



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, 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 Summary	2
2. Introduction.....	3
3. Liberty Alliance Perspective on Privacy.....	4
4. Privacy laws.....	5
5. Fair Information Principles	6
6. Liberty Alliance Privacy Recommendations.....	8
7. Security	20
8. Internet Security Vulnerabilities and Precautions	23
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

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

43 **Security, Internet Protocols and Browsers:**

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

52 **2. Introduction**

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

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

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

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

75 Companies that implement the Liberty Specifications are advised to consult with local counsel to ensure that the
76 services they provide, based upon the Liberty Specifications, comply with applicable law. Please note that these best
77 practices are intended to provide guidelines, not serve as an exhaustive resource. Furthermore, from a technical
78 standpoint, these best practices are non-normative – they are not the rules defining the Liberty Specifications, but
79 rather identify the privacy and security concerns that should be addressed when implementing Liberty Specifications.
80 It is important to note that the Liberty Specifications are based upon existing Internet architecture and well-known
81 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.”

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

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

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

99 **3. Liberty Alliance Perspective on Privacy**

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

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

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

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

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

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

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

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

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

146 **4. Privacy laws**

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

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

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

162 The EU Data Protection Directive (95/46/EC) aims to protect the privacy of EU citizens and harmonize differing laws
163 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.”

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

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

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

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

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

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

201 **5. Fair Information Principles**

202 **General.** In addition to existing privacy laws, several organizations have set forth fair information practices governing
203 the use and disclosure of personal information. These organizations include, among others, the Online Privacy
204 Alliance (“**OPA**”), the Organization for Economic Co-operation and Development (“**OECD**”), the Center for
205 Democracy and Technology (“**CDT**”), the Network Advertising Initiative (“**NAI**”), Health Internet Ethics (“**Hi-**
206 **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.

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

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

213 • **Adoption and Implementation of a Privacy Policy** – An organization should adopt and implement a policy
214 for protecting the privacy of individually identifiable information.

215 • **Notice and Disclosure** – The privacy policy should be clear, easy to find, and available at or prior to the
216 time individually identifiable information is collected. It should state “what information is being collected;
217 the use of that information; possible third-party distribution of that information; the choices available to an
218 individual regarding collection, use and distribution of the collected information; a statement of the
219 organization's commitment to data security; and what steps the organization takes to ensure data quality
220 and access. It should also disclose the consequences, if any, of an individual's refusal to provide
221 information. The policy should also include a clear statement of what accountability mechanism the
222 organization uses, including how to contact the organization.”

223 • **Choice/Consent** – Individuals must be given the opportunity to exercise choice regarding how individually
224 identifiable information collected from them online may be used when such use is unrelated to the purpose
225 for which the information was collected or where there is third-party distribution of such data unrelated to
226 the purpose for which it is collected. At a minimum, individuals should be given the opportunity to opt out
227 of such use or third-party distribution.

228 • **Data Security** – Organizations creating, maintaining, using or disseminating individually identifiable
229 information should take appropriate measures to assure its reliability and should take reasonable
230 precautions to protect it from loss, misuse or alteration. Organizations should take reasonable steps to
231 assure that third parties to which they transfer such information are aware of these security practices, and
232 that the third parties also take reasonable precautions to protect any transferred information.

233 • **Data Quality and Access** – Organizations creating, maintaining, using or disseminating individually
234 identifiable information should take reasonable steps to assure that the data are accurate, complete and
235 timely for the purposes for which they are to be used. Organizations should establish appropriate
236 processes or mechanisms so that inaccuracies in material individually identifiable information, such as
237 account or contact information, may be corrected. These processes and mechanisms should be simple and
238 easy to use, and provide assurance that inaccuracies have been corrected. Other procedures to assure data
239 quality may include use of reliable sources and collection methods, reasonable and appropriate consumer
240 access and correction, and protections against accidental or unauthorized alteration.

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

246 • **Collection Limitation** – There should be limits to the collection of personal data and any such data should
247 be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data
248 subject.

249 • **Data Quality** – Personal data should be relevant to the purposes for which they are to be used, and, to the
250 extent necessary for those purposes, should be accurate, complete and kept up-to-date.

251 • **Purpose Specification** – The purposes for which personal data are collected should be specified not later
252 than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or
253 such others as are not incompatible with those purposes and as are specified on each occasion of change of
254 purpose.

255 • **Use Limitation** – Personal data should not be disclosed, made available or otherwise used for purposes
256 other than those specified in accordance with Article 9 (the purpose specification principle) except: (a)
257 with the consent of the data subject; or (b) by the authority of law.

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

273 6. Liberty Alliance Privacy Recommendations

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

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

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

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

311 • **Quality.** Consumer facing Liberty-Enabled Providers that collect and maintain personally identifiable
312 information should permit Principals a reasonable opportunity to provide corrections to the personally
313 identifiable information that is stored by such entities.

314 • **Relevance.** Liberty-Enabled Providers should use PII for the purpose for which it was collected, or the
315 purposes about which the Principal has consented.

316 • **Timeliness.** Liberty-Enabled Providers should retain PII only so long as is necessary or requested and
317 consistent with a retention policy accepted by the Principal.

318 • **Complaint Resolution.** Liberty-Enabled Providers should offer a complaint resolution mechanism for
319 Principals who believe their PII has been mishandled.

320 • **Security.** Liberty-Enabled Providers should take reasonable steps to protect and provide an adequate level
321 of security for PII.

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

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

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

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

346 • **Principal** – A Principal is an entity that can acquire a federated identity that is capable of making
347 decisions and can be authenticated and vouched for by an Identity Provider. In a business-to-consumer
348 (B2C) context, the Principal is the consumer. In other contexts, the Principal could be an individual, a
349 corporation, or another legal entity. The fair information best practices set forth in this document are
350 aimed to protect the confidentiality of the Principal's personally identifiable information. Principals
351 should be vigilant when they provide their credentials (e.g., passwords, secure tokens, etc., entered
352 over secure channels) or attributes over the web to protect themselves from being spoofed or otherwise
353 providing such information to an unintended party. In addition, Principals should use care when
354 establishing or modifying credentials. Also, Principals should become familiar with an entity's posted
355 data practices before providing personally identifiable data to such entity.

356 • **Service Provider** – A Service Provider is an entity that provides services to Principals. Liberty
357 envisions that the Service Provider will, upon request from a Principal, request that the Identity
358 Provider (which may be itself or another party) authenticate the Principal. After the Principal has been
359 authenticated, the Service Provider may request that certain attributes regarding the Principal be

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

367 • **Identity Provider** – An Identity Provider is an entity that creates, maintains, and manages identity
368 information for Principals. It authenticates and vouches for the Principal to other Service Providers
369 within an Authentication Domain. The Identity Provider should also safeguard the Principal's identity
370 credentials, and have some mechanisms in place to require the Authentication Domain to use the
371 credentials in a proper manner.

372 • **Attribute Provider** – An Attribute Provider is an entity that provides attributes to a requester (i.e., a
373 Service Provider) in accordance with its own policies and a Principal's permissions. Attribute
374 Providers store and negotiate access control information defining the circumstances under which a
375 Service Provider will be granted access to a given attribute(s). Attribute Providers store and negotiate
376 usage directives that specify the manner in which attributes can be used, stored, and disclosed. An
377 Attribute Provider has at least the same responsibilities as Service Providers with respect to clear
378 notice (including notice to the Principal regarding what are the default usage directives and how the
379 Principal can change such usage directives), choice, security, and responsible use and sharing of a
380 Principal's data.

381 • **Discovery Service** – A Discovery Service is an entity (usually an Identity Provider) that has the ability
382 to direct attribute requesters to the relevant Attribute Provider who provides the requested classes of
383 attributes for the specified Principal. The Discovery Service should register only those Attribute
384 Providers in accordance with the consent or usage directives of the Principal. The Discovery Service
385 should permit the Principal to see which Attribute Providers have been registered on the Principal's
386 behalf. An attribute requester can locate the Attribute Providers for a given Principal, even though the
387 attribute requester and Attribute Providers do not have a common name for the Principal.

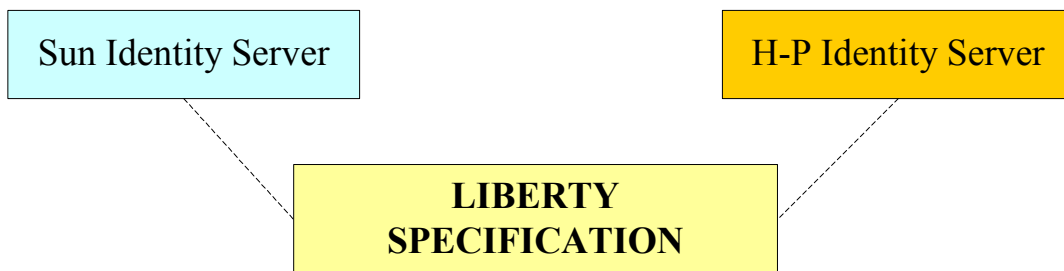
388 The following are two hypothetical examples of implementation of the Liberty Specifications by various companies.
389 In Example 1, we start with the actual equipment manufacturers who could build Internet infrastructure software
390 utilizing the specifications. Example 1 goes through the steps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

393

393 **Hypothetical Example 1**

394 *1. Technology Implementation*

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

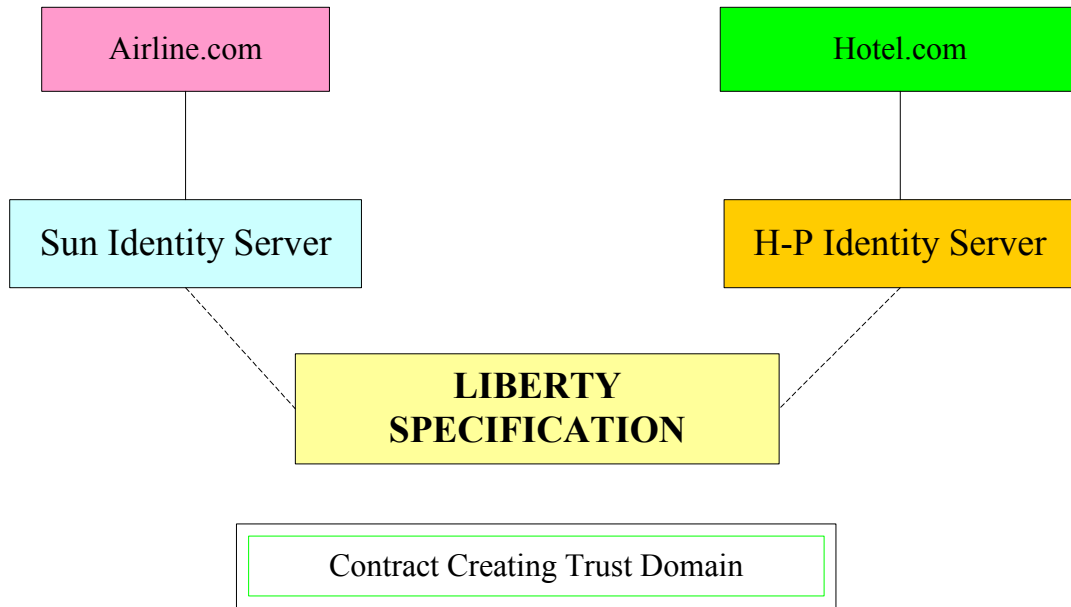


401

402

403

- 403 2. *Services Deployment*
- 404 a. Airline employs a Sun Identity Server to authenticate users to its website, maintain frequent flyer
- 405 information, and provide linkage to its reservation system.
- 406 b. Hotel uses an HP Identity Server to authenticate users to its website and facilitate online reservations.
- 407



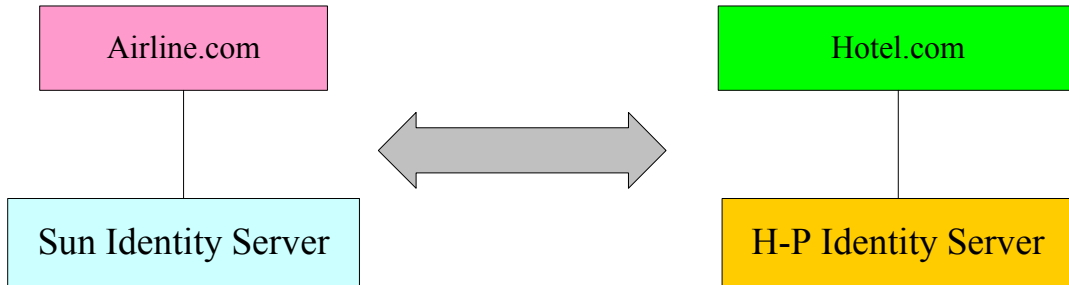
408

409

409 3. Trust Domain

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

413

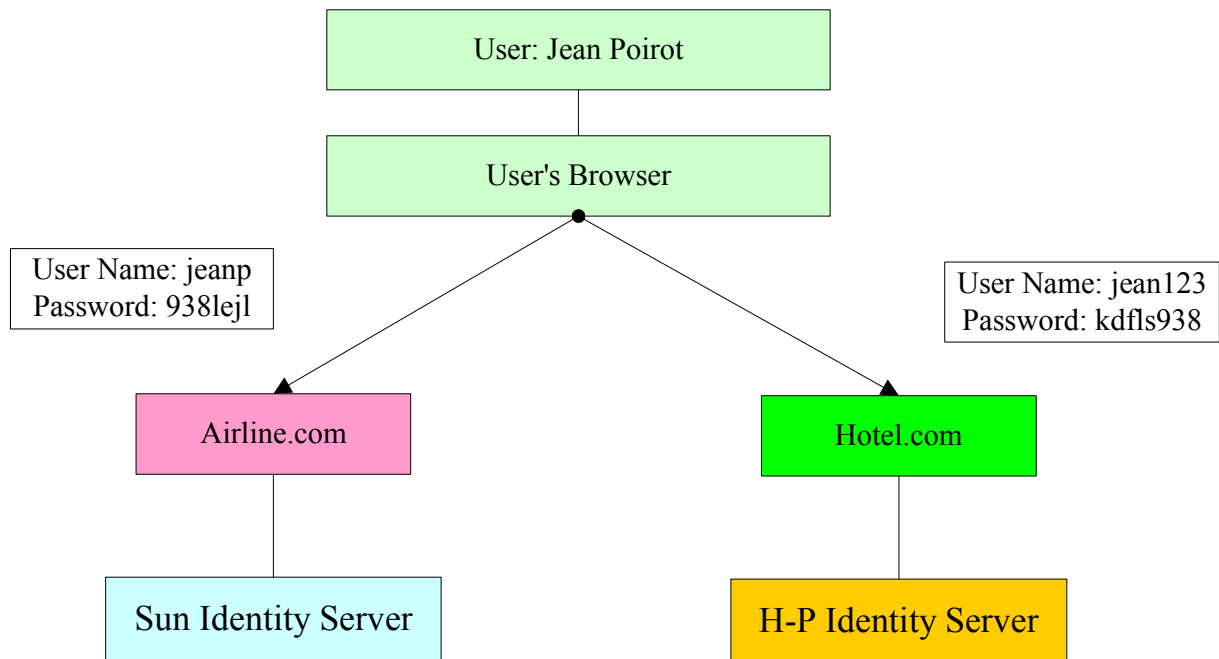


414

415 4. Account Establishment

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

418



419

420

421

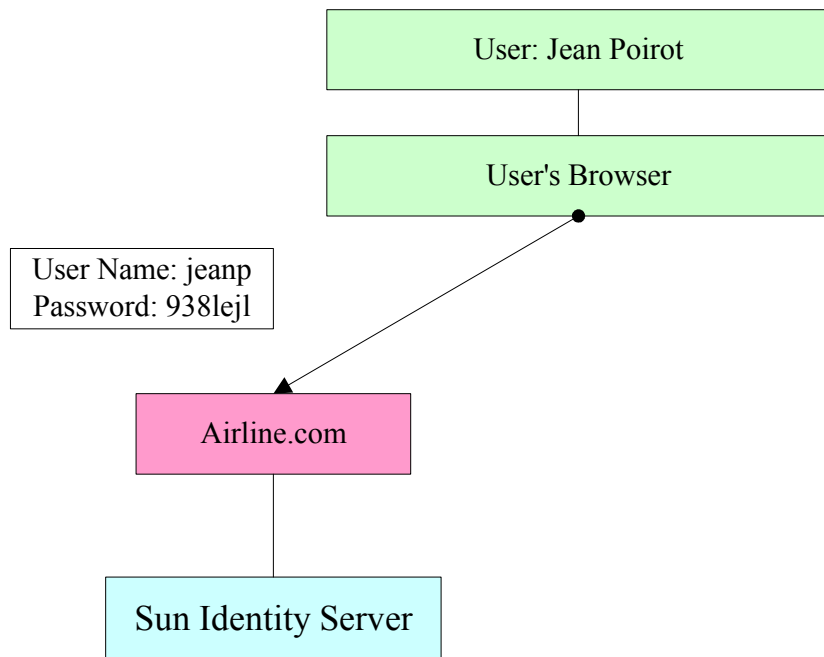
422

423

424 5. *Linking Accounts*

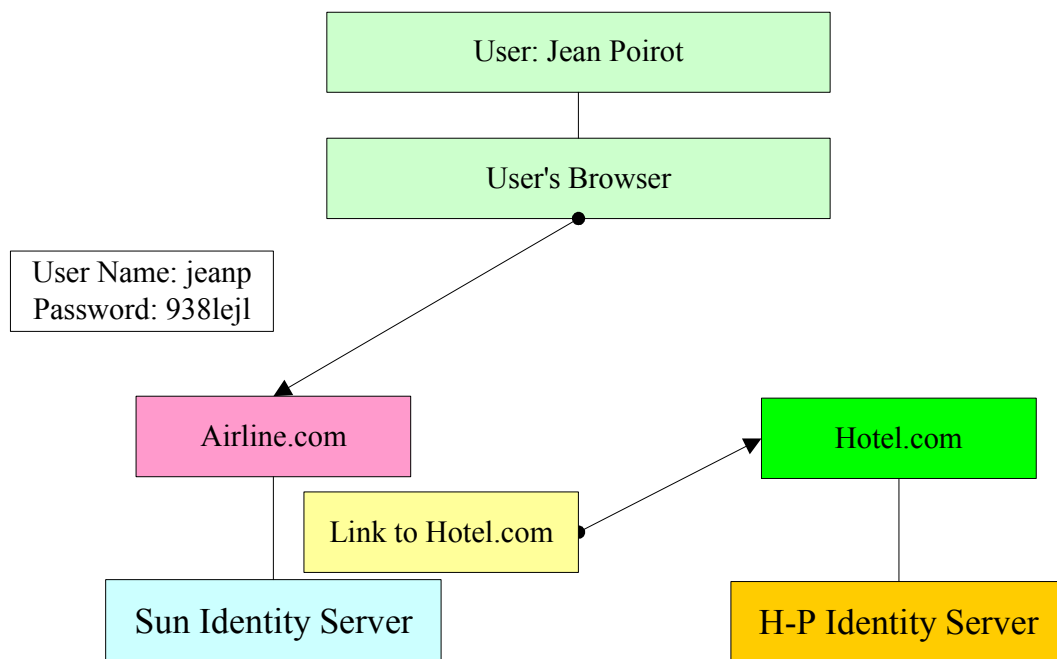
425 a. Jean logs onto the Airline site with user name and password

426



427

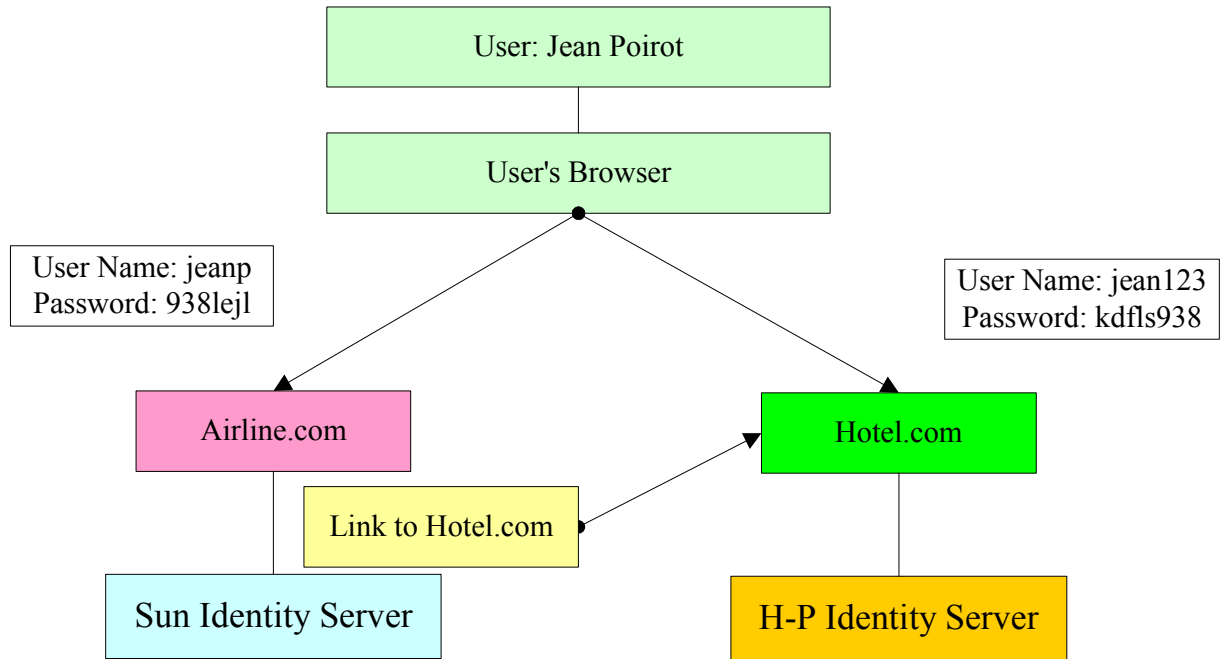
428 b. Airline has a link that JeanP can use to go to the Hotel website.



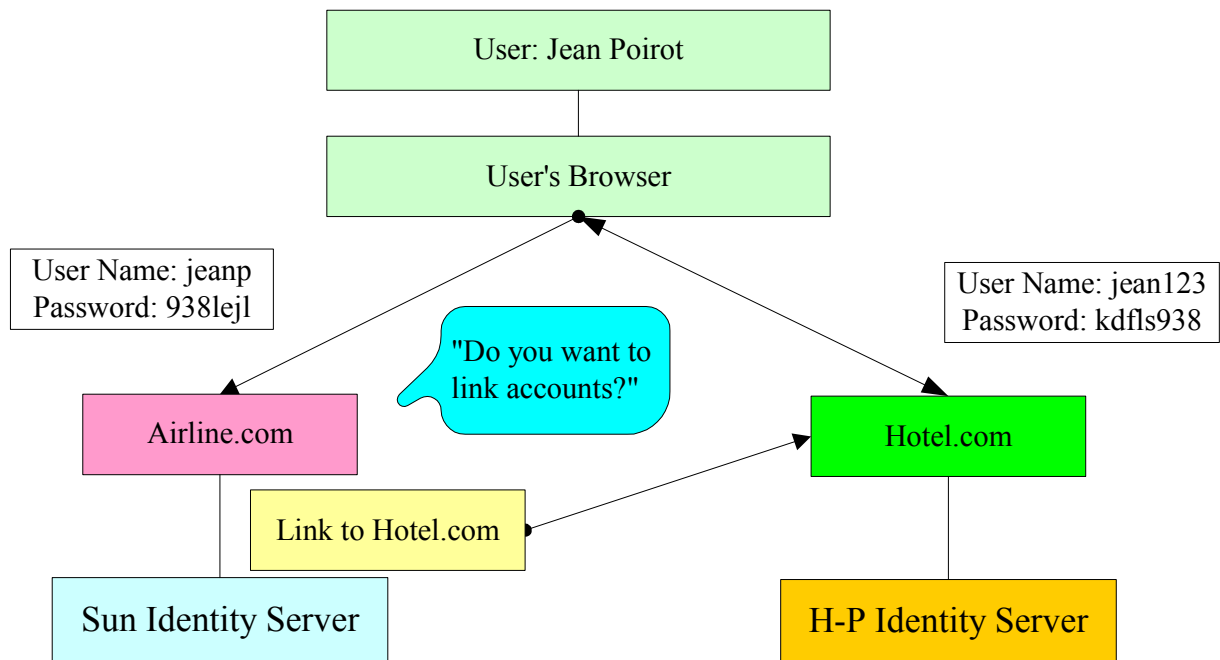
429

430

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

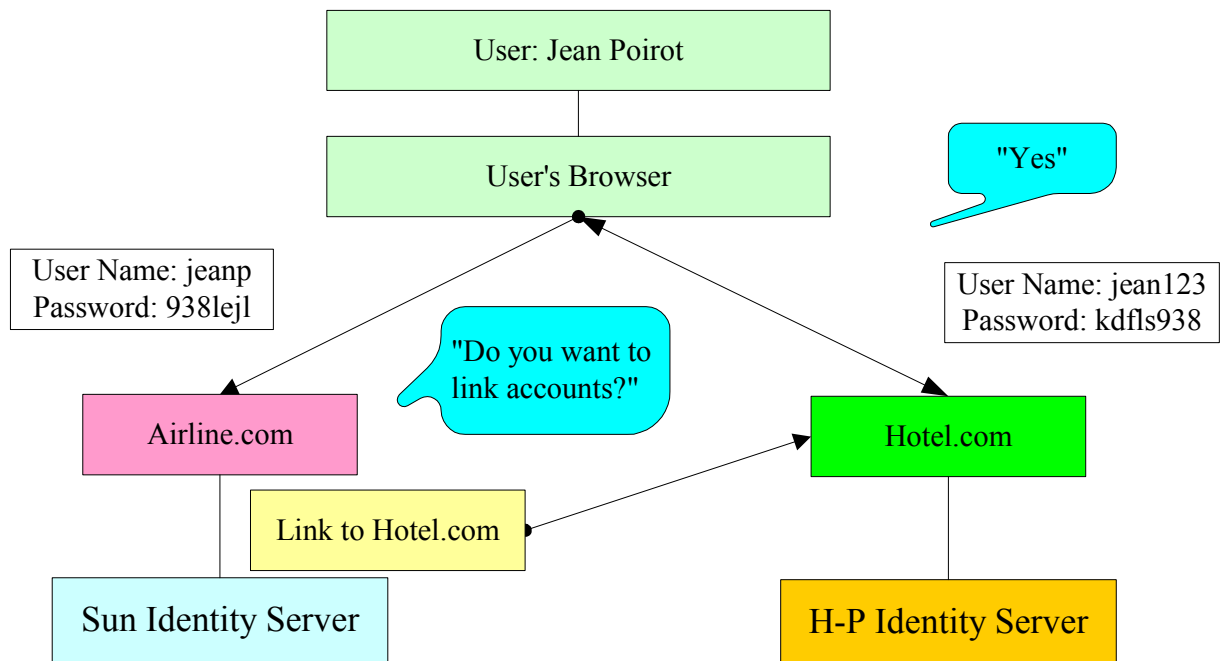


- 432
433 d. Hotel would know that Jean123 came from the Airline site and asks if Jean123 would like to link his
434 account at Airline with his account at Hotel, enabling single sign-on between the two accounts.



- 435
436
437
438

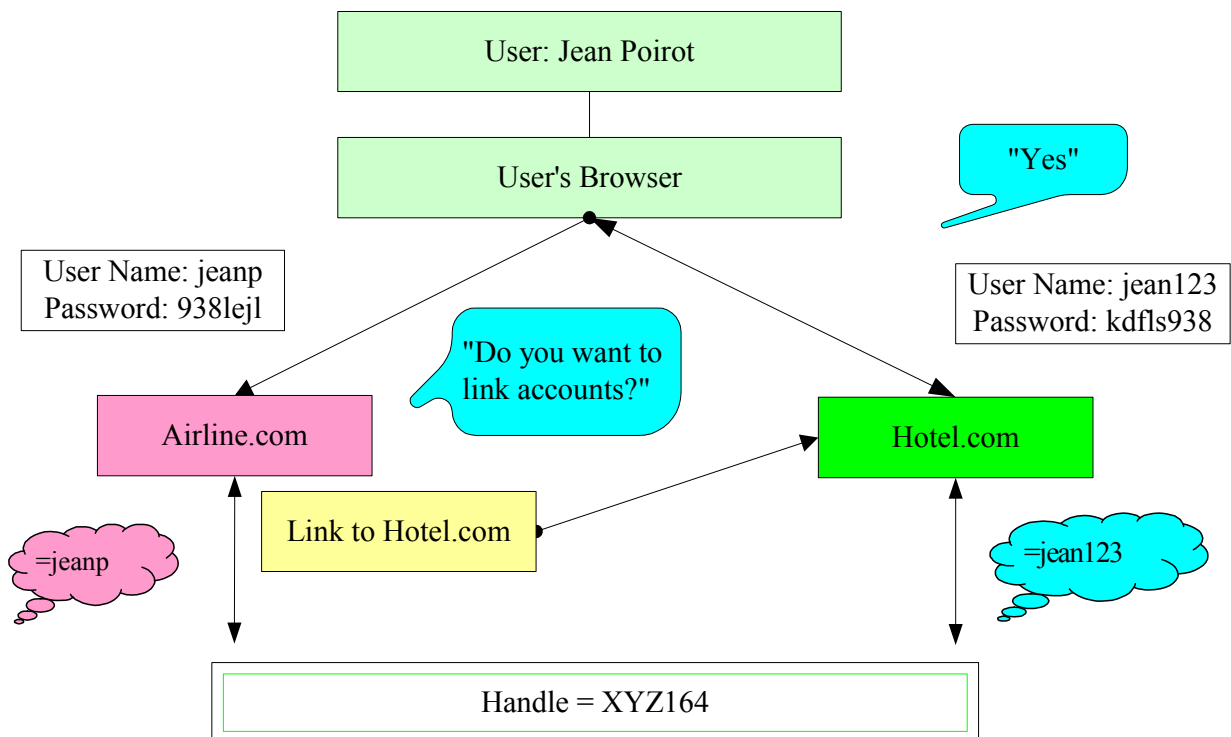
439 e. Jean123 indicates his consent by clicking “yes”.



440

441

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

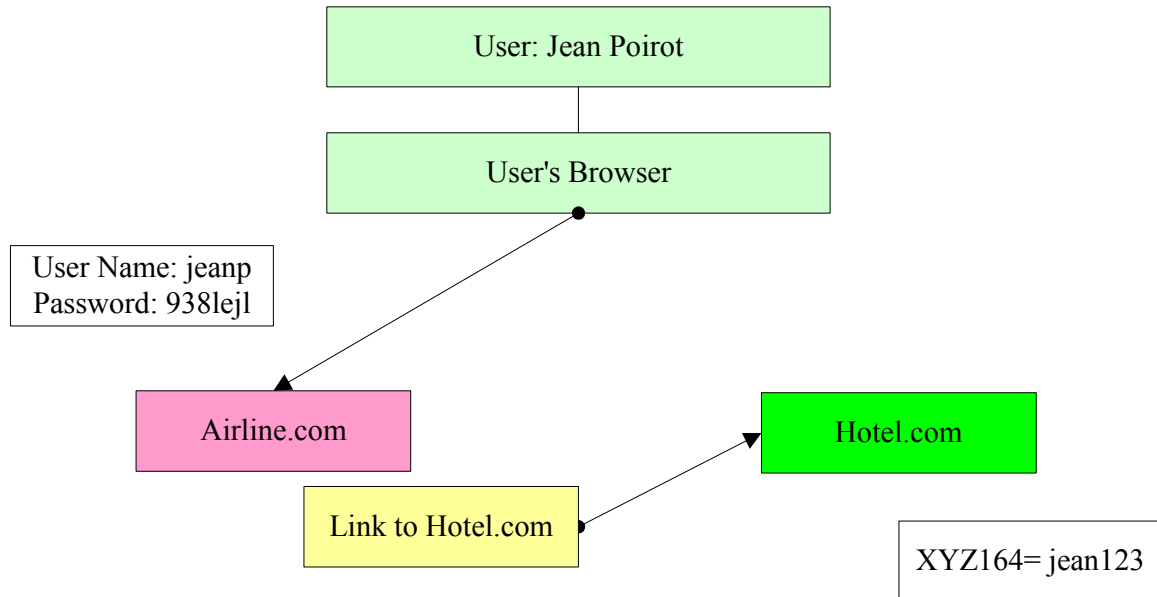


444

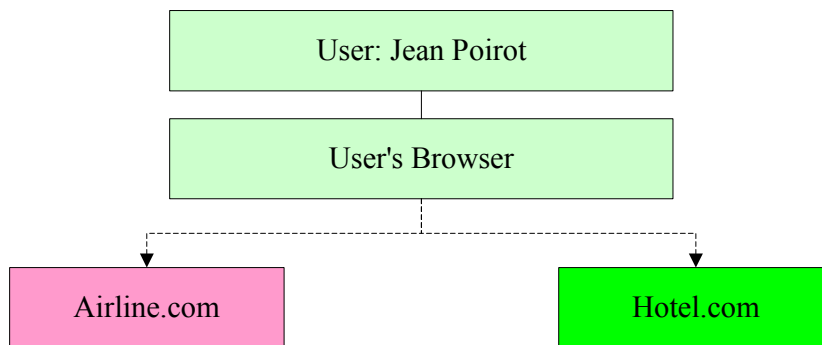
445

446

- 447 6. *Simplified sign-on (SSO)*
448 a. User goes to Airline and logs in as JeanP and password.
449 b. User clicks on link to Hotel website.
450 c. Airline sends opaque handle to Hotel site with username.
451 d. Hotel receives opaque handle and recognizes user as authenticated Jean123.
452

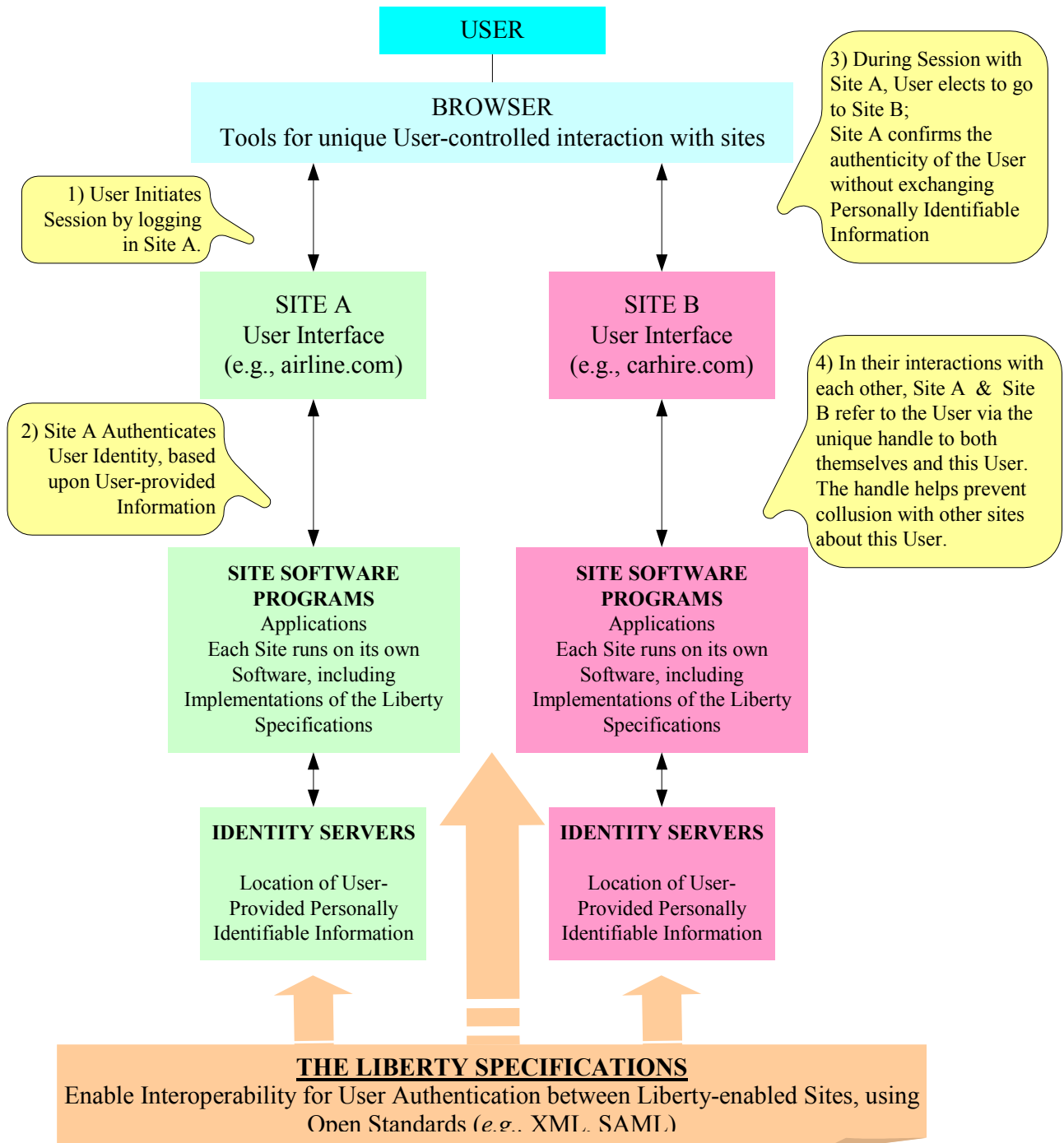


- 453
454 e. When Jean logs out of either site, he is automatically logged out of both sites.



455
456
457

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



458
 459

460

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

562 7. Security

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

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

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

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

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

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

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

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

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

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

609 *1) Awareness*

610 *Participants should be aware of the need for security of information systems and networks and what they can do to*
611 *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.”

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

618 **2) Responsibility**

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

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

627 **3) Response**

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

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

634 **4) Ethics**

635 ***Participants should respect the legitimate interests of others.***

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

640 **5) Democracy**

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

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

646 **6) Risk assessment**

647 ***Participants should conduct risk assessments.***

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

655 **7) Security design and implementation**

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

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

664 **8) Security management**

665 ***Participants should adopt a comprehensive approach to security management.***

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

672 **9) Reassessment**

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

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

677 **8. Internet Security Vulnerabilities and Precautions**

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

682 • **Denial-of-service.** Prevents authorized users from accessing the system resource or delays authorized
683 operations and functions. This can cause severe problems, e.g., for the Liberty-enabled providers' business
684 and brand.

685 • **Dictionary.** An attack that uses a technique of successively trying all the words in some large, exhaustive
686 list. This is a lesser kind of brute-force attack generally targeted at password authentication mechanisms.
687 This kind of attack may lead, for example, to the impersonation of a user if an attacker can break the user's
688 password.

689 • **Brute-force.** An attack that uses a technique of successively trying all possible combinations. This kind of
690 attack may also lead, for example, to impersonation of the user if an attack can break the user's password.
691 This attack requires more resources from an attacker compared to a dictionary attack but will provide
692 better results when there is not a good dictionary available or when passwords are protected against being
693 recognizable words.

694 • **Replay.** An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the
695 originator or by an adversary who intercepts the data and retransmits it, possibly as part of a spoofing
696 attack.

697 • **Spoofing.** An attack in which one system entity illegitimately poses as (assumes the identity of) another
698 entity. There is no way to prevent an attacker from erecting a false facade that mimics the appearance and

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

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

712 8.1. Common Weaknesses

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

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

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

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

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

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

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

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

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

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

755 8.2. Browser Vulnerabilities

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

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

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

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

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

786 However, in addition to the common domain cookie, it is recognized that many websites, in order to provide a
787 "seamless" user experience, will rely on the state management properties of cookies. Note that this issue is not
788 specific to the Liberty Specifications. Any website that uses cookies for state management – with or without Liberty
789 Specifications – is subject to the risks regarding the exposure of cookie contents. The actual risk depends on how the
790 website constructs their cookies, the lifetime of the cookie, and the cookie contents. If a cookie were to present the
791 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.

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

795 **Cross Site Scripting** – Cross Site Scripting (CSS) was originally published as a CERT advisory [CSS] in February
796 2000. To date this is still a very common threat and has been used to trick browsers to make incorrect trust decisions
797 such as erroneously trusting malicious code.

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

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

811 **8.3. Protocol Vulnerabilities**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

881 NTP is designed to keep the clocks of distributed systems synchronized. NTP is not a secure protocol and measures
882 must be taken to prevent an attacker from disrupting the service. To defend against a rogue system influencing the
883 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.

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

886 **8.4. Summary**

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

894 **9. Terminology**

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

897

898 **Access control**

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

901

902 **Attribute**

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

904

905 **Attribute class**

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

908

909 **Attribute Provider (AP)**

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

912

913 **Authentication**

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

915

916 **Authentication Domain (AD)**

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

918

919 **Authentication session**

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

923

924 **Authorization**

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

926

927 **Credentials**

928 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."

929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985

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)

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

989

990 **Service Provider (SP)**

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

992

993 **Usage directives**

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

995

996 **10. References**

997 BBB Online, Inc. and the Council of Better Business Bureaus, Inc. "A Review of Federal and State Privacy
998 Laws." http://www.bbbonline.org/UnderstandingPrivacy/library/fed_statePrivLaws.pdf (accessed April 11,
999 2003).

1000 Berman, J., and D. Mulligan. "Privacy in the Digital Age: Work in Progress." 23 Nova Law Review 2 1999.
1001 <http://www.cdt.org/publications/lawreview/1999nova.shtml>.

1002 Canadian Parliament. Canadian Privacy Act. S.C. 2000, c.5 (2003).

1003 Cantor, Scott, Kemp, John, eds. (19 July 2003). "Liberty ID-FF Protocols and Schema Specification," Version
1004 1.2-13, Liberty Alliance Project. <http://www.projectliberty.org/specs>.

1005 CDT Web Site. "Privacy Basics: Fair Information Practices." <http://www.cdt.org/privacy/guide/basic/fips.html>
1006 (accessed August 6, 2003).

1007 Center for Democracy and Technology (CDT) Web Site. "Data Privacy." <http://www.cdt.org/privacy> (accessed
1008 August 6, 2003).

1009 Ellison, Gary, ed. (25 July 2003) "Liberty ID-WSF Security Mechanisms," Version 1.0-17, Liberty Alliance
1010 Project. <http://www.projectliberty.org/specs>.

1011 European Parliament and the Council of 12 July 2002. Directive 2002/58/EC on privacy and electronic
1012 communications.
1013 [http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002L](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002L0058&model=guichett)
1014 [0058&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002L0058&model=guichett) (accessed April 11, 2003).

1015 European Parliament and the Council of 24 October 1995. Directive 95/46/EC on data protection.
1016 http://www.privacy.org/pi/intl_orgs/ec/eudp.html (accessed April 11, 2003).

1017 GBDe. "Personal Data Privacy Protection Guidelines." <http://www.gbde.org/privacy1.html> (accessed August 6,
1018 2003).

1019 Hi-Ethics Web Site. www.hi-ethics.org (accessed April 2003).

1020 Hi-Ethics. "Health Internet Ethics: Ethical Principles For Offering Internet Health Services to Consumers."
1021 <http://www.hi-ethics.org/Principles/index.asp> (accessed April 2003).

1022 Hodges, J., R. Morgan, and M. Wahl. "Lightweight Directory Access Protocol (v3): Extension for Transport
1023 Layer Security." May 2000. <http://www.isi.edu/in-notes/rfc2830.txt> (accessed April 11, 2003).

1024 Hodges, Jeff, ed. (October 11, 2002). "Version 1.0 Errata." Version 1.0, Liberty Alliance Project.
1025 http://www.projectliberty.org/specs/archive/v1_0/draft-liberty-version-1-errata-00.pdf.

1026 International Security, Trust and Privacy Alliance (ISTPA). "Privacy Framework v.1.1." <http://www.istpa.org/>
1027 (accessed April 11, 2003).

1028 Kemp, John , Wason, Tom, eds. (25 July 2003). "Liberty ID-FF Bindings and Profiles Specification," Version
1029 1.2-14, Liberty Alliance Project. <http://www.projectliberty.org/specs>.

1030 Landau, Susan, ed. (24 July 2003). "Liberty ID-WSF Security and Privacy Overview," Draft version 1.0-09,
1031 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-
notes/rfc2595.txt](http://www.isi.edu/in-
1041 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>.