

Liberty Alliance Project Specifications

As a contributor to the Liberty Alliance Project, a consortium of 160 companies, I defined the user experience for Authentication, Identity, and Privacy. My work brought a human-machine interaction perspective to a highly technical team and domain, ensuring that user-centric principles informed the development of federated identity management and identity-based web service specifications.

These specifications laid the foundation for modern web authentication and security practices—enabling cross-system interoperability while upholding privacy regulations. I contributed to guidelines addressing data collection, quality, purpose specification, and usage limitations, aligning technical standards with ethical and user-centered design principles.

Contribution: User Experience Design



Privacy and Security Best Practices

Version 2.0

November 12, 2003

Editor:

Christine Varney, Hogan & Hartson

Contributors:

Piper Cole, Sun Microsystems
William Duserick, Fidelity
Jill Lesser, David Taylor, AOL
Gary Podorowsky, Sony
Paule Sibieta, France Telecom
Charlotte Thornby, Sun Microsystems

Abstract:

Privacy and security are key concerns in the implementation of Liberty Alliance specifications. As such, the Liberty Alliance has and will continue to provide tools and guidance to implementing companies that enable them to build more secure, privacy-friendly identity-based services that can comply with local regulations and create a more trusted relationship with customers and partners. The following document highlights certain national privacy laws, fair information practices and implementation guidance for organizations using the Liberty Alliance specifications.

Contents

1. Executive Summary2

2. Introduction.....3

3. Liberty Alliance Perspective on Privacy.....4

4. Privacy laws.....5

5. Fair Information Principles6

6. Liberty Alliance Privacy Recommendations.....8

7. Security20

8. Internet Security Vulnerabilities and Precautions23

 8.1. Common Weaknesses.....24

 8.2. Browser Vulnerabilities.....25

 8.3. Protocol Vulnerabilities.....26

 8.4. Summary.....28

9. Terminology.....28

10. References.....30

1. Executive Summary

The Liberty Alliance Project is a consortium of more than 150 organizations worldwide working together to create open, technical specifications for federated network identity. These specifications, which are available for any organization to download and incorporate into products and services, provide:

- Simplified sign-on capabilities using a federated network identity architecture that supports all current and emerging network access devices.
- Permissions-based attribute sharing to enable organizations to provide users with choice and control over the use and disclosure of their personal information.
- A commonly accepted platform and mechanism for building and managing identity-based web services based on open industry standards.

Because companies will implement Liberty's specifications in connection with their web-based offerings, privacy and security are key concerns. As such, Liberty has and will continue to provide tools and guidance to implementing companies to lead them to build more secure, privacy-friendly identity-based services that can be in compliance with local regulations and create a more trusted relationship with customers and partners.

The Liberty specifications will enable companies to adhere to information practices that comply with national privacy laws and regulations, or in the absence of such laws, industry best practices. It is however, important to note that Liberty, as a standards body, will not manage companies' compliance with those laws.

The following document highlights certain national privacy laws, fair information practices and implementation guidance for organizations using the Liberty Alliance specifications. Below is a brief summary of key points made in the paper, but the Alliance would encourage all parties to read through the entire document.

Liberty's Perspective on Privacy:

- The Liberty Alliance considers privacy and security of a Principal's personal information to be extremely important. This philosophy has driven many decisions crucial in the specification development process.
- Because the Liberty specifications represent a novel approach to account linking and data exchange, we believe it is important to identify implementation best practices to accompany the specifications.
- The Alliance also recommends that companies implementing any identity-related services or applications consult with local counsel to ensure that the services they provide comply with applicable privacy laws and regulations.

Privacy Laws and Fair Information Practices:

- There are several privacy laws, in varying states of development, enacted worldwide. This document highlights some of the more pertinent regulations in the U.S., Canada, Europe and other regions.
- This paper also describes certain practices and frameworks created by various organizations that address the use and disclosure of personal information. Topics addressed include adoption and implementation of privacy policies, notice and disclosure, choice and consent, data quality, security safeguards and accountability.

Liberty Alliance Privacy Recommendations:

- In addition to current laws and organizational guidelines, the Liberty Alliance offers in this paper a baseline set of fair information practices for any entity using the Liberty specifications.
- Liberty-enabled providers can function in multiple roles within an identity management relationship. These roles come with certain responsibilities – whether their role is Principal, Service Provider, Identity

Provider, Attribute Provider or Discovery Service. This paper reviews these roles and responsibilities in the context of privacy and security.

Security, Internet Protocols and Browsers:

- In developing its specifications, Liberty has evaluated the weaknesses of several well-known and frequently used Internet protocols and browsers. The Liberty Alliance has made every effort to provide secure standards, but since the standards are built on top of insecure protocols, there are some unavoidable potential vulnerabilities. This should not be misconstrued to suggest that the Liberty Specifications are insecure, but that implementations are dependent on all the underlying protocols, and thus care must be taken in implementation. The Liberty specifications neither increase nor eliminate these vulnerabilities.
- To that end, this best practices document provides definitions and information about security vulnerabilities and offers mitigating information to avoid the most common of them.

2. Introduction

The Liberty Alliance Project (“**Liberty Alliance**” or “**Liberty**”) is an unincorporated, contract-based group of more than 150 companies and organizations from around the world. Liberty’s objective is to create open, technical specifications (“**Liberty Specifications**”) that (i) enable simplified sign-on through federated network identification on all current and emerging network access devices, and (ii) support and promote permissions-based attribute sharing to enable a user’s (“**Principal’s**”) choice and control over the use and disclosure of such Principal’s personal information. Liberty anticipates that these specifications will expedite the growth of e-commerce because they are designed to increase consumer convenience and confidence and to provide businesses with new business and cost-saving opportunities.

Liberty envisions that organizations will implement the Liberty Specifications in connection with their web-based offerings. Because privacy is important in these contexts, the Liberty Specifications include the necessary features and facilities to enable an implementing company to comply with its national privacy laws and regulations, or in the absence of law or regulation, best practices. Thus the Liberty Specifications will enable companies to adhere to information practices that comply with those laws and regulations.

The Liberty Alliance offers the guidance set forth in this document to implement the Liberty Specifications in an appropriately secure and privacy-friendly manner. Liberty also provides guidelines regarding privacy and security in a variety of documents, and intends to provide such guidance for future versions of the Liberty Specifications as well.¹

This document first presents Liberty’s perspective on privacy, followed by a discussion of certain general privacy laws and fair information practices. It then highlights certain “best practices” that will help those using the Liberty Specifications to ensure that privacy concerns are addressed. We offer some observations on security issues generally and Internet protocols and browsers more specifically. Finally, also attached for easy reference are links to books, papers, and other materials that discuss online security and privacy issues, as well as a broad sample of the variety of contemporary privacy paradigms that exist.

Companies that implement the Liberty Specifications are advised to consult with local counsel to ensure that the services they provide, based upon the Liberty Specifications, comply with applicable law. Please note that these best practices are intended to provide guidelines, not serve as an exhaustive resource. Furthermore, from a technical standpoint, these best practices are non-normative – they are not the rules defining the Liberty Specifications, but rather identify the privacy and security concerns that should be addressed when implementing Liberty Specifications. It is important to note that the Liberty Specifications are based upon existing Internet architecture and well-known protocols. The Liberty Specifications cannot and do not cure the well documented security challenges inherent in the

¹ Further guidelines on privacy and security can be found in the following Liberty specification documents: Liberty Alliance, “Liberty Security Bulletin October 11, 2002;” Thomas Wason, “Architectural Overview Version 1.0-2.0;” Paul Madsen, “Liberty Authentication Context Specification;” Gary Ellison, “ID-WSF Security Mechanisms;” Susan Landau, “ID-WSF Security and Privacy Overview;” John Kemp and Tom Wason, “ID-FF Bindings and Profiles;” Scott Cantor and John Kemp, “Liberty ID-FF Protocols and Schema Specification;” and John Linn, “Liberty Trust Models.”

architecture of the Internet. Because companies from any part of the world, whether for-profit or not-for-profit, whether or not a member of the Liberty Alliance, may use the Liberty Specifications, the best practices identified in this document cannot and do not capture or address each potentially applicable legal privacy regime. Companies that implement the Liberty Specifications are advised to consult with local counsel to ensure that the services they provide, based upon the Liberty Specifications, comply with applicable privacy laws and regulations.

In addition, readers of this document should be aware that the Liberty Specifications are just that – specifications only. Given the global nature of e-commerce, the myriad of laws that apply to privacy, and the fact that the Liberty Alliance itself does not provide any services, the Liberty Alliance cannot and does not (i) advise as to what laws, regulations, or fair information practices are applicable to any given company, (ii) condition use of the Liberty Specifications on adoption of a particular set of fair information practices, (iii) monitor, audit or enforce compliance with applicable laws and regulations, nor (iv) have any liability with respect to an implementing company's use of the Liberty Specifications. The implementing companies remain responsible for monitoring implementation and, as is the case today, remain answerable to local enforcement authorities for non-compliance with applicable laws.

Similarly, implementing companies should monitor the ever-changing status of security challenges, and should take these into account when designing their implementations. To aid in this effort, we present in this document some of the well-known Internet and protocol security vulnerabilities that should be taken into account when implementing the Liberty Specifications.

3. Liberty Alliance Perspective on Privacy

The Liberty Alliance considers privacy and security of a Principal's personal information to be extremely important. Privacy, security and consumer considerations drive many decisions the Liberty Alliance made about the world of online commerce that the Liberty Specifications enable. In particular, the Liberty Alliance made the following fundamental decisions regarding the Liberty Specifications:

- To use a de-centralized architecture, where it is not necessary to have data stored with a single entity;
- To use a federated architecture, where parties are free to link networks as business judgment dictates;
- To support and promote permissions-based attribute sharing to enable consumer choice and control over the use and disclosure of his or her personal information;
- To provide open specifications that are not centrally administered;
- To provide interoperable specifications that can be used on a wide variety of network access devices;
- To leverage existing systems, standards, and protocols where they work well;
- To enable companies to transmit information using the specifications with the best available security;
- To include in the specifications, tools that enable companies to respond to consumer interests regarding privacy and security and to compete on that basis.

Our perspective on privacy is necessarily informed by two key characteristics of our work:

1. The Liberty Alliance is a group of individual companies writing open technical specifications and, except for the specifications, the Liberty Alliance does not provide products or services directly to the public; and
2. The Liberty Alliance is composed of individual member companies from around the globe and from myriad sectors of the economy. Many of the Liberty Alliance members serve consumers directly and others create the infrastructure products that are used by companies to serve consumers directly and by companies to run their internal operations. Some companies serve global markets, and others serve regional markets in Europe, Japan, Korea, and the United States.

Given the goals of facilitating e-commerce and providing a mechanism that permits compliance with local law and appropriate security, Liberty believes that the responsible approach is to create flexible, interoperable specifications that can be implemented around the globe in a variety of different ways to satisfy applicable privacy and security concerns and related laws. Thus, the Liberty Specifications provide tools that can be used by implementing companies to address privacy and security concerns. As noted earlier, the implementing companies are solely responsible for

deploying the Liberty Specifications in a secure manner that complies with applicable privacy laws and fair information practices.

Because the Liberty Specifications represent a novel approach to account linking and data exchange, we believe it is important to identify implementation best practices to accompany the specifications. The best practices below simply explain what fair information principles Liberty-enabled providers should address, depending upon which role(s) they perform. This document also explains the tools contained in the specifications that can be used to respond to such considerations, including elements of the Liberty Specifications that enable implementers to more effectively utilize various rights expression languages to communicate information about usage directives that may be associated with a given attribute.

Finally, it is important to note that the Liberty Specifications are built on a framework that presumes data exchange of personal attributes will occur in the context of permissioning. While, as noted, the Liberty Alliance has no role in providing services, many of the architectural decisions made in creating the Liberty Specifications were made on the presumption that those providing services based on the Liberty Specifications would be engaging in permissions-based attribute sharing.

These architectural considerations, as well as specific features of the Liberty Specifications reflect the fact that the Liberty Alliance is both very conscious of the importance of privacy, security and other public policy considerations, and cognizant of the fact that the Liberty Alliance is, fundamentally, an open specifications body that cannot – and should not – enforce particular implementations on parties using the Liberty Specifications.

4. Privacy laws

There are a variety of privacy protection laws throughout the world, each with its unique set of requirements and obligations. The following discussion highlights some, but by no means all, of these laws, and the differences between those highlighted.²

Some of the privacy laws that have been enacted include, among others:

- European Union Directive on Data Protection of individuals with regard to the processing of personal data and the free movement of such data.³
- European Union Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector.⁴
- In Canada – The Personal Information Protection and Electronic Documents Act.⁵
- In the United States – The Children’s Online Privacy Protection Act, The Graham-Leach-Bliley Act, The Health Insurance Portability and Accountability Act, and more generally, the Federal Trade Commission has challenged online privacy policies under Section 5 of the Federal Trade Commission Act.⁶
- In Other Territories – According to Privacy International’s Privacy and Human Rights: An International Survey of Privacy Laws and Developments, 2003, there are several other territories that have enacted or enforced some form of privacy laws.⁷

The EU Data Protection Directive (95/46/EC) aims to protect the privacy of EU citizens and harmonize differing laws and regulations in the Member States. The EU Data Protection Directive covers any information relating to an

² The summaries of law provided below are for informational purposes only, and are not intended to be legal advice.

³ EU Data Protection Directive 95/46/EC.

⁴ EU Directive on Privacy and Electronic Communications 2002/58/EC.

⁵ Canadian Privacy Act. S.C. 2000.

⁶ See 15 U.S.C.A. § 6501 (2000); 15 U.S.C.A. § 6801 et. seq. (1999); 42 U.S.C.A. §§ 1320(d) et. seq. (1996); 15 U.S.C.A. § 45(a) (2000).

⁷ Privacy International, “Privacy and Human Rights: An International Survey of Privacy Laws and Developments, 2002.”

individual, even if collected purely in a business context, such as contact details of business clients, and not just consumers. Data about a company's employees is also covered.

The Directive imposes duties on data "controllers," those who determine the purpose and means of processing data. In addition to imposing registration requirements with data commissioners in Member States, the Directive requires that data be (i) processed fairly, (ii) collected for specified, explicit and legitimate purposes and not used in ways incompatible with those purposes, (iii) collected only to the extent that it is adequate and relevant, and not excessive in relation to the purposes for which it was collected, (iv) accurate and kept up to date, (v) kept no longer than necessary for the purposes for which it was collected, and (vi) not transferred to third-party countries that do not ensure an adequate level of protection for the data. Data may generally be processed either by unambiguous consent or where necessary to perform a contract. However, certain data is considered sensitive requiring explicit consent before processing. In addition, data subjects are to be given notice of the data controller, purposes of processing their data, recipients of the data, and the right to access and correct the data. This notice to the data subject is to be provided even when the data has been obtained not from the data subject but from a third party.

The EU Data Protection Directive for electronic communications (2002/58/EC) complements the aforementioned Directive for the electronic communications sector. It includes inter alia specific provisions regarding the confidentiality of communications, the handling of traffic and location data and the requirements and restrictions applying to the use of cookies as well as to unsolicited electronic communications. Member States are required to implement the Directive by 31 October 2003.

The Canadian Privacy Act sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities. The Act is centered around ten (10) underlying principles regarding (i) accountability, (ii) identifying purpose, (iii) consent, (iv) limiting collection, (v) limiting use, disclosure, and retention, (vi) accuracy, (vii) safeguards, (viii) openness, (ix) individual access, and (x) challenging compliance.

United States laws, on the other hand, take a more vertical approach with express federal privacy related statutes for specific sectors. For example, the Graham-Leach Bliley-Act ("**GLB Act**") governs the use of personal information that is given to and managed by financial service providers. The Health Insurance Portability and Accountability Act ("**HIPAA**") mandates standards for the use of protected health care data. The Children's Online Privacy Protection Act ("**COPPA**") governs the use and collection of personal information about children under age 13. Each of these laws requires some form of notice and consent before disclosure of the personal information at issue, and requires that a party use reasonable safeguards to maintain the confidentiality of such personal information. Under the GLB Act, for example, consent to share personal information with unaffiliated third parties for marketing purposes via an "opt-out" procedure rather than express or an "opt-in" consent, may be acceptable. In other cases, the Federal Trade Commission has exercised its authority under Section 5 of the Federal Trade Commission Act to challenge certain privacy practices as "unfair and deceptive."⁸

Given the breadth and variety of privacy laws that may be applicable depending upon the jurisdiction in which a company does business, the Liberty Alliance strongly recommends that any entity implementing the Liberty Specifications consult with local counsel to determine which laws are applicable to the company's business and how best to comply with those laws.

5. Fair Information Principles

General. In addition to existing privacy laws, several organizations have set forth fair information practices governing the use and disclosure of personal information. These organizations include, among others, the Online Privacy Alliance ("**OPA**"), the Organization for Economic Co-operation and Development ("**OECD**"), the Center for Democracy and Technology ("**CDT**"), the Network Advertising Initiative ("**NAI**"), Health Internet Ethics ("**Hi-Ethics**"), and the Global Business Dialogue on Electronic Commerce ("**GBDe**").⁹

⁸ For an overview of U.S. federal and state privacy laws, see BBB Online, Inc. and the Council of Better Business Bureaus, Inc., "A Review of Federal and State Privacy Laws."

⁹ Links to several of these fair information practices or privacy guidelines are noted in the References section of this document.

There are no universal standards among these organizations as to what fair information practices entail. The differences seen in these fair information practices are partially attributable to geography, and partially attributable to the sector to which the fair information practices apply.

OPA Guidelines. OPA is a U.S.-based organization which provides a general framework in which any U.S. company can operate, calling for customization and enhancement as appropriate to a company's business or industry sector. These guidelines generally provide as follows:

- **Adoption and Implementation of a Privacy Policy** – An organization should adopt and implement a policy for protecting the privacy of individually identifiable information.
- **Notice and Disclosure** – The privacy policy should be clear, easy to find, and available at or prior to the time individually identifiable information is collected. It should state “what information is being collected; the use of that information; possible third-party distribution of that information; the choices available to an individual regarding collection, use and distribution of the collected information; a statement of the organization's commitment to data security; and what steps the organization takes to ensure data quality and access. It should also disclose the consequences, if any, of an individual's refusal to provide information. The policy should also include a clear statement of what accountability mechanism the organization uses, including how to contact the organization.”
- **Choice/Consent** – Individuals must be given the opportunity to exercise choice regarding how individually identifiable information collected from them online may be used when such use is unrelated to the purpose for which the information was collected or where there is third-party distribution of such data unrelated to the purpose for which it is collected. At a minimum, individuals should be given the opportunity to opt out of such use or third-party distribution.
- **Data Security** – Organizations creating, maintaining, using or disseminating individually identifiable information should take appropriate measures to assure its reliability and should take reasonable precautions to protect it from loss, misuse or alteration. Organizations should take reasonable steps to assure that third parties to which they transfer such information are aware of these security practices, and that the third parties also take reasonable precautions to protect any transferred information.
- **Data Quality and Access** – Organizations creating, maintaining, using or disseminating individually identifiable information should take reasonable steps to assure that the data are accurate, complete and timely for the purposes for which they are to be used. Organizations should establish appropriate processes or mechanisms so that inaccuracies in material individually identifiable information, such as account or contact information, may be corrected. These processes and mechanisms should be simple and easy to use, and provide assurance that inaccuracies have been corrected. Other procedures to assure data quality may include use of reliable sources and collection methods, reasonable and appropriate consumer access and correction, and protections against accidental or unauthorized alteration.

OECD Guidelines. The OECD is an international organization focusing on global economic cooperation and development. OECD guidelines on the protection of privacy and trans-border flows of personal data are close to the European approach to privacy. Unlike the United States, Europe has more comprehensive privacy statutes and vests significant authority in its regulatory bodies to enforce privacy legislation. OECD's guidelines set forth the following eight principles:

- **Collection Limitation** – There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality** – Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- **Purpose Specification** – The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- **Use Limitation** – Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Article 9 (the purpose specification principle) except: (a) with the consent of the data subject; or (b) by the authority of law.

- **Security Safeguards** – Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
- **Openness** – There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- **Individual Participation** – An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
- **Accountability** – A data controller should be accountable for complying with measures which give effect to the principles stated above.

6. Liberty Alliance Privacy Recommendations

As evident from the preceding sections, there is a wide range of fair information practices that have been promoted around the world. In an effort to promote “best practices,” Liberty recommends that an implementing company comply with all relevant laws. In the absence of laws, an implementing company should follow the most appropriate fair information practices applicable to the jurisdiction and industry sector in which the company intends to do business or offer products or services. Where applicable, an entity should not request or provide more information than is necessary for the interaction.

In addition, the Liberty Alliance offers the following baseline set of fair information practices as guidelines that companies, whether in the role of Service Provider, Identity Provider, Attribute Provider, Discovery Service or otherwise, should consider adopting when implementing Liberty Specifications. These recommended fair information practices are based on principles of notice, choice and control, access, security, quality, relevance, timeliness and accountability. Each of these practices, and its appropriateness in the context of Liberty Services, is briefly described below.

- **Notice.** Consumer facing Liberty-Enabled Providers should provide to the Principal clear notice of who is collecting the information, what information they collect, how they collect it (e.g., directly or through non-obvious means, such as cookies), how they provide choice, access, security, quality, relevance and timeliness to Principals, whether they disclose the information collected to other entities, and whether other entities are collecting information through them. Providing notice is particularly important for Service Providers who may seek additional information beyond what is provided through other Liberty-Enabled Providers.
- **Choice.** Consumer facing Liberty-Enabled Providers should offer Principals choices, to the extent appropriate given the circumstances, regarding what personally identifiable information is collected and how the personally identifiable information is used beyond the use for which the information was provided. In addition, consumer facing Liberty-Enabled Providers should allow Principals to review, verify, or update consents previously given or denied. The Liberty Specifications provide for both access permissions to allow a Principal to specify whether and under what circumstances a Service Provider can obtain given attributes, as well as an “envelope” for the discovery of or negotiation of usage directives as part of profile sharing. Both aspects of the privacy capabilities established by the Liberty Specifications should be fully implemented in a responsible manner and be easy for the Principal to configure. In particular, Liberty-Enabled Providers should provide for “usage directives” for data through either contractual arrangements, or through the use of Rights Expression Languages, as well as implementing the access authorization elements contained in the Liberty Specifications that permit the Principal to make certain choices regarding collection and use of personally identifiable information.
- **Principal Access to Personally Identifiable Information (PII).** Consumer facing Liberty-Enabled Providers that maintain PII should offer, consistent with and as required by relevant law, a Principal reasonable access to view the non-proprietary PII that it collects from the Principal or maintains about the

Principal. Access should not be construed to require access to proprietary data, public record data, or aggregate data.

- **Quality.** Consumer facing Liberty-Enabled Providers that collect and maintain personally identifiable information should permit Principals a reasonable opportunity to provide corrections to the personally identifiable information that is stored by such entities.
- **Relevance.** Liberty-Enabled Providers should use PII for the purpose for which it was collected, or the purposes about which the Principal has consented.
- **Timeliness.** Liberty-Enabled Providers should retain PII only so long as is necessary or requested and consistent with a retention policy accepted by the Principal.
- **Complaint Resolution.** Liberty-Enabled Providers should offer a complaint resolution mechanism for Principals who believe their PII has been mishandled.
- **Security.** Liberty-Enabled Providers should take reasonable steps to protect and provide an adequate level of security for PII.

Implementing companies should be aware that the Liberty Specifications provide tools the implementing company can use to help it comply with fair information practices, regardless of which protocol is adopted. These tools are discussed in more detail below. However, implementing companies should also be aware that any of these fair information practices (as well as any recommendations set forth in this document) are only guidelines, and may or may not satisfy or be consistent with the privacy laws, rules, and regulations applicable to the implementing company. Therefore, Liberty strongly recommends that any implementing company consult with local counsel to determine which laws are applicable to the company's business and how best to comply with those laws.

In order to address various privacy concerns and implement fair information practices using the Liberty Specifications, it is important for an implementing company to understand how certain schemas and protocols in the specifications operate and be aware of certain tools contained in the specifications that can be used to respond to such considerations.

Consumer choice and permission are central to Liberty's vision. The framework of the Liberty Specifications is built upon the presumption that PII will be shared ("attribute sharing") in the context of permissioning, i.e., upon the consent of the Principal and in accordance with the usages expressed by the Principal. Such attribute sharing should be predicated upon not only a prior agreement between the Liberty-Enabled Providers, but also upon providing notice to the Principal and obtaining the Principal's consent. The Liberty Specifications allow for recording both the notice and consent in an auditable fashion. Liberty recognizes that depending upon the particular implementation, for example in financial services transactions, it may be important to both the Principal and the Liberty-Enabled Provider to have increased certainty regarding their transaction. Such certainty may be achieved through the use of auditable records of notice and consent. In addition, Liberty-enabled providers should take reasonable measures to prevent unauthorized acquisition of a principal's personal information (e.g. by harvesting).

Within this framework, the Liberty Specifications identify various roles that comprise the federated identity infrastructure. Each of these roles has certain responsibilities in relation to protecting the privacy and security of a Principal's personally identifiable information. Liberty-Enabled Providers may function in multiple provider roles. These roles and their respective responsibilities include, among others:

- **Principal** – A Principal is an entity that can acquire a federated identity that is capable of making decisions and can be authenticated and vouched for by an Identity Provider. In a business-to-consumer (B2C) context, the Principal is the consumer. In other contexts, the Principal could be an individual, a corporation, or another legal entity. The fair information best practices set forth in this document are aimed to protect the confidentiality of the Principal's personally identifiable information. Principals should be vigilant when they provide their credentials (e.g., passwords, secure tokens, etc., entered over secure channels) or attributes over the web to protect themselves from being spoofed or otherwise providing such information to an unintended party. In addition, Principals should use care when establishing or modifying credentials. Also, Principals should become familiar with an entity's posted data practices before providing personally identifiable data to such entity.
- **Service Provider** – A Service Provider is an entity that provides services to Principals. Liberty envisions that the Service Provider will, upon request from a Principal, request that the Identity Provider (which may be itself or another party) authenticate the Principal. After the Principal has been authenticated, the Service Provider may request that certain attributes regarding the Principal be

provided to it in order to provide the requested services to the Principal. Service Providers should inform Principals of their data practices, provide the Principal with certain choices regarding secondary uses of the Principal's personally identifiable information, maintain the security of a Principal's personally identifiable information within their control, and not use or share such information except in accordance with the Service Provider's privacy policy and/or the consent or usage directives of the Principal. The Service Provider should at all times ensure that its data practices conform with applicable local law and practice.

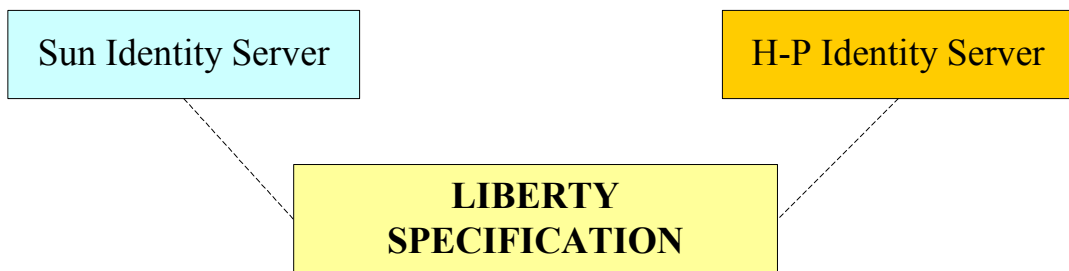
- **Identity Provider** – An Identity Provider is an entity that creates, maintains, and manages identity information for Principals. It authenticates and vouches for the Principal to other Service Providers within an Authentication Domain. The Identity Provider should also safeguard the Principal's identity credentials, and have some mechanisms in place to require the Authentication Domain to use the credentials in a proper manner.
- **Attribute Provider** – An Attribute Provider is an entity that provides attributes to a requester (i.e., a Service Provider) in accordance with its own policies and a Principal's permissions. Attribute Providers store and negotiate access control information defining the circumstances under which a Service Provider will be granted access to a given attribute(s). Attribute Providers store and negotiate usage directives that specify the manner in which attributes can be used, stored, and disclosed. An Attribute Provider has at least the same responsibilities as Service Providers with respect to clear notice (including notice to the Principal regarding what are the default usage directives and how the Principal can change such usage directives), choice, security, and responsible use and sharing of a Principal's data.
- **Discovery Service** – A Discovery Service is an entity (usually an Identity Provider) that has the ability to direct attribute requesters to the relevant Attribute Provider who provides the requested classes of attributes for the specified Principal. The Discovery Service should register only those Attribute Providers in accordance with the consent or usage directives of the Principal. The Discovery Service should permit the Principal to see which Attribute Providers have been registered on the Principal's behalf. An attribute requester can locate the Attribute Providers for a given Principal, even though the attribute requester and Attribute Providers do not have a common name for the Principal.

The following are two hypothetical examples of implementation of the Liberty Specifications by various companies. In Example 1, we start with the actual equipment manufacturers who could build Internet infrastructure software utilizing the specifications. Example 1 goes through the steps to an end user experience. Example 2 is a one page summary illustration of the process undertaken and explained in Example 1. Where Example 1 starts with software manufacturer, Example 2 shows the same process, in summary form, starting with the user.

Hypothetical Example 1

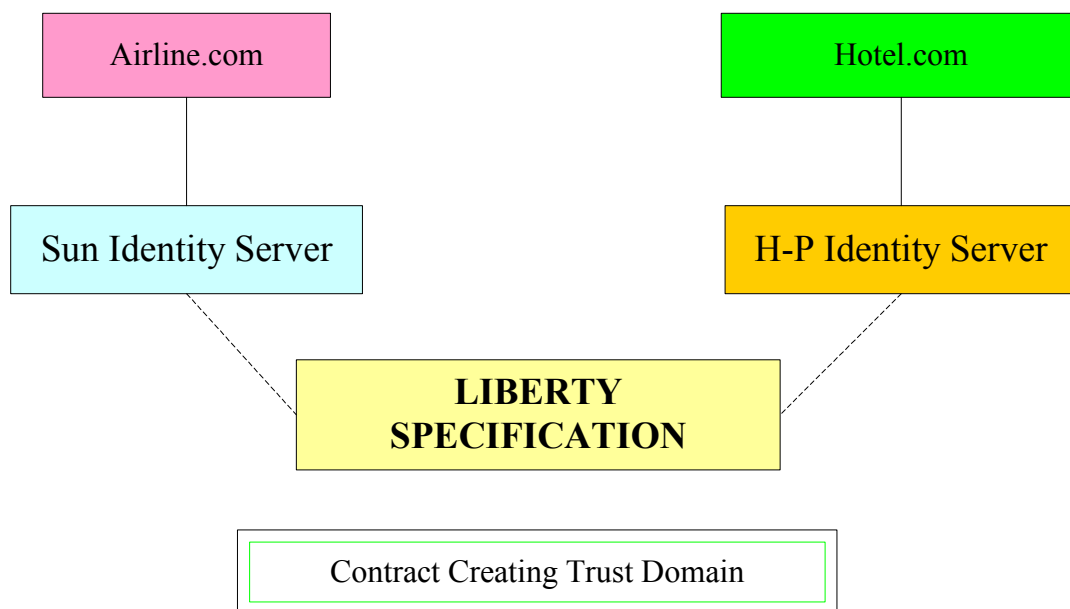
1. Technology Implementation

- a. Sun develops an identity server (infrastructure software) using the Project Liberty Alliance specifications (Liberty Specification) in order to allow the Sun identity server to interoperate with other technology products that implement the Liberty Specification.
- b. H-P develops an identity server (infrastructure software) using the Liberty Specification in order to allow the H-P identity server to interoperate with other technology products that implement the Liberty Specification.



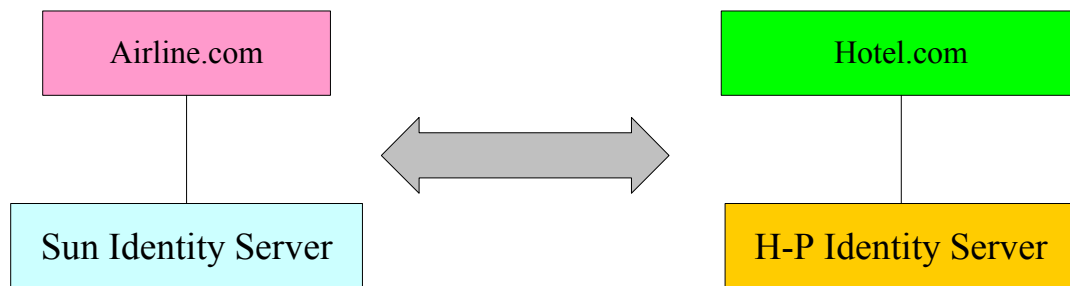
2. *Services Deployment*

- a. Airline employs a Sun Identity Server to authenticate users to its website, maintain frequent flyer information, and provide linkage to its reservation system.
- b. Hotel uses an HP Identity Server to authenticate users to its website and facilitate online reservations.



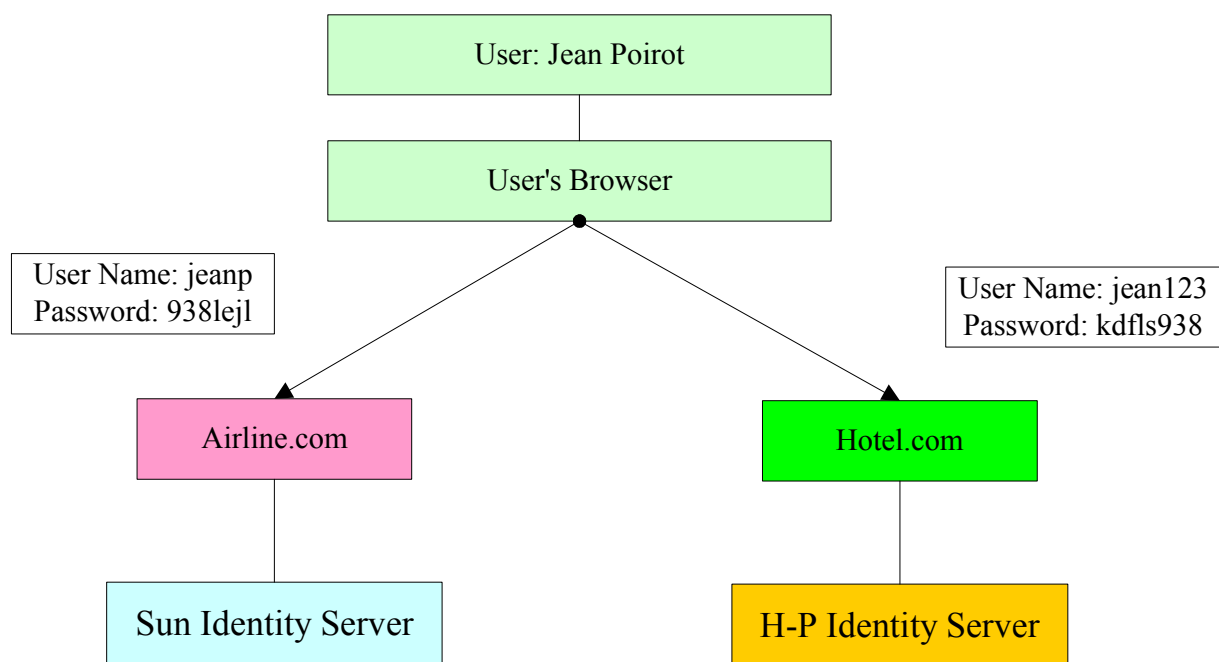
3. *Trust Domain*

- a. Airline and Hotel enter into a contract, which requires, among other things, that Hotel will accept Airline's authentication of a customer that is a customer of both Airline and Hotel (Airline is an Identity Provider and Hotel is a Service Provider.)



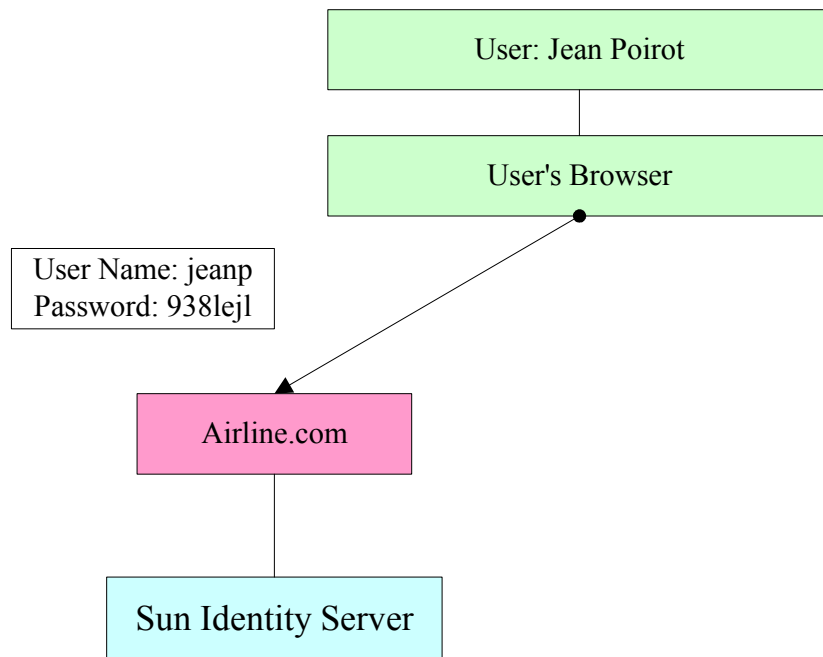
4. *Account Establishment*

- a. User establishes an account with Airline.com with User ID JeanP and a password.
- b. User establishes an account at Hotel.com with user name Jean123 and a password.

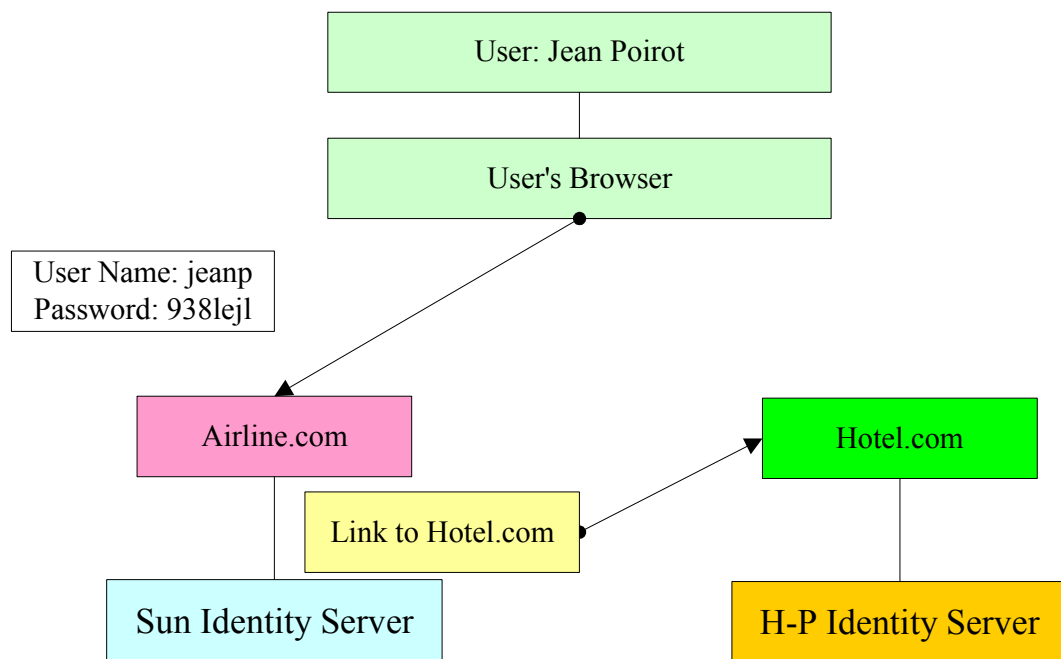


5. *Linking Accounts*

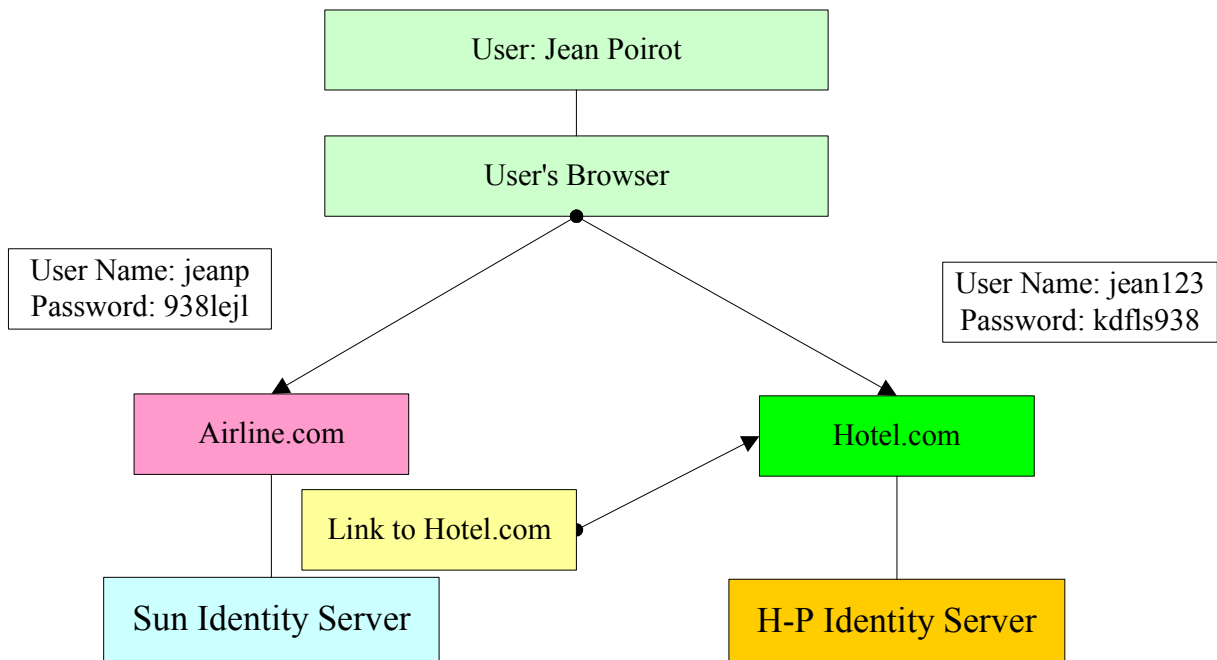
- a. Jean logs onto the Airline site with user name and password



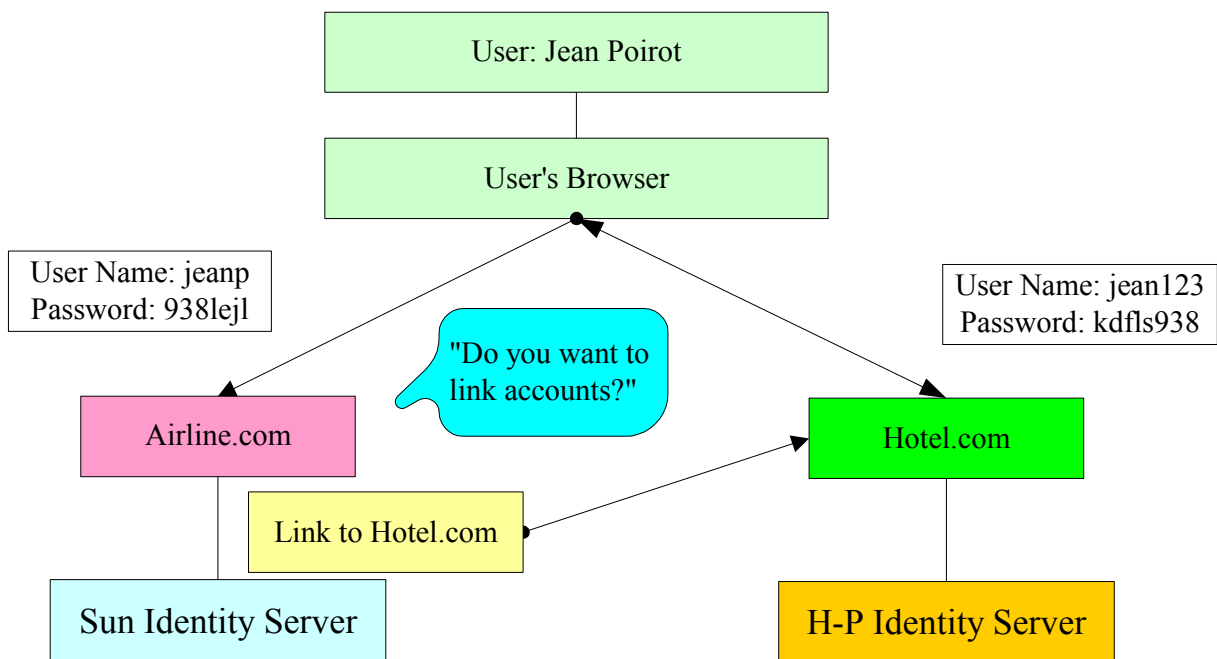
- b. Airline has a link that JeanP can use to go to the Hotel website.



- 430 c. JeanP clicks on that link and goes to the Hotel website and logs in with username Jean123 and
431 password.

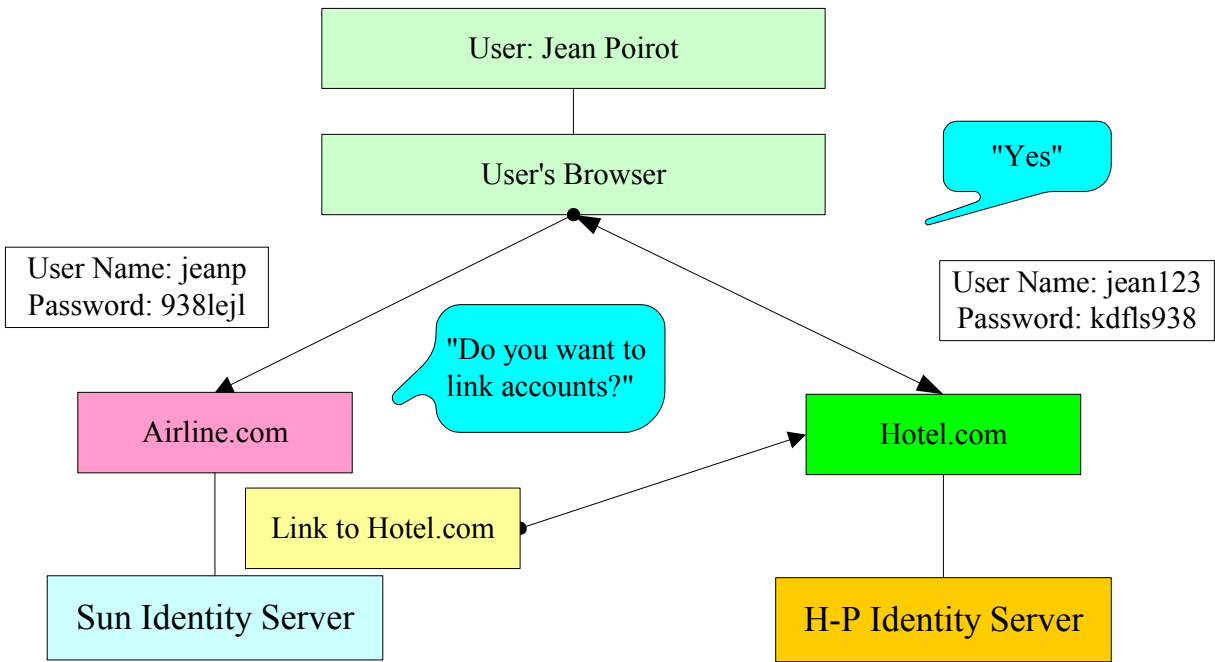


- 432
433 d. Hotel would know that Jean123 came from the Airline site and asks if Jean123 would like to link his
434 account at Airline with his account at Hotel, enabling single sign-on between the two accounts.

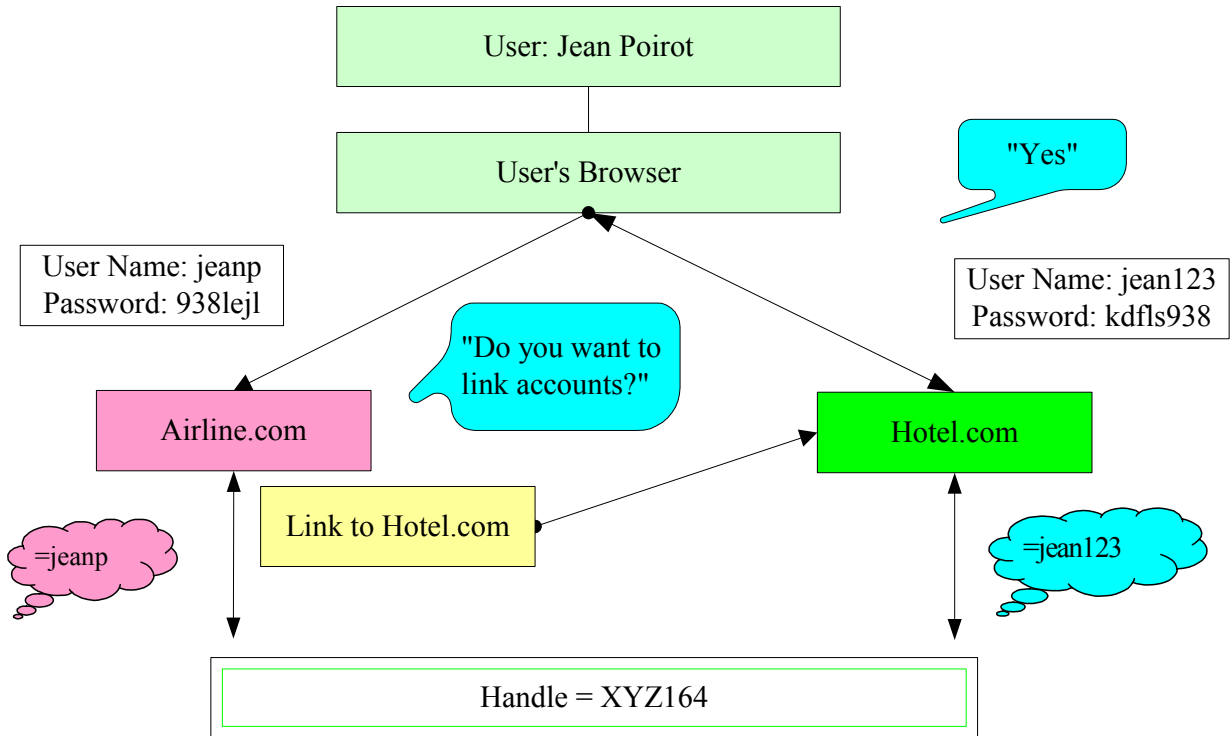


435
436
437
438

e. Jean123 indicates his consent by clicking “yes”.

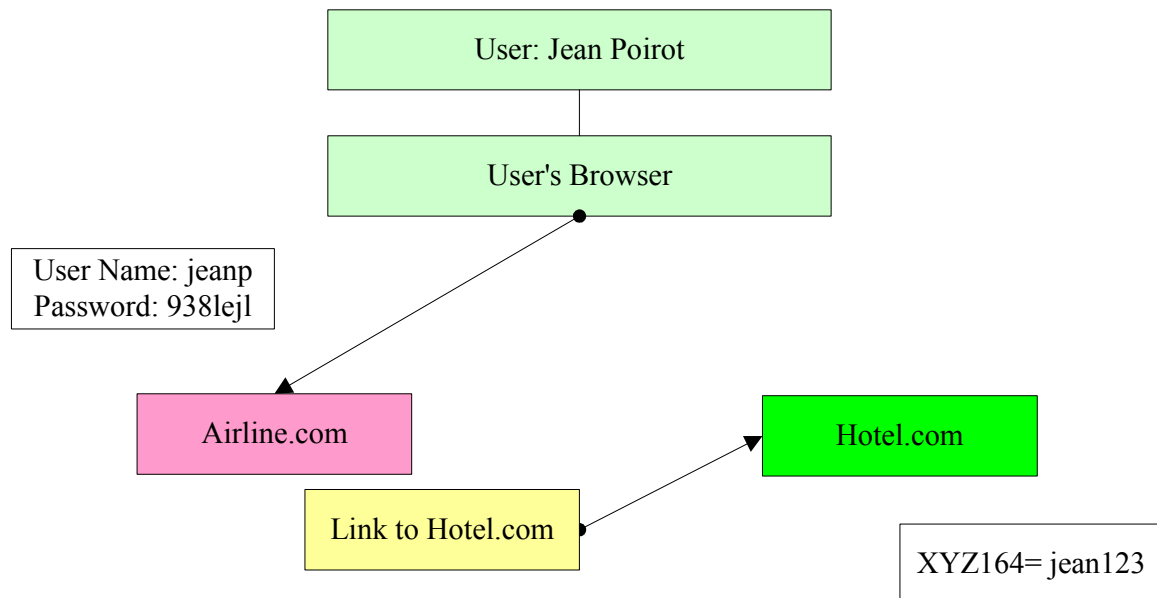


f. Airline and Hotel agree on a random set of characters (handle) by which each will recognize user as their customer (e.g., Airline: XYZ164 = authenticated JeanP; Hotel: XYZ164 = authenticated Jean123)

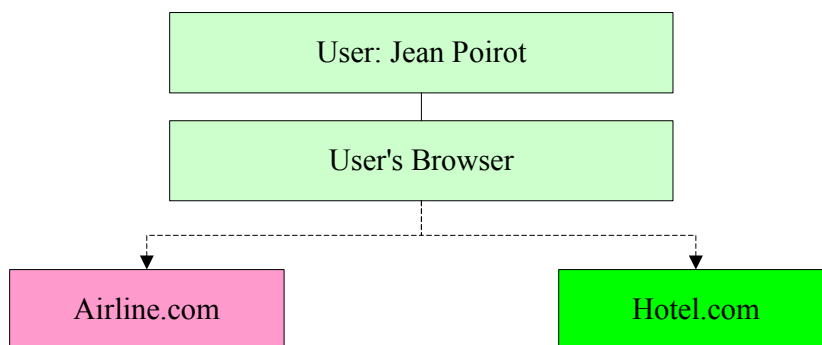


6. *Simplified sign-on (SSO)*

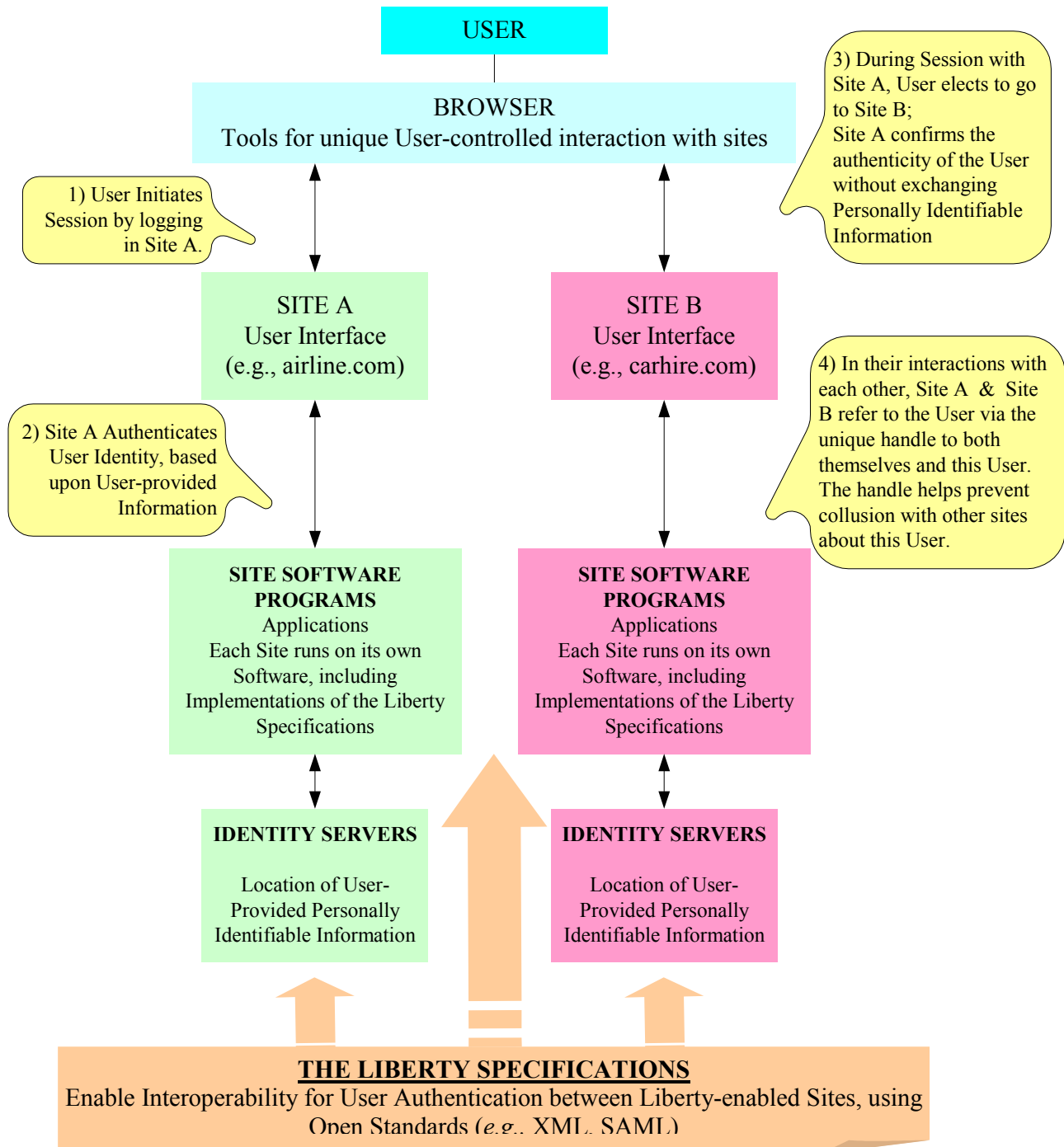
- a. User goes to Airline and logs in as JeanP and password.
- b. User clicks on link to Hotel website.
- c. Airline sends opaque handle to Hotel site with username.
- d. Hotel receives opaque handle and recognizes user as authenticated Jean123.



- e. When Jean logs out of either site, he is automatically logged out of both sites.



The following diagram is a summary hypothetical example of deployment by various companies:



In either example, if starting at an Identity Provider, the Principal makes an initial authentication by presenting a user name (real or pseudonymous) and a corresponding password. Next, the Principal establishes a local account with various Service Providers. The final step is for the Principal to link accounts. Account linking will likely be a two-step process. First the Principal consents to account linking and then provides specific consent for each Service Provider. After these steps, the Principal will be able to benefit from SSO and surf the Internet in a Trust Domain using the same name and password given initially to the Identity Provider.

Alternatively, a Principal may wish to connect to a Service Provider without first going to an Identity Provider. In this case the Service Provider will typically provide the Principal with a list of all Identity Providers with whom the Service Provider has formed a Trust Domain, and the Principal will be offered the opportunity to click on its preferred Identity Provider in order to authenticate. The Service Provider will redirect the Principal's browser to the chosen Identity Provider who will recognize the Principal by name and password (which the Principal will have to disclose). The Principal is then authenticated for all Providers within that Trust Domain for this session of Internet use.

At the end of the session, the Principal will benefit from an automatic Single-Log-Out performed by the system, i.e., by logging out of any site, the Principal can be automatically logged out of all of the other sites visited during that particular session of Internet use.

Of course, it is also possible for a Principal to visit a single Service Provider and log into that Service Provider using its user name and password recognized by that Service Provider, but it will not be able to take advantage of SSO until it authenticates at an Identity Provider.

In the preceding illustration, Jean now has a federated identity between Airline and Hotel. Assume that Jean has also federated his identity at Bank with his Airline and Hotel identities. Jean's identity at Airline includes Jean's name, address, and frequent flier information. Jean's account at Bank includes an electronic wallet where Jean stores his credit card information. Bank has previously notified Airline that it has credit card information related to Jean. Jean logs in at the Airline website, visits the Hotel website, and desires to make a reservation for a hotel room. In order to take a reservation, Hotel needs information regarding Jean's name, address, and credit card information. Hotel requests this information from Airline. After checking Jean's preferences regarding data, Airline provides the name and address information to Hotel, and directs Hotel to obtain credit card information from Bank. After checking Jean's preferences regarding data disclosure, Bank provides credit card information to Hotel. All of these interactions between Hotel, Airline, and Bank are done "behind the scenes." After Jean makes his request to make a reservation, his name, address, and credit card information are automatically included in the form presented to Jean at Hotel's website to make his reservation.

In this example, Airline acts not only as an Identity Provider (authenticating Jean's identity for Hotel), but also as an Attribute Provider (providing name and address information to Hotel) and as a Discovery Service (letting Hotel know that Jean's credit card information may be obtained from Bank). Bank is also an Attribute Provider because it provides credit card information to Hotel.

The roles of each of the Liberty-Enabled providers should be viewed within a privacy policy framework in which fair information practices are implemented. The framework should address both whether an attribute requester may obtain access to certain classes of a Principal's attributes, and if yes, what fine-grained methods are allowed, and what data is returned to the attribute requester.

In order to enable implementers to set up this framework, the Liberty Specifications include a number of tools designed to (i) increase a Principal's choice and control with respect to (a) the federation of his identity within an Authentication Domain and (b) use and disclosure of personally identifiable information, and (ii) facilitate certain interactions among Identity Providers, Service Providers, and Attribute Providers without disclosing a Principal's identity. These tools include:

- **Access Controls** – The Liberty Specifications enable Liberty Providers to make access control decisions on behalf of the Principal. Liberty-Enabled Providers should provide a mechanism by which the Principal can specify his or her authorization policy. Thus, for example, a Principal might not allow his or her home address to go to a newspaper website, but might allow it to be sent to an online store as part of a sales transaction.
- **Usage Directives** – The Liberty Specifications describe a container that may be used to list or point to usage directives regarding either the intended use of a requested attribute (from the requester), or the allowed usage of a requested attribute (from the attribute owner/holder). The Attribute Provider and the Service Provider may negotiate acceptable usage directives. The Attribute Provider can provide the Service Provider with a list of acceptable usage directives when the intended usage requested by the Service Provider doesn't match the Principal's usage directives.
- **Opaque Handles** – The Liberty Specifications support opaque handles, the assignment of an arbitrary sequence of characters by the Identity Provider or Service Provider to identify a Principal. The opaque handle has meaning only in the context of the relationship between the Identity Provider and the Service Provider. Thus a Principal's identity and actions are harder to track as the Principal navigates among SPs.

The opaque handle mechanism allows the Service Provider to know which of their own customers, with local accounts, has navigated to the site. It facilitates identity federation between the Principal's accounts at the Identity Provider and the Service Provider *without* transferring any PII about the Principal to the Service Provider prior to identity federation.

- **Anonymous Identity Protocols** – The Liberty Specifications contain protocols for sharing personalization data with a Service Provider on an anonymous basis to allow for personalization of websites and services without disclosure of the identity of the Principal or requiring the Principal to have an account with the Service Provider. Using this tool, the Principal's actual identity is not released to the Service Provider. Rather, a transient name identifier is given to the Service Provider for each session that the Identity Provider can map to its account for the Principal.

In order for a company to effectively set up a privacy framework and implement fair information practices, Liberty recognizes that there are several points within the Liberty infrastructure where privacy concerns can be addressed and enforced. Liberty calls these "Policy Enforcement Points." For example,

1. The Identity Provider can decide whether or not to authenticate a Principal based on the credentials provided and the Identity Providers authentication policy.
2. At the point where a Service Provider receives an authentication from an Identity Provider, the Service Provider can decide whether a Principal's authentication context is sufficient based on the Service Provider's authentication policy.
3. At the point where an attribute requester requests Attribute Provider information for certain attributes from a Discovery Service, the Discovery Service can decide whether to facilitate an attribute requester's interaction with an Attribute Provider, based on a Principal-managed policy and the Discovery Service's policy.
4. At the point where an Attribute Provider has received the attribute request, the Attribute Provider may mediate an attribute requester's access to its services and data, based on a Principal-managed policy and the Attribute Provider's policy.

As noted previously, Principals should have the capability to specify policies governing access to their attributes. These Principal-specific policies could be defined by assigning some predefined rules to a particular class of attribute requesters, or via a user interface enabling Principals to define sophisticated rules. Also, the Service Provider, Identity Provider, Attribute Provider, and Discovery Service will need to write policies governing their infrastructure and their service. In any event, Principal specific permission rules should override default rules if they intersect. Most of these policies can be enforced at the Policy Enforcement Points numbers 3 and 4 identified above.

The access controls noted above can be used by an implementing company to set up an access management system to determine when and under what conditions various requesters may have access to requested information. The access decisions may be determined based on (i) what information is requested, (ii) what the requester wants to do with that information, (iii) the characteristics of the requester, and/or (iv) whether the owner of the requested information (i.e., the Principal) is online with a certain authentication context, etc. An implementing company should comply with its fair information practices when setting up its access management system.

In addition, by using the usage directives, implementing companies should give Principals the opportunity to specify how their personal information will be disclosed or accessed in a default context. In addition, under the Liberty Specifications, Principals can create the opportunity to validate, override, or update the Principal's default policies at request time by specifying obligations in their policies that are fulfilled by returning *permission exceptions* to requesting attribute requesters. These permission exceptions signal that the Principal must interactively validate, override, update or supply her instructions in the context of a particular transaction.

7. Security

Security is a critical component of any computing system, providing the necessary safeguards for data protection and integrity. Security is also a fundamental basis of consumer trust and confidence in any computing environment. As with privacy, it is incumbent upon all participants to provide and practice good security. Liberty-Enabled Providers must establish and maintain the level of security appropriate to the transaction and the data. Principals should be equally vigilant to protect themselves from security risks inherent in the architecture of the Internet.

Social vulnerabilities abound when deploying Internet technology; several factors contribute. A non-exhaustive list includes: human nature, rogues, buggy software, insecure systems, bad designs, poor human interfaces, and a large installed computing base of untrusted systems. These factors present a spectrum of opportunities for malicious behavior. Robust security precautions and implementations help to limit such opportunities. The Liberty Alliance specifications are based on existing, well known Internet protocols and mechanisms. Security weaknesses inherent in the architecture of the Internet are neither increased nor eliminated by the Liberty Specifications.

Security builds trust between the user and system and allows the user to let the system perform certain actions – therefore security will actually play a significant role in every system and environment. In a perfect situation, security is built as an almost invisible but strong service, which will protect the user against different attacks and/or minimize possible negative consequences.

Strong security is an essential part of a well-working network service solution, and Liberty offers security measures and guidance designed to prevent attackers from causing troubles for Liberty-Enabled Providers or for the Principal. The Liberty Alliance has referenced both the work of the OECD and the U.S. Federal Trade Commission (FTC) in providing this security framework.

The U.S. Federal Trade Commission examined security issues in 2000. The Final Report of the FTC Advisory Committee on Online Access and Security bears quoting in part:

Most consumers – and most companies – would expect commercial Web sites that collect and hold personal data to provide some kind of security for that data. Identifying the most effective and efficient solution for data security is a difficult task. Security is application-specific and process-specific. Different types of data warrant different levels of protection.

Security – and the resulting protection for personal data – can be set at almost any level depending on the costs one is willing to incur, not only in dollars but in inconvenience for users and administrators of the system. Security is contextual: to achieve appropriate security, security professionals typically vary the level of protection based on the value of the information on the systems, the cost of particular security measures and the costs of a security failure in terms of both liability and public confidence.

To complicate matters, both computer systems and methods of violating computer security are evolving at a rapid clip, with the result that computer security is more a process than a state. Security that was adequate yesterday is inadequate today. Anyone who sets detailed computer security standards – whether for a company, an industry, or a government body – must be prepared to revisit and revise those standards on a constant basis.

When companies address this problem, they should develop a program that is a continuous life cycle designed to meet the needs of the particular organization or industry. The cycle should begin with an assessment of risk; the establishment and implementation of a security architecture and management of policies and procedures based on the identified risk; training programs; regular audits and continuous monitoring; and periodic reassessment of risk. These essential elements can be designed to meet the unique requirements of organizations regardless of size.¹⁰

In addition to the above FTC recommendations, the Liberty Alliance offers the OECD Security principles for consideration by implementing companies in accordance with particular service offerings in various jurisdictions. These nine principles are applicable to all Liberty-Enabled Providers, or in OECD terms, “participants.” The specific responsibilities of any Liberty-Enabled Provider will vary according to their roles. The OECD Security Principles are:¹¹

1) Awareness

Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

¹⁰ US Federal Trade Commission Advisory Committee, “Final Report on Online Access and Security.”

¹¹ OECD, “OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.”

Awareness of the risks and available safeguards is the first line of defense for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Participants should be aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants.

2) Responsibility

All participants are responsible for the security of information systems and networks.

Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.

3) Response

Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

Recognizing the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation.

4) Ethics

Participants should respect the legitimate interests of others.

Given the pervasiveness of information systems and networks in our societies, participants need to recognize that their action or inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and to promote conduct that recognizes security needs and respects the legitimate interests of others.

5) Democracy

The security of information systems and networks should be compatible with essential values of a democratic society.

Security should be implemented in a manner consistent with the values recognized by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.

6) Risk assessment

Participants should conduct risk assessments.

Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others.

7) Security design and implementation

Participants should incorporate security as an essential element of information systems and networks.

Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimize security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organization's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.

8) Security management

Participants should adopt a comprehensive approach to security management.

Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.

9) Reassessment

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks.

8. Internet Security Vulnerabilities and Precautions

Regardless of the fair information principles and privacy practices adopted, security remains a universal vital tenet of fair information practices. Security vulnerabilities exist due to both system defects and human error or malice. There is a risk that these vulnerabilities will be exploited in an attack of some form. Attacks have different properties depending on which vulnerabilities are being exploited. Below are descriptions of the most common types of attacks.

- **Denial-of-service.** Prevents authorized users from accessing the system resource or delays authorized operations and functions. This can cause severe problems, e.g., for the Liberty-enabled providers' business and brand.
- **Dictionary.** An attack that uses a technique of successively trying all the words in some large, exhaustive list. This is a lesser kind of brute-force attack generally targeted at password authentication mechanisms. This kind of attack may lead, for example, to the impersonation of a user if an attacker can break the user's password.
- **Brute-force.** An attack that uses a technique of successively trying all possible combinations. This kind of attack may also lead, for example, to impersonation of the user if an attack can break the user's password. This attack requires more resources from an attacker compared to a dictionary attack but will provide better results when there is not a good dictionary available or when passwords are protected against being recognizable words.
- **Replay.** An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a spoofing attack.
- **Spoofing.** An attack in which one system entity illegitimately poses as (assumes the identity of) another entity. There is no way to prevent an attacker from erecting a false facade that mimics the appearance and

behavior of a legitimate website. If an attacker can lure the user into visiting such a site, then the user may be fooled into believing he/she is visiting the authentic website. If the fake site happens to imitate a site at which the user typically logs in, then the fake website may be able to collect the users credentials, such as, an account name and password. The attacker could then use this information to impersonate the user at a legitimate website. There is nothing about this attack, or the weaknesses exploited to carry it out, that are specific to Liberty Specifications. It is a general vulnerability that both Principals and Liberty-Enabled Providers must guard against.

Our purpose in presenting potential routes of attack is to explain the security vulnerabilities inherent in the Internet, so that Liberty-Enabled Providers are aware of the various risks and threats and thus are able to safeguard against such risks and threats. Implementers should closely monitor security risks noted in the industry, because the situation changes rapidly, with new bugs found and existing ones corrected. Regardless of which avenue of attack is exploited, several common security weaknesses can exacerbate the potential for breach. The following sections discuss some of the more well known Internet insecurities and recommends precautions that may be taken.

8.1. Common Weaknesses

Weak Passwords – So-called “reusable passwords” are a typical means of authenticating users. Reusable means that the password is constant and used multiple times to gain access to an account. User may choose weak, “guessable” passwords which render their account susceptible to relatively simple guessing attacks (also known as “dictionary attacks”). The risks of weak passwords are significantly compounded when users choose the same password to access different accounts. This is especially true in a single sign-on environment.

Using arbitrary, unchecked, reusable passwords in conjunction with a single sign-on environment means that multiple accounts may be compromised at once by guessing one password. If the user were to choose different, unrelated passwords for each site, then the multiple sites would be better protected. But if the user does not, then the vulnerability of the multiple sites is essentially the same with or without the single sign-on environment.

Where appropriate, Identity Providers should support other forms of authentication in addition to User ID and password. In addition, Identity Providers should inform Principals how to formulate and protect their passwords from unauthorized use. In the case of password usage, IdPs can also use password-checking mechanisms to check the Principal’s password. However Liberty Specifications do not force these functionalities and their usage is dependent on the IdP.

Embedded Login Forms – The ID-FF Architecture Overview 1.2 describes a deployment scenario where an Identity Provider’s login form is embedded within a page presented by a Service Provider. Users often prefer the seamlessness of this embedded form mechanism, which submits the users’ credentials back to the Identity Provider. However, embedded forms may permit the inadvertent exposure of Identity Provider credentials to the Service Provider in unencrypted clear text. Thus, when using authentication via embedded form, deployers should have contracts in place requiring the protection of embedded login forms.

Publicly Available Terminals– If a Principal accesses a Liberty-Enabled site using a public browser (such as at an airport kiosk or Internet cafe), there may be no rapid way for the user to terminate the session. If a Principal leaves a public browser without fully terminating the session, a subsequent Internet user may have access to the Principal’s browser session.

To prevent session hijacking at a public browser, short-session times are recommended for Identity Providers. This, of course, creates a problem for Principals who leave a browser session inactive, but intend to return after some time period. This is a classic tradeoff problem, and the Liberty Alliance recommendation is in favor of security.

In addition, when during a slightly shorter interval the account shows activity by the Principal at a Service Provider, the Service Provider with whom the activity is occurring sends a refresh message to the Identity Provider. One plausible way to perform the “refresh” is for the Service Provider to send an Authentication Request (AuthnRequest) message to the Identity Provider over the preferred channel containing some defined combination of the AuthnRequest parameters, thus signaling that “the user is still active over here.”

We recommend that Identity Providers have a mechanism that enables the Principal to later return using a different browser session and terminate the previous session. We also recommend that a change password feature be available

which challenges the user for their old password before accepting the new one. In addition, the Liberty Alliance currently intends to provide a refresh message mechanism in future versions of the Liberty Specifications.

Weak Cryptography – One of the most vexing issues in securing web services is that the currently installed browser base includes many browsers that only have weak 40-bit cryptography enabled. It is well known that 40-bit ciphers are considered weak and can be compromised with minimal computing effort. This poses a risk since users' encrypted communication may be easily recovered to the unencrypted form. However, the Liberty Specifications recommend cipher suites that minimally have effective secret key sizes of 112-bits. In case of signatures and public key cryptosystems the recommended minimum key length is 1024-bits.

8.2. Browser Vulnerabilities

Social vulnerabilities abound when deploying Internet technology; many factors contribute. A non-exhaustive list includes: human nature, rogues, buggy software, insecure systems, bad designs, poor human interfaces, and a large installed computing base of untrusted systems. These factors present a spectrum of opportunities to exploit one or a combination of weaknesses.

When using Internet browsers, we also need to consider their potential weaknesses. It is widely known that browsers have security-related weaknesses which can lead to information leakage. This best practices document provides information about such vulnerabilities and tips on how to avoid the most common vulnerabilities. Specifically, the security considerations section of the Liberty ID-FF Bindings and Profiles Specification describes potential vulnerabilities that are present as a consequence of implementation decisions and gives guidance in constructing name identifiers, which are a privacy-enhancing mechanism.¹² For more information about the secure implementation of Liberty version 2, please refer to the Liberty Alliance.¹³ This section discusses specific browser weakness and suggests mitigation strategies. In the next section we examine security issues related to well-established protocols.

Account Federation – The Liberty Specifications enable the Principal to federate identities, binding accounts together. If done improperly, the binding could release PII. The Liberty Specifications avoid this problem by recommending implementations that generate opaque handles using arbitrary sequences of characters that map into the account. The Liberty Specifications provide for the exchange of opaque handles to federate accounts. Additionally, Identity Providers are required to create unique opaque handles for each of the Principal's federated accounts. This diminishes the threat of collusion and tracking.

Cookie Exposure – Many web browsers implement a technology known as HTTP cookies. The intended function of cookies is to supplement web protocols with state management (or session) capabilities. Cookies can be transient (used just for the lifetime of the browser session) or persistent. A persistent cookie is saved to permanent storage so that it is available the next time the user starts a web browser. The various manners in which cookies are used may sometimes violate users' privacy. For example, a cookie may collect PII without a user's consent. In addition, web browsers and other Internet software have been shown to be susceptible to inadvertent disclosure of cookies to unauthorized parties. Since a cookie may contain PII, or could even be used to impersonate a Principal, this represents an additional security and privacy risk.

The Liberty Specifications do not mandate the use of cookies, but allows for an optional cookie-based mechanism which is used to simplify single sign-on. The information in this cookie is not a privacy risk since the only information revealed are the locations or websites at which the Principal authenticates. This particular cookie is referred to as the "common domain cookie" in the Liberty Specifications.

However, in addition to the common domain cookie, it is recognized that many websites, in order to provide a "seamless" user experience, will rely on the state management properties of cookies. Note that this issue is not specific to the Liberty Specifications. Any website that uses cookies for state management – with or without Liberty Specifications – is subject to the risks regarding the exposure of cookie contents. The actual risk depends on how the website constructs their cookies, the lifetime of the cookie, and the cookie contents. If a cookie were to present the above mentioned risks, an attacker would need to discover a software defect or have access to a Principal's computer

¹² John Kemp and Tom Wason, "ID-FF Bindings & Profiles Specification."

¹³ Jonathan Tourzan, "ID-WSF Architecture Overview." , ID-WSF Security and Privacy Guidelines and ID-WSF Security Profiles.

in order to exploit the vulnerability. Principals should normally have the opportunity and guidance necessary to decline cookies. For service offerings that are cookie dependent, care should be taken that the cookie does not collect or store PII.

Cross Site Scripting – Cross Site Scripting (CSS) was originally published as a CERT advisory [CSS] in February 2000. To date this is still a very common threat and has been used to trick browsers to make incorrect trust decisions such as erroneously trusting malicious code.

A CSS vulnerability could potentially be used to collect HTTP cookies or the URL history and disseminate the data to an unauthorized party. Note that this is not an issue specific to the Liberty Specifications. Combining a CSS vulnerability with a social vulnerability could potentially fully compromise a user's accounts in a single sign-on environment. The CSS vulnerability is related to browser security and avoiding this problem requires changes in browsers' architecture, which is beyond the scope of the Liberty Alliance. However, Principals should be warned as to the potential CSS vulnerability and take necessary precautions, including being very selective and limiting their use of hyperlinks in emails or instant messages to only those communications from known or trusted senders.

Related Documents/RDF – The "Related Documents Feature" (RDF) implemented in both Netscape and Internet Explorer, "Smart Browsing/What's Related" and "Show Related Documents" respectively, is known to be a very leaky channel. Essentially when the feature is enabled, the browser reports to the RDF service the referring URL and the URL to which the browser is being navigated. Like CSS, this vulnerability is inherent in the architecture of the browser. Principals should be warned of the potential for leakage and may wish to avoid the use of RDF in some circumstances.

8.3. Protocol Vulnerabilities

The Liberty Specifications were built on existing Internet technologies, meaning both browsers and protocols. The previous section discussed browser weaknesses. We now turn to protocol weaknesses. The core Internet protocols used whenever online include the Transmission Control Protocol (TCP), the Internet Protocol version 4 (IP), the User Datagram Protocol (UDP) and the Domain Name System (DNS). When browsing the Web there is another layer of protocol with the Hypertext Transfer Protocol (HTTP). These protocols are insecure. They do not support fundamental security properties of integrity, confidentiality or authenticity. In the event that a website needs to securely communicate with the browser, the Transport Layer Security version 1.0 (TLS) or Secure Socket Layer version 3.0 (SSL) protocol is inserted in a layer between TCP/IP and HTTP. This combination yields the protocol scheme known as HTTPS.

The most common tool used to access Internet resources – and thus make use of the protocols mentioned above – is the web browser. Web browsers also have insecure aspects. The remainder of this section describes vulnerabilities of these protocols and browsers and the risks and threats they pose. Please note that the issues discussed herein are present whenever anyone browses the Internet – regardless of whether Liberty Specifications are being used.

DNS – A DNS server resolves the host names found in Uniform Resource Locators (URL) into a numeric Internet address. There are two well-known ways that DNS spoofing can occur, and both can result in a user connecting to a rogue site and mistakenly believing it is real.

First, there is no assurance in the protocol that replies to queries are genuine and have not been tampered with. It has been demonstrated that rogue DNS address records can contaminate the cache of an otherwise trusted resolver. The obvious threat this spoofing attack presents is that the peer host may end up connecting to the rogue site.

The second DNS vulnerability is the possibility of a compromised DNS server. If a DNS server is hijacked, then what seems to be legitimate address resolution may also result in the user connecting to a rogue website.

In both scenarios the user has no way of knowing that he/she is not communicating with the correct host. This contributes to the "spoofing" social vulnerability discussed above

To be more resilient to these sorts of attacks, deployers can utilize SSL server authentication via HTTPS. Generally the subject name in the public key certificate bears the domain name of the server, which should match the host name in the URL used for contacting the server. Thus, along with proper certificate path validation of the server domain

name from the certificate, one can verify that both that name and the host name in the URL indeed match, and are bona fide.¹⁴

Structural remedies for the DNS vulnerabilities are available but not widely deployed. The Domain Name System Security Extensions define extensions which integrity protect the records returned through the use of digital signatures. Also, the security extensions provide for the optional authentication of DNS protocol interactions.

HTTP – HTTP, the prevalent web protocol, makes extensive use of URLs. URLs have a syntax enabling the embedding of adjunct information. The Liberty Specification makes extensive use of this capability. At times, such embedded information may contain sensitive data. HTTP implementations must convey and consume URLs; thus the information embedded in a URL must be visible to the endpoints. Thus there are no provisions in HTTP for protecting such sensitive, URL-embedded information. Therefore, the onus is upon HTTP implementations – browsers and web servers – to avoid inadvertently disclosing this information. The Liberty Specifications recommend implementers protect the sensitive data carried in URLs. The recommended method to protect this information in transit is for the Service Provider to protect the sensitive relay state information. Since the Service Provider is both the producer and consumer of the relay state information, the Liberty Specifications do not mandate what specific cryptographic algorithms and primitives to use. The acquired data must be stored securely. URL leaks are discussed in more detail below.

URL – The Liberty Specifications may be used to convey sensitive information between parties in URLs. There are numerous methods in which referenced URLs can leak. For example, most browsers maintain a history of visited web addresses; browsers may report to the visited website the referring URL and most websites maintain logs of activity by capturing the URLs being requested as well as the referring URL. In addition, web proxy servers are deployed within intranets to facilitate passing web traffic through the corporate firewall, and proxy servers also maintain logs of the URLs requested. Finally, firewalls typically log traffic passing through them for auditing purposes. All of these retention points pose a risk if the data in the URL is sensitive and exposed to an unauthorized party.

In designing the Liberty Specifications, common-sense efforts were made to minimize the chance of disclosing the information conveyed in the URL to an unauthorized party. Liberty Specifications prescribe the following two recommendations:

First, the Liberty Specifications recommend that entry points and subsequent protocol exchanges be initiated over a secure communication transport, TLS or SSL, which implies the URLs should specify the HTTPS scheme. By following this guidance, sensitive information contained in URLs is available only at the points where it is produced, relayed (via the browser) and consumed. More simply stated, unauthorized observers cannot see the exchanged URLs and confidential information in them.

Second, the Liberty Specifications recommend that state information passed in the URL be integrity and confidentiality protected. This is a privacy enhancing measure that limits the exposure of the Principal's Service Provider activities. It also protects the Service Provider from initiating actions on behalf of the user if the state information were fabricated or tampered with.

Network Time Protocol (NTP) Weaknesses – Both the Liberty Specifications and the Security Assertion Markup Language version 1.0 specifications employ time-based mechanisms to qualify the validity of a message and the assertions they contain. This suggests that the clocks of participating systems are synchronized so that the validity periods can be accurately verified and honored. The time-based qualifiers may also be used as countermeasures against replay attack (described above). By enforcing the validity periods, we minimize the attackers window of opportunity. The smaller the time window between the generation of an assertion and its consumption, the better the security of the protocol. Therefore, if such a countermeasure is deployed, then it will be necessary to keep the clocks of the participating sites synchronized.

NTP is designed to keep the clocks of distributed systems synchronized. NTP is not a secure protocol and measures must be taken to prevent an attacker from disrupting the service. To defend against a rogue system influencing the synchronization process by broadcasting invalid time information, authentication and access controls should be used to

¹⁴ Procedures for performing such name matching, also known as a “server identity check,” are specified in C. Newman, 1999 and J. Hodges, R. Morgan, and M. Wahl, 2000.

limit potential synchronization sources. A more thorough coverage of this topic can be found in the Sun Blueprint Series.¹⁵

8.4. Summary

The Liberty Alliance developed a set of standards for single sign-on and federated network identity building on currently-deployed browsers. The vulnerabilities described above, from the serious ones of Cross-Site Scripting to the more arcane problems of Network Time Protocol, are problems of the underlying infrastructure. The Liberty Alliance has made every effort to provide secure standards, but the standards are built on top of insecure existing Internet protocols and, unavoidably, present potential vulnerabilities. This is not to suggest that the Liberty Specifications are insecure, but that implementations are dependent on all the underlying protocols. Thus, care should be taken in implementation and the Liberty Alliance Implementation Guidelines should be carefully followed.¹⁶

9. Terminology

Below please find a glossary of certain terms used throughout this document. For more information regarding Liberty terms, please see the Liberty Glossary.¹⁷

Access control

The act of mediating requested access to a resource based on privilege attributes of the requester and control attributes of the requested resource.

Attribute

A distinct characteristic of a Principal. A Principal's attributes are said to describe it.

Attribute class

A predefined set of attributes, such as the constituents of a Principal's name (prefix, first name, middle name, last name, and suffix). Liberty entities may standardize such classes.

Attribute Provider (AP)

The attribute provider (AP) provides ID-PP information. Sometimes called a ID-PP provider, the AP is an ID-WSF web service that hosts the ID-PP.

Authentication

The process of verifying the ability of a communication party to "talk" in the name of a Principal.

Authentication Domain (AD)

A formal community of Liberty-enabled entities that interact using a set of well-established common rules.

Authentication session

The period of time starting after A has authenticated B and until A stops trusting B's identity assertion and requires reauthentication. Also known as "session," it is the state between a successful login and a successful logout by the Principal.

Authorization

A right or a permission that is granted to a system entity to perform an action.

Credentials

Known data attesting to the truth of certain stated facts.

¹⁵ J. Hodges, R. Morgan, and M. Wahl, 2000.

¹⁶ Susan Landau, "Liberty Security and Privacy Overview."

¹⁷ Tom Wason, "Liberty Glossary."

Data

Any information that a Principal provides to an Identity Provider or a service provider.

Discovery Service (DS)

An entity that has the ability to direct attribute requesters to the relevant attribute provider who provides the requested classes of attributes for the specified Principal.

Federate

To link accounts at two or more entities together.

Federated architecture

An architecture that supports multiple entities provisioning Principals among peers within the Liberty Authentication Domain.

Federation

An association comprising any number of Service Providers and Identity Providers.

Identity

The essence of an entity, often described by its characteristics.

Identity federation

Associating, connecting, or binding multiple accounts for a given Principal at various Liberty-enabled entities within an Authentication Domain.

Identity Provider (IdP)

A Liberty-enabled entity that creates, maintains, and manages identity information for Principals and provides Principal authentication to other Service Providers within an Authentication Domain. An Identity Provider may also be a Service Provider.

Liberty-Enabled Provider

As used herein, and only herein, LEP may be either an Attribute Provider (AP), Discovery Service (DS), Service provider (SP), or Identity Provider (IdP) who collects, transfers, or receives the Personally Identifiable Information (PII) of a Principal.

Permission

Privileges granted to each user with respect to what data that the user is allowed to access and what menus options or commands he or she is allowed to use.

Personally Identifiable Information (PII)

Any data that identifies or locates a particular person, consisting primarily of name, address, telephone number, e-mail address, bank accounts, or other unique identifiers such as Social Security numbers.

Principal

A Principal is an entity that can acquire a federated identity, that is capable of making decisions, and to which authenticated actions are performed on its behalf. Examples of Principals include an individual user, a group of individuals, a corporation, other legal entities, or a component of the Liberty architecture.

Privacy

Proper handling of personal information throughout its life cycle, consistent with the preferences of the data subject.

Profile

Data comprising the broad set of attributes that may be maintained for an identity, over and beyond its identifiers and the data required to authenticate under that identity. At least some of those attributes (for example, addresses, preferences, card numbers) are provided by the Principal.

Rights Expression Languages (RELs)

A machine-based language that enables communication about usage directives. RELs allow an information provider to request intended uses of information before the information is exchanged and to designate approved uses for information exchanged during a particular transaction.

Service Provider (SP)

An entity that provides services and/or goods to Principals.

Usage directives

Directives that specify the manner in which attributes can be used, stored, and disclosed.

10. References

- BBB Online, Inc. and the Council of Better Business Bureaus, Inc. "A Review of Federal and State Privacy Laws." http://www.bbbonline.org/UnderstandingPrivacy/library/fed_statePrivLaws.pdf (accessed April 11, 2003).
- Berman, J., and D. Mulligan. "Privacy in the Digital Age: Work in Progress." 23 Nova Law Review 2 1999. <http://www.cdt.org/publications/lawreview/1999nova.shtml>.
- Canadian Parliament. Canadian Privacy Act. S.C. 2000, c.5 (2003).
- Cantor, Scott, Kemp, John, eds. (19 July 2003). "Liberty ID-FF Protocols and Schema Specification," Version 1.2-13, Liberty Alliance Project. <http://www.projectliberty.org/specs>.
- CDT Web Site. "Privacy Basics: Fair Information Practices." <http://www.cdt.org/privacy/guide/basic/fips.html> (accessed August 6, 2003).
- Center for Democracy and Technology (CDT) Web Site. "Data Privacy." <http://www.cdt.org/privacy> (accessed August 6, 2003).
- Ellison, Gary, ed. (25 July 2003) "Liberty ID-WSF Security Mechanisms," Version 1.0-17, Liberty Alliance Project. <http://www.projectliberty.org/specs>.
- European Parliament and the Council of 12 July 2002. Directive 2002/58/EC on privacy and electronic communications. http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002L0058&model=guichett (accessed April 11, 2003).
- European Parliament and the Council of 24 October 1995. Directive 95/46/EC on data protection. http://www.privacy.org/pi/intl_orgs/ec/eudp.html (accessed April 11, 2003).
- GBDe. "Personal Data Privacy Protection Guidelines." <http://www.gbde.org/privacy1.html> (accessed August 6, 2003).
- Hi-Ethics Web Site. www.hi-ethics.org (accessed April 2003).
- Hi-Ethics. "Health Internet Ethics: Ethical Principles For Offering Internet Health Services to Consumers." <http://www.hi-ethics.org/Principles/index.asp> (accessed April 2003).
- Hodges, J., R. Morgan, and M. Wahl. "Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security." May 2000. <http://www.isi.edu/in-notes/rfc2830.txt> (accessed April 11, 2003).
- Hodges, Jeff, ed. (October 11, 2002). "Version 1.0 Errata." Version 1.0, Liberty Alliance Project. http://www.projectliberty.org/specs/archive/v1_0/draft-liberty-version-1-errata-00.pdf.
- International Security, Trust and Privacy Alliance (ISTPA). "Privacy Framework v.1.1." <http://www.istpa.org/> (accessed April 11, 2003).
- Kemp, John, Wason, Tom, eds. (25 July 2003). "Liberty ID-FF Bindings and Profiles Specification," Version 1.2-14, Liberty Alliance Project. <http://www.projectliberty.org/specs>.
- Landau, Susan, ed. (24 July 2003). "Liberty ID-WSF Security and Privacy Overview," Draft version 1.0-09, Liberty Alliance Project.

- 1032 Liberty Alliance. "Security Bulletin." October 10, 2002,
1033 http://www.projectliberty.org/specs/archive/v1_0/security_bulletin.html.
- 1034 Linn, John, ed. (25 July 2003). "Liberty Trust Models Guidelines," Draft version 1.0-07, Liberty Alliance
1035 Project. <http://www.projectliberty.org/specs>.
- 1036 Madsen, Paul , ed. (25 July 2003). "Liberty Authentication Context Specification," Version 1.2-07,Liberty
1037 Alliance Project. <http://www.projectliberty.org/specs>.
- 1038 NAI. "Self-Regulatory Principles." http://www.networkadvertising.org/aboutnai_principles.asp (accessed April
1039 2003).
- 1040 Newman, C. "Using TLS with IMAP, POP3 and ACAP." RFC 2595, June 1999. [http://www.isi.edu/in-](http://www.isi.edu/in-notes/rfc2595.txt)
1041 [notes/rfc2595.txt](http://www.isi.edu/in-notes/rfc2595.txt) (accessed April 11, 2003).
- 1042 OECD. "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of
1043 Security." <http://www.oecd.org/pdf/M00033000/M00033182.pdf> (accessed April 11, 2003).
- 1044 OPA. "Guidelines for Online Privacy Policies." <http://www.privacyalliance.org/resources/ppguidelines.shtml>
1045 (accessed April 2003).
- 1046 Organization for Economic Co-operation and Development (OECD). Web Pages regarding privacy and security
1047 concerns. <http://www.oecd.org/EN/home/0,,EN-home-43-1-no-no-no-43,00.html> (accessed April 2003).
- 1048 Privacy International, "Privacy and Human Rights: An International Survey of Privacy Laws and Developments,
1049 2002." <http://www.privacyinternational.org/survey/phr2002/> (accessed April 2003).
- 1050 The Global Business Dialogue on Electronic Commerce (GBDe) Web Site. <http://www.gbde.org/gbde2003.html>
1051 (accessed August 6, 2003).
- 1052 The Network Advertising Initiative (NAI) Web Site. <http://www.networkadvertising.org/> (accessed April 2003).
- 1053 The Online Privacy Alliance (OPA) Web Site. <http://www.privacyalliance.org/> (accessed April 2003).
- 1054 U.S. Federal Trade Commission Advisory Committee. "Final Report on Online Access and Security." (2000)
1055 <http://www3.ftc.gov/acoas/papers/acoasdraft1.htm> (accessed April 11, 2003).
- 1056 USCA. 15 U.S.C.A. § 6501 (2000); 15 U.S.C.A. § 6801 et. seq. (1999); 42 U.S.C.A. §§ 1320(d) et. seq. (1996);
1057 15 U.S.C.A. § 45(a) (2000).
- 1058 Wason, Thomas, ed. (06 August 2003). "Liberty Architecture Glossary," Version 1.2-09, Liberty Alliance
1059 Project. <http://www.projectliberty.org/specs>.
- 1060 Wason, Thomas, ed. (25 July 2003). "Liberty ID-FF Architecture Overview," Version 1.2-03,Liberty Alliance
1061 Project. <http://www.projectliberty.org/specs>.
- 1062 Wason, Tom, ed. (14 Apr 2003). "Liberty ID-FF Implementation Guidelines," Version 1.2-08, Liberty Alliance
1063 Project. <http://www.projectliberty.org/specs>.
- 1064 Weitzel, David, ed. (August 1, 2003). "Liberty ID-WSF Implementation Guide," Version 1.0-01, Liberty Alliance
1065 Project. <http://www.projectliberty.org/specs>.