumer privacy. Most of the privacy issues discussed here are not identified within Liberty specification documents or non-normative security and privacy documents (e.g. [14, 24]). In addition, we will clarify any privacy concerns that are not clearly explained. In this privacy analysis, most of the identified possible privacy breaches are not necessarily because of direct privacy flaws in the Liberty specifications. In fact, the various design options in resolving the non-determinism of the Liberty specifications are what could cause the majority of these privacy breaches. Moreover, some of these breaches are indirect results of privacy weaknesses in Internet protocols and browsers, upon which the Liberty specifications are built. It is also important to note that the proposed solutions to the identified privacy breaches are not intended to be complete, fully-specified solutions. Rather, many of these proposals are actually recommendations or improvements to enhance consumer privacy in a general sense. More strict, privacy-aware, and comprehensive Liberty specifications (taking these proposals into consideration) will help to diminish these privacy concerns; ultimately, this will enhance consumer privacy in federated frameworks.

In the CoT, the user usually trusts some providers more than others. Identity providers are usually the most trusted parties. In fact, the user chooses the IdP because she trusts it more than other providers. The same case applies to the user attribute provider. IdPs themselves trust some SPs more than others and so they deal with them differently according to the SPs' security and privacy policies and practices. Moreover, providers interact with the Liberty services differently according to the trustworthiness of the provider hosting the service. We will assume this in the discussion below. For each subsection, we will list the possible privacy breaches together with the proposed solutions.

#### 5.2.1 Identity Federation

- ***Privacy Concern.*** The idea of IdP introducing the user to members of the affinity group seems a simple direct concept, but this introduction could lead to a privacy contravention. It is not sufficient that IdP gets a general user consent to introduce the user. Some SPs' privacy polices may not match with the user privacy preferences. In this case, giving only one general consent may lead to a privacy breach.

*Proposed Solution.* The IdP needs to get a user consent for every single introduction with a member in the CoT. Moreover, the user needs to have the choice of knowing the privacy practices of every member that s/he will be introduced to and whether it matches the user's privacy preferences or not. This seems to be a lot of work for the user (since one of the Liberty objectives is to enable simplified and fast user sign-on through federated network identification). However, aside from the fact that this introduction only happens once, there are several ways to facilitate the verification of providers' privacy polices by the user. As we propose in 5.3.1, if the user can specify the privacy preferences in advance and there is an automated mechanism to compare SP privacy policy with the user privacy preferences, then this can act in place of the user and give warnings in case of discrepancies. If it is difficult to go through this process before the introduction step, then this can be done when the user visits the SP and before federation. Adding a new member to the affinity group at a later time requires obtaining another consent from the user for introduction. In this case, the IdP will either interact with the user via the Interaction Service, or wait for the user login in order to get the introduction permission for the new member. The IdP should enable a mechanism for the user to opt-out from the introduction consent for each member independently.

- ***Privacy Concern.*** Nonrepudiable clear user consent for Identity federation between IdP and SP is another important requirement. Giving this consent to the SP side may cause some privacy impacts. This is because any SP is always trusted less than other providers and it is not easy to prove that the user has given consent for the identity federation between SP and IdP.

  *Proposed Solution.* It is always preferable that the user gives this consent to the IdP side [19]. Therefore, there should be a mechanism to enable the SP to interact with the user IdP through a back-channel and request a user consent. Then the IdP will contact the user via the user agent interaction service as defined in ID-WSF. In this case, the IdP will probably authenticate the user first and then get a nonrepudiable user consent.

- ***Privacy Concern.*** Some design options in the Liberty specification enable SPs (especially the ones to whom a user agrees to be introduced) to know some basic information about the user even before federating the identity with the user IdP. Examples of this information are user IdPs list, user preferred IdP (or the most recently established IdP session which is the last one in the list), and other introduction details. Moreover, SPs could exchange such information with each other.

  *Proposed Solution.* Introduction information should remain private (by both the user and his IdP) regardless of what introduction technique is used, either via the Identity Provider Introduction Profile (i.e. Common Domain Cookie) or when the user agent is a LE client or proxy (LECP). When the user gives his consent to be introduced to a SP, the SP should not know any information about this introduction until the user visits the SP website and he wants to federate. For example, if the user has more than one IdP, then the SP should not know the user's preferred IdP unless the user wants to federate his identity with the SP. The SP (where the user federated his identity) should protect the privacy of this information (user IdPs list and user preferred IdP). Furthermore, other SPs should not even know that the user has given consent to be introduced to a specific SP.

### 5.2.2 Single Sign-On

- ***Privacy Concern.*** Federation domain cookie: one of the design choices in ID-FF is to use a federation common domain cookie. This cookie can be used to find out whether the user has been authenticated recently by the IdP. Note that the most recently established identity provider session is the last one in the list. This cookie is accessible by any federated SP in the CoT (when the user visits the SP Web site). This represents a privacy breach since other members in the CoT do not need to always know the user's authentication status (the most recent IdP that authenticated the user). For example, in our scenario, if the user has a local account with SP2 and wants to access the SP2 Web site using only her local credentials, then it is not necessary for SP2 to know her authentication status with her IdP.

  *Proposed Solution.* This cookie should not be used to reveal user authentication status (the most recent IdP that authenticated the user). Moreover, this cookie should not divulge the user's preferred IdP or any other information (other than a list of user IdPs). If we remove the restriction that the most recently established IdP session should be the last one in the common domain cookie IdPs list (so the list becomes random), then the visited SP would not be able to discover the last IdP the user logged into. SP should always be able to contact the user IdP through a back-channel and request user authentication status if necessary.

- ***Privacy Concern.*** Browser redirect for SSO: The ID-FF specification has the option for browser-redirect messages to carry some information. This information may contain users' personal information (either identifiable or not). Since redirect message length is limited and it is not usually encrypted, this is a privacy breach (in case of eavesdropping attacks).

  *Proposed Solution.* There should be a strict rule to not include any valuable information in the redirect itself. For example, in step 3.a, the artifact that comes with the authentication response redirect should not contain any user PII. The artifact should be always an arbitrary number that is known only to the IdP. Any PII that the IdP needs to send to the SP should be through a back-channel between them using encrypted SAML assertions.

- ***Privacy Concern.*** Redirection between SPs: When the user is redirected from SP1 to SP2, SP2 will know that the user came from SP1. This is a potential user privacy breach as an indirect result of privacy weakness in Internet protocols and browsers. Let us assume that SP1 and SP2 have different access policies to the user attributes stored in her IdP, so SP1 may get a user attribute that SP2 is not authorized to get and vice versa. SP1 gets a non-identifiable attribute att1 from the user IdP according to the user privacy policy and SP2 gets a non-identifiable attribute att2 from the user IdP according to the corresponding user privacy policy. SP1 is not authorized to get att2 and SP2 is not authorized to get att1 where none of them is intended to know any PII about the user. The IdP uses a unique user pseudonym to deal with each SP, so SP1 and SP2 have no way to link the user. However if SP2 knows that the user was redirected from SP1, then SP2 knows it is the same user and they can exchange att1 and att2 illegally. Moreover, knowing att1 and att2 could lead to deducing identifiable attributes and may reveal user identity. In addition, SP2 may show customized ads for the user knowing that she just visited phnABC.

*Proposed Solution.* This situation requires more attention from the user IdP. For example, the IdP may decide not to expose att2 to SP2 when it notices successive authentication requests (SP1 followed by SP2). An audit trail mechanism at either a trusted third party or the IdP could help in discovering such cooperation so that the appropriate actions are taken.

- ***Privacy Concern.*** Authentication information: federated SPs have the right to re-authenticate the user (via his IdP) whenever they want. Moreover, they can query the user IdP for the authentication method and other related detail (e.g., password length). This information helps SPs to evaluate the authentication mechanism. The SP may ask for stronger authentication or ask the user to re-authenticate before carrying out some transactions at the SP. However, this information can be a threat to the user privacy and security in the case of a malicious SP. The authentication method information and authentication repetition can help the attacker to figure out user access credentials.

  *Proposed Solution.* To limit these consequences, the user should have control over which SPs can get this information, either through direct consent or through her privacy preferences. Furthermore, the user IdP may warn the user after a specific number of re-authentications within the same session, or apply strict security mechanisms for further re-authentications.

#### 5.2.3 Discovery Service

- ***Privacy Concern.*** If the user policy within DS PDP allows the SP to get the address of the user attribute resource holder, the SP may locally store the address information. When the user changes the DS PDP at a later time, the same SP may no longer be allowed to get the address of the resource holder. However, the SP still has the resource address stored locally.

  *Proposed Solution.* The SP must not store the resource address after getting the needed resources. The existence of a mandatory trusted third party that can monitor SP privacy policies and monitor privacy practices can help in diminishing this privacy breach. Another option is that the DS should give the SP the resource address in an artifact with a timestamp (signed by the DS). So that the resource holder (Attribute Provider) will accept the SP attribute request only if the artifact is not expired.

- ***Privacy Concern.*** Using the current ID-WSF specification, the SP can request resource-holder address for more than one user attribute within the same request message as in step 9.a; however the SP may use only one Usage Directive SOAP header to specify only one usage purpose and other usage information (e.g., retention time). This may lead to a privacy breach since the declared purpose may apply only to some requested attributes.

  *Proposed Solution.* There must be a separate Usage Directive SOAP header for each attribute resource-holder address where the attribute requester must send a request that contains the purpose for the request, the retention period, and other necessary usage information. The response should contain elements for any privacy obligations that are to be imposed upon the requester. Alternatively, if the SP will request more than one address in one lookup request message with one Usage Di-

rective header, then there should be a standard way to express more than one purpose and other usage information within the single usage field of the lookup request.

- ***Privacy Concern.*** Privacy expression language: Lack of standard privacy expressions could lead to inconsistent interpretation of data privacy directives.
  *Proposed Solution.* A standard fine-grained, machine-readable, and dynamic privacy expression language (e.g., XACML) will enable providers to understand the syntax and semantics of privacy elements. The standard language will be used by both the PDP at the discovery service and the PDP at the attribute provider.

#### 5.2.4 Interaction Service

- ***Privacy Concern.*** The user SP (or may be the user Attribute Provider or IdP) can fabricate user consent. Moreover, an unencrypted channel between the user and one of her providers may enable the attacker to illegitimately post a user consent. In the ID-WSF IS specification, the `<InteractionRequest>` can include a "`signed`" attribute which indicates that recipient (e.g., IS) should attempt to obtain a signed `<InteractionStatement>` from the user, so the SP can ask the user to sign his consent. However, it is not clear how the user can control the integrity of either the request or the response. The user has no direct way to force the SP to sign a request for consent. Moreover, the user can not sign the response if the SP did not ask for the signature. This enables user non-repudiation (user can not deny his consent) but not SP non-repudiation.
  *Proposed Solution.* There must be a mechanism in the specification to enable users to control the integrity of consent request messages. Furthermore, it is usually hard for users to manage digital signature mechanisms. Hence, it is more appropriate that IS signs user consents on behalf of the user. This however requires that the user logs in to the IS first (e.g., userID and password) before giving his consent. In this case, the IS must be trusted by the user.
- ***Privacy Concern.*** ISs hosted by other providers may have privacy impacts.
  *Proposed Solution.* If the IS is not hosted by the user agent itself then the provider hosting the user IS should be very trusted by the user. The fact that the interaction service is responsible for gathering user consents makes it a very sensitive service. User IdP is one trusted provider that could host user IS.
- ***Privacy Concern.*** With the current ID-WSF specification, SP is able to deny its query to the user, as well as user consent (or user deny) returned. There is no suggested way that enables the user or a trusted third party to verify this exchange.
  *Proposed Solution.* SP queries to the user should be recorded by the interaction service. SPs should digitally sign each query to the user; moreover, SPs should sign a confirmation of receipt for the user consent (or denial) together with the request itself (with timestamp). This provides an audit trail mechanism in case of any dispute.

### 5.2.5 User Attribute Access Control

- ***Privacy Concern.*** SP cooperation: if the user deals with two SPs, and each of them knows some identifiable attributes of a user, then there is a risk of attribute exchange between them.

  *Proposed Solution.* An audit trail mechanism can help in exposing such leakages. The fact that the user can check her personal information usage will enable her to discover any unauthorized attribute sharing. The existence of a trusted third party for the audit trail will give more confidence to the user. In addition, the existence of a seal service (as in section 5.3.2) will enable the user to carefully select her SPs.

- ***Privacy Concern.*** Attribute deduction: if an SP collects more than one non-identifiable attribute about the same user for different needs on different sessions, this SP may be able to deduce an identifiable user attribute that leads to user identity. Furthermore, if more than one SP collects non-identifiable attributes about the user and they are able to infer that it is the same user, then they may work together to deduce an identifiable user attribute.

  *Proposed Solution.* A privacy seal trusted third party that can certify and monitor SP privacy policies, monitor privacy practices, and monitor cooperation, can help to diminish this privacy concern. More privacy precautions are also needed by attribute providers.

- ***Privacy Concern.*** ID-WSF architecture enables an SP to request more than one user attribute from the attribute provider within the same request message as in step 10.a (the provided user scenario in section 5.1); however the attribute requester may use only one Usage Directive SOAP header to specify the usage purpose and other usage information. This may violate user privacy since the declared purpose and other directives may apply only to some requested attributes. Moreover, the attribute provider response could have only one field for attribute obligations and other usage directives.

  *Proposed Solution.* There must be a separate Usage Directive SOAP header for each attribute, and the attribute requester must send a request that contains the purpose for each attribute and any other necessary data privacy directives (preferably using a standard usage directive language). The response should contain elements for any privacy obligations that are to be imposed upon the requester. (See Discovery Service privacy concern above.)

- ***Privacy Concern.*** If the attribute provider relies on the discovery service to be the PEP, then this could lead to a privacy violation. The SP can reuse or share the information about the attribute provider holding the user's attributes, so the same SP or other providers may access the user's attributes illegitimately.

  *Proposed Solution.* Both the discovery service and the attribute provider should act as a PEP. At the attribute provider, the PEP must always be designed as a back-line guard by the entity hosting or exposing the resource (as in step 10). On the other hand, the discovery service PEP acts as a first-line guard for user information access (as in step 9).

- ***Privacy Concern.*** If there is a conflict between the attribute provider local access control policy and the user privacy policy at the attribute provider PDP, then unexpected decision results may occur.

*Proposed Solution.* Each attribute provider should predefine a conflict strategy to deal with this case. For example, a deny-overrides combining algorithm (see XACML) can be used to deny the attribute request if either policy denies it.

### 5.3 Proposal for New Services in ID-FF and ID-WSF

In this section, we propose three new services that can merge with the current Liberty ID-FF and ID-WSF frameworks. These services enhance user privacy when using Liberty-enabled sites and services.

#### 5.3.1 User Privacy Preferences Service

One of the main objectives of identity federation is to enable simplified and fast user sign-on while browsing to different service providers. Thus, when the user visits an SP Web site, he will be automatically signed on and some of his information may be transferred from his IdP to the visited SP (upon a previous user permission) for better customization and service. Nevertheless, as we noted in the previous section, to enhance user privacy, we need to make the user aware of the excessive transactions occuring and to request his permission in many cases. Consequently, the user may be overwhelmed by many access permission requests and so identity federation will no longer be a fast, easy-to-use mechanism.

We propose a user privacy preferences service that can be part of the ID-WSF specification. The new service will enable the user to enter his default privacy preferences. A user can have several preferences categorized by a generic classification of SPs according to different levels of privacy practices. The best place to host this service appears to be the user IdP. A Liberty-enabled user agent can host this service too; however, the user may then not be able to use his privacy preferences in case of using a different machine. Using this service, some access permission requests (e.g., step 10.d) can be directed first to the user privacy preferences service to find out whether the user's default preferences allow the requested access.

This new service will raise some new privacy concerns. For instance, SPs should not know the user's privacy preferences unless required. A detailed specification is needed for this service; however, the service does not have to be mandatory but can be a design option when deploying the Liberty ID-WSF specification. It is also possible to integrate the proposed service with some existing techniques such as, for example, browser-based privacy preferences languages (e.g., APPEL in P3P).

#### 5.3.2 Privacy Seal Service

It is always difficult to ensure that a user attribute requester will adhere to its stated privacy policy and its declared purposes and other attribute usage directives. If no technical mechanism exists, the user will need to rely on his trust of the attribute requester. Here, we propose a Liberty privacy seal service by a trusted third party that can certify and monitor identity and service providers' privacy policies, monitor privacy practices, and resolve any user disputes. The user will need this service in many cases. At the time of federation introduction, this service will assure the user that an SP privacy policy accurately states what personal information the SP gathers and how

it is handled. Moreover, this service can be consulted by an attribute provider PDP before revealing any information. Typically, a trusted third party is the best place to host the service. The service can be part of the ID-WSF specification. It can help tremendously in increasing user trust in using Liberty-enabled services. It is important to note, however, that Web privacy seal organizations do not always revoke a seal certification from a business even after privacy violations have occurred. This indicates the need for strict rules (e.g., an automatic revocation mechanism) when deploying a Liberty seal service.

#### 5.3.3 Audit Trail Service

Using the existing Liberty architecture, a user may have many privacy concerns about the different providers exchanging his personal information without his permission. In addition, many other transactions need to be recorded (for example, transactions in steps 6, 9, and 10). The user needs to know if any privacy violation has been committed by any SP so he can take the appropriate action for future transactions and so that he can update his privacy preferences accordingly. An audit trail service as part of the Liberty architecture can achieve this task. The user (and probably his IdP) can access this service to review the transaction record. The provider hosting this service may need to notify the user in case of potentially dangerous violations. This provider may be the same one who hosts the Liberty privacy seal service.

## 6 Conclusion

This paper has looked at the Liberty Identity Federation and the Liberty Identity Web Services frameworks from the perspective of user privacy. In particular, we presented a detailed user experience scenario that integrates both these frameworks, and identified and analyzed possible privacy breaches within the different transactions of the scenario. In each case, we discussed proposals for improvements that would enhance privacy. Furthermore, three new services were proposed (a user privacy preferences service, a privacy seal service, and an audit trail service) that can merge with the current Liberty ID-FF and ID-WSF frameworks.

Some directions for future work in this area include finding additional privacy breaches, analyzing SAML V2.0 and the Liberty Identity Service Interface Specifications (ID-SIS) framework (privacy analysis), and specifying the three new proposed services in greater detail. We expect to report on some of this work in a future paper.

**Acknowledgments**

We thank Liam Peyton and Paul Madsen for helpful discussions. This research was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Ontario Research Network for Electronic Commerce (ORNEC).

## References


1. Aarts, R., Björksten, M., Deadman, S., Duserick, B., Karhuluoma, N., et al., *"Liberty architecture framework for supporting Privacy Preference Expression Languages (PPELs)"*. Nov 2003, Version 1.0, Liberty Alliance Project. Available from: http://www.projectliberty.org/about/whitepapers.php.
2. Ahn, G.-J. and Lam, J. "Managing privacy preferences for federated identity management". In *Proceedings of the 2005 workshop on Digital identity management*, Fairfax, VA, USA, November 2005. ACM Press.
3. Ahn, G.-J., Shin, D., and Hong, S.-P. "Information Assurance in Federated Identity Management: Experimentations and Issues". In *Proceedings of the 5th International Conference on Web Information Systems Engineering: Web Information Systems – WISE 2004*, Brisbane, Australia, November 2004. LNCS, Volume 3306, Jan 2004, Pages 78 - 89.
4. Bhargav-Spantzel, A., Squicciarini, A. C., and Bertino, E. "Establishing and protecting digital identity in federation systems". In *Proceedings of the 2005 workshop on Digital identity management*, Fairfax, VA, USA, November 2005. ACM Press.
5. Brown, K. "Security Briefs: Step-by-Step Guide to InfoCard". April 2006. MSDN Magazine, Microsoft. Available from: http://msdn.microsoft.com/msdnmag/issues/06/05/SecurityBriefs/default.aspx [Accessed: April 25, 2006].
6. BusinessWeek online. “Business Week/Harris Poll: A Growing Threat”. March, 2000. Available from: http://businessweek.com/2000/00_12/b3673010.htm [Accessed: January 16, 2006].
7. Ellison, G. and Madsen, P., *"Liberty ID-WSF Security Mechanisms"*, version 2.0-03, Liberty Alliance Project. Available from: http://www.projectliberty.org/resources/specifications.php.
8. Fox, S. "Trust and Privacy Online: Why Americans Want to Rewrite the Rules". August 2000. Pew Internet & American Life Project. Available from: http://www.pewinternet.org/pdfs/PIP_Trust_Privacy_Report.pdf [Accessed: February 17, 2006].
9. Gartner Group. 2003. Industry watchdog Gartner Group. Available from: http://www.gartner.com [Accessed: October 21, 2005].
10. Groß, T. "Security analysis of the SAML Single Sign-on Browser/Artifact profile". In *Proceedings of the 19th Annual Computer Security Applications Conference.*, Dec 2003. IEEE.
11. Hommel, W. "Using XACML for Privacy Control in SAML-Based Identity Federations". In *Proceedings of the TC-11International Conference, CMS 2005*, Salzburg, Austria, September 2005. Lecture Notes in Computer Science, Volume 3677, Sep 2005, Pages 160 - 169.
12. Johnston, S. J. "Pondering Passport: Do You Trust Microsoft With Your Data?" September, 2001. PCWorld.com. Available from: http://pcworld.about.com/news/Sep242001id63244.htm [Accessed: January 10, 2006].
13. Kellomäki, S. and Lockhart, R., *"Liberty ID-SIS Personal Profile Service Specification"*. 2003, Version 1.1, Liberty Alliance Project. Available from: http://www.projectliberty.org/resources/specifications.php.
14. Landau, S., *"Liberty ID-WSF Security & Privacy Overview"*. 2003, Version 1.0, Liberty Alliance Project. Available from: http://www.projectliberty.org/resources/specifications.php.
15. Liberty Alliance Project. Available from: http://www.projectliberty.org/ [Accessed: October 2005].

16. Liberty Alliance Project. "Liberty Alliance Whitepaper: Identity Theft Primer". December 2005. Available from: http://www.projectliberty.org/resources/id_Theft_Primer_Final.pdf [Accessed: January 2006].
17. Madsen, P. and Takahashi, Y. K. K. "Federated identity management for protecting users from ID theft". In *Proceedings of the 2005 workshop on Digital identity management*, Fairfax, VA, USA, November 2005. ACM Press.
18. OASIS Security Services (SAML) TC. "Security Assertion Markup Language (SAML)". OASIS Standards. Available from: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security [Accessed: December 2005].
19. Pfitzmann, B. "Privacy in Enterprise Identity Federation - Policies for Liberty Single Signon -". In *Proceedings of the 3rd Workshop on Privacy Enhancing Technologies (PET)*, Dresden, Germany, March 2003. Lecture Notes in Computer Science, Volume 2760, Dec 2003, Pages 189 - 204.
20. Pfitzmann, B. and Waidner, M. "Federated Identity-Management Protocols — Where User Authentication Protocols May Go". In *Proceedings of the 11th Cambridge Workshop on Security Protocols*, Cambridge, UK, April 2003. Lecture Notes in Computer Science, Volume 3364, Pages 153 - 174.
21. Pfitzmann, B. and Waidner, M. "Privacy in browser-based attribute exchange". In *Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society*, Washington, DC, USA, November 2002. ACM Press.
22. SourceID. "Digital Identity Basics". Available from: http://www.sourceid.org/content/primer [Accessed: December 2005].
23. Taylor, K. and Murty, J. "Implementing role based access control for federated information systems on the web". In *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003 - Volume 21*, Adelaide, Australia, 2003. ACM Press.
24. Varney, C. and Hartson, H., *"Privacy and Security Best Practices"*. November 2003, Version 2.0, Liberty Alliance Project. Available from: http://www.projectliberty.org/resources/specifications.php.
25. Varney, C. and Sheckler, V., *"Deployment Guidelines for Policy Decision Makers"*. September 2005, Version 2.9, Liberty Alliance Project. Available from: http://www.projectliberty.org/about/whitepapers.php.
26. Wason, T., *"Liberty ID-FF Architecture Overview"*. 2004, Version: 1.2-errata-v1.0, Liberty Alliance Project. Available from: http://www.projectliberty.org/resources/specifications.php.