



# Liberty ID-WSF Implementation Guide

Version: 2.0-02

## **Editors:**

David Weitzel, Mitretek Systems

## **Contributors:**

Conor Cahill, America Online, Inc.

Yuzo Koga, NTT

Susan Landau, Sun

Andrew Lindsey-Stewart, Vodafone

Paul Madsen, Entrust

John Kemp, IEEE-ISTO

Rob Lockhart, IEEE-ISTO

Tom Wason, IEEE-ISTO

## **Abstract:**

This Liberty Web Services Framework (WSF) Implementation Guideline (IG) conveys insights to developers implementing the Liberty WSF architecture. It is not an overview, but rather strives to give examples, lessons learned, and best practices for implementing the Liberty WSF specifications. It should be used in conjunction with the normative specifications of the Liberty WSF document suite by those who have a solid working understanding of web services technologies and protocols.

**Filename:** draft-liberty-idwsf-implementation-guidelines-v2.0-02.pdf

1 **Notice**

2 This document has been prepared by Sponsors of the Liberty Alliance. Permission is hereby granted to use the  
3 document solely for the purpose of implementing the Specification. No rights are granted to prepare derivative works  
4 of this Specification. Entities seeking permission to reproduce portions of this document for other uses must contact  
5 the Liberty Alliance to determine whether an appropriate license for such use is available.

6 Implementation of certain elements of this document may require licenses under third party intellectual property  
7 rights, including without limitation, patent rights. The Sponsors of and any other contributors to the Specification are  
8 not, and shall not be held responsible in any manner for identifying or failing to identify any or all such third party  
9 intellectual property rights. **This Specification is provided "AS IS", and no participant in the Liberty Alliance  
10 makes any warranty of any kind, express or implied, including any implied warranties of merchantability,  
11 non-infringement of third party intellectual property rights, and fitness for a particular purpose.** Implementors  
12 of this Specification are advised to review the Liberty Alliance Project's website (<http://www.projectliberty.org/>) for  
13 information concerning any Necessary Claims Disclosure Notices that have been received by the Liberty Alliance  
14 Management Board.

15 Copyright © 2005 Adobe Systems; America Online, Inc.; American Express Company; Amsoft Systems Pvt Ltd.;  
16 Avatier Corporation; Axalto; Bank of America Corporation; BIPAC; BMC Software, Inc.; Computer Associates  
17 International, Inc.; DataPower Technology, Inc.; Diversinet Corp.; Enosis Group LLC; Entrust, Inc.; Epok, Inc.;  
18 Ericsson; Fidelity Investments; Forum Systems, Inc.; France Télécom; French Government Agence pour le  
19 développement de l'administration électronique (ADAE); Gamefederation; Gemplus; General Motors; Giesecke &  
20 Devrient GmbH; GSA Office of Governmentwide Policy; Hewlett-Packard Company; IBM Corporation; Intel  
21 Corporation; Intuit Inc.; Kantega; Kayak Interactive; MasterCard International; Mobile Telephone Networks (Pty)  
22 Ltd; NEC Corporation; Netegrity, Inc.; NeuStar, Inc.; Nippon Telegraph and Telephone Corporation; Nokia  
23 Corporation; Novell, Inc.; NTT DoCoMo, Inc.; OpenNetwork; Oracle Corporation; Ping Identity Corporation;  
24 Reactivity Inc.; Royal Mail Group plc; RSA Security Inc.; SAP AG; Senforce; Sharp Laboratories of America;  
25 Sigaba; SmartTrust; Sony Corporation; Sun Microsystems, Inc.; Supremacy Financial Corporation; Symlabs, Inc.;  
26 Telecom Italia S.p.A.; Telefónica Móviles, S.A.; Trusted Network Technologies; Trustgenix; UTI; VeriSign, Inc.;  
27 Vodafone Group Plc.; Wave Systems Corp. All rights reserved.

28 Liberty Alliance Project  
29 Licensing Administrator  
30 c/o IEEE-ISTO  
31 445 Hoes Lane  
32 Piscataway, NJ 08855-1331, USA  
33 info@projectliberty.org

## 34 Contents

35	1. Introduction	5
36	2. Goals and Scope	6
37	2.1. Overview of WSFs in the LA Context	6
38	2.2. Assumed Knowledge of the Liberty Specifications	6
39	2.3. Assumed Knowledge of Internet Technology	7
40	3. Process	8
41	3.1. First Implementers	8
42	3.2. Key Environments	8
43	3.2.1. Enterprise	8
44	3.2.2. E-Commerce	8
45	3.2.3. Mobile	8
46	3.2.4. E-Government	8
47	4. Structure	9
48	4.1. Elements of WSF	9
49	4.2. Relation to ID-FF	9
50	4.3. Relation to Liberty Services Specifications: ID-PP and ID-EP Services	9
51	5. Implementation Lessons Learned	10
52	5.1. SAML Version Interoperability	10
53	5.2. Discovery	10
54	5.3. Interaction Service	10
55	5.4. Data Services Template	10
56	5.5. Security Mechanisms	10
57	5.6. Key Environments	11
58	5.6.1. Enterprise	11
59	5.6.2. E-Commerce	11
60	5.6.3. Mobile	11
61	5.6.4. E-Government	12
62	5.7. Special Issues	12
63	5.7.1. Underlying Protocols	12
64	5.7.2. Privacy and Security	13
65	5.7.3. Time Synchronization	15
66	5.7.4. Development Environments	15
67	6. Authentication Example Sessions	16
68	6.1. Overview	16
69	6.2. Liberty ID-WSF Sample User Experience and Use Case	16
70	6.2.1. Sample Scenario	16
71	6.2.2. Sequence Flows and Exchanged Messages	17
72	7. Anonymous B2B Example Sessions	34
73	7.1. Overview	34
74	7.2. Scenario	34
75	7.3. User Experience	34
76	7.4. Message Flow	35
77	7.4.1. Step 1	36
78	7.4.2. Step 2	36
79	7.4.3. Step 3	36
80	7.4.4. Step 4	37
81	7.4.5. Step 5	39
82	7.4.6. Step 6	40
83	7.4.7. Step 7	42
84	7.4.8. Step 8	43
85	7.5. Optimizations	44
86	7.6. Summary	44

---

87	8. Device Authentication Example Sessions .....	46
88	8.1. Device Boot Up .....	46
89	8.2. Device Initiates Authentication .....	46
90	8.3. Auth Server Responds with Auth Mechanism Choice .....	46
91	8.4. Device Submits Credentials to Auth Server .....	47
92	8.5. Auth Server Returns Security Token & Discovery Info .....	47
93	8.6. Device Requests Service Info from Discovery Service .....	49
94	8.7. Discovery Service Returns Service Info .....	50
95	8.8. Device Requests Data from Radio Service .....	52
96	8.9. Radio Service Returns Info .....	53
97	8.10. Device Requests Additional Info from Radio .....	54
98	8.11. Radio Service Returns Info .....	54
99	8.12. Device Requests Photo Service Info from Discovery Service .....	55
100	8.13. Discovery Service Returns Photo Service Info .....	55
101	8.14. Device Requests Info from Photo Service .....	57
102	8.15. Photo Service Returns Info .....	58
103	8.16. Device Renews Security Token .....	58
104	8.17. The Authentication Server Returns New Token .....	60
105	References .....	62

## 106 1. Introduction

107 Liberty Alliance provides several documents in addition to the specifications. These documents are defined as "non-  
108 normative," meaning that they are not requirements, but are supportive documents serving to explain various facets  
109 and applications of the specifications. The mode may be more conversational than normative documents. These  
110 documents are classified as "Other Supporting Documents" and are subject to the Liberty copyright constraints.

111 A Liberty Alliance implementation guidelines document is a complement to the normative specification documents;  
112 it provides guidelines on how the specifications should actually be implemented. Implementation guidelines provide  
113 clarification on the specifications as well as wisdom learned—often the hard way—by developers. The audience is  
114 application developers.

115 An implementation guidelines is a dynamic document that may change frequently as experience teaches effective  
116 means for implementing the specifications. It provides a narrative discussion of important issues and their resolution.  
117 The implementation guidelines may, at times, provide input to future versions of the specifications. It will make  
118 specific references to specific sections of the specifications, but is not a complete index to the specifications.

119 An implementation guidelines provides representative examples of implementations, or parts of implementations, that  
120 exercise specific functionality. For example, it demonstrates how specific protocols are executed, how security  
121 is maintained in specific scenarios and so forth. An implementation guidelines provides explanations of effective  
122 architectures, methods for optimizing performance, scaling notes, and warnings. It may illustrate with block and flow  
123 diagrams, sample messages and code fragments.

124 This document is *non-normative*. However, it provides implementers and deployers guidance in the form of policy,  
125 security, and technical notes. Further details of the Liberty ID-FF architecture are given in several normative technical  
126 documents associated with this implementation guide, specifically [[LibertyDST](#)], [[LibertyInteract](#)], [[LibertyDisco](#)],  
127 [[LibertySecMech](#)], and [[LibertySOAPBinding](#)] as well as the non-normative [[LibertyIDWSFOverview](#)]. Note: The  
128 more global term "Principal" is used for "user" in Liberty's technical documents. Definitions for Liberty-specific  
129 terms can be found in the [[LibertyGlossary](#)]. Also, many abbreviations are used in this document without immediate  
130 definition because the authors believe these abbreviations are widely known, for example, HTTP and SSL. However,  
131 the definitions of these abbreviations can also be found in [[LibertyGlossary](#)]. Note: Phrases and numbers in brackets  
132 [ ] refer to other documents; details of these references can be found in [References](#) (at the end of this document). As  
133 this document is non-normative, it does not use terminology "MUST," "MAY," "SHOULD" in a manner consistent  
134 with [[RFC2119](#)].

135 An implementation guidelines document should be considered a complement to the Liberty Alliance specifications  
136 and provides guidelines for how the Liberty specifications should be implemented. It provides additional clarifications  
137 on some issues in the specifications, as well as errata on the specifications. This document should be viewed as a  
138 continuing work in progress meant to assist serious implementers. If a reader is looking for basic overview information,  
139 deployment guidance, static conformance information, or certification specifications, they must look elsewhere in the  
140 Liberty document set.

## 141 2. Goals and Scope

142 This Liberty Alliance Web Services Framework Implementation Guide (WSF-IG) only covers the Liberty Alliance  
143 specifications in the Web Services Framework (WSF) arena. Other Implementation Guides exist or are contemplated  
144 for other elements of the Liberty Alliance specifications.

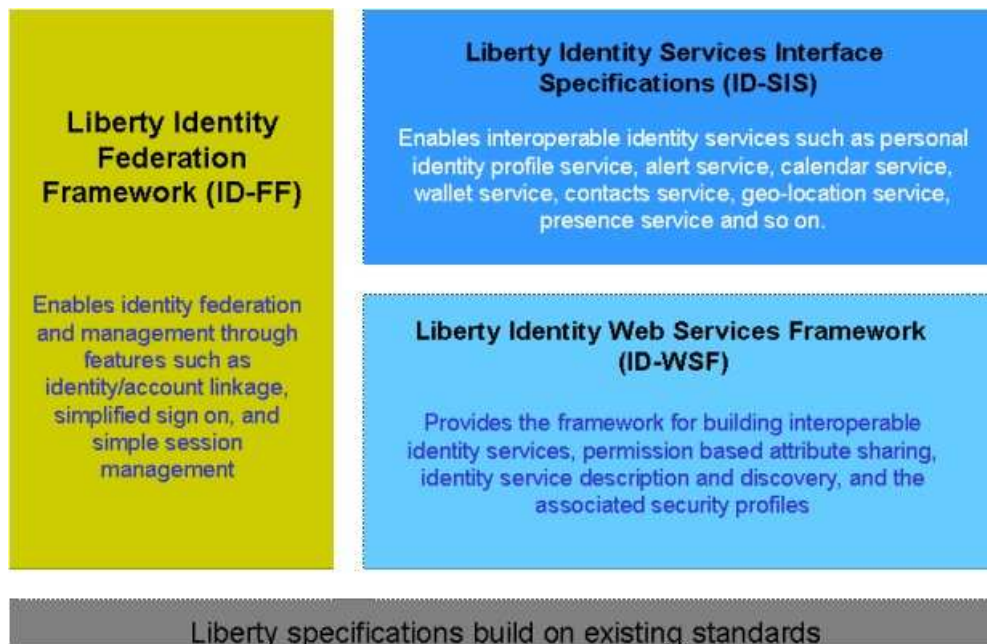
145 As a non-introductory, non-normative document, this section of the WSF-IG will lay out:

- 146 • Overview of WSFs
- 147 • Assumed knowledge of Liberty architecture
- 148 • Assumed knowledge of web services and Internet technology

149 These items are described below.

### 150 2.1. Overview of WSFs in the LA Context

151 The goal of the WSF-IG is to help developers understand the implementation details of the Liberty Alliance WSF  
152 architecture and to share best practices and lessons learned by earlier implementers of the framework. The major  
153 architectural components identified in [Figure 1](#) should be familiar to those who have a working knowledge of the  
154 Liberty Alliance specifications. To reiterate, this WSF-IG is meant to concentrate on the WSF components of the  
155 Liberty specifications and will only touch on other parts of the Liberty Architecture as they relate to the WSF  
156 components.



157

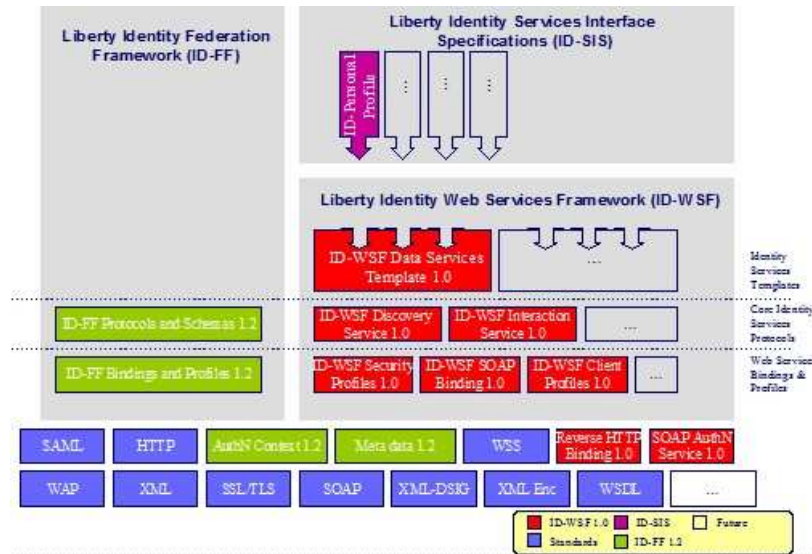
158

Figure 1. Liberty Architecture

### 159 2.2. Assumed Knowledge of the Liberty Specifications

160 The normative technical specifications of the Liberty Alliance are identified in a series of documents explaining  
161 the format and syntax of each of the components. They are identified in [Figure 2](#) along with significant Internet  
162 technologies that are utilized in the Liberty specifications. This WSF-IG document is meant to help developers  
163 implement the features and functions of the normative specifications of the Liberty WSF components. To become

164 familiar with other components of the Liberty specifications one must look to the appropriate normative and  
 165 normative documents for those components. An overview of the Liberty Alliance technical architecture is also  
 166 available in the [LibertyIDWSFOverview] document. A good starting place for other architectural components  
 167 should be the appropriate Overview document related to the component of interest.



168

169

Figure 2. Liberty Modules

### 170 2.3. Assumed Knowledge of Internet Technology

171 There are a number of evolving Internet resources which are utilized by the Liberty Alliance specifications including  
 172 such protocols such as Extensible Markup Language (XML), Simple Object Access Protocol (SOAP) and Security  
 173 Assertion Markup Language (SAML). Additionally, an implementer of Liberty Alliance specifications should  
 174 be familiar with basic Internet architectures, basic Public Key Infrastructure (PKI) digital signature concepts,  
 175 basic Internet security, Secure Socket Layer/Transport Layer Security (SSL/TLS), Hypertext Transfer Protocol  
 176 (HTTP) HTTP Secure (HTTPS), Uniform Resource Identifiers (URIs), Domain Name System (DNS), Web Services  
 177 Description Language (WSDL), the Liberty Alliance WSF components they wish to implement as well as the Liberty  
 178 components that must be utilized to implement or interface to the Liberty WSF component being implemented.

## 179 **3. Process**

180 This implementation guide concentrates on several areas. They are [Section 3.1](#) and [Section 3.2](#).

### 181 **3.1. First Implementers**

182 An implementation guidelines document should be considered a complement to the Liberty Alliance specifications  
183 and provides guidelines for how the Liberty specifications should be implemented. It provides additional clarifications  
184 on some issues in the specifications, as well as errata on the specifications.

### 185 **3.2. Key Environments**

186 There are several key service environments that this implementation guide will concentrate on. They are [Section 3.2.1](#),  
187 [Section 3.2.2](#), [Section 3.2.3](#), and [Section 3.2.4](#).

#### 188 **3.2.1. Enterprise**

189 Rather than jump into a heterogeneous authentication architecture outside the enterprise, many Liberty members have  
190 found that significant hurdles exist in merely rationalizing intra-enterprise authentication and web services. Developers  
191 should take heed both from development and marketing perspective of this fact. First they should stand up Liberty  
192 architectures in a simulated intra-enterprise environment both because it is somewhat simpler and second it simulates  
193 the first deployments of many organizational users of the Liberty specifications. However, due to the complexity  
194 of many modern enterprises, little comfort should be taken. Because many enterprises span multiple architectures,  
195 component systems, legacy authentication schemes, and world-wide footprints, the deployment of intra-enterprise  
196 authentication using Liberty components is far from easy.

#### 197 **3.2.2. E-Commerce**

198 Most users of the Liberty specifications anticipate utilizing the power of the specifications in full-blown inter enterprise  
199 deployments. In this environment very few simplifying assumptions can be made. Thus, step wise and component  
200 wise deployment strategies are recommended. Fortunately, the development of the Liberty specifications facilitates  
201 this approach. One can utilize the power of the Liberty ID-FF framework without having to delve into much of the  
202 Liberty WSF realm. One can develop Liberty WSF-compliant software without having to deploy specific services on  
203 top of it. Of course, many user organizations anticipate full development and broad deployment of the full suite of  
204 Liberty specifications.

#### 205 **3.2.3. Mobile**

206 The mobile environment presents both unique opportunities and unique challenges in the authentication environment.  
207 The widespread worldwide deployment of mobile devices is a ripe opportunity for the coordination of authentication  
208 architectures. The continued convergence of phone and personal digital assistant technology calls for devices that can  
209 utilize the full power of both the mobile telephony and wireless data environments. However, due to limitations  
210 on power, memory size, display size, and bandwidth mobile environments must live within certain constraints.  
211 Additionally, some legacy architectural decisions present current constraints on deployment of architectures and  
212 capabilities anticipated by the Liberty specifications.

#### 213 **3.2.4. E-Government**

214 Governments play a special role in e-authentication both as a user and as a holder of identity information. We  
215 anticipate a number of different Service Providers will also serve as Identity Provider and in the business environment,  
216 consumers will have choice as to which Identity Providers they use. Due to the unique role of government, users of  
217 e-government services, however, may be required to use the government's choice of Identity Provider(s). For this  
218 reason, it is extremely important that governments choose e-authentication systems that appropriately protect both  
219 privacy and confidentiality. For transparency's sake, systems that depend upon open standards provide a better choice  
220 for government.



## 221 **4. Structure**

222 The Liberty WSF architecture can be viewed as a suite of capabilities to enable intra- and inter-enterprise web services  
223 to operate in a heterogeneous authentication environment. In short, in a Liberty enabled environment one should be  
224 able to interoperate with multiple principals, service providers and identity providers in a fashion where real-time and  
225 near real-time decisions can be made about what trust can be given to formerly-unknown providers.

### 226 **4.1. Elements of WSF**

227 The web services model is rapidly gaining acceptance in the Internet community as a scalable and adaptable model  
228 for implementing services and systems that need to interoperate among multiple systems providers utilizing multiple  
229 components. To meet this emerging Internet development model the Liberty Alliance has adopted with use of a web  
230 services framework for implementing the core architecture of the Liberty Alliance specifications.

231 Specifically, the components of the Liberty ID-WSF framework are outlined in the [[LibertyIDWSFOverview](#)].

### 232 **4.2. Relation to ID-FF**

233 The Liberty ID-WSF framework works in conjunction with the structure of the Authentication techniques developed  
234 in the ID-FF framework. It is generally anticipated that most deployments of Liberty ID-WSF technologies will be  
235 done in conjunction with the use of ID-FF capabilities. Implementers of ID-FF should have a strong grounding in the  
236 techniques and capabilities of the ID-FF framework. They are well served to have a strong working knowledge of the  
237 companion [[LibertyIDFFOverview](#)] and [[LibertyImplGuide](#)].

### 238 **4.3. Relation to Liberty Services Specifications: ID-PP and ID-EP** 239 **Services**

240 The Liberty ID-WSF framework forms a foundation of structures that can be used to implement identity service  
241 specifications. The Liberty ID-PP and ID-EP services are the first two specifications that have been created in this  
242 fashion. However, many more identity services can be envisioned to utilize the Liberty ID-WSF framework. For  
243 developers, examination of the [[LibertyIDPPP](#)] and [[LibertyIDEP](#)] specifications can assist in learning how the ID-  
244 WSF framework can be put to use. For developers these insights may be helpful from both a development and testing  
245 perspective.

## 246 **5. Implementation Lessons Learned**

247 Many of the best implementation insights are those gained by developers who have already succeeded in implementing  
248 a specification. To that end, the early developers of systems invoking the ID-WSF specifications have begun to share  
249 their development insights and lessons learned.

### 250 **5.1. SAML Version Interoperability**

251 Both ID-FF and ID-WSF use SAML assertions to communicate authentication and attribute information regarding  
252 system actors. ID-FF 1.2 is based on SAML 1.1 [[SAMLCore11](#)]. ID-WSF 1.0 supports SAML 1.1, ID-WSF 2.0  
253 supports both SAML 1.1 and SAML 2.0 [[SAMLCore2](#)] assertions. Additionally, SAML 2.0 can be used to enable  
254 single sign-on functionality exactly comparable to that provided by ID-FF 1.2.

255 It is therefore possible that an ID-WSF implementation can use a different version of SAML assertions than the single  
256 sign-on infrastructure on which it builds. This scenario will most often occur through varying deployment schedules  
257 for the different components. For instance, a SAML 2.0-based ID-WSF 2.0 implementation could be deployed on top  
258 of a previously existing SAML 1.1-based ID-FF 1.2 implementation. Generally speaking, the implication of such a  
259 scenario is that one or more of the system actors must be able to understand both assertion formats.

260 A tighter connection between the single sign-on infrastructure and the ID-WSF infrastructure is created by the so-called  
261 *bootstrap* mechanism - by which the identity provider provides to the service provider information about the location  
262 of the relevant principal's discovery service as well as (optionally) credentials to be used in querying that discovery  
263 service. If present, these credentials take the form of a SAML assertion carried within the Advice element of the parent  
264 SAML assertion that enables single sign-on. As neither ID-FF 1.2 nor SAML 2.0 stipulate that this bootstrap assertion  
265 must be of the same SAML version as the parent single sign-on assertion, it is possible that a SAML 1.1-based ID-  
266 FF 1.2 single sign-on assertion could carry an embedded SAML 2.0 bootstrap assertion (or theoretically vice versa  
267 as well). This might occur if a SAML2.0-based ID-WSF 2.0 implementation was deployed on top of an ID-FF 1.2  
268 deployment and the decision was made to keep the ID-WSF components SAML 2.0 only – thereby necessitating that  
269 the bootstrap assertion be SAML 2.0.

### 270 **5.2. Discovery**

271 An implementer should be familiar with the Conceptual Model and Terminology section of the normative [[LibertyDisco](#)].  
272 The model gives a solid introduction to understanding what the normative portion of the specification  
273 describes. The end of that document also contains the XSD, WSD, and example XSL stylesheets.

### 274 **5.3. Interaction Service**

275 An implementer should be familiar with the Interaction Service cases identified in the [[LibertyInteract](#)]. Similarly,  
276 the end of that document also contains the XSD, WSD, and example XSL stylesheets.

277 Interoperability note: If a Service Provider, SP, does not send the UserInteraction header then it probably can not  
278 redirect. So, the SP should warn that it is OK to redirect but this SP can not do the redirection. Also, if the SP does  
279 send the UserInteraction header with redirect, then it should have the user available.

### 280 **5.4. Data Services Template**

281 An implementer should familiarize themselves with the specification check list provide in section 4 of the [[LibertyDST](#)]  
282 specification. Since identity service specifications such as ID-PP and ID-EP utilize the DST specification  
283 extensively, an implementer can aid their understanding of the uses of the [[LibertyDST](#)] specification by looking at  
284 the normative and non-normative documents of the [[LibertyIDPP](#)] and [[LibertyIDEP](#)] services.

### 285 **5.5. Security Mechanisms**

286 The Liberty ID-WSF Security Mechanisms document contains several non-normative sections that help an imple-  
287 menter understand the purpose of the security mechanisms.

288 A quality policy engine is critical. There is an important role of the Policy Decision Point and Policy Enforcement  
289 Point in enforcing good security practice. While Liberty will not make any specific recommendation, an implementer  
290 should evaluate the various offerings closely.

## 291 **5.6. Key Environments**

292 The developers of systems utilizing Liberty ID-WSF specifications in the key environments identified in the previous  
293 section have similarly shared their insights and lessons learned.

### 294 **5.6.1. Enterprise**

295 Many early deployments of the Liberty specifications are occurring in enterprise environments. The deployments  
296 anticipate the ability to integrate many formerly unconnected authentication and attribute systems into a seamless  
297 enterprise instantiation of standards-based authentication web services.

### 298 **5.6.2. E-Commerce**

299 Most commercial deployments of the Liberty ID-WSF framework will be in the general e-commerce web services  
300 environment. Such a deployment must anticipate the seemingly limitless uses that the deployment may be called  
301 upon to support. Rigorous development lab testing, boundary case testing, stress testing and interoperability testing  
302 should be utilized.

303 One particular issue that has been raised is the possible security impact of too short a cache life thus not being able to  
304 detect a replay attack. Another is the judicious use of fault logging.

### 305 **5.6.3. Mobile**

306 Privacy should be of increased concern in the mobile environment and typically should allow for affirmative end user  
307 action before using a service offering.

#### 308 **5.6.3.1. Roaming**

309 The current specifications do not yet provide a robust solution to share an identity's data when roaming across circles of  
310 trust. However, when the functionality becomes available mobile operators should be able to leverage the established  
311 trust that they have with their existing voice roaming agreements.

#### 312 **5.6.3.2. LUAD-WSP:**

313 • Dual Identity Services:

314 As the LUAD-WSP may not always be reachable, there is a strong likelihood that there will be a dual network-  
315 based identity service registered with the DS. Therefore, there should be a mechanism for the client to synchronize  
316 its service information with that of the network-based service such that the end-user only has to update one service  
317 and the data propagated to other dual identity service. Possible options might include:

318 1. An existing protocol e.g., SyncML, or ...

319 2. Add a synchronization method to the DST specification.

320 As identity services can be extensible, "limited" storage devices may only store a subset of an identity service.  
321 Therefore, the synchronization mechanism should also be able to cope with this "limited" identity service.

322 • Security/Privacy

323 Since a LUAD-WSP needs to advertise the presence of a service, there is a higher risk the privacy of an end-user  
324 may be compromised by a rogue service provider. PAOS-enabled clients should therefore:

325 1. Allow for affirmative end-user action before advertising the service to a service provider; and

326 2. For the service residing on the client, enable privacy/permission preferences under the control of the end-user.

327 Due to the limited bandwidth of current mobile networks, when using PAOS with message level security, the SOAP  
328 messages should not include the certificates but URL references to them.

329 Key management issue from privacy point of view ... (see Client Profiles document)

330 • Discovery

331 The identity service should not be listed in the discovery service as the client cannot act in the role of a standard  
332 WSP being without an IP address or having reachable, associated metadata. (see Client Profiles document)

333 **5.6.3.3. LUAD-WSC**

334 There may be use cases where Group System Mobile (GSM) authentication information may need to be exchanged  
335 using the SOAP Authentication protocol. Currently, the Simple Authentication and Security Layer (SASL) registry  
336 does not hold such a mechanism and therefore it would need to be added. Procedures for registering SASL  
337 mechanisms are given in [RFC2222]. Schedules for specifying the mechanism would be tied to Internet Engineering  
338 Task Force (IETF) timelines. Alternatively, GSS API can be used.

339 **5.6.3.4. Interaction Service:**

340 As mobile operators have (1) a number of established, reliable channels of communication with end-users such as  
341 Secure Messaging System (SMS) or Wireless Access Protocol (WAP) push, (2) the trust relationship with both the  
342 service providers and end-users, and (3) would like to provide a consistent user experience, it is recommended that an  
343 operator host an interaction service registered as an end-user service.

344 Deployment of an interaction service should specify the possible communication channel interfaces with the network.  
345 For mobile operators, these might include SMS, WAP push, or Interactive Voice Response (IVR).

346 A key benefit of the Liberty technology for end-users is the ease-of-use when using Liberty-enabled services  
347 particularly in the case of mobile devices, having limited display and input capabilities. To reinforce this ease-of-use,  
348 it is recommended that mobile operators promote, where possible, a consistent user experience when interacting with  
349 end-users across service categories. For example, in the service category of secure, mobile transactions, Mobile  
350 electronic Transactions (MeT) Ltd. have developed specifications establishing a framework, ensuring a consistent user  
351 experience independent of device, service and network experience.

352 **5.6.4. E-Government**

353 Government authentication systems have all of the complexities of enterprise and general ecommerce authentication  
354 systems with the added responsibilities that a government has in protecting core citizen identity and attributes from  
355 unauthorized access or use. National government authentication systems should strive for interoperability with  
356 regional and provincial systems so that citizens can have the ability to reuse identification credentials. Often as the  
357 repository of basic identity information, government authentication and attribute sharing systems should utilize greater  
358 security than general e-commerce authentication and attribute sharing systems.

359 **5.7. Special Issues**

360 Not all implementation issues fall neatly within the categories identified above. Some issues exist with items not  
361 within the scope of the Liberty specifications such as the underlying Internet based protocols. Some issues deal with

362 the Liberty enabled tools utilized by the Liberty ID-WSF specifications. Yet other issues arise from the use of certain  
363 development environments and tools. Each of these is dealt with below.

### 364 **5.7.1. Underlying Protocols**

365 The Liberty architecture has utilized standards based protocols where possible. Some of these protocols are  
366 under active development and revision. This circumstance has created challenges for implementers of the Liberty  
367 architecture. Likewise, resolution of conflicts among similarly named protocol components has created certain  
368 challenges.

369 A number of implementers have been challenged by maintaining proper major and minor version numbers depending  
370 on whether certain assertions are "pure SAML" (version 1.1) or Liberty adapted SAML assertions (version 1.2). This  
371 is especially troublesome where a response to a Liberty adapted SAML assertion utilizes a "pure SAML" assertion.

372 At least one development team encountered interoperability issues by not sufficiently canonicalizing their XML  
373 schemas.

### 374 **5.7.2. Privacy and Security**

375 Implementers should be familiar with the [[LibertyIDWSFSecurityPrivacyGuidelines](#)]. Liberty specifications require  
376 that all communications from Principals to Liberty-enabled sites be integrity protected and confidentiality must be  
377 ensured. Liberty-enabled sites must use SSL 3.0 or TLS 1.0 for conducting communications with Principals. The  
378 security of the SSL or TLS session depends upon the chosen cipher suite; Liberty specifications recommend the use of  
379 at least a 112-bit symmetric key. Use of TLS should be preferred and non-use can lead to operational security issues.

380 If there are no intermediaries in the message path, then transport layer protection mechanisms (SSL/TLS) suffice to  
381 ensure the integrity and confidentiality of the message exchange. If there are intermediaries in the message path, then  
382 the content of `<S:Body>` must be encrypted using the confidentiality mechanisms in [[WSScore](#)]. Information supplied  
383 by a TA may contain private information and thus the TA and ultimate recipient must use the mechanisms of Encrypted  
384 *Name Identifier* and *Encrypted URI*.

385 If there are no intermediaries in the message path, then peer authentication can use SSL/TLS mutual authentication as  
386 outlined in section 6.2 of [[LibertySecMech](#)]. In the presence of active intermediaries, Web Services Security SOAP  
387 Message Security, [[X.509](#)] token profile sender authentication or Web Services Security SOAP Message Security,  
388 SAML token profile sender authentication must be used.

389 Trusted Authorities (TA) may issue assertions that will be subsequently used in conjunction with accessing a resource  
390 at an identity service. TAs must enforce any access control policies pertaining to the resource and the assertion must  
391 be by the TA.

392 Before authorization data can be consumed, the sender must authenticate itself to the recipient and the recipient must  
393 authenticate the sender, including checking the sender's certificate is still valid (e.g., has not been revoked). The  
394 recipient must locate the security token and verify that it is properly structured, that the signature is valid, etc.

395 Generally when there is risk to a principal of release of personal or financial information, stronger security mechanisms  
396 should be preferred where practicable.

**Table 1. Liberty Service, Protocol - Recommendations**

<i>Liberty Service</i>	<i>Liberty Protocol</i>	<i>Recommendations</i>
Discovery Service	Query Response	<p>Responders should construct a response to be as qualified as possible. The Discovery Service provider should provide security tokens if it knows that these tokens will be necessary and it is able to provide them based on the security token included in the request.</p> <p>The ResourceID must be sent encrypted using a key encrypted with the public key of the resource provider. This encrypted key must exhibit nonce-like capabilities.</p>
Discovery Service	Modify	<p>Access control policy for the resource offering may be placed in the any element of the ResourceOffering attribute.</p> <p>If the AuthorizeRequester directive is specified for a resource, then the discovery service provider should include a SAML assertion containing a Resource Access Statement in any future QueryResponse for the resource. If the Authenticate-SessionContext directive is specified for a resource, then the discovery service provider should include a SAML assertion in the Session Context Statement in any future QueryResponse.</p> <p>If there is a proxy resource offering and identity of the requester is not the identity of the provider of the proxy resource offering, the result set for that service type must contain only the proxy resource offering as well as all other resource offerings for which the requester is the provider.</p> <p>If the identity of the requester is the provider of the proxy resource offering, the result set must contain all resource offerings for the specified service type, including the proxy resource offering. Additionally, the directives for all instances of the requested service type must be aggregated when formulating the security tokens, as the proxying agent will need these tokens to fulfill the request.</p>
Interaction Service	Interaction Request	<p>In the InteractionRequest, if the attribute ds:KeyInfo is present, the attribute signed must also be present.</p> <p>If the response is be signed (that is, the “signed” attribute is present), the InteractionRequest should contain only a single query.</p> <p>The Inquiry element Id component lays out the importance of its nonce-like properties.</p> <p>If the InteractionResponse contains a signed InteractionStatement, the recipient must verify the signature and also that the id attribute of the signed inquiry matches the id of the corresponding request inquiry. The response must be discarded if the signature cannot be verified.</p>

398

**Table 2. Liberty Service, Protocol - Recommendations**

<i>Liberty Service</i>	<i>Liberty Protocol</i>	<i>Recommendations</i>
Interaction Service	Interaction Response	<p>If the InteractionRequest requests signing, then the recipient should attempt to obtain a signed InteractionStatement from the Principal. If the value of the signed attribute is "strict," then the InteractionResponse must include either an InteractionStatement or a status element with its code attribute set to NotSigned.</p> <p>The Interaction Service should authenticate the Principal and save the proof of authentication. To prove that the information provided was provided by the Principal, the Interaction Service could have the Principal sign the response with the private key for which the requester (the WSC) has the corresponding public key.</p>
Metadata	Metadata Publication	<p>Metadata should always be transported securely, e.g., via SSL/TLS. Entities should publish their metadata document location via a "well-known location" or through DNS. DNS signatures and TLS Server authentication are recommended, and the use of Metadata ds:signature is strongly recommended.</p> <p>Consumers of metadata documents should observe the validUntil and cacheDuration of documents, and must use the most restrictive of these if they conflict.</p>

399 **5.7.3. Time Synchronization**

400 If the clocks of the WSC and DS are not synchronized, a WSC may decide to either not use or prematurely renew  
 401 a valid assertion. WSC's are advised to use the timestamp attribute on the Correlation header in the response from  
 402 the DS generating an assertion in order to determine the clock skew between the two servers. With this information,  
 403 the WSC can better determine the "real" validity period of an assertion it receives from that DS. For example, if the  
 404 time on the WSC is 12 noon on 6/25/04 and the timestamp attribute in the Correlation header is 6pm on 6/25/04, the  
 405 approximate time difference between the WSC and the DS is 6 hours and the client should add 6 hours to its time (or  
 406 decrement by 6 hours the times in the assertion) when assessing validity periods.

407 **5.7.4. Development Environments**

408 A number of web services development environments contain support documentation that may assist an implementer  
 409 in the proper utilization of the various web services related protocols used within the Liberty guidelines.

## 410 6. Authentication Example Sessions

411 This document describes sample user experience and use-case of Liberty ID-WSF, which are simple and easy-to-  
412 understand. The user experience is described so that readers can intuitively understand what is Liberty ID-WSF, and  
413 what they can do with it, while the use-case is described with XML message traces so that implementers can refer for  
414 their implementation.

415 A more simplified version of the example is given in the Liberty ID-WSF Overview document.<sup>1</sup>

### 416 6.1. Overview

417 In the sample scenario, three websites appears, that are WhiteBroadBand.COM, BlueLiquor.COM, and Yellow-  
418 Pizza.COM. [Table 3](#) shows their roles in the scenario, and [Figure 3](#) depicts overview of these three websites and  
419 their modules from the computational viewpoint.

420 **Table 3. Three Web Sites In The Scenario**

<i>Abbr.</i>	<i>Web Site Name</i>	<i>Explanation</i>
IDP	WhiteBroadBand.COM	This is Identity Provide and also hosts Discovery Service (DS).
SP1	BlueLiquor.COM	This is Service Provider that sells liquors on the Internet and delivers them to customers. This website holds customer attributes, (e.g., address information) and is able to share them with other websites based on Liberty ID-WSF and ID-SIS Personal Profile (i.e., it can behave as Attribute Provider).
SP2	YellowPizza.COM	This is Service Provider that sells pizzas on the Internet, and delivers them to customers. This website does not holds customer's attributes except for loginname and password, but is able to retrieve them from other websites based on Liberty ID-WSF and ID-SIS Personal Profile.

## 421 6.2. Liberty ID-WSF Sample User Experience and Use Case

### 422 6.2.1. Sample Scenario

#### 423 6.2.1.1. Assumptions

424 Joe Self (a Principal) has accounts at WhiteBroadBand.COM (IDP), BlueLiquor.COM (SP1), and YellowPizza.COM  
425 (SP2), and these are federated between them based on Liberty ID-FF. Joe Self's attributes are maintained at  
426 BlueLiquor.COM (SP1), and BlueLiquor.COM can acts as Attribute Provider under the Liberty context.

#### 427 6.2.1.2. Scenario

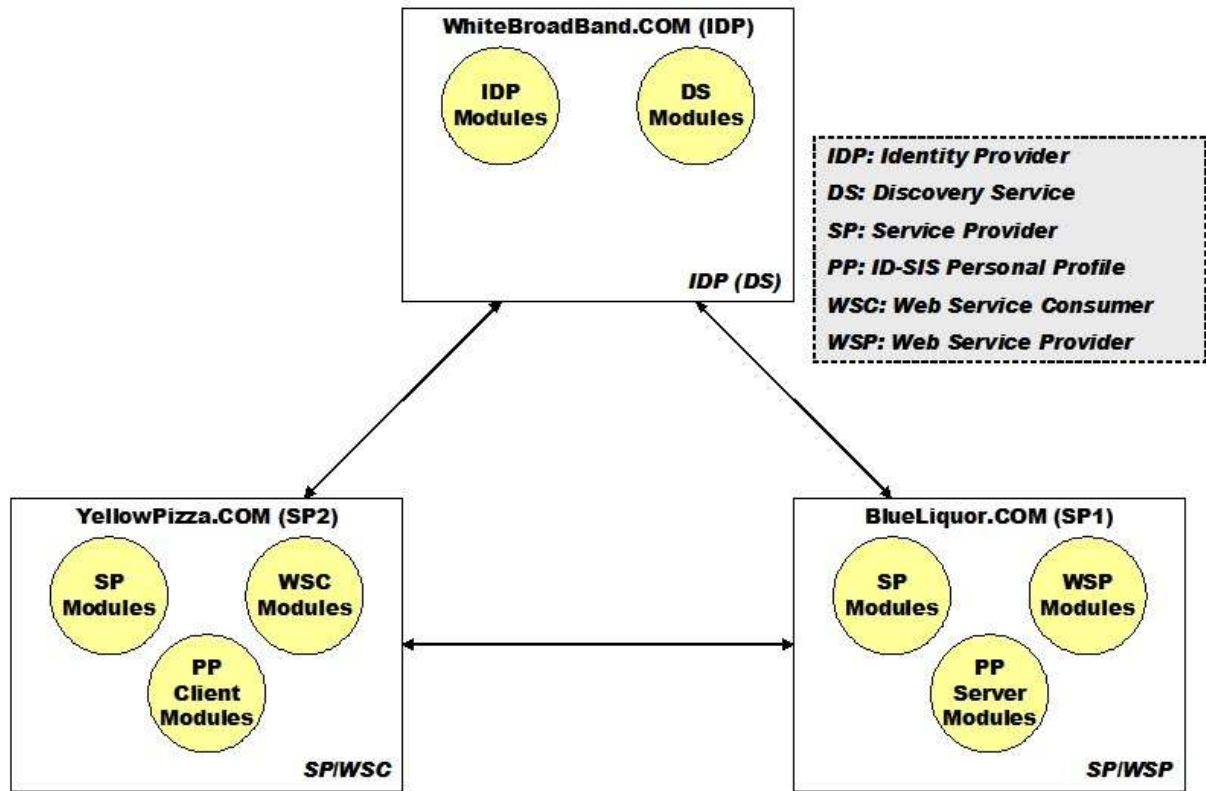
428 Joe Self orders liquors and pizzas on-line.

- 429 1. He makes access to BlueLiquor.COM, and clicks a single sign-on link.
- 430 2. He is redirected to WhiteBroadBand.COM, and authenticates with password
- 431 3. He is redirected again to BlueLiquor.COM. BlueLiquor.COM gets SAML assertion from WhiteBroadBand.COM  
432 that states he has been authenticated, and responds to Joe Self with user-menu page.
- 433 4. He orders some beers on-line, and they are delivered to the address where he has registered at BlueLiquor.COM.

<sup>1</sup>This example is provided by Liberty Alliance member NTT



- 434 5. He requests BlueLiquor.COM to register its ResourceOffering to Discovery Service, so that his Personal Profile  
435 attribute at BlueLiquor.COM can be shared with other site.
- 436 6. BlueLiquor.COM sends Discovery Update message to Discovery Service.  
437



438

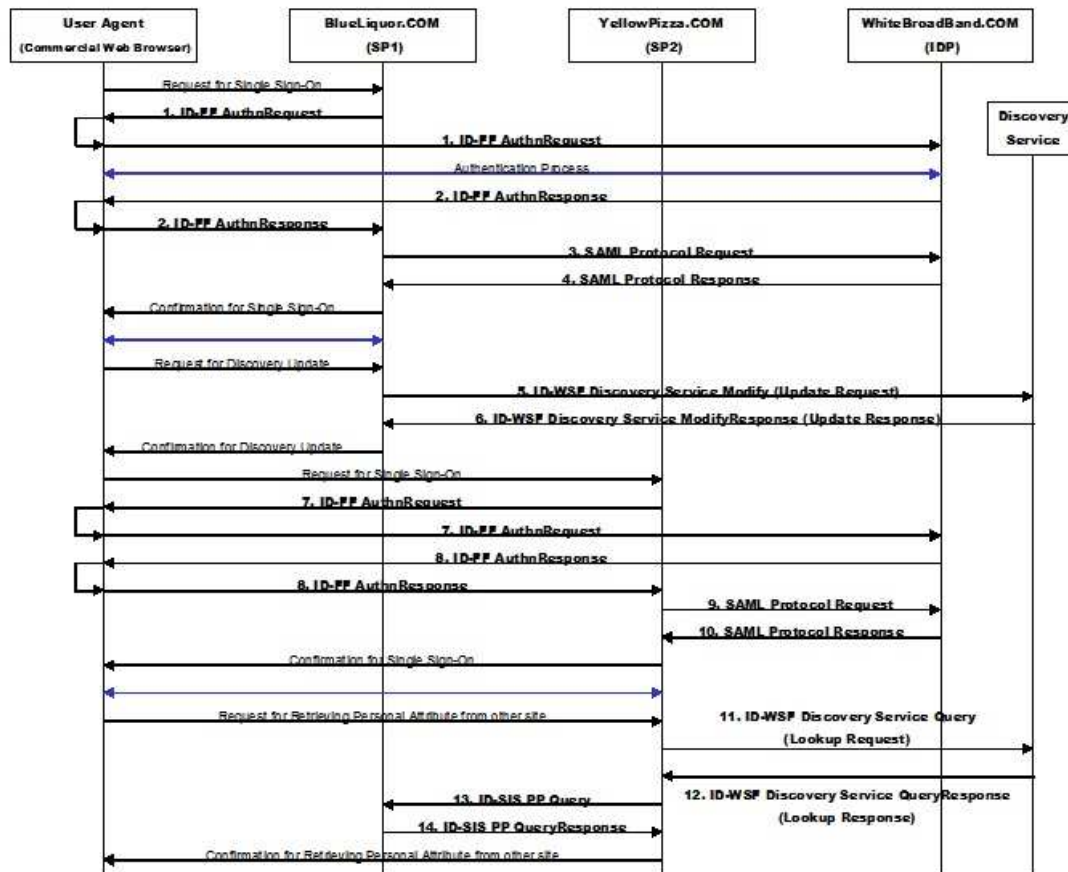
439 **Figure 3. Three Websites and System Modules on the Scenario**

- 440 7. He subsequently makes access to YellowPizza.COM. Since he has been authenticated by WhiteBroad-  
441 Band.COM, YellowPizza.COM can get SAML assertion from WhiteBroadBand.COM, and responds to Joe Self  
442 with user-menu page.
- 443 8. He orders pizza on-line.
- 444 9. He is asked by YellowPizza.COM where they deliver it.
- 445 10. He requests YellowPizza.COM to get his Personal Profile attributes from other site.
- 446 11. YellowPizza.COM sends Discovery Lookup request to Discovery Service, and gets ResourceOffering of  
447 BlueLiquor.COM.
- 448 12. YellowPizza.COM sends Query message to BlueLiquor.COM, and gets his Personal Profile attribute from them.
- 449 13. YellowPizza.COM delivers ordered pizza to the address where they got from BlueLiquor.COM.

## 450 6.2.2. Sequence Flows and Exchanged Messages

### 451 6.2.2.1. Sample Sequence Flows

452 Figure 4 shows sequence flows between entities, that realizes the sample scenario described in section 6.1.1.2. In this  
453 figure, each Liberty specific flow (i.e., Liberty-specific message exchange between entities) is numbered sequentially.



454

455 Figure 4. Sample Sequence Flow

### 456 6.2.2.2. Liberty-Specific Messages Exchanged between Entities

457 In this section, each Liberty-specific message in Figure 4 is explained with its sample XML trace.

#### 458 6.2.2.2.1. ID-FF AuthnRequest

459 SP1 that has received single sign-on request from a Principal, and that confirms a session of the request has not been  
460 authenticated, subsequently sends ID-FF AuthnRequest to IDP using HTTP redirection. IDP that receives ID-FF  
461 AuthnRequest and that confirms the session of the request has not been authenticated, then authenticates a Principal  
462 (e.g., using loginname and password).

463 The following shows an example of ID-FF AuthnRequest message. In this example, SP1 specifies to use the  
464 Browser/Artifact profile for single sign-on process.

465 Example: ID-FF AuthnRequest Message Sent from SP1 to IDP

```
466 https://whitebroadband.com:8443/idp/authn?RequestID=NTT2B3F4EEF8834E572B8A40E0A7A3AABBD&
467 MajorVersion=1&MinorVersion=2&consent=urn%3Aliberty%3Aconsent%3Aobtained&IssueInstant=2004
468 -03-10T05%3A57%3A08Z&ProviderID=https%3A%2F%2Fntt-a.liberty-iop.org%3A8443%2Fsp1%2Fmetadat
469 a&NameIDPolicy=none&ForceAuthn=true&IsPassive=false&ProtocolProfile=http%3A%2F%2Fprojectli
470 berty.org%2Fprofiles%2Fbrws-art&RelayState=NTT77B9A190DF6F02C785E973386BC17C64
471
```

#### 472 6.2.2.2. ID-FF AuthnResponse

473 After authenticating a Principal, IDP sends ID-FF AuthnResponse to SP1 using HTTP redirection. Since  
474 SP1 specifies the Browser/Artifact profile in the AuthnRequest (sequence #1), an artifact is embedded in the  
475 AuthnResponse message.

476 The following shows an example of ID-FF AuthnResponse message.

477 Example: ID-FF AuthnResponse message sent from IDP to SP1

```
478 https://blueliquor.com:8443/sp1/asscon?SAMLart=AAPRT9itmuXxsq1PkKyrh3qQ6xW1gUtShydc%2FjJ
479 yrtzQ2UmMu%2B1Cev3u
480
```

#### 481 6.2.2.3. SAML Protocol Request

482 SP1 that has received ID-FF AuthnResponse, sends SAML Protocol Request message to IDP in order to get SAML  
483 assertion. In the message, an artifact that SP1 received with ID-FF AuthnResponse is embedded.

484 The following shows an example of SAML Protocol Request message.

485 Example: SAML Protocol Request message sent from SP1 to IDP

```
486 <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
487 <soapenv:Body>
488 <samlp:Request IssueInstant="2004-03-10T05:57:16Z" MajorVersion="1" MinorVersion="0"
489 RequestID="NTTC9483587E959EE239CEFA5CF6B65C871"
490 xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol">
491 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
492 <ds:SignedInfo>
493 <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
494 <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
495 <ds:Reference URI="#NTTC9483587E959EE239CEFA5CF6B65C871">
496 <ds:Transforms>
497 <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
498 <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
499 </ds:Transforms>
500 <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
501 <ds:DigestValue>3sNTt/sDyn2G5r6r4GLQAbafT0=</ds:DigestValue>
502 </ds:Reference>
503 </ds:SignedInfo>
504 <ds:SignatureValue>
505 j5yODphPGGP0rhkJkXbYwN0ZfSChJ/4MZSie0jPpCNk4bzw+1WM7F2TuMc4AHAGTKqBqpmURqpW9
506 Qe77fNzuoQhBI12z1KIoMYG/5c33Lxg2lz5Iy1hGzT0yj5Ns0EeU9o6wyJCX18z+pU4UV+TgDj4J
507 V+Jax2rGysYw7/uujwo=
508 </ds:SignatureValue>
509 </ds:Signature>
510 <samlp:AssertionArtifact>
511 AAPRT9itmuXxsq1PkKyrh3qQ6xW1gUtShydc/jJyrtzQ2UmMu+1Cev3u
512 </samlp:AssertionArtifact>
513 </samlp:Request>
514 </soapenv:Body>
515 </soapenv:Envelope>
516
```

517 **6.2.2.2.4. SAML Protocol Response**

518 IDP that has received SAML Protocol Request, embeds SAML assertion that corresponds to specified artifact, and  
 519 sends SAML Protocol Response to SP1. SP1 that receives the response, subsequently checks that SAML assertion,  
 520 and consequently confirms that a Principal is authenticated by IDP.

521 The following shows an example of SAML Protocol Response message.

522 Example: SAML Protocol Response Message Sent from IDP to SP1

```

523 <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
524   <soapenv:Body>
525     <samlp:Response InResponseTo="NTTC9483587E959EE239CEFA5CF6B65C871"
526       IssueInstant="2004-03-10T05:57:20Z" MajorVersion="1" MinorVersion="0"
527       ResponseID="NTTA6D451D50F0D7303FAF2C3F38668DC76"
528       xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol">
529       <samlp:Status>
530         <samlp:StatusCode Value="samlp:Success"/>
531       </samlp:Status>
532       <lib:Assertion AssertionID="NTT7C39BA4B9CC702CD8D00E7BB3D195669"
533         InResponseTo="NTT2B3F4EEF8834E572B8A40E0A7A3AABBD"
534         IssueInstant="2004-03-10T05:57:15Z"
535         Issuer="https://whitebroadband.com:8443/idp/metadata"
536         MajorVersion="1" MinorVersion="2"
537         xmlns:lib="urn:liberty:iff:2003-08">
538         <saml:Conditions NotBefore="2004-03-10T05:57:15Z"
539           NotOnOrAfter="2004-03-11T15:00:00Z"
540           xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"/>
541         <lib:AuthenticationStatement AuthenticationInstant="2004-03-10T05:57:15Z"
542           AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
543           <lib:Subject>
544             <saml:NameIdentifier Format="urn:liberty:iff:nameid:federated"
545               NameQualifier="https://blueliquor.com:8443/sp1/metadata"
546               xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
547               cd8cf101468a7744f07bb57c8bc49e41
548             </saml:NameIdentifier>
549             <saml:SubjectConfirmation xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
550               <saml:ConfirmationMethod>
551                 urn:oasis:names:tc:SAML:1.0:cm:artifact
552               </saml:ConfirmationMethod>
553             </saml:SubjectConfirmation>
554             <lib:IDPProvidedNameIdentifier Format="urn:liberty:iff:nameid:federated"
555               NameQualifier="https://blueliquor.com:8443/sp1/metadata">
556               cd8cf101468a7744f07bb57c8bc49e41
557             </lib:IDPProvidedNameIdentifier>
558           </lib:Subject>
559         </lib:AuthenticationStatement>
560         <saml:AttributeStatement xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
561           <saml:Attribute AttributeName="DiscoveryResourceOffering"
562             AttributeNamespace="urn:liberty:disco:2003-08">
563             <saml:AttributeValue>
564               <disco:ResourceOffering xmlns:disco="urn:liberty:disco:2003-08">
565                 <disco:ResourceID>
566                   https://whitebroadband.com:8443/idp/metadata/37e66f7af c918eb5c27b7b15fca55a01
567                 </disco:ResourceID>
568                 <disco:ServiceInstance>
569                   <disco:ServiceType>urn:liberty:disco:2003-08</disco:ServiceType>
570                   <disco:ProviderID>https://whitebroadband.com:8443/idp/metadata</disco:ProviderID>
571                   <disco:Description>
572                     <disco:SecurityMechID>urn:liberty:security:2003-08:TLS:X509</disco:SecurityMechID>
573                     <disco:SecurityMechID>urn:liberty:security:2003-08:TLS:null</disco:SecurityMechID>
574                   <disco:Endpoint>
575                     https://whitebroadband.com:8443/idp/services/disco
576                   </disco:Endpoint>
577                 </disco:Description>
578               </disco:ServiceInstance>

```

```
579     </disco:ResourceOffering>
580   </saml:AttributeValue>
581 </saml:Attribute>
582 <lib:Subject>
583   <saml:NameIdentifier Format="urn:liberty:iff:nameid:federated"
584     NameQualifier="https://blueliquor.com:8443/spl/metadata">
585     cd8cf101468a7744f07bb57c8bc49e41
586   </saml:NameIdentifier>
587 </lib:Subject>
588 </saml:AttributeStatement>
589 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
590   <ds:SignedInfo>
591     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
592     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
593     <ds:Reference URI="#NTT7C39BA4B9CC702CD8D00E7BB3D195669" >
594       <ds:Transforms>
595         <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
596         <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
597       </ds:Transforms>
598       <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
599       <ds:DigestValue>+GpMzKtRAGzyP3qKe8W8vbU9ZMk=</ds:DigestValue>
600     </ds:Reference>
601   </ds:SignedInfo>
602   <ds:SignatureValue>
603     C99cr3ObEaRjSQL61uu7ObMjH0sK/5k+x0y9tysQa25q75eaGUGuspAN4YQcG7oFR/yyunIC0Hsf
604     5boJSwj+1Re8yvOlianrlb4mEa4XcV8vATsCCGjjhSr1FjLxUCnSDzJs z0cWVW89EA0QStI58NmY
605     XeWv2xkk5p2a5Ut4940=
606   </ds:SignatureValue>
607 </ds:Signature>
608 </lib:Assertion>
609 </samlp:Response>
610 </soapenv:Body>
611 </soapenv:Envelope>
612
```

#### 613 6.2.2.2.5. ID-WSF Discovery Service Modify (Discovery Update Request)

614 SP1 maintains Principal's attributes (e.g., address information) and is able to acts as Attribute Provider. By being  
615 requested by a Principal, SP1 registers its ResourceOffering to Discovery Service (DS). This process can be done by  
616 sending ID-WSF Discovery Service Modify message.

617 The following example shows ID-WSF Discovery Service Modify message sent from SP1 to DS.

618 Example: Modify Message Sent from SP1 to DS

```
619 <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
620   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
621   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
622   <soapenv:Header>
623     <sb:Correlation id="NTT999DB7BE847E1693D8B90896D7BB481B"
624       messageID="uuid:f11b9e67-b855-0709-5e7e-f65f8b9ff9b1"
625       timestamp="2004-03-10T05:58:25Z"
626       soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
627       soapenv:mustUnderstand="1"
628       xmlns:sb="urn:liberty:sb:2003-08" />
629     <sb:Provider providerID="https://blueliquor.com:8443/spl/metadata"
630       soapenv:mustUnderstand="0"
631       xmlns:sb="urn:liberty:sb:2003-08" />
632     <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
633       soapenv:mustUnderstand="1"
634       xmlns:wsse="http://schemas.xmlsoap.org/ws/2003/06/secext">
635       <wsse:BinarySecurityToken
636         EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-securi
637 ty-1.0#Base64Binary"
638         ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1
```

```
639 .0#X509v3"
640     wsu:Id="X509Token"
641     xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility">
642     MIICBDCCAW2gAwIBAgIBUTANBgkqhkiG9w0BAQQFADAlMQswCQYDVQQGEwJVUzEUMBIGALUEChML
643     TGliZXJ0eSBjTlAxEDA0BgNVBAMTB1Rlc3QgQ0EwHhcNMDMxMjA1MTQ0MjI1WWhcNMDQxMjA0MTQ0
644     MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlicXJ0eSBjTlAgamtzMzSMwIQYDVQQDExp
645     dhQtYS1zaWduLmXpYmVydHktaW9wLm9yZzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAq9S1
646     +JvcHKNjttE/v70TKMMXo+Ft05RBy/XUruHZsuH0b206MYG+C CBoPyJ6Jv+6+ZsCgIEjJfJ61qRZR
647     ZmPdGv92zcBH0L/k1/GG7FPNFH+mrUm/66nRDysv6JFMzW7+Ct7132IUuIEVj45CXHEcyy8JUf
648     fd1J1+F0rVweAEUCawEAAaMNMAsWCQYDVR0TBAlwADANBgkqhkiG9w0BAQQFAAOBgQBwqsW22HMT
649     LTcxn3jiifP+yBjKRAYpikrRzffeJ8XtLUrHCkm7ZOX/OeqidHAARB41TxmITCB3LbHmViAk4G66
650     K4Yb9Y0FFVJCFyayHnY6W6oLDkTv5IMqDL//vV6QF9bo02gvTpap4WL5+6meNmCyWKoeO4CuwX3q
651     ys5yrA8opg==
652 </wsse:BinarySecurityToken>
653 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
654   <ds:SignedInfo>
655     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
656     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
657     <ds:Reference URI="#NTT999DB7BE847E1693D8B90896D7BB481B">
658       <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
659       <ds:DigestValue>q2lVlJG2WV8mnpPeCTdY5SHj8FQ=</ds:DigestValue>
660     </ds:Reference>
661     <ds:Reference URI="#NTTA68A82625412949E477FFB33ACF48560">
662       <ds:Transforms>
663         <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
664       </ds:Transforms>
665       <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
666       <ds:DigestValue>C1fHwpAa/XR29boFKsmZuYbxoTk=</ds:DigestValue>
667     </ds:Reference>
668   </ds:SignedInfo>
669   <ds:SignatureValue>
670     V3vmsz0BI3l7ZqP27PjikWfzqDvDew3DHPDuXJ98b kedG1GzPHjstvtpNvxD0SylhtiJWSC6 eemR2
671     JEJvQfEmG05ScsjZURJcdyS6thbDwfsNhBhPv3nZtEX0 zMkfvxlnNU3wd3QfsAGMHuxXhl7U8jAt
672     4/8A3nHupJldkefFqXg=
673   </ds:SignatureValue>
674   <ds:KeyInfo>
675     <wsse:SecurityTokenReference Usage="sec:MessageAuthentication"
676       xmlns:sec="urn:liberty:sec:2003-08">
677       <wsse:Reference URI="#X509Token"/>
678     </wsse:SecurityTokenReference>
679   </ds:KeyInfo>
680 </ds:Signature>
681 </wsse:Security>
682 </soapenv:Header>
683 <soapenv:Body>
684   <disco:Modify id="NTTA68A82625412949E477FFB33ACF48560" xmlns:disco="urn:liberty:disco:20
685   03-08">
686     <disco:ResourceID>
687       https://whitebroadband.com:8443/idp/metadata/37e66f7afc918eb5c27b7b15fca55a01
688     </disco:ResourceID>
689     <disco:InsertEntry>
690       <disco:ResourceOffering>
691         <disco:ResourceID>uuid:e427014e-1fde-cc03-85dd-690333bf695a</disco:ResourceID>
692       <disco:ServiceInstance>
693         <disco:ServiceType>urn:liberty:id-sis-pp:2003-08</disco:ServiceType>
694         <disco:ProviderID>https://blueliquor.com:8443/spl/metadata</disco:ProviderID>
695         <disco:Description>
696           <disco:SecurityMechID>urn:liberty:security:2003-08:TLS:X509</disco:SecurityMechID>
697           <disco:SecurityMechID>urn:liberty:security:2003-08:TLS:null</disco:SecurityMechID>
698           <disco:Endpoint>https://blueliquor.com:8443/spl/services/idpp</disco:Endpoint>
699         </disco:Description>
700       </disco:ServiceInstance>
701     </disco:Options>
702     <disco:Option>urn:liberty:id-sis-pp:home</disco:Option>
703     <disco:Option>urn:liberty:id-sis-pp:personal</disco:Option>
704     <disco:Option>urn:liberty:id-sis-pp:cn</disco:Option>
705     <disco:Option>urn:liberty:id-sis-pp:informalName</disco:Option>
```

```

706         <disco:Option>urn:liberty:id-sis-pp:demographics</disco:Option>
707     </disco:Options>
708     <disco:Abstract>identity service for demonstration</disco:Abstract>
709 </disco:ResourceOffering>
710 </disco:InsertEntry>
711 </disco:Modify>
712 </soapenv:Body>
713 </soapenv:Envelope>
714

```

### 715 6.2.2.2.6. ID-WSF Discovery Service ModifyResponse (Discovery Update Response)

716 DS that has received ID-WSF Discovery Service Modify message, registers specified ResourceOffering, and responds  
717 to SP1 with ID-WSF Discovery Service Modify Response message.

718 The following example shows ID-WSF Discovery Service ModifyResponse message.

719 Example: ID-WSF Discovery Service ModifyResponse Message Sent from DS to SP1

```

720 <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
721     xmlns:xsd="http://www.w3.org/2001/XMLSchema"
722     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
723 <soapenv:Header>
724     <sb:Provider id="NTT52DBE45FADF6384EFC295BDDA45C1CE0"
725         providerID="https://whitebroadband.com:8443/idp/metadata"
726         soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
727         soapenv:mustUnderstand="0"
728         xmlns:sb="urn:liberty:sb:2003-08"/>
729     <sb:Correlation id="NTT1E236AD1E4C6A098E03ABBB75DC43AE2"
730         messageID="uuid:1fa7c4d0-8e26-7819-b236-eb92eb6b4fc6"
731         refToMessageID="uuid:f11b9e67-b855-0709-5e7e-f65f8b9ff9b1"
732         timestamp="2004-03-10T05:58:26Z"
733         soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
734         soapenv:mustUnderstand="1"
735         xmlns:sb="urn:liberty:sb:2003-08"/>
736     <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
737         soapenv:mustUnderstand="1"
738         xmlns:wsse="http://schemas.xmlsoap.org/ws/2003/06/secext">
739         <wsse:BinarySecurityToken
740             EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-mes
741 sage-security-1.0#Base64Binary"
742             ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token
743 -profile-1.0#X509v3"
744             wsu:Id="X509Token"
745             xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility">
746 MIICBCCAW2gAwIBAgIBUTANBgkqhkiG9w0BAQQFADAlMQswCQYDVQQGEwJVUzEUMBIGALUEChML
747 TGliZXJ0eSBjTlAxEDA0BgNVBAMTB1Rlc3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQxMjA0MTQ0
748 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx
749 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx
750 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx
751 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx
752 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx
753 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx
754 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx
755 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx
756 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx
757 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx
758 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx
759 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx
760 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx
761 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx
762 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx
763 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx
764 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx
765 MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA0MTQ0MjI1WWhcNMDQx

```

```

766     <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
767     <ds:DigestValue>QWlqgzPycEFNwOIP3cIPLXv+Pk=</ds:DigestValue>
768 </ds:Reference>
769 <ds:Reference URI="#NTT18821653A7C16BEFF877DDC9A7D09B33">
770   <ds:Transforms>
771     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
772   </ds:Transforms>
773   <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
774   <ds:DigestValue>GSZWYAtwKaTR1FP+a8bxa7sGI6w=</ds:DigestValue>
775 </ds:Reference>
776 </ds:SignedInfo>
777 <ds:SignatureValue>
778   JMlQLXFqtBVZyfo7TRGfqkFiPfNveU1X0yf+WwJqnHP1ADS3s7nBdW1SzKEwufZi4k+JNAy8E6Fk
779   Lh+nH0XdN9Pmw56DzAYNBK8JAZ2B7tGhntJwJHKLbZ3XgRXuH6A+wC7uvjTbu2ZQ9kcSY4EuWpxt
780   4tJYqQTqFYyRcVEAFLM=
781 </ds:SignatureValue>
782 <ds:KeyInfo>
783   <wsse:SecurityTokenReference Usage="sec:MessageAuthentication"
784     xmlns:sec="urn:liberty:sec:2003-08" >
785     <wsse:Reference URI="#X509Token" />
786   </wsse:SecurityTokenReference >
787 </ds:KeyInfo>
788 </ds:Signature>
789 </wsse:Security>
790 </soapenv:Header>
791 <soapenv:Body>
792   <disco:ModifyResponse id="NTT18821653A7C16BEFF877DDC9A7D09B33"
793     newEntryIDs="uuid:1c1ccaeb-0c36-229b-d510-7ae33406ada4"
794     xmlns:disco="urn:liberty:disco:2003-08">
795     <disco:Status code="disco:OK" />
796   </disco:ModifyResponse>
797 </soapenv:Body>
798 </soapenv:Envelope>
799

```

#### 800 6.2.2.2.7. ID-FF AuthnRequest

801 SP2 that has received single sign-on request from a Principal, and that confirms a session of the request has not been  
802 authenticated, subsequently sends ID-FF AuthnRequest to IDP using HTTP redirection. IDP that receives ID-FF  
803 AuthnRequest and that confirms the session of the request has not been authenticated, then authenticates a Principal  
804 (e.g., using loginname and password). Figure 6.9 shows an example of ID-FF AuthnRequest message.

805 In this example, SP2 also specifies to use the Browser/Artifact profile for single sign-on process.

806 Example: ID-FF AuthnRequest Message Sent from SP2 to IDP

```

807 https://whitebroadband.com:8443/idp/authn?RequestID=NTTEC6D3DDAE91E0379423F1AD3B178C752&
808 MajorVersion=1&MinorVersion=2&consent=urn%3Aliberty%3Aconsent%3Aobtained&IssueInstant=2004
809 -03-10T05%3A58%3A44Z&ProviderID=https%3A%2F%2Fntt-a.liberty-iop.org%3A8443%2Fsp%2Fmetadat
810 a&NameIDPolicy=none&ForceAuthn=true&IsPassive=false&ProtocolProfile=http%3A%2F%2Fprojectli
811 berty.org%2Fprofiles%2Fbrws-art&RelayState=NTTD4C48FF08D6098698A7EB5CE08BA9BB0
812

```

#### 813 6.2.2.2.8. ID-FF AuthnResponse

814 After confirming that a requested message's session has been authenticated, IDP sends ID-FF AuthnResponse to SP2  
815 using HTTP redirection. Since SP2 specifies the Browser/Artifact profile in the AuthnRequest (sequence #1), an  
816 artifact is embedded in the AuthnResponse message. The following shows an example of ID-FF AuthnResponse  
817 message.

818 Example: ID-FF AuthnResponse Message Sent from IDP to SP2



819 https://yellowpizza.com:8443/sp2/asscon?SAMLart=AAPRT9itmuXxsqlPkKyrh3qQ6xWlgc%2BR4UjUyH  
 820 KNba6xUwkCIPVUUr34  
 821

### 822 6.2.2.2.9. SAML Protocol Request

823 SP2 that has received ID-FF AuthnResponse, sends SAML Protocol Request message to IDP in order to get SAML  
 824 assertion. In the message, an artifact that SP2 received with ID-FF AuthnResponse is embedded.

825 The following shows an example of SAML Protocol Request message.

826 Example: SAML Protocol Request Message Sent from SP2 to IDP

```
827 <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
828   <soapenv:Body>
829     <samlp:Request IssueInstant="2004-03-10T05:58:46Z"
830       MajorVersion="1" MinorVersion="0"
831       RequestID="NTTB7CCE49363C5007F8CCC6277B217ED71"
832       xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol">
833     <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
834       <ds:SignedInfo>
835         <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
836         <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
837         <ds:Reference URI="#NTTB7CCE49363C5007F8CCC6277B217ED71">
838           <ds:Transforms>
839             <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
840             <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
841           </ds:Transforms>
842           <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
843           <ds:DigestValue>pw3BfCHpGQCf3w5DHelZsZLzbqY=</ds:DigestValue>
844         </ds:Reference>
845       </ds:SignedInfo>
846       <ds:SignatureValue>
847         Q9Kn95nnNU71taHA4X8HY7kE02ineOW0yWRSpC2IZQPvt6zS30G+OPy5U021ELsLwtNMqwyHBT9
848         OBY4k7HZNVCEwVNwcGBslodKaOvV5neTSs iOgjZzvw+acrRha7qADCh0P5JAB3d0dRsy7f+odZlS
849         vll6/b7m6cAQA6rvLI4=
850       </ds:SignatureValue>
851     </ds:Signature>
852     <samlp:AssertionArtifact>
853       AAPRT9itmuXxsqlPkKyrh3qQ6xWlgc+R4UjUyHKNba6xUwkCIPVUUr34
854     </samlp:AssertionArtifact>
855   </samlp:Request>
856 </soapenv:Body>
857 </soapenv:Envelope>
858
```

### 859 6.2.2.2.10. SAML Protocol Response

860 IDP that has received SAML Protocol Request, embeds SAML assertion that corresponds to specified artifact, and  
 861 sends SAML Protocol Response to SP2. SP2 that receives the response, subsequently checks that SAML assertion,  
 862 and consequently confirms that a Principal is authenticated by IDP.

863 The following shows an example of SAML Protocol Response message.

864 Example: SAML Protocol Response Message Sent from IDP to SP2

```
865 <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
866   <soapenv:Body>
867     <samlp:Response InResponseTo="NTTB7CCE49363C5007F8CCC6277B217ED71"
868       IssueInstant="2004-03-10T05:58:48Z"
869       MajorVersion="1" MinorVersion="0"
870       ResponseID="NTT53BF476E93C913C1CBEEB8A402C29EC7"
871
```

```

872         xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol">
873     <samlp:Status>
874         <samlp:StatusCode Value="samlp:Success" />
875     </samlp:Status>
876     <lib:Assertion AssertionID="NTT3E0343B5B13442509112CDB32A81D461 "
877         InResponseTo="NTTEC6D3DDAE91E0379423F1AD3B178C752"
878         IssueInstant="2004-03-10T05:58:46Z"
879         Issuer="https://whitebroadband.com:8443/idp/metadata"
880         MajorVersion="1" MinorVersion="2"
881         xmlns:lib="urn:liberty:iff:2003-08">
882     <saml:Conditions NotBefore="2004-03-10T05:58:46Z"
883         NotOnOrAfter="2004-03-11T15:00:00Z"
884         xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion" />
885     <lib:AuthenticationStatement
886         AuthenticationInstant="2004-03-10T05:58:46Z"
887         AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
888
889     <lib:Subject>
890     <saml:NameIdentifier Format="urn:liberty:iff:nameid:federated"
891         NameQualifier="https://yellowpizza.com:8443/sp2/metadata"
892         xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
893         da275058804ee420d957623280d2f5f5
894     </saml:NameIdentifier>
895     <saml:SubjectConfirmation xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
896
897     <saml:ConfirmationMethod>
898         urn:oasis:names:tc:SAML:1.0:cm:artifact
899     </saml:ConfirmationMethod>
900     </saml:SubjectConfirmation>
901     <lib:IDPProvidedNameIdentifier
902         Format="urn:liberty:iff:nameid:federated"
903         NameQualifier="https://yellowpizza.com:8443/sp2/metadata">
904         da275058804ee420d957623280d2f5f5
905     </lib:IDPProvidedNameIdentifier>
906     </lib:Subject>
907 </lib:AuthenticationStatement>
908 <saml:AttributeStatement xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
909
910     <saml:Attribute AttributeName="DiscoveryResourceOffering"
911         AttributeNamespace="urn:liberty:disco:2003-08">
912     <saml:AttributeValue>
913         <disco:ResourceOffering xmlns:disco="urn:liberty:disco:2003-08">
914
915         <disco:ResourceID>
916             https://whitebroadband.com:8443/idp/metadata/37e66f7afc918eb5c27b7b15fca55a01
917         </disco:ResourceID>
918         <disco:ServiceInstance>
919             <disco:ServiceType>urn:liberty:disco:2003-08</disco:ServiceType>
920             <disco:ProviderID>
921                 https://whitebroadband.com:8443/idp/metadata
922             </disco:ProviderID>
923             <disco:Description>
924                 <disco:SecurityMechID>
925                     urn:liberty:security:2003-08:TLS:X509
926                 </disco:SecurityMechID>
927                 <disco:SecurityMechID>
928                     urn:liberty:security:2003-08:TLS:null
929                 </disco:SecurityMechID>
930                 <disco:Endpoint>
931                     https://whitebroadband.com:8443/idp/services/disco
932                 </disco:Endpoint>
933             </disco:Description>
934             </disco:ServiceInstance>
935         </disco:ResourceOffering>
936     </saml:AttributeValue>
937 </saml:Attribute>
938 </lib:Subject>

```

```

939     <saml:NameIdentifier Format="urn:liberty:iff:nameid:federated"
940       NameQualifier="https://yellowpizza.com:8443/sp2/metadata">
941       da275058804ee420d957623280d2f5f5
942     </saml:NameIdentifier>
943   </lib:Subject>
944 </saml:AttributeStatement>
945 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
946   <ds:SignedInfo>
947     <ds:CanonicalizationMethod
948       Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
949     <ds:SignatureMethod
950       Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
951     <ds:Reference URI="#NTT3E0343B5B13442509112CDB32A81D461" >
952       <ds:Transforms>
953         <ds:Transform
954           Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
955         <ds:Transform
956           Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
957       </ds:Transforms>
958       <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
959       <ds:DigestValue>UEWe8B8foWlICZ68GoUl+Uz44Ws</ds:DigestValue>
960     </ds:Reference>
961   </ds:SignedInfo>
962   <ds:SignatureValue>
963     oAb+mpZOVArfaMIA4+T6y23mW5A10Thc4Ggqsnt4 1H8yCwiweRBA5WdNnpXkezRdu/s2n/ iheZM7
964     2uI2Z5mYjxkAV9FLGFISanLbHq5KoyVYgl0tiQaI/TCVysfZ9pYAuYVoB5Tu6EsUPDZ+C2z VnS9N
965     gxwk64H+S4rnAvGrxcU=
966   </ds:SignatureValue>
967 </ds:Signature>
968 </lib:Assertion>
969 </samlp:Response>
970 </soapenv:Body>
971 </soapenv:Envelope>
972

```

### 973 6.2.2.2.11. ID-WSF Discovery Service Query (Discovery Lookup Request)

974 SP2 does not maintain Principal's attributes. Therefore, by being requested by a Principal, SP2 tries to retrieve  
975 Principal's attributes from other websites. This process is realized by sending ID-WSF Query message to DS, and  
976 SP2 uses ResourceOffering of DS for sending the message, that it has received from IDP with ID-FF AuthnResponse  
977 (i.e., ResourceOffering of DS is embedded in the ID-FF AuthnResponse that is exchanged with sequence #10), and  
978 queries ResourceOfferings of other websites (i.e., Attribute Providers).

979 The following shows an example of ID-WSF Discovery Service Query message.

980 Example: ID-WSF Discovery Service Query message sent from SP2 to DS

```

981 <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
982   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
983   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
984
985   <soapenv:Header>
986     <sb:Correlation id="NTTAEB9DE0EB0B1A89B00797A14C6EE85F6"
987       messageID="uuid:debbffd3-4ea8-973e-5463-e5ecc2d95dde"
988       timestamp="2004-03-10T05:59:01Z"
989       soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
990       soapenv:mustUnderstand="1"
991       xmlns:sb="urn:liberty:sb:2003-08" />
992     <sb:Provider providerID="https://yellowpizza.com:8443/sp2/metadata"
993       soapenv:mustUnderstand="0"
994       xmlns:sb="urn:liberty:sb:2003-08" />
995     <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
996       soapenv:mustUnderstand="1"
997       xmlns:wsse="http://schemas.xmlsoap.org/ws/2003/06/secure">

```

```

998
999     <wsse:BinarySecurityToken
1000       EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-mes
1001 sage-security-1.0#Base64Binary"
1002       ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token
1003 -profile-1.0#X509v3"
1004       wsu:Id="X509Token"
1005       xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility" >
1006         MIICBCCAww2gAwIBAgIBUTANBgkqhkiG9w0BAQQFADAlMQswCQYDVQQGEwJVUzEUMBIGALUEChML
1007         TGliZXJ0eSBjTlAxEDA0BgNVBAMTB1Rlc3QgQ0EwHhcNMDMxMjAlMTQOMjI1WWhcNMDQxMjA0MTQ0
1008         MjI1WjBMMQswCQYDVQQGEwJVUzEYMBYGA1UEChMPTGlicXJ0eSBjTlAgamtzMSMwIQYDVQQDExpudHQtYS1zaWduLm
1009         xpYmVydHktaW9wLm9yZzZCbzANBgkqhkiG9w0BAQEFAAOBjQAwGgYkCgYEAq9S1
1010         +JvcHKNjttE/v70TKMMXo+Ft05RBy/XUruHZsuH0b206MYG+CCBoPyJ6Jv+6+ZsCgIEjFJ6lqRZR
1011         ZmPdGv92zcBH01/k1/GG7FPNFH+mrUm/66nRDysv6JFMzW7+Ct7132IUUiTEvj45CXHECyy8JUf
1012         fd1Jl+F0rVweAEUCAwEAAMNMAswCQYDVR0TBAlwADANBgkqhkiG9w0BAQQFAAOBgQBwqsW22HMT
1013         LTCxn3jiifP+yBjKRAYpikrRzffeJ8XtLUrHCKm7ZOX/OeqidHAARB4lTxmITCB3LbHmViAk4G66
1014         K4Yb9Y0FFVJCFyayHnY6W6oLDkTv5I MqDL//vV6QF9bo02gvTpap4WL5+6meNmCyWKoe04CuwX3q
1015         ys5yrA8opg==
1016     </wsse:BinarySecurityToken>
1017     <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
1018       <ds:SignedInfo>
1019         <ds:CanonicalizationMethod
1020           Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
1021         <ds:SignatureMethod
1022           Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
1023         <ds:Reference URI="#NTTAE9DE0EB0B1A89B00797A14C6EE85F6">
1024           <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1025           <ds:DigestValue>/vqZkvIo2MkbAntQ3j0+I0QsZ4k=</ds:DigestValue>
1026         </ds:Reference>
1027         <ds:Reference URI="#NTT43EBDA48A7965082DA284C13DE33EFDE">
1028           <ds:Transforms>
1029             <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
1030           </ds:Transforms>
1031           <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1032           <ds:DigestValue>js4CmrBteuy9Epti9409+xFj7yk=</ds:DigestValue>
1033         </ds:Reference>
1034       </ds:SignedInfo>
1035       <ds:SignatureValue>
1036         Rh9MenehPh/9zIB/8wNg4tCKaLIs5ayiRbfKrepXpD9qbsIOVjZ0/2R1Chix/WaDANTvtdfj/sD3
1037         utjTLRniXKF45RWKQtzZT3eRG2elAfm7a9ZnWgFBm0Q+/kSPmPHzo3aCx9K8yVUPmdg/S8Bwjh5
1038         VLvz9U99JDJKF4FEx3o=
1039       </ds:SignatureValue>
1040       <ds:KeyInfo>
1041         <wsse:SecurityTokenReference Usage="sec:MessageAuthentication"
1042           xmlns:sec="urn:liberty:sec:2003-08">
1043           <wsse:Reference URI="#X509Token" />
1044         </wsse:SecurityTokenReference>
1045       </ds:KeyInfo>
1046     </ds:Signature>
1047   </wsse:Security>
1048 </soapenv:Header>
1049 <soapenv:Body>
1050   <disco:Query id="NTT43EBDA48A7965082DA284C13DE33EFDE"
1051     xmlns:disco="urn:liberty:disco:2003-08">
1052     <disco:ResourceID>
1053       https://whitebroadband.com:8443/idp/metadata/37e66f7afc918eb5c27b7b15fca55a01
1054     </disco:ResourceID>
1055     <disco:RequestedServiceType>
1056       <disco:ServiceType>urn:liberty:id-sis-pp:2003-08</disco:ServiceType>
1057     <disco:Options>
1058       <disco:Option>urn:liberty:id-sis-pp:home</disco:Option>
1059       <disco:Option>urn:liberty:id-sis-pp:informalName</disco:Option>
1060     </disco:Options>
1061   </disco:RequestedServiceType>
1062 </disco:Query>
1063 </soapenv:Body>
1064

```

1065 </soapenv:Envelope>  
 1066

1067 **6.2.2.2.12. ID-WSF Discovery Service QueryResponse (Discovery Lookup Response)**

1068 DS that has received ID-WSF Discovery Service Query message, responds to SP2 with ID-WSF Discovery Service  
 1069 QueryResponse in which ResourceOfferings that mach with specified ResourceID and ServiceType are embedded.  
 1070 Figure 6.14 shows an example of ID-WSF Discovery Service QueryResponse message.

1071 In the previous example, SP2 specifies some Option keywords. These Option keywords are defined in ID-SIS  
 1072 Personal Profile specification, and are used to specify particular attributes of Personal Profile and query them if they  
 1073 are available to share.

1074 In this example, SP2 gets SP1's ResourceOffering.

1075 Example: ID-WSF Discovery Service QueryResponse Message Sent from DS to SP2

```

1076 <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
1077     xmlns:xsd="http://www.w3.org/2001/XMLSchema"
1078     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
1079
1080   <soapenv:Header>
1081     <sb:Provider id="NTTE820FAA18F168B2AD7E627689489D4ED"
1082         providerID="https://whitebroadband.com:8443/idp/metadata"
1083         soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
1084         soapenv:mustUnderstand="0"
1085         xmlns:sb="urn:liberty:sb:2003-08" />
1086     <sb:Correlation id="NTTE8AE0B45F78061FE570DFBFB06EC62DB"
1087         messageID="uuid:9ea67cd2-f414-c756-cb06-917d7f84dfe5"
1088         refToMessageID="uuid:debbffd3-4ea8-973e-5463-e5ecc2d95dde"
1089         timestamp="2004-03-10T05:59:02Z"
1090         soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
1091         soapenv:mustUnderstand="1"
1092         xmlns:sb="urn:liberty:sb:2003-08" />
1093     <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
1094         soapenv:mustUnderstand="1"
1095         xmlns:wsse="http://schemas.xmlsoap.org/ws/2003/06/secext">
1096
1097       <wsse:BinarySecurityToken
1098         EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-so
1099 ap-message-security-1.0#Base64Binary"
1100         ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509
1101 -token-profile-1.0#X509v3"
1102         wsu:Id="X509Token"
1103         xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility">
1104         MIICBDCCAW2gAwIBAgIBUTANBgkqhkiG9w0BAQQFADA1MQswCQYDVQQGEwJVUzEUMBIGALUEChML
1105         TGliZXJ0eSBjTlAxEDA0BGNVBAW2gAwIBAgIBUTANBgkqhkiG9w0BAQQFADA1MQswCQYDVQQGEwJVUzEUMBIGALUEChML
1106         MjI1WjBMMQswCQYDVQQGEwJVUzEUMBIGALUEChMPTGlicXJ0eSBjTlAgamtzMSMwIQYDVQQDEExpu
1107         dHQYSlzaWduLmVudHktaW9wLm9yZzCBbnANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAq9S1
1108         +JvcHKNjttE/v70TKMMXo+Ft05RBy/XUruHZsuH0b206MYG+CCBoPyJ6Jv+6+ZsCgIEjFJ6lqRZR
1109         ZmPdGv92zcBHH01/k1/GG7FPNFH+mrUm/66nRDy sv6JFMzW7+Ct7132IUUiTEvj45CXHE cyy8JUf
1110         fd1J1+F0rVweAUEUCAwEAAaMNMAwCQYDVROTBAlwADANBgkqhkiG9w0BAQQFAA0BQwqsw22HMT
1111         LTCxn3jiiFP+yBjKRaYpikrRzffeJ8XtLURHCKm7ZOX/OeqidHAARB41TxmITCB3LbHmViAk4G66
1112         K4Yb9Y0FFVJCFyaYHnY6W6oLDkTv5IMqDL//vV6QF9boO2gvTpap4WL5+6meNmCyWKoeO4CuwX3q
1113         ys5yrA8opg==
1114       </wsse:BinarySecurityToken>
1115     <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
1116       <ds:SignedInfo>
1117         <ds:CanonicalizationMethod
1118           Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
1119         <ds:SignatureMethod
1120           Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
1121         <ds:Reference URI="#NTTE820FAA18F168B2AD7E627689489D4ED">
1122           <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    
```

```

1123     <ds:DigestValue>8PAUP7vDPOYT2JHoRBCky rF8jTU=</ds:DigestValue>
1124 </ds:Reference>
1125 <ds:Reference URI="#NTTE8AE0B45F78061FE570DBFBB06EC62DB" >
1126   <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1127   <ds:DigestValue>mZBMURT5gUco82RQsEEJHo3lC4U=</ds:DigestValue>
1128 </ds:Reference>
1129 <ds:Reference URI="#NTTE6CF51BEB0320300DF0F4070CD04D1B6">
1130   <ds:Transforms>
1131     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
1132   </ds:Transforms>
1133   <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1134   <ds:DigestValue>KEXH0Z48Y59j/dEI50AGm0z PO4M=</ds:DigestValue>
1135 </ds:Reference>
1136 </ds:SignedInfo>
1137 </ds:Signature>
1138 <ds:Signature>
1139   <ds:SignatureValue>
1140     aFly651gBlQd5kNeOIE12Sku/fARaG+pf8j2emc2qt9F1BmJr TFF9SeRdnkCXAGA7zxbdytUbKBI
1141     mzn7OAmRdgzUN/AUqtTD/fqPulm3KYGzn8otTsX6lJV/73ZIEgP2 +vC9/Tsa8VD8mTAcexEiEzRb
1142     ZNEyWnfWhyhLPf5TgX0=
1143   </ds:SignatureValue>
1144   <ds:KeyInfo>
1145     <wsse:SecurityTokenReference Usage="sec:MessageAuthentication"
1146       xmlns:sec="urn:liberty:sec:2003-08">
1147       <wsse:Reference URI="#X509Token" />
1148     </wsse:SecurityTokenReference>
1149   </ds:KeyInfo>
1150 </ds:Signature>
1151 </wsse:Security>
1152 </soapenv:Header>
1153 <soapenv:Body>
1154   <disco:QueryResponse id="NTTE6CF51BEB0320300DF0F4070CD04D1B6"
1155     xmlns:disco="urn:liberty:disco:2003-08">
1156     <disco:Status code="OK" />
1157     <disco:ResourceOffering entryID="uuid:1c1ccaeb-0c36-229b-d510-7ae33406ada4">
1158
1159       <disco:ResourceID>
1160         uuid:e427014e-1fde-cc03-85dd-690333bf695a
1161       </disco:ResourceID>
1162       <disco:ServiceInstance>
1163         <disco:ServiceType>
1164           urn:liberty:id-sis-pp:2003-08
1165         </disco:ServiceType>
1166         <disco:ProviderID>
1167           https://blueliquor.com:8443/sp1/metadata
1168         </disco:ProviderID>
1169         <disco:Description>
1170           <disco:SecurityMechID>
1171             urn:liberty:security:2003-08:TLS:X509
1172           </disco:SecurityMechID>
1173           <disco:SecurityMechID>
1174             urn:liberty:security:2003-08:TLS:null
1175           </disco:SecurityMechID>
1176           <disco:Endpoint>
1177             https://blueliquor.com:8443/sp1/services/idpp
1178           </disco:Endpoint>
1179         </disco:Description>
1180       </disco:ServiceInstance>
1181       <disco:Options>
1182         <disco:Option>urn:liberty:id-sis-pp:home</disco:Option>
1183         <disco:Option>urn:liberty:id-sis-pp:personal</disco:Option>
1184         <disco:Option>urn:liberty:id-sis-pp:cn</disco:Option>
1185         <disco:Option>urn:liberty:id-sis-pp:informalName</disco:Option>
1186         <disco:Option>urn:liberty:id-sis-pp:demographics</disco:Option>
1187       </disco:Options>
1188       <disco:Abstract>identity service for demonstration</disco:Abstract>
1189     </disco:ResourceOffering>

```

```
1190     </disco:QueryResponse>
1191 </soapenv:Body>
1192 </soapenv:Envelope>
1193
```

### 1194 6.2.2.2.13. ID-SIS Personal Profile Query

1195 SP2 that has received SP1's ResourceOffering with sequence #12, sends ID-SIS Personal Profile Query message to  
 1196 SP1 so as to get necessary attributes of a Principal. This message is defined in the ID-WSF Data Service Template  
 1197 specification.

1198 The following shows an example of ID-SIS Personal Profile message.

1199 Example: ID-SIS Personal Profile Query Message Sent from SP2 to SP1

```
1200 <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
1201     xmlns:xsd="http://www.w3.org/2001/XMLSchema"
1202     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
1203   <soapenv:Header>
1204     <sb:Correlation id="NTT4128D3FA79CC812662B92C8E962A2AD5"
1205       messageID="uuid:8419e396-01fd-a411-fb7f-46721c7a0bbb"
1206       timestamp="2004-03-10T05:59:03Z"
1207       soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
1208       soapenv:mustUnderstand="1"
1209       xmlns:sb="urn:liberty:sb:2003-08" />
1210     <sb:Provider id="NTTD98E695B9B665694504972D1DF00A2B2"
1211       providerID="https://yellowpizza.com:8443/sp2/metadata"
1212       soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
1213       soapenv:mustUnderstand="0"
1214       xmlns:sb="urn:liberty:sb:2003-08" />
1215     <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
1216       soapenv:mustUnderstand="1"
1217       xmlns:wsse="http://schemas.xmlsoap.org/ws/2003/06/secext">
1218       <wsse:BinarySecurityToken
1219         EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-messa
1220 ge-security-1.0#Base64Binary"
1221         ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-p
1222 rofile-1.0#X509v3"
1223         wsu:Id="X509Token"
1224         xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility">
1225         MIICBCCAW2gAwIBAgIBUTANBqkqhkiG9w0BAQQFADALMQswCQYD VQQGEwJVUzEUMBIGALUEChML
1226         TGliZXJ0eSBjTlAxEDA0BgNVBAMTB1Rlc3QgQ0EwHhcNMDMxMjA1MTQ0MjE1WWhcNMDQxMjA0MTQ0
1227         MjI1WjBMMQswCQYD VQQGEwJVUzEYMBYGA1UEChMPTGlic3QgQ0EwHhcNMDMxMjA1MTQ0MjE1WWhcNMDQxMjA0MTQ0
1228         dHQtYS1zaWduLm9yYmVydHktYW9wLm9yZzCBn zANBqkqhkiG9w0BAQEFAAOBjQAwYkCgYEAq9S1
1229         +JvcHKNjttE/v70TKMMXo+Ft05RBy/XUruHZsuH0b206MYG+CCBoPyJ6Jv+6+ZsCgIEjJfJ61qRZR
1230         ZmPdGv92zcBHH01/k1/GG7FPNFH+mrUm/66nRDysv6JFMzW7+Ct7132IUUiTEvj45CXHECyy8JUf
1231         fd1J1+FOrVweAEUCAwEAAMNMAswCQYDVR0TBAIwADANBqkqhkiG9w0BAQQFAAOBjQAwYkCgYEAq9S1
1232         LTcxn3jiifP+yBjKRaYpikrRzffeJ8XtLURHCKm7ZOX/OeqidHAARB41T xmITCB3LbHmViAk4G66
1233         K4Yb9Y0FFVJCFyaYHnY6W6oLDkTv5IMqDL//vV6QF9boO2gvTpap4WL5+6meNmCyWKoeO4CuwX3q
1234         ys5yrA8opg==
1235       </wsse:BinarySecurityToken>
1236     <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
1237       <ds:SignedInfo>
1238         <ds:CanonicalizationMethod
1239           Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
1240         <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
1241         <ds:Reference URI="#NTT4128D3FA79CC812662B92C8E962A2AD5">
1242           <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1243           <ds:DigestValue>M9rSK/PxICulsYEHUilGVu4JE0s</ds:DigestValue>
1244         </ds:Reference>
1245         <ds:Reference URI="#NTTD98E695B9B665694504972D1DF00A2B2">
1246           <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1247           <ds:DigestValue>VjPKcTmqRbKxhN2s24YIiuSTCBg</ds:DigestValue>
1248         </ds:Reference>
1249       </ds:SignedInfo>
1250     </ds:Signature>
1251   </soapenv:Header>
1252   <soapenv:Body>
1253     <id:PersonalProfileQuery />
1254   </soapenv:Body>
1255 </soapenv:Envelope>
```

```

1250     <ds:Reference URI="#NTT279922C20F1473B04D14F21F5B929890">
1251     <ds:Transforms>
1252         <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
1253     </ds:Transforms>
1254     <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1255     <ds:DigestValue>h6IAX/jtHLE/Swqw xw2k+q6l7YM=</ds:DigestValue>
1256 </ds:Reference>
1257 </ds:SignedInfo>
1258 <ds:SignatureValue>
1259 NXz1NSu0BWGFkXpN42ka6Ub4G7ZE0AhZrsC0MgLi j itfwHRPM/zeWfxKGR+msjDbhzIkZs/+icnv
1260 JD10Mc4ktqGLRRQ02JianF+SXEI r9k xTtwVb/mXnLrXbIE DaQZ3q3KtF14Q4 XEXreBVjczDDJbrw
1261 bVZg2rvo7bmtPIy7DeQ=
1262 </ds:SignatureValue>
1263 <ds:KeyInfo>
1264     <wsse:SecurityTokenReference Usage="sec:MessageAuthentication"
1265         xmlns:sec="urn:liberty:sec:2003-08">
1266         <wsse:Reference URI="#X509Token" />
1267     </wsse:SecurityTokenReference>
1268 </ds:KeyInfo>
1269 </ds:Signature>
1270 </wsse:Security>
1271 </soapenv:Header>
1272 <soapenv:Body>
1273     <pp:Query id="NTT279922C20F1473B04D14F21F5B929890"
1274         xmlns:pp="urn:liberty:id-sis-pp:2003-08">
1275         <pp:ResourceID>
1276             uuid:e427014e-1fde-cc03-85dd-690333bf695a</pp:ResourceID>
1277         <pp:QueryItem includeCommonAttributes="0">
1278             <pp:Select>/pp:PP/pp:InformalName</pp:Select>
1279         </pp:QueryItem>
1280         <pp:QueryItem includeCommonAttributes="0">
1281             <pp:Select>
1282                 /pp:PP/pp:AddressCard/pp:Address/pp:PostalAddress</pp:Select>
1283         </pp:QueryItem>
1284     </pp:Query>
1285 </soapenv:Body>
1286 </soapenv:Envelope>
1287

```

#### 1288 6.2.2.14. ID-SIS Personal Profile QueryResponse

1289 SP1 that has received ID-SIS Personal Profile Query message with sequence #13, responds to SP2 with ID-SIS  
1290 Personal Profile QueryResponse message in which Principal's attributes are embedded. In the example in,  
1291 InformalName and PostalAddress are requested. Therefore, these two kinds of attribute values are embedded in  
1292 the QueryResponse.

1293 The following shows an example of ID-SIS Personal Profile QueryResponse message.

1294 Example: ID-SIS Personal Profile QueryResponse Message Sent from SP1 to SP2

```

1295 <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
1296     xmlns:xsd="http://www.w3.org/2001/XMLSchema"
1297     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
1298
1299     <soapenv:Header>
1300         <sb:Correlation id="NTT8EF885B720C0B633948923E992DD86CF"
1301             messageID="uuid:2e56b5e3-52c9-8876-102e-23c8f1b2a40c"
1302             refToMessageID="uuid:8419e396-01fd-a411-fb7f-46721c7a0bbb"
1303             timestamp="2004-03-10T05:59:06Z"
1304             soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
1305             soapenv:mustUnderstand="1" xmlns:sb="urn:liberty:sb:2003-08" />
1306         <sb:Provider id="NTTD65ZK695B9B635354504972D1DF00N85A"
1307             providerID="https://blueliquor.com:8443/sp1/metadata"
1308             soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
1309             soapenv:mustUnderstand="0" xmlns:sb="urn:liberty:sb:2003-08" />

```



```

1310 <wssse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
1311     soapenv:mustUnderstand="1"
1312     xmlns:wssse="http://schemas.xmlsoap.org/ws/2003/06/secext">
1313
1314     <wssse:BinarySecurityToken
1315         EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-me
1316 ssage-security-1.0#Base64Binary"
1317         ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-tok
1318 n-profile-1.0#X509v3"
1319         wsu:Id="X509Token"
1320         xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility">
1321 MIICBDCCA2gAwIBAgIBUTANBgkqhkiG9w0BAQQFADAlMQswCQYDVQGEWJVUzEUMBIGALUEChML
1322 TGliZXJ0eSBJTT1AxEADAOBGNVBAMTB1Rlc3QgQ0EwHhcNMMDMxMjA1MTQ0MTQ0MjU1WjcNMDDQxMjA0MTQ0
1323 MjI1WjBMMQswCQYDVQQGEWJVUzEYMBYGALUEChMPTGliZXJ0eSBJTT1AgamtZMSMWIQYDVQQDEXpu
1324 dHQtYS1zaWduLmVudHktaW9wLm9yZzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAg9S1
1325 +JvcHKNjttE/v70TKMMXo+Ft05RBy/XUruHZsuh0b206MYG+CCBoPyJ6Jv+6+ZsCgIEjFJ6lqRZR
1326 ZmPdGv92zcBH01/k1/GG7FPNFH+mrUm/66nRDysv6JfMzW7+Ct7132IUUiTEvJ45CXHEcyy8JUf
1327 fd1Jl+F0rVweAEUCAwEAAAMNMAswCQYDVROTBAlwADANBgkqhkiG9w0BAQQFAAOBjQAwgYkCgYEAg6G
1328 LTCxn3jiifP+yBjKRAYpikrRzffeJ8XtLUrHCKm7ZOX/OeqidHAARB41TxmITCB3LbHmViAk4G66
1329 K4Yb9Y0FFVJCfyaYHnY6w6oLDkTv5IMqDL/vv6QF9b002gvTpap4WL5+6meNmCyWKoeO4CuwX3g
1330 ys5yrA8opg==
1331 </wssse:BinarySecurityToken>
1332 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
1333 <ds:SignedInfo>
1334 <ds:CanonicalizationMethod
1335     Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
1336 <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
1337 <ds:Reference URI="#NTT8EF885B720C0B633948923E992DD86CF">
1338 <ds:Transforms>
1339 <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
1340 </ds:Transforms>
1341 <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1342 <ds:DigestValue>
1343 d5vebdZmHHJtct1YnmSeG9kDcPK=</ds:DigestValue>
1344 </ds:Reference>
1345 </ds:SignedInfo>
1346 <ds:SignatureValue>
1347 FnGxfjUGKsliOnVRSuqvtkhwoJRhVoIdtDVGjh5IzmXNi2AxU8MKDxhFw3sGkDEm6uufwy6xstf0
1348 6bGyJd2Vt1Wpr38fASBfnXNbltCdFQF9s9sJtdjpsENTkxaa8v5ZVkJaik4TlaxGf53ui0xxQ6KDJ
1349 onIernnDeAT8vDa3U5g=
1350 </ds:SignatureValue>
1351 <ds:KeyInfo>
1352 <wssse:SecurityTokenReference Usage="sec:MessageAuthentication"
1353     xmlns:sec="urn:liberty:sec:2003-08">
1354
1355     <wssse:Reference URI="#X509Token" />
1356 </wssse:SecurityTokenReference>
1357 </ds:KeyInfo>
1358 </ds:Signature>
1359 </wssse:Security>
1360 </soapenv:Header>
1361 <soapenv:Body>
1362 <pp:QueryResponse timeStamp="2004-03-10T05:59:06Z"
1363     xmlns:pp="urn:liberty:id-sis-pp:2003-08">
1364 <pp:StatusCode>"OK" />
1365 <pp:Data>
1366 <pp:InformalName>Yuzo KOGA</pp:InformalName>
1367 </pp:Data>
1368 <pp:Data>
1369 <pp:PostalAddress>TOKYO</pp:PostalAddress>
1370 </pp:Data>
1371 </pp:QueryResponse>
1372 </soapenv:Body>
1373 </soapenv:Envelope>
1374

```

## 1375 **7. Anonymous B2B Example Sessions**

1376 This document describes how Liberty ID-FF & ID-WSF can be applied in the particular scenario of anonymous  
1377 Principal B2B interactions. <sup>2</sup>

### 1378 **7.1. Overview**

1379 Liberty ID-Federation Framework (ID-FF) and ID-Web Services Framework (ID-WSF) define general frameworks  
1380 for federated identity. As such, they offer a variety of options and mechanisms to enable information sharing  
1381 (authentication status and attributes) between providers. In many real-world scenarios, only a fraction of these options  
1382 will be relevant and so, the full complexity of the specifications can be profiled down to this subset.

1383 This document demonstrates the application of ID-FF and ID-WSF to a particular scenario: an employee of an  
1384 enterprise needing to access the resources/services of a business partner in order to perform their duties. As the  
1385 employee will not be offered any customizations or individualized access, the business partner does not need to know  
1386 the specific identity of the employee, rather merely that they have the appropriate entitlements, as captured in a role  
1387 assigned to them by their employer. This captures a frequent reality in B2B transactions. Ultimately, a company needs  
1388 to know that a partner will stand behind the actions of their employees in any dealings between the companies; in  
1389 many cases the identity (either real or a pseudonym) of the individual is irrelevant.

### 1390 **7.2. Scenario**

1391 Geoff Smith is an employee of Acme Widgets, a leading manufacturer of widgets for the thingymajig industry. Geoff's  
1392 role within Acme is a Junior Purchasing Agent, this role means that Acme authorizes him to place parts orders with  
1393 Acme's suppliers up to a value of \$1,000 at a time. Geoff occasionally deals with Acme's supplier Bolts-R-U's, placing  
1394 orders for bolts through Bolts-R-U's' ordering interface. In the past, Geoff has had to maintain an account at Bolts-  
1395 R-U's. In order to place an order, he would need to sign-in using a username and password used only at Bolts-R-U's.  
1396 Such a system has many issues:

- 1397 • the sporadic nature of Geoff's dealings there meant he often forgot both the account name and/or the password,  
1398 causing delay for Geoff and support costs for Bolts-R-U's.
- 1399 • the fast turnaround in Junior Purchasing Agents has meant that Bolts-R-U's has often had to create new accounts  
1400 for Acme's new hires, an expensive process when the information needs to be verified by Acme.
- 1401 • because he might apply for employment at Bolts-R-U's in the future, Geoff would prefer that his purchasing activity  
1402 not be traceable to him (maybe he always bought the cheap stuff?)

1403 Fortunately, both Acme and Bolts-R-U's have recently implemented support for Liberty's specifications into their  
1404 identity infrastructure (even though neither did so motivated by the thought of interacting with the other). Liberty's  
1405 technologies will allow Geoff to maintain his identity information at Acme which will, in order to enable appropriate  
1406 access at Bolts-R-U's for Geoff, share with the supplier the relevant information regarding him.

1407 Liberty's technology will address the issues listed above as follows:

- 1408 • Geoff will not be required to establish an account at Bolts-R-U's. He will be able to access the appropriate resources  
1409 there based on an authentication he performed to his own company, i.e., signing into Acme's intranet in the  
1410 morning.
- 1411 • As Bolts-R-U's will not need to maintain accounts for Acme's individual Purchasing Agents, they will be unaffected  
1412 as Acme's employees come and go.
- 1413 • Geoff's actions at Bolts-R-us will be untraceable because his identity will be unknown and untraceable to them.

---

<sup>2</sup>This example is provided by Liberty Member Entrust

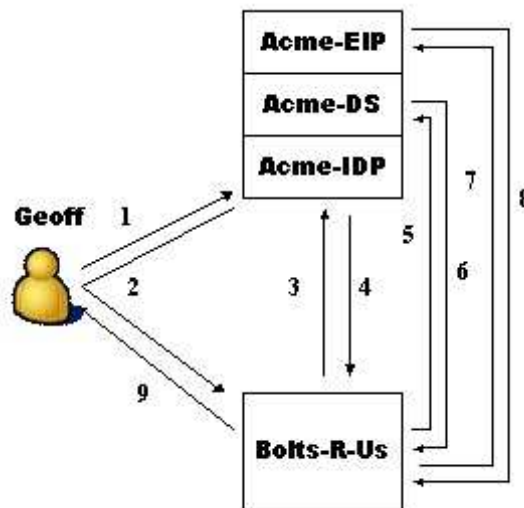
1414 The next sections describes the User Experience and the sequence of operations.

### 1415 **7.3. User Experience**

- 1416 1. Geoff goes to Acme's intranet portal.
- 1417 2. Geoff logs in using an X.509 certificate issued to him by Acme.
- 1418 3. Geoff sees a customized Acme interface, including a link "Order at Bolts-R-Us."
- 1419 4. As he knows Acme is running low on £45 bolts, Geoff clicks on "Order at Bolts-R-Us" link.
- 1420 5. Geoff sees Bolts-R-Us' ordering interface.
- 1421 6. Geoff orders 20,000 £45 bolts at a unit cost of \$0.10.
- 1422 7. Geoff sees an alert that his order has failed because the amount exceeds his purchasing amount authorization.
- 1423 8. Geoff changes the order to 10,000 £45 bolts.
- 1424 9. Geoff sees an acknowledgement that the order has gone through.

### 1425 **7.4. Message Flow**

1426 The figure below illustrates the message flow.



1427

1428

**Figure 5. Message Flow**

1429 The steps are as follows:

- 1430 1. Geoff authenticates to Acme-IDP. Geoff clicks on "Order at Bolts-R-Us" button, browser is sent to Bolts-R-Us  
1431 with artifact.
- 1432 2. Bolts-R-Us requests SAML assertion corresponding to artifact.
- 1433 3. Acme-IDP returns SAML assertion for Geoff containing anonymous one-time identifier for Geoff and bootstrap  
1434 information for Geoff's DS.

- 1435 4. SP queries Acme-DS for Geoff's EP service.
- 1436 5. Acme-DS returns ResourceOffering for EP service, contains all necessary tokens.
- 1437 6. Bolts-R-Us queries Acme-EP for Geoff's EmployeeType.
- 1438 7. Acme-EP returns Geoff's EmployeeType.
- 1439 8. Based on returned roles, Bolts-R-Us can make authorization decisions with respect to what resources Geoff can  
1440 access.
- 1441 The following sections present in more detail the different messages that flow between Acme and Bolts-R-Us.

#### 1442 **7.4.1. Step 1**

- 1443 Geoff authenticates to Acme's company intranet using an Acme account and password. He is presented with an  
1444 interface customized to his "Junior Purchasing Agent" job responsibilities.
- 1445 In addition to the usual News, Employee Resources, and Classified sections, Geoff's page contains a list of links  
1446 to suppliers with which he often deals. In the past, clicking on these links would take Geoff to a login page of the  
1447 particular supplier where he would authenticate using an account and password specific to that supplier.
- 1448 Geoff knows that Acme is running dangerously low on £45 bolts and he knows that Bolts-R-Us is the preferred  
1449 provider for these bolts. Amongst the other suppliers, he sees a "Bolts-R-Us Order Page" link that he clicks on.

#### 1450 **7.4.2. Step 2**

- 1451 Message 2 is a message sent from Acme-IDP to Bolts-R-Us, unsolicited because, in this scenario, it is not sent in  
1452 response to a previous AuthnRequest from Bolts-R-Us. When Geoff clicks on the "Order at Bolts-R-Us" button on his  
1453 customized Acme intranet home page, his browser is initially sent to a transfer service URL at Acme. It is the transfer  
1454 service that creates the Liberty artifact that will be sent to Bolts-R-Us. After creating the artifact, Acme-IDP sends it  
1455 as a query parameter to the appropriate Bolts-R-Us assertion consumer service URL (this obtained from previously  
1456 exchanged Bolts-R-Us metadata.)

1457  
1458  
1459 HTTP/1.0 302 Found  
1460 Location: http://acs.boltsrus.com?SAMLart=AAM1uXw6+f+jyA/4XuFHqPl7QDvc/LIQL9+t7YQtG1Gwk9bp  
1461 h0Adl+o+  
1462 <other HTTP 1.0 or 1.1 components>  
1463

#### 1464 Step 2 Notes

- 1465 1. Message 2 is sent by Acme to the Bolts-R-Us Assertion Consumer Service at "http://acs.boltsrus.com" - this URL  
1466 previously specified by Bolts-R-Us to Acme.
- 1467 2. The SAML artifact is passed as a URL query parameter, i.e., that which follows the "?" in the above URL. Sending  
1468 an artifact in this manner rather than the actual authentication assertion addresses the limitations for URL length.

1469 **7.4.3. Step 3**

1470 Message 3 is a SOAP message sent from Bolts-R-Us to Acme-IDP in which Bolts-R-Us presents the artifact it just  
 1471 received in Message 2 and requests that it be exchanged for the corresponding Authentication assertion for Geoff.

```

1472
1473
1474 POST /soap HTTP/1.0
1475 Host: idp.acme.com
1476 Content-length: ...
1477 Content-type: text/xml
1478 <s:Envelope
1479   xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
1480   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
1481   xmlns:sb="urn:liberty:sb:2003-08"
1482   xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol">
1483   <s:Header>
1484     <sb:Correlation
1485       s:mustUnderstand="true"
1486       messageId="NK44V79NdfPaE5jCw1k_"
1487       timestamp="2003-06-06T12:06:12Z"/>
1488   </s:Header>
1489   <s:Body>
1490     <samlp:Request IssueInstant="2002-12-12T10:08:56Z"
1491       MajorVersion="1" MinorVersion="1"
1492       RequestID="e4d71c43-c89a-426b-853e-a2b0c14a5ed8"
1493       id="b6dc3636-f2ad-42d1-9427-220f2cf70ec1">
1494       <samlp:AssertionArtifact>
1495         AAM1uXw6+f+jyA/4XuFHqPl7QDvc/LIQL9+t7YQtG1Gwk9bph0Adl+o+
1496       </samlp:AssertionArtifact>
1497     </samlp:Request>
1498   </s:Body>
1499 </s:Envelope>
1500
```

1501 Step 3 Notes

- 1502 1. Message 3 is sent by Bolts-R-Us to Acme at idp.acme.com - this URL previously specified by Acme.
- 1503 2. The messageId attribute on the Correlation element has the value "NK44V79NdfPaE5jCw1k\_." This will allow  
 1504 Bolts-R-Us to correlate Acme's response with this request.
- 1505 3. The AssertionArtifact element carries the string "AAM1uXw6+f+jyA/4XuFHqPl7QDvc/LIQL9+t7YQtG1Gwk9bph0Adl+o+"  
 1506 - this the value of the artifact sent in Message 2.

1507 **7.4.4. Step 4**

1508 Message 4 is a SOAP response message sent from Acme-IDP to Bolts-R-Us in which the SAML authentication  
 1509 assertion is returned to Bolts-R-Us.

```

1510
1511
1512 HTTP/1.0 200 OK
1513 Content-length: ...
1514 Content-type: text/xml
1515
1516 <s:Envelope
1517   xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
1518   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
1519   xmlns:sb="urn:liberty:sb:2003-08"
1520   xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
1521   xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
1522   xmlns:lib="urn:liberty:iff:2003-08">
1523   <s:Header>
```

```

1524     <sb:Correlation
1525         s:mustUnderstand="true"
1526         refToMessageId="NK44V79NdfPaE5jCwIk_"
1527         messageId="uuid:0048345-47329874-45873278"
1528         timestamp="2003-06-06T12:07:12Z"/>
1529     </s:Header>
1530     <s:Body>
1531         <samlp:Response
1532             InResponseTo="e4d71c43-c89a-426b-853e-a2b0c14a5ed8"
1533             IssueInstant="2003-10-31T21:42:13Z" MajorVersion="1" MinorVersion="1"
1534             Recipient="http://www.boltsrus.com"
1535             ResponseID="LANWfL2xLybnc+BCwgY+pl/vIVAj">
1536             <samlp:Status>
1537                 <samlp:StatusCode>
1538                     Value="qns:Success">
1539                 </samlp:StatusCode>
1540             </samlp:Status>
1541             <lib:Assertion AssertionID="SqMC8Hs2vJ7Z+t4UiLSmhKOSU00U"
1542                 InResponseTo="e4d71c43-c89a-426b-853e-a2b0c14a5ed8"
1543                 IssueInstant="2003-06-06T12:07:12Z" Issuer="http://idp.acme.com"
1544                 MajorVersion="1" MinorVersion="2">
1545                 <saml:Conditions
1546                     NotBefore="2003-06-06T12:07:12Z"
1547                     NotOnOrAfter="2003-06-06T12:10:12Z">
1548                     <saml:AudienceRestrictionCondition>
1549                         <saml:Audience>http://www.boltsrus.com</saml:Audience>
1550                     </saml:AudienceRestrictionCondition>
1551                 </saml:Conditions>
1552                 <lib:AuthenticationStatement
1553                     AuthenticationInstant="2003-06-06T12:07:12Z"
1554                     AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
1555                     <lib:Subject xsi:type="lib:SubjectType">
1556                         <saml:NameIdentifier Format="urn:liberty:iff:nameid:one-time">
1557                             S2T4R5E7A8K1I8S9O2V9E0R
1558                         </saml:NameIdentifier>
1559                         <saml:SubjectConfirmation>
1560                             <saml:ConfirmationMethod>
1561                                 urn:oasis:names:tc:SAML:1.0:cm:artifact-01
1562                             </saml:ConfirmationMethod>
1563                         </saml:SubjectConfirmation>
1564                         <lib:IDPProvidedNameIdentifier
1565                             NameQualifier="http://idp.acme.com"
1566                             Format="urn:liberty:iff:nameid:one-time">
1567                             S2T4R5E7A8K1I8S9O2V9E0R
1568                         </lib:IDPProvidedNameIdentifier>
1569                     </lib:Subject>
1570                     <lib:AuthnContext>
1571                         <lib:AuthnContextClassRef>
1572                             http://www.projectliberty.org/schemas/authtctx/classes/PasswordProtectedTransport
1573                         </lib:AuthnContextClassRef>
1574                     </lib:AuthnContext>
1575                 </lib:AuthenticationStatement>
1576                 <saml:AttributeStatement>
1577                     <saml:Subject>
1578                         <saml:NameIdentifier Format="urn:liberty:iff:nameid:one-time">
1579                             S2T4R5E7A8K1I8S9O2V9E0R
1580                         </saml:NameIdentifier>
1581                     </saml:Subject>
1582                     <saml:Attribute AttributeName="DiscoveryResourceOffering"
1583                         AttributeNamespace="urn:liberty:disco:2003-08">
1584                     <saml:AttributeValue>
1585                         <lib:ResourceOffering>
1586                             <disco:ResourceID>http://disco.acme.com/d0CQF8elJTDLmzEo</disco:ResourceID>
1587                             <disco:ServiceInstance>
1588                                 <disco:ServiceType>urn:liberty:disco:2003-08</disco:ServiceType>
1589                                 <disco:ProviderID>http://disco.acme.com</disco:ProviderID>
1590                             <disco:Description>

```

```

1591         <SecurityMechID>
1592         urn:liberty:security:2003-08:TLS:X509
1593         </SecurityMechID>
1594         <disco:Endpoint>https://disco.acme.com</disco:Endpoint>
1595         </disco:Description>
1596     </ServiceInstance>
1597     <Abstract>Acme Discovery service</Abstract>
1598 </lib:ResourceOffering>
1599 </saml:AttributeValue>
1600 </saml:Attribute>
1601 </saml:AttributeStatement>
1602 <ds:Signature>
1603 Acme digital signature
1604 </ds:Signature>
1605 </lib:Assertion>
1606 </samlp:Response>
1607 </s:Body>
1608 </s:Envelope>
1609

```

#### 1610 Step 4 Notes

- 1611 1. Message 4 is sent by Acme to Bolts-R-Us in response to Message 3.
- 1612 2. The `refToMessageID` on the `Correlation` element has the value "NK44V79NdfPaE5jCw1k\_." This matches the  
1613 `messageId` of Message 3.
- 1614 3. The `SAML Status` element indicates that Message 4 is a successful response.
- 1615 4. The `Format` attribute on the `AuthenticationStatement/Subject/NameIdentifier` element indicates that the  
1616 identifier being returned for Geoff (namely "S2T4R5E7A8K1I8S9O2V9E0R") is "one-time," i.e., it does not  
1617 correspond to any previously-used identifier for either Geoff or another Acme employee.
- 1618 5. The `IDPProvidedNameIdentifier` element contains the same string of "S2T4R5E7A8K1I8S9O2V9E0R" indicating  
1619 that this is the string that Acme (the IDP) has chosen to represent Geoff. If this were not a "one-time" interaction,  
1620 Bolts-R-Us could specify its own preferred value as an `SPPProvidedNameIdentifier` element.
- 1621 6. The `AuthnContext` element indicates that that Geoff originally authenticated to Acme using a password over SSL.
- 1622 7. As well as the assertion for Geoff, Acme-IDP returns to Bolts-R-Us a `ResourceOffering` for the relevant  
1623 `DiscoveryService` as an `AttributeStatement`. The `ResourceID` for this `ResourceOffering` has a value of  
1624 "http://disco.acme.com/d0CQF8e1JTDLmzEo" - this string will be used by Bolts-R-Us on subsequent calls  
1625 to Acme's Discovery Service to refer to Geoff (anonymously).
- 1626 8. The `SecurityMechID` element contains the value "urn:liberty:security:2003-08:TLS:X509" - indi-  
1627 cating that subsequent queries to the Discovery Service must be protected with both SSL and an X.509 based  
1628 message-layer signature.
- 1629 9. The `EndPoint` element within the `ResourceOffering` contains the string "disco.acme.com" - this is the Acme  
1630 URL to which Bolts-R-Us will send subsequent discovery queries.

1631 **7.4.5. Step 5**

1632 Message 5 is a request from Bolts-R-Us to Acme-DS in which Bolts-R-Us queries for the location of Geoff's EP  
1633 Service.

```
1634
1635
1636 POST /soap HTTP/1.0
1637 Host: disco.acme.com
1638 Content-length: ...
1639 Content-type: text/xml
1640
1641 <s:Envelope
1642   xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
1643   xmlns:disco="urn:liberty:disco:2003-08 "
1644   xmlns:sb="urn:liberty:sb:2003-08">
1645   <s:Header>
1646     <sb:Correlation
1647       id="K8H6F53gh89HGY"
1648       s:mustUnderstand="1"
1649       messageID="K8H6F53gh89HGY"
1650       timestamp="2003-06-06T12:08:12Z"/>
1651     <ws:Security>
1652       <ds:Signature>
1653         Bolts-R-Us signature as specified by Acme.
1654         Needs detail
1655       </ds:Signature>
1656     </ws:Security>
1657   </s:Header>
1658   <s:Body>
1659     <disco:Query>
1660       <disco:ResourceID>http://disco.acme.com/d0CQF8e1JTDLmzEo</disco:ResourceID>
1661       <disco:RequestedServiceType>
1662         <disco:ServiceType>urn:liberty:id-sis-ep:2003-08</disco:ServiceType>
1663       </disco:RequestedServiceType>
1664     </disco:Query>
1665   </s:Body>
1666 </s:Envelope>
1667
```

1668 Step 5 Notes

- 1669 1. Message 5 is sent by Bolts-R-Us to Acme at disco.acme.com - this the URL specified in the Endpoint element of  
1670 Message 4's ResourceOffering.
- 1671 2. The messageID attribute on the Correlation element has the value "K8H6F53gh89HGY." This will allow Bolts-  
1672 R-Us to correlate Acme's response with this request.
- 1673 3. The ResourceID element in the Query element contains the identifier "http://disco.acme.com/d0CQF8e1JTDLmzEo"  
1674 previously provided to Bolts-R-Us by Acme in Message 4.
- 1675 4. The RequestedServiceType indicates to Acme's Discovery Service that Bolts-R-Us is interested in the location  
1676 of Geoff's EP Service.



## 1677 7.4.6. Step 6

1678 Message 6 is the response to Message 5 in which Acme's Discovery Service returns to Bolts-R-U's the relevant  
1679 ResourceOffering for the EP Service.

```

1680
1681
1682 HTTP/1.0 200 OK
1683 Content-length: ...
1684 Content-type: text/xml
1685
1686 <s:Envelope
1687   xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
1688   xmlns:disco="urn:liberty:disco:2003-08"
1689   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
1690   xmlns:sb="urn:liberty:sb:2003-08"
1691   xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
1692   xmlns:lib="urn:liberty:iff:2003-08"
1693   xmlns:ws="http://schemas.xmlsoap.org/ws/2003/06/secext"
1694   xmlns:sec="urn:liberty:sec:2003-08">
1695   <s:Header>
1696     <sb:Correlation
1697       s:mustUnderstand="true"
1698       refToMessageId="K8H6F53gh89HGY"
1699       messageId="uuid:008678-98538765-27589543"
1700       timestamp="2003-06-06T12:09:12Z">
1701   </s:Header>
1702   <s:Body>
1703     <disco:QueryResponse>
1704       <Status code="OK"/>
1705       <disco:ResourceOffering entryID="1">
1706         <disco:ResourceID>http://ep.acme.com/zsjsdkjfsdf</disco:ResourceID>
1707         <disco:ServiceInstance>
1708           <disco:ServiceType>urn:liberty:id-sis-ep:2003-08</disco:ServiceType>
1709           <disco:ProviderID>http://www.acme.com/</disco:ProviderID>
1710           <disco:Description>
1711             <disco:SecurityMechID>urn:liberty:security:2003-08:TLS:X509</disco:SecurityMechID>
1712             <disco:CredentialRef>SqMkfgghjs2v+jskhd fHU</disco:CredentialRef>
1713             <disco:Endpoint>https://ep.acme.com:443/soap</disco:Endpoint>
1714           </disco:Description>
1715         </disco:ServiceInstance>
1716         <disco:Abstract>Anonymous User's Employee Profile</disco:Abstract>
1717       </disco:ResourceOffering>
1718     </disco:QueryResponse>
1719   </s:Body>
1720 </s:Envelope>
1721

```

## 1722 Step 6 Notes

- 1723 1. Message 6 is sent by Acme to Bolts-R-U's in response to Message 5. It contains a ResourceOffering for Geoff's  
1724 EP Service.
- 1725 2. Acme used the ResourceOffering element in Message 4 to specify where Geoff's Discovery Service was located,  
1726 here it uses the same element structure (but not values) to specify where Geoff's EP Service is located.
- 1727 3. The location of Geoff's EP Service is provided in the Endpoint element of the returned ResourceOffering element  
1728 - namely the URL "https://ep.acme.com:443/soap."
- 1729 4. The refToMessageID on the Correlation element has the value "K8H6F53gh89HGY." This matches the  
1730 messageId of Message 5.

- 1731 5. The ResourceID element contains the string "http://ep.acme.com/zsjsdkjfsdf." - this will be used by  
1732 Bolts-R-us on subsequent queries of the EP Service to refer to Geoff. In a more distributed scenario in which the  
1733 DS and EIS were not co-located, then the DS would need to ensure that the Service provider (Bolts-R-Us in this  
1734 scenario) would be unable to directly read the ResourceID - it would do so by encrypting the value for the EIS.  
1735 The Service provider would be able to forward this encrypted value onto the EIS in subsequent queries but would  
1736 be unable to use this identifier in a privacy-inappropriate manner.
- 1737 6. The SecurityMechID element indicates the Security Mechanisms that Bolts-R-Us is expected to use in  
1738 subsequent interactions with the EP Service - namely TLS and an X.509-based signature.

#### 1739 7.4.7. Step 7

1740 Message 7 is a request from Bolts-R-Us to Acme's EP Service for the EmployeeType of Geoff.

```
1741
1742
1743 POST /soap HTTP/1.0
1744 Host: ep.acme.com
1745 Content-length: ...
1746 Content-type: text/xml
1747 <s:Envelope
1748   xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
1749   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
1750   xmlns:sb="urn:liberty:sb:2003-08"
1751   xmlns:lib="urn:liberty:iff:2003-08"
1752   xmlns:ws="http://schemas.xmlsoap.org/ws/2003/06/secext"
1753   xmlns:sec="urn:liberty:sec:2003-08"
1754   xmlns:ep="urn:liberty:id-sis-ep:2003-08">
1755
1756   <s:Header>
1757     <sb:Correlation
1758       s:mustUnderstand="1"
1759       messageID="LJY756FGt96GBHF"
1760       timestamp="2003-06-06T12:11:12Z" />
1761     <ws:Security>
1762       <ds:Signature>
1763         Bolts-R-Us signature as specified by Acme.
1764         Needs detail
1765       </ds:Signature>
1766     </ws:Security>
1767   </ws:Security>
1768 </s:Header>
1769 <s:Body>
1770   <ep:Query>
1771     <ep:ResourceID>http://ep.acme.com/zsjsdkjfsdf</ep:ResourceID>
1772     <ep:QueryItem itemID="type">
1773       <ep>Select>/ep:EP/ep:EmployeeType</ep>Select>
1774     </ep:QueryItem>
1775   </ep:Query>
1776 </s:Body>
1777 </s:Envelope>
1778
```

#### 1779 Step 7 Notes

- 1780 1. Message 7 is sent by Bolts-R-Us to Acme at ep.acme.com - this the URL specified in the Endpoint element of  
1781 Message 6's ResourceOffering for the EP Service.
- 1782 2. The messageId attribute on the Correlation element has the value "LJY756FGt96GBHF." This will allow Bolts-  
1783 R-Us to correlate Acme's response with this request.

- 1784 3. The `ResourceID` element in the `Query` element contains the identifier "`http://ep.acme.com/zsjsdkjfsdf`"  
1785 previously provided to Bolts-R-U's by Acme in Message 6.
- 1786 4. The `QueryItem` element contains the string "`/ep:EP/ep:EmployeeType`" to indicate that Bolts-R-U's is specif-  
1787 ically interested in Geoff's `EmployeeType` rather than the other data elements in the EP schema.

#### 1788 **7.4.8. Step 8**

1789 Message 8 is the response to Message 7 in which Acme-EP returns the `EmployeeType` of Geoff to Bolts-R-U's.

```
1790
1791
1792 HTTP/1.0 200 OK
1793 Content-length: ...
1794 Content-type: text/xml
1795
1796 <s:Envelope
1797   xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
1798   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
1799   xmlns:sb="urn:liberty:sb:2003-08"
1800   xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
1801   xmlns:lib="urn:liberty:iff:2003-08"
1802   xmlns:ws="http://schemas.xmlsoap.org/ws/2003/06/secext"
1803   xmlns:sec="urn:liberty:sec:2003-08"
1804   xmlns:ep="urn:liberty:id-sis-ep:2003-08">
1805   <s:Header>
1806     <sb:Correlation
1807       s:mustUnderstand="1"
1808       refToMessageID="LJY756FGt96GBHF"
1809       messageID="uuid:0032945-28686728-25695608"
1810       timestamp="2003-06-06T12:12:12Z" />
1811   </s:Header>
1812   <s:Body>
1813     <ep:QueryResponse>
1814       <ep:Status code="OK"/>
1815       <ep:Data itemIDRef="type">
1816         <ep:EmployeeType>
1817           JuniorPurchasingAgent
1818         </ep:EmployeeType>
1819       </ep:Data>
1820     </ep:QueryResponse>
1821   </s:Body>
1822 </s:Envelope>
1823
```

#### 1824 Step 8 Notes

- 1825 1. Message 8 is sent by Acme to Bolts-R-U's in response to Message 7. It contains a `QueryResponse` containing  
1826 Geoff's `EmployeeType`.
- 1827 2. The `refToMessageID` on the `Correlation` element has the value "`LJY756FGt96GBHF`." This matches the  
1828 `messageId` of Message 7.
- 1829 3. The `EmployeeType` element carries Geoff's role, namely that he is a "`JuniorPurchasingAgent`." Acme and  
1830 Bolts-R-us would have had to have previously agreed on what this attribute represents and Bolts-R-U's would  
1831 have defined appropriate authorizations for this role.
- 1832 4. Section 7.5.9. Step 9
- 1833 5. With its knowledge of Geoff's role at Acme of Junior Purchasing Agent, Bolts-R-U's can provide a customized  
1834 experience for him (i.e., ensure that he isn't presented with the ability to place orders on big-ticket items) and  
1835 make appropriate authorization decisions for those orders he does place.

1836 6. Its important to note that Bolts-R-Us would be unable to provide to Geoff any sort of "Past Activity" information  
1837 that was specific to him - this because the identifier Acme provided for Geoff was one-time and so prevented this  
1838 sort of correlation. The best Bolts-R-Us could do would be create a list of products that "Other Junior Purchasing  
1839 Agents have ordered in the past."

## 1840 7.5. Optimizations

1841 As illustrated, a number of message pairs are exchanged between Acme and Bolts-R-Us before Bolts-R-Us obtains  
1842 the necessary attribute information for Geoff, namely his "EmployeeType." This general flow can be optimized as  
1843 described below:

```
1844 <s:Envelope  
1845   <s:Body>  
1846     <samlp:Response>  
1847       <lib:Assertion>  
1848         <lib:AuthenticationStatement>  
1849  
1850         </lib:AuthenticationStatement>  
1851         <saml:AttributeStatement>  
1852           <saml:Subject>  
1853             <saml:NameIdentifier Format="urn:liberty:iff:nameid:one-time ">  
1854               S2T4R5E7A8K1I8S9O2V9E0R  
1855             </saml:NameIdentifier>  
1856           </saml:Subject>  
1857           <saml:Attribute  
1858             AttributeName="EmployeeType"  
1859             AttributeNamespace="http://ep.acme.com">  
1860             <saml:AttributeValue>JuniorPurchasingAgent</saml:AttributeValue>  
1861           </saml:Attribute>  
1862         </saml:AttributeStatement>  
1863       </lib:Assertion>  
1864     </samlp:Response>  
1865   </s:Body>  
1866 </s:Envelope>  
1867
```

1868 1. If Acme knew that Bolts-R-Us required Geoff's EmployeeType, then it could include this information in the  
1869 original assertion it sent to Bolts-R-Us (Message 4 above). Message 4 would then appear (omitting previous  
1870 details).

1871 2. While this model significantly decreases the traffic between Acme and Bolts-R-Us, it assumes that Acme can  
1872 anticipate all the attributes for Geoff that Bolts-R-Us might eventually need. This may or may not be realistic.  
1873 For instance, in addition to EmployeeType, Bolts-R-Us might want to know if Geoff had a fixed spending limit.

1874 3. A potential compromise between the two extremes is to have Acme return a ResourceOffering for its EP  
1875 service (rather than its Discovery Service) in the original assertion it creates for Bolts-R-Us (Message 4). This  
1876 model would remove a request/response pair (Messages 5 & 6) and yet still allow Bolts-R-Us to subsequently  
1877 query Acme's EP service for other attributes if necessary.

## 1878 7.6. Summary

1879 From Geoff's point of view, Liberty provides the following advantages over the previous model:

1880 1. He no longer has to maintain an identity at Bolts-R-Us - meaning no account name and password to remember.  
1881 The value of this grows significantly if Geoff deals with many other Acme suppliers.

1882 2. He is given a customized interface at Bolts-R-Us based on the authentication he performed at Acme. Throughout  
1883 the day, his interactions with other Liberty-enabled suppliers will be the same.

1884 From Acme's point of view, Liberty provides the following advantages over the previous model:

- 1885 1. Acme's employees can concentrate on their job responsibilities rather than remembering maintaining identity  
1886 information at the business partners with which they interact.
- 1887 2. Acme can be confident that the actions of its employees at its business partners will be consistent with the  
1888 entitlements associated with their role.
- 1889 3. The privacy of Acme's employees is protected, Acme not unnecessarily disclosing information on these employ-  
1890 ees to its business partners.
- 1891 4. There is no need for Acme to provision new employees into its business partners in order to ensure that they are  
1892 set up with the appropriate authorizations. As the new employees interact with the business partners, the Liberty  
1893 infrastructure will ensure that these authorizations "flow with them" as required. Importantly, there is also no  
1894 need for Acme to deprovision its employees from its business partners when its employees leave - all Acme need  
1895 do is remove that employee from its own systems to ensure that the ex-employee will not be able, inappropriately,  
1896 to access business partners.
- 1897 5. The infrastructure Acme puts in place to support Bolts-R-U's can be leveraged with all other Liberty-enabled  
1898 companies with which its employees interact, the cost amortized across all.

1899 From Bolts-R-U's point of view, Liberty provides the following advantages over the previous model:

- 1900 1. Bolts-R-U's no longer needs to bear the costs associated with supporting (e.g., password resets) the employees of  
1901 its business partners.
- 1902 2. The infrastructure Bolts-R-U's puts in place to support Acme can be leveraged with all other Liberty-enabled  
1903 companies with which its employees interact, the cost amortized across all.

## 1904 8. Device Authentication Example Sessions

1905 This section walks through the complete messages passed from and to a client invoking a service.<sup>3</sup>

1906 In this example, a digital media adapter device is used to present the user with both radio and photo services in their  
 1907 entertainment center. The steps taken here are but one example of performing the tasks. There are several other ways  
 1908 to accomplish the same task that might be more appropriate in different circumstances. This is just one example.

1909 In this example, the device has previously been associated with a user account so the user does not need to perform  
 1910 any authentication/registration process.

### 1911 8.1. Device Boot Up

1912 The user turns on the device which brings up the main screen for the user. There are several areas on this screen that  
 1913 require user specific content (such as the "now playing" area for radio or a "what's new" area for data in their photo  
 1914 service).

### 1915 8.2. Device Initiates Authentication

1916 Needing user content, the device initiates a device authentication with the authentication server. This request is  
 1917 submitted to "https://auth.ws.aol.com" (the bootstrap entry point for the authentication service).

```

1918 <?xml version="1.0" encoding="utf-8" ?>
1919 <S:Envelope
1920   xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
1921   xmlns:aol=" http://schemas.corp.aol.com/"
1922   xmlns:sb="urn:liberty:wsf:soap-bind:1.0"
1923   xmlns:sa="urn:liberty:wsf:soap-auth:1.0" >
1924   <S:Header>
1925     <sb:Correlation S:mustUnderstand="1"
1926       messageID="uuid:0023923-28329023-238239023"
1927       timestamp="2003-06-06T12:10:10Z" />
1928   </S:Header>
1929   <S:Body>
1930     <sa:SASLRequest advisoryAuthnID="123456789012:10023923"
1931       mechanism="CRAM-MD5" />
1932   </S:Body>
1933 </S:Envelope>
1934
```

### 1935 8.3. Auth Server Responds with Auth Mechanism Choice

1936 The authentication server responds, choosing to use CRAM-MD5 as the authentication method and providing the  
 1937 challenge data.

```

1938 <?xml version="1.0" encoding="utf-8" ?>
1939 <S:Envelope
1940   xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
1941   xmlns:aol=" http://schemas.corp.aol.com/"
1942   xmlns:sb="urn:liberty:wsf:soap-bind:1.0"
1943   xmlns:sa="urn:liberty:wsf:soap-auth:1.0" >
1944   <S:Header>
1945     <sb:Correlation S:mustUnderstand="1"
1946       messagID="uuid:00287-83782-238891-09981"
1947       refToMessageID ="uuid:0023923-28329023-238239023"
1948       timestamp="2003-06-06T12:10:10Z" />

```

<sup>3</sup>With minor editorial changes, this example is taken from the document "Digital Media Services - Draft Services Invocation Framework Specification," Conor P. Cahill, America OnLine, Inc., February 9, 2004.

At each step, the complete SOAP message is included, headers and all. Note that the security tokens passed will not be verifiable (the signatures are fake) as these are only example messages.

```
1949 </S:Header>
1950 <S:Body>
1951   <sa:SASLResponse serverMechanism="CRAM-MD5">
1952     <Status code="continue" />
1953     <Data>
1954       1896.697170952@postoffice.example.net
1955     </Data>
1956   </sa:SASLResponse>
1957 </S:Body>
1958 </S:Envelope>
1959
```

1960 Notes:

- 1961 1. The "refToMessageID" field is set to the message ID in the Auth Request from the client.
- 1962 2. The value inside of the <SASLResponse> is the CRAM-MD5 challenge value for the client. In this case, it is a  
1963 value directly out of [SASLCram] to make it easier to see how the specification is incorporated into this protocol.
- 1964 3. The code of "continue" indicates that this is a continuing authentication operation.

## 1965 8.4. Device Submits Credentials to Auth Server

1966 The device prepares the MD5 digest using the provided challenge as well as the shared secret (in this case  
1967 "tanstaaftanstaaf") and sends a response to the Authentication Server. Please review for details on how the  
1968 digest is generated. (This particular value was actually lifted from the document.)

```
1969 <?xml version="1.0" encoding="utf-8" ?>
1970 <S:Envelope>
1971   xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
1972   xmlns:aol="http://schemas.corp.aol.com/soap/sif-2004-02"
1973   xmlns:sb="urn:liberty:wsf:soap-bind:1.0"
1974   xmlns:sa="urn:liberty:wsf:soap-auth:1.0" >
1975   <S:Header>
1976     <sb:Correlation S:mustUnderstand="1"
1977       messageID="uuid:0023923-28329023-238239026"
1978       refToMessageID="uuid:00287-83782-238891-09981"
1979       timestamp="2003-06-06T12:10:11Z" />
1980   </S:Header>
1981   <S:Body>
1982     <sa:SASLRequest authzID="123456789012:10023923"
1983       mechanism="CRAM-MD5">
1984       dGltIGI5MTNhNjAyYzdlZGE3YTQ5NWl0ZTZlNzZmNGQzODkw
1985     </sa:SASLRequest>
1986   </S:Body>
1987 </S:Envelope>
1988
```

1989 Notes:

- 1990 1. The authzID was included in this request even though it was included on the original request. This is mostly  
1991 for clarity since the server must be able to reconnect the authentication request with a previous response (since it  
1992 needs to correlate this response to the challenge data).
- 1993 2. The refToMessageID ties this request to the previous response so that the authentication server can correlate  
1994 this message to the challenge it sent in the previous message.

## 1995 8.5. Auth Server Returns Security Token & Discovery Info

1996 The server processes the request and returns the security token to the caller along with the bootstrap information for  
 1997 accessing the discovery service.

```

1998 <?xml version="1.0" encoding="utf-8" ?>
1999 <S:Envelope>
2000   xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
2001   xmlns:aol="http://schemas.corp.aol.com/soap/sif-2004-02"
2002   xmlns:disco="urn:liberty:disco:2003-08"
2003   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
2004   xmlns:sb="urn:liberty:wsf:soap-bind:1.0"
2005   xmlns:sa="urn:liberty:wsf:soap-auth:1.0" >
2006   <S:Header>
2007     <sb:Correlation S:mustUnderstand="1"
2008       messageID="uuid:00287-23928392-193482390"
2009       refToMessageID="uuid:0023923-28329023-238239026"
2010       timestamp="2003-06-06T12:10:11Z" />
2011   </S:Header>
2012   <S:Body>
2013     <sa:SASLResponse>
2014       <sa:Status code="success" />
2015       <disco:ResourceOffering>
2016         <disco:ResourceID>urn:liberty:isf:implied-resource</disco:ResourceID>
2017         <disco:ServiceInstance>
2018           <disco:ServiceType>urn:liberty:disco:2003-08</disco:ServiceType>
2019           <disco:ProviderID>http://discovery.aol.com</disco:ProviderID>
2020           <disco:Description CredentialRef="e06e5a28-bc80-4ba6-9ecb-712949db686e">
2021             <disco:SecurityMechID>...</disco:SecurityMechID>
2022             <disco:Endpoint>https://discovery.ws.aol.com</disco:Endpoint>
2023           </disco:Description>
2024         </disco:ServiceInstance>
2025       </disco:ResourceOffering>
2026       <sa:Credentials>
2027         <saml:Assertion MajorVersion="1" MinorVersion="1"
2028           AssertionID="e06e5a28-bc80-4ba6-9ecb-712949db686e"
2029           Issuer="http://idp.aol.com"
2030           IssueInstant="2003-06-06T12:10:11Z"
2031           InResponseTo="uuid:0023923-28329023-238239026">
2032           <saml:Conditions NotOnOrAfter="2003-06-07T12:10:10Z" >
2033             <saml:AudienceRestrictionCondition>
2034               <saml:Audience>http://discovery.aol.com</saml:Audience>
2035             </saml:AudienceRestrictionCondition>
2036           </saml:Conditions>
2037           <lib:AuthenticationStatement
2038             AuthenticationInstant="2003-06-06T12:10:11Z"
2039             SessionIndex="1" >
2040             <lib:AuthnContext>
2041               <lib:AuthnContextClassRef>
2042                 http://schemas.corp.aol.com/authctx/classes/DeviceProtectedTransport
2043               </lib:AuthnContextClassRef>
2044             </lib:AuthnContext>
2045             <saml:Subject>
2046               <saml:NameIdentifier>
2047                 <saml:NameQualifier>http://aol.com</saml:NameQualifier>
2048                 <saml:Format>urn:liberty:iff:nameid:federated</saml:Format>
2049                 AOLScreenname
2050               </saml:NameIdentifier>
2051             <saml:SubjectConfirmation>
2052               <saml:ConfirmationMethod>
2053                 urn:oasis:names:tc:SAML:1.0:cm:Bearer
2054               </saml:ConfirmationMethod>
2055             </saml:SubjectConfirmation>
2056           </saml:Subject>
2057           </lib:AuthenticationStatement>
2058           <saml:AttributeStatement>
2059             <saml:Subject>

```



```
2060         <saml:NameIdentifier>
2061             <saml:NameQualifier>http://aol.com</saml:NameQualifier>
2062             <saml:Format>urn:liberty:iff:nameid:federated</saml:Format>
2063             AOLScreenname
2064         </saml:NameIdentifier>
2065     </saml:Subject>
2066     <saml:Attribute AttributeName="devUPC"
2067         AttributeNamespace="http://schemas.corp.aol.com">
2068         <saml:AttributeValue>123456789012</saml:AttributeValue>
2069     </saml:Attribute>
2070 </saml:AttributeStatement>
2071 <ds:Signature>
2072     Signature data goes here
2073 </ds:Signature>
2074 </saml:Assertion>
2075 </sa:Credentials>
2076 </sa:SASLResponse>
2077 </S:Body>
2078 </S:Envelope>
2079
```

2080 Notes:

2081 1. There are 2 key pieces of information in this message: the discovery service resource offering and the  
2082 authentication assertion to be used at that service.

## 2083 8.6. Device Requests Service Info from Discovery Service

2084 The device now submits a request to the Discovery Service (at the entry point returned in the previous message  
2085 "https://discovery.ws.aol.com" – Note that this address could change on a user by user, call by call basis,  
2086 so the client MUST retrieve the correct value from the message returned during the authentication process) for  
2087 information about the radio service.

```
2088 <?xml version="1.0" encoding="utf-8" ?>
2089 <S:Envelope>
2090     xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
2091     xmlns:aol="http://schemas.corp.aol.com/soap/sif-2004-02"
2092     xmlns:disco="urn:liberty:disco:2003-08"
2093     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
2094     xmlns:sb="urn:liberty:wsf:soap-bind:1.0"
2095     xmlns:sa="urn:liberty:wsf:soap-auth:1.0" >
2096 <S:Header>
2097     <sb:Correlation S:mustUnderstand="1"
2098         messageID="uuid:0023923-28329328-23789404578"
2099         timestamp="2003-06-06T12:10:12Z" />
2100 <wsse:Security>
2101     <saml:Assertion MajorVersion="1" MinorVersion="1"
2102         AssertionID="e06e5a28-bc80-4ba6-9ecb-712949db686e"
2103         Issuer="http://idp.aol.com"
2104         IssueInstant="2003-06-06T12:10:11Z"
2105         InResponseTo="uuid:0023923-28329023-238239026">
2106     <saml:Conditions NotOnOrAfter="2003-06-07T12:10:10Z" >
2107         <saml:AudienceRestrictionCondition>
2108             <saml:Audience>http://discovery.aol.com</saml:Audience>
2109         </saml:AudienceRestrictionCondition>
2110     </saml:Conditions>
2111     <lib:AuthenticationStatement
2112         AuthenticationInstant="2003-06-06:12:10:11Z"
2113         SessionIndex="1" >
2114     <lib:AuthnContext>
2115         <lib:AuthnContextClassRef>
2116             http://schemas.corp.aol.com/authctx/classes/DeviceProtectedTransport
2117         </lib:AuthnContextClassRef>
2118     </lib:AuthnContext>
2119     <saml:Subject>
```

```

2120         <saml:NameIdentifier>
2121             <saml:NameQualifier>http://aol.com</saml:NameQualifier>
2122             <saml:Format>urn:liberty:iff:nameid:federated</saml:Format>
2123             AOLScreenname
2124         </saml:NameIdentifier>
2125     <saml:SubjectConfirmation>
2126         <saml:ConfirmationMethod>
2127             urn:oasis:names:tc:SAML:1.0:cm:Bearer
2128         </saml:ConfirmationMethod>
2129     </saml:SubjectConfirmation>
2130 </saml:Subject>
2131 </lib:AuthenticationStatement>
2132 <saml:AttributeStatement>
2133     <saml:Subject>
2134         <saml:NameIdentifier>
2135             <saml:NameQualifier>http://aol.com</saml:NameQualifier>
2136             <saml:Format>urn:liberty:iff:nameid:federated</saml:Format>
2137             AOLScreenname
2138         </saml:NameIdentifier>
2139     </saml:Subject>
2140     <saml:Attribute AttributeName="devUPC"
2141         AttributeNamespace="http://schemas.corp.aol.com">
2142         <saml:AttributeValue>123456789012</saml:AttributeValue>
2143     </saml:Attribute>
2144 </saml:AttributeStatement>
2145 <ds:Signature>
2146     Signature data goes here
2147 </ds:Signature>
2148 </saml:Assertion>
2149 </wsse:Security>
2150 </S:Header>
2151 <S:Body>
2152     <disco:Query>
2153         <ResourceID urn:liberty:isf:implied-resource</ResourceID>
2154         <RequestedServiceType>
2155             <ServiceType>urn:aol-com:services:radio</ServiceType>
2156         </RequestedServiceType>
2157     </disco:Query>
2158 </S:Body>
2159 </S:Envelope>
2160

```

2161 Notes:

- 2162 1. The Assertion returned from the authentication process is included in the <ws:Security> header in the message.
- 2163 2. There is no "refToMessageID" in the <Correlation> header because this message is the first message in the
- 2164 communication with the Discovery Service.

## 2165 8.7. Discovery Service Returns Service Info

2166 The Discovery Service processes the request and responds to the client with the radio server resource offering, the  
2167 necessary credentials for the radio server, and a session context for subsequent calls to the discovery service.

```

2168 <?xml version="1.0" encoding="utf-8" ?>
2169 <S:Envelope>
2170     xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
2171     xmlns:aol="http://schemas.corp.aol.com/soap/sif-2004-02"
2172     xmlns:disco="urn:liberty:disco:2003-08"
2173     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
2174     xmlns:sb="urn:liberty:wsf:soap-bind:1.0" >
2175 <S:Header>
2176     <sb:Correlation S:mustUnderstand="1"
2177         messageID="uuid:00287-23234564-098098798"
2178         refToMessageID="uuid:0023923-28329328-23789404578"

```

```

2179     timestamp="2003-06-06T12:10:12Z" />
2180 <sb:ServiceInstanceUpdate mustUnderstand="1">
2181   <sec:SecurityMechID>
2182     urn:liberty:security:2003-08:TLS:Bearer
2183   </sec:SecurityMechID>
2184   <Credential NotOnOrAfter="2003-06-06T09:30Z">
2185     <wsse:BinarySecurityToken wsu:Id="..."
2186       ValueType="anyPrefix:ServiceSessionContext">
2187       A233asdfjwe8ldghweoiidfdlsjdwe (Base 64 Encoded Data)
2188     </wsse:BinarySecurityToken>
2189   </Credential>
2190 </sb:ServiceInstanceUpdate>
2191 </S:Header>
2192 <S:Body>
2193   <disco:QueryResponse>
2194     <Status code="OK" />
2195     <disco:ResourceOffering EntryID="1">
2196       <disco:ResourceID>urn:liberty:isf:implied-resource</disco:ResourceID>
2197       <disco:ServiceInstance>
2198         <disco:ServiceType>urn:aol-com:services:radio</disco:ServiceType>
2199         <disco:ProviderID>http://radio.ws.aol.com/</disco:ProviderID>
2200         <disco:Description CredentialRef="9f3d54a0-4899-8a3d-9328-328ad3e4ef90">
2201           <SecurityMechID>
2202             http://ws.aol.com/security/2003-11:TLS:bearer
2203           </SecurityMechID>
2204           <Endpoint>https://radio.ws.aol.com/</Endpoint>
2205         </disco:Description>
2206       </disco:ServiceInstance>
2207     </disco:ResourceOffering>
2208     <disco:Credentials>
2209       <saml:Assertion MajorVersion="1" MinorVersion="1"
2210         AssertionID="9f3d54a0-4899-8a3d-9328-328ad3e4ef90"
2211         Issuer="http://idp.aol.com"
2212         IssueInstant="2003-06-06T12:10:11Z"
2213         InResponseTo="uuid:0023923-28329023-238239026">
2214         <saml:Conditions NotOnOrAfter="2003-06-07T12:10:10Z" >
2215           <saml:AudienceRestrictionCondition>
2216             <saml:Audience>http://radio.ws.aol.com</saml:Audience>
2217           </saml:AudienceRestrictionCondition>
2218         </saml:Conditions>
2219         <lib:AuthenticationStatement
2220           AuthenticationInstant="2003-06-06:12:10:11Z"
2221           SessionIndex="1" >
2222           <lib:AuthnContext>
2223             <lib:AuthnContextClassRef>
2224               http://schemas.corp.aol.com/authctx/classes/DeviceProtectedTransport
2225             </lib:AuthnContextClassRef>
2226           </lib:AuthnContext>
2227           <saml:Subject>
2228             <saml:NameIdentifier>
2229               <saml:NameQualifier>http://aol.com</saml:NameQualifier>
2230               <saml:Format>urn:liberty:iff:nameid:federated</saml:Format>
2231               AOLScreenname
2232             </saml:NameIdentifier>
2233           <saml:SubjectConfirmation>
2234             <saml:ConfirmationMethod>
2235               urn:oasis:names:tc:SAML:1.0:cm:Bearer
2236             </saml:ConfirmationMethod>
2237           </saml:SubjectConfirmation>
2238         </lib:AuthenticationStatement>
2239         <saml:AttributeStatement>
2240           <saml:Subject>
2241             <saml:NameIdentifier>
2242               <saml:NameQualifier>http://aol.com</saml:NameQualifier>
2243               <saml:Format>urn:liberty:iff:nameid:federated</saml:Format>
2244               AOLScreenname
2245             </saml:NameIdentifier>

```

```

2246         </saml:NameIdentifier>
2247     </saml:Subject>
2248     <saml:Attribute AttributeName="devUPC"
2249         AttributeNamespace="http://schemas.corp.aol.com">
2250         <saml:AttributeValue>123456789012</saml:AttributeValue>
2251     </saml:Attribute>
2252 </saml:AttributeStatement>
2253 <ds:Signature>
2254     Signature data goes here
2255 </ds:Signature>
2256 </saml:Assertion>
2257 </disco:Credentials>
2258 </disco:QueryResponse>
2259 </S:Body>
2260 </S:Envelope>
2261

```

## 2262 8.8. Device Requests Data from Radio Service

2263 The device, having the contact information and credentials for the Radio service, submit a service request to the Radio  
2264 server (to the Endpoint identified in the Resource Offering: "https://radio.ws.aol.com").

```

2265 <?xml version="1.0" encoding="utf-8" ?>
2266 <S:Envelope>
2267     xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
2268     xmlns:aol="http://schemas.corp.aol.com/soap/sif-2004-02"
2269     xmlns:disco="urn:liberty:disco:2003-08"
2270     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
2271     xmlns:sb="urn:liberty:wsf:soap-bind:1.0" >
2272 <S:Header>
2273     <sb:Correlation S:mustUnderstand="1"
2274         messageID="uuid:9897923-82398723-092739723"
2275         timestamp="2003-06-06T12:10:16Z" />
2276 <wsse:Security>
2277     <saml:Assertion MajorVersion="1" MinorVersion="1"
2278         AssertionID="9f3d54a0-4899-8a3d-9328-328ad3e4ef90"
2279         Issuer="http://idp.aol.com"
2280         IssueInstant="2003-06-06T12:10:11Z"
2281         InResponseTo="uuid:0023923-28329023-238239026">
2282     <saml:Conditions NotOnOrAfter="2003-06-07T12:10:10Z" >
2283         <saml:AudienceRestrictionCondition>
2284             <saml:Audience>http://radio.ws.aol.com</saml:Audience>
2285         </saml:AudienceRestrictionCondition>
2286     </saml:Conditions>
2287     <lib:AuthenticationStatement
2288         AuthenticationInstant="2003-06-06:12:10:11Z"
2289         SessionIndex="1" >
2290     <lib:AuthnContext>
2291         <lib:AuthnContextClassRef>
2292             http://schemas.corp.aol.com/authctx/classes/DeviceProtectedTransport
2293         </lib:AuthnContextClassRef>
2294     </lib:AuthnContext>
2295     <saml:Subject>
2296         <saml:NameIdentifier>
2297             <saml:NameQualifier>http://aol.com</saml:NameQualifier >
2298             <saml:Format>urn:liberty:iff:nameid:federated</saml:Format>
2299             AOLScreenname
2300         </saml:NameIdentifier>
2301     </saml:SubjectConfirmation>
2302     <saml:ConfirmationMethod>
2303         urn:oasis:names:tc:SAML:1.0:cm:Bearer
2304     </saml:ConfirmationMethod>
2305 </saml:SubjectConfirmation>
2306 </saml:Subject>
2307 </lib:AuthenticationStatement>

```

```

2308     <saml:AttributeStatement>
2309         <saml:Subject>
2310             <saml:NameIdentifier>
2311                 <saml:NameQualifier>http://aol.com</saml:NameQualifier>
2312                 <saml:Format>urn:liberty:iff:nameid:federated</saml:Format>
2313                 AOLScreenname
2314             </saml:NameIdentifier>
2315         </saml:Subject>
2316         <saml:Attribute AttributeName="devUPC"
2317             AttributeNamespace="http://schemas.corp.aol.com">
2318             <saml:AttributeValue>123456789012</saml:AttributeValue>
2319         </saml:Attribute>
2320     </saml:AttributeStatement>
2321     <ds:Signature>
2322         Signature data goes here
2323     </ds:Signature>
2324 </saml:Assertion>
2325 </wsse:Security>
2326 </S:Header>
2327 <S:Body>
2328     <GetStationList/>
2329 </S:Body>
2330 </S:Envelope>
2331

```

2332 Notes:

- 2333 1. The authentication assertion returned with the Discovery Service response is included in the request to the Radio  
2334 Service to identify the user.

## 2335 8.9. Radio Service Returns Info

2336 The Radio Service processes the request and returns the list of stations to the client.

```

2337 <?xml version="1.0" encoding="utf-8" ?>
2338 <S:Envelope>
2339     xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
2340     xmlns:aol="http://schemas.corp.aol.com/soap/sif-2004-02"
2341     xmlns:sb="urn:liberty:wsf:soap-bind:1.0" >
2342     <S:Header>
2343         <sb:Correlation S:mustUnderstand="1"
2344             messageID="uuid:23452-7345097234-0974234097"
2345             refToMessageID=" uuid:9897923-82398723-092739723"
2346             timestamp="2003-06-06T12:10:16Z" />
2347     <sb:ServiceInstanceUpdate mustUnderstand="1">
2348         <sec:SecurityMechID>
2349             urn:liberty:security:2003-08:TLS:Bearer
2350         </sec:SecurityMechID>
2351         <Credential NotOnOrAfter="2003-06-07T12:10:10Z">
2352             <wsse:BinarySecurityToken wsu:Id="..."
2353                 ValueType="anyPrefix:ServiceSessionContext">
2354                 A233asdfjwe8lwefjisde8asddj2weqw9ejajdh2hqdh72zxc2easad
2355             </wsse:BinarySecurityToken>
2356         </Credential>
2357         <Endpoint>https://Radio15.ws.aol.com/</Endpoint>
2358     </sb:ServiceInstanceUpdate>
2359 </S:Header>
2360 <S:Body>
2361     // Station List data included here
2362 </S:Body>
2363 </S:Envelope>
2364

```

2365 Notes:

- 2366 1. The Radio Service returned a session context for the client for use on subsequent requests.
- 2367 2. The NotOnOrAfter attribute on the credential was set to the same expiration time as the assertion which initiated  
2368 the session.
- 2369 3. The Radio Service told the client to submit subsequent requests to a new server ("https://Radio15.ws.aol.com/").

## 2370 8.10. Device Requests Additional Info from Radio

2371 The Device now needs the detailed station info for one of the stations returned in the previous. This  
2372 time, because of the <ServiceSessionContext> returned in the previous call, the request is submitted to:  
2373 "https://Radio15.ws.aol.com" and the Assertion is not needed on the request.

```
2374 <?xml version="1.0" encoding="utf-8" ?>
2375 <S:Envelope>
2376   xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
2377   xmlns:aol="http://schemas.corp.aol.com/soap/sif-2004-02"
2378   xmlns:sb="urn:liberty:wsf:soap-bind:1.0" >
2379   <S:Header>
2380     <sb:Correlation S:mustUnderstand="1"
2381       messageID="uuid:23409723497-20972347-23407234"
2382       refToMessageID="uuid:23452-7345097234-0974234097"
2383       timestamp="2003-06-06T12:10:16Z" />
2384     <wsse:Security>
2385       <wsse:BinarySecurityToken wsu:Id="..."
2386         ValueType="anyPrefix:ServiceSessionContext">
2387         A233asdfjwe8lwefjisde8asddj2weqw9ejajdh2hqdh72zxcb2easad
2388       </wsse:BinarySecurityToken>
2389     </wsse:Security>
2390   </S:Header>
2391   <S:Body>
2392     // Get Station Detail command
2393   </S:Body>
2394 </S:Envelope>
2395
```

2396 Notes:

- 2397 1. Because the <wsse:BinarySecurityToken> was included, the assertion is not necessary.
- 2398 2. The "refToMessageID" attribute is set to the message id of the previous response message from the radio server.

## 2399 8.11. Radio Service Returns Info

2400 The Radio Service processes the request and returns the detailed station info.

```
2401 <?xml version="1.0" encoding="utf-8" ?>
2402 <S:Envelope>
2403   xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
2404   xmlns:aol="http://schemas.corp.aol.com/soap/sif-2004-02"
2405   xmlns:sb="urn:liberty:wsf:soap-bind:1.0" >
2406   <S:Header>
2407     <sb:Correlation S:mustUnderstand="1"
2408       messageID="uuid:23568989-07123493294-23723"
2409       refToMessageID="uuid:23409723497-20972347-23407234"
2410       timestamp="2003-06-06T12:10:16Z" />
2411   </S:Header>
2412   <S:Body>
2413     // Station Details
2414   </S:Body>
2415 </S:Envelope>
2416
```

2417 Notes:

2418 1. The Radio Server did not return another <ServiceSessionContext> to the caller. This means the existing  
 2419 context is still valid and should be used on the next request.

## 2420 8.12. Device Requests Photo Service Info from Discovery Service

2421 The user selects the photo tab on the display and the device now needs to contact the photo service. So the device  
 2422 submits a discovery request to lookup the photo service contact information.

```

2423 <?xml version="1.0" encoding="utf-8" ?>
2424 <S:Envelope>
2425   xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
2426   xmlns:aol="http://schemas.corp.aol.com/soap/sif-2004-02"
2427   xmlns:disco="urn:liberty:disco:2003-08"
2428   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
2429   xmlns:sb="urn:liberty:wsf:soap-bind:1.0"
2430   <S:Header>
2431     <sb:Correlation S:mustUnderstand="1"
2432       messageID="uuid:09213802-230987987-238797234"
2433       refToMessageID="uuid:00287-23234564-098098798"
2434       timestamp="2003-06-06T18:29:18Z" />
2435     <wsse:Security>
2436       <wsse:BinarySecurityToken wsu:Id="..."
2437         ValueType="anyPrefix:ServiceSessionContext">
2438         A233asdfjwe8ldghweoiidfldlsjdwe (Base 64 Encoded Data)
2439       </wsse:BinarySecurityToken>
2440     </wsse:Security>
2441   </S:Header>
2442   <S:Body>
2443     <disco:Query>
2444       <disco:ResourceID> urn:liberty:isf:implied-resource</disco:ResourceID>
2445       <disco:RequestedServiceType>
2446         <disco:ServiceType>urn:aol-com:services:photo</disco:ServiceType>
2447       </disco:RequestedServiceType>
2448     </disco:Query>
2449   </S:Body>
2450 </S:Envelope>
2451
```

2452 Notes:

2453 1. The request included the session context returned from the Discovery Service in step 0 and does not include a  
 2454 Liberty assertion in the header.

2455 2. Since this is essentially a continuation of the conversation with the DS, we include the message ID of the last  
 2456 response from the DS in this request.

## 2457 8.13. Discovery Service Returns Photo Service Info

2458 The Discovery Service processes the request and responds to the client with the radio server resource offering, the  
 2459 necessary credentials for the radio server, and a session context for subsequent calls to the discovery service.

```

2460 <?xml version="1.0" encoding="utf-8" ?>
2461 <S:Envelope>
2462   xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
2463   xmlns:aol="http://schemas.corp.aol.com/soap/sif-2004-02"
2464   xmlns:disco="urn:liberty:disco:2003-08"
2465   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
2466   xmlns:sb="urn:liberty:wsf:soap-bind:1.0"
2467   xmlns:sa="urn:liberty:wsf:soap-auth:1.0" >
2468   <S:Header>
2469     <sb:Correlation S:mustUnderstand="1"
2470       messageID="uuid:33489-8972323-89798237912"
2471       refToMessageID="uuid:09213802-230987987-238797234"

```

```

2472         timestamp="2003-06-06T18:29:18Z" />
2473     </S:Header>
2474     <S:Body>
2475         <disco:QueryResponse>
2476             <Status code="OK" />
2477             <disco:ResourceOffering EntryID="1">
2478                 <disco:ResourceID>urn:liberty:isf:implied-resource</disco:ResourceID>
2479                 <disco:ServiceInstance>
2480                     <disco:ServiceType>urn:aol-com:services:photo</disco:ServiceType>
2481                     <disco:ProviderID>http://photo.ws.aol.com/</disco:ProviderID>
2482                     <disco:Description CredentialRef="9fd3eda-b34a-9008-a334-3234dea90f5">
2483                         <SecurityMechID>
2484                             http://ws.aol.com/security/2003-11:TLS:bearer
2485                         </SecurityMechID>
2486                         <Endpoint>https://photo.ws.aol.com/</Endpoint>
2487                     </disco:Description>
2488                 </disco:ServiceInstance>
2489             </disco:ResourceOffering>
2490             <disco:Credentials>
2491                 <saml:Assertion MajorVersion="1" MinorVersion="1"
2492                     AssertionID="9fd3eda-b34a-9008-a334-3234dea90f5"
2493                     Issuer="http://idp.aol.com"
2494                     IssueInstant="2003-06-06T18:29:18Z"
2495                     InResponseTo="uuid:0023923-28329023-238239026">
2496                     <saml:Conditions NotOnOrAfter="2003-06-07T12:10:10Z" >
2497                         <saml:AudienceRestrictionCondition>
2498                             <saml:Audience>http://photo.ws.aol.com</saml:Audience>
2499                         </saml:AudienceRestrictionCondition>
2500                     </saml:Conditions>
2501                     <lib:AuthenticationStatement
2502                         AuthenticationInstant="2003-06-06:12:10:11Z"
2503                         SessionIndex="1" >
2504                         <lib:AuthnContext>
2505                             <lib:AuthnContextClassRef>
2506                                 http://schemas.corp.aol.com/authctx/classes/DeviceProtectedTransport
2507                             </lib:AuthnContextClassRef>
2508                         </lib:AuthnContext>
2509                         <saml:Subject>
2510                             <saml:NameIdentifier>
2511                                 <saml:NameQualifier>http://aol.com</saml:NameQualifier>
2512                                 <saml:Format>urn:liberty:iff:nameid:federated</saml:Format>
2513                                 AOLScreenname
2514                             </saml:NameIdentifier>
2515                         </saml:SubjectConfirmation>
2516                         <saml:ConfirmationMethod>
2517                             urn:oasis:names:tc:SAML:1.0:cm:Bearer
2518                         </saml:ConfirmationMethod>
2519                     </saml:SubjectConfirmation>
2520                     </saml:Subject>
2521                 </lib:AuthenticationStatement>
2522                 <saml:AttributeStatement>
2523                     <saml:Subject>
2524                         <saml:NameIdentifier>
2525                             <saml:NameQualifier>http://aol.com</saml:NameQualifier>
2526                             <saml:Format>urn:liberty:iff:nameid:federated</saml:Format>
2527                             AOLScreenname
2528                         </saml:NameIdentifier>
2529                     </saml:Subject>
2530                     <saml:Attribute AttributeName="devUPC"
2531                         AttributeNamespace="http://schemas.corp.aol.com">
2532                         <saml:AttributeValue>123456789012</saml:AttributeValue>
2533                     </saml:Attribute>
2534                 </saml:AttributeStatement>
2535                 <ds:Signature>
2536                     Signature data goes here
2537                 </ds:Signature>
2538             </saml:Assertion>

```



```

2539         </disco:Credentials>
2540     </disco:QueryResponse>
2541 </S:Body>
2542 </S:Envelope>
2543

```

2544 Notes:

2545 1. [reserved]

## 2546 8.14. Device Requests Info from Photo Service

2547 The device requests a list of folders from the photo service.

```

2548 <?xml version="1.0" encoding="utf-8" ?>
2549 <S:Envelope>
2550     xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
2551     xmlns:aol="http://schemas.corp.aol.com/soap/sif-2004-02"
2552     xmlns:disco="urn:liberty:disco:2003-08"
2553     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
2554     xmlns:sb="urn:liberty:wsf:soap-bind:1.0" >
2555     <S:Header>
2556         <sb:Correlation S:mustUnderstand="1"
2557             messageID="uuid:958312848-29348938-232342121"
2558             timestamp="2003-06-06T18:29:18Z" />
2559     <wsse:Security>
2560         <saml:Assertion MajorVersion="1" MinorVersion="1"
2561             AssertionID="9fd3eda-b34a-9008-a334-3234dea90f5"
2562             Issuer="http://idp.aol.com"
2563             IssueInstant="2003-06-06T18:29:18Z"
2564             InResponseTo="uuid:0023923-28329023-238239026">
2565             <saml:Conditions NotOnOrAfter="2003-06-07T12:10:10Z" >
2566                 <saml:AudienceRestrictionCondition>
2567                     <saml:Audience>http://photo.ws.aol.com</saml:Audience>
2568                 </saml:AudienceRestrictionCondition>
2569             </saml:Conditions>
2570             <lib:AuthenticationStatement
2571                 AuthenticationInstant="2003-06-06T12:10:11Z"
2572                 SessionIndex="1" >
2573                 <lib:AuthnContext>
2574                     <lib:AuthnContextClassRef>
2575                         http://schemas.corp.aol.com/authctx/classes/DeviceProtectedTransport
2576                     </lib:AuthnContextClassRef>
2577                 </lib:AuthnContext>
2578                 <saml:Subject>
2579                     <saml:NameIdentifier>
2580                         <saml:NameQualifier>http://aol.com</saml:NameQualifier>
2581                         <saml:Format>urn:liberty:iff:nameid:federated</saml:Format>
2582                         AOLScreenname
2583                     </saml:NameIdentifier>
2584                 <saml:SubjectConfirmation>
2585                     <saml:ConfirmationMethod>
2586                         urn:oasis:names:tc:SAML:1.0:cm:Bearer
2587                     </saml:ConfirmationMethod>
2588                 </saml:SubjectConfirmation>
2589             </saml:Subject>
2590             </lib:AuthenticationStatement>
2591             <saml:AttributeStatement>
2592                 <saml:Subject>
2593                     <saml:NameIdentifier>
2594                         <saml:NameQualifier>http://aol.com</saml:NameQualifier>
2595                         <saml:Format>urn:liberty:iff:nameid:federated</saml:Format>
2596                         AOLScreenname
2597                     </saml:NameIdentifier>
2598                 <saml:SubjectConfirmation>
2599                     <saml:ConfirmationMethod>

```

```

2600         urn:oasis:names:tc:SAML:1.0:cm:Bearer
2601     </saml:ConfirmationMethod>
2602 </saml:SubjectConfirmation>
2603 </saml:Subject>
2604     <saml:Attribute AttributeName="devUPC"
2605         AttributeNamespace="http://schemas.corp.aol.com">
2606         <saml:AttributeValue>123456789 012</saml:AttributeValue>
2607     </saml:Attribute>
2608 </saml:AttributeStatement>
2609 <ds:Signature>
2610     Signature data goes here
2611 </ds:Signature>
2612 </saml:Assertion>
2613 </wsse:Security>
2614 </S:Header>
2615 <S:Body>
2616     // Photo Service Request
2617 </S:Body>
2618 </S:Envelope>
2619

```

2620 Notes:

- 2621 1. As this is the first request to the Photo Service, there is no "refToMessageID" included.
- 2622 2. The Assertion returned with the Discovery Service response is included in this message.

## 2623 8.15. Photo Service Returns Info

2624 The Photo Service returns the requested information.

```

2625 <?xml version="1.0" encoding="utf-8" ?>
2626 <S:Envelope>
2627     xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
2628     xmlns:aol="http://schemas.corp.aol.com/soap/sif-2004-02"
2629     xmlns:sb="urn:liberty:wsf:soap-bind:1.0" >
2630 <S:Header>
2631     <sb:Correlation S:mustUnderstand="1"
2632         messageID="uuid:23452-734509723 4-0974234097"
2633         refToMessageID="uuid:958312848-29 348938-232342121"
2634         timestamp="2003-06-06T12:10:16Z" />
2635 <sb:ServiceInstanceUpdate mustUnderstand="1">
2636     <sec:SecurityMechID>
2637         urn:liberty:security:2003-08:TLS:Bearer
2638     </sec:SecurityMechID>
2639     <Credential NotOnOrAfter="2003-06-07T12:10:10Z">
2640         <wsse:BinarySecurityToken wsu:Id="..."
2641             ValueType="anyPrefix:ServiceSessionContext">
2642             A233asdfjwe8lwefjjsde8asddj2weqw9ejajdh2hqdh72zxcb2easad
2643         </wsse:BinarySecurityToken>
2644     </Credential>
2645 </sb:ServiceInstanceUpdate>
2646 </S:Header>
2647 <S:Body>
2648     // Station List data included here
2649 </S:Body>
2650 </S:Envelope>
2651

```

2652 Notes:

- 2653 1. As the Radio Service did, the Photo Service returns a <ServiceInstanceUpdate> to the caller. However, in
- 2654 this response, the Photo Service does not redirect the user to a different SOAP Endpoint.

## 2655 8.16. Device Renews Security Token

2656 It is now almost 24 hours since the original authentication by the device and the device, being a good client, has  
 2657 monitored the validity period on the security token it received and so knows that it needs to perform a renewal of the  
 2658 token. This request is submitted to the authentication server, the same place where the original authentication took  
 2659 place.

```

2660 <?xml version="1.0" encoding="utf-8" ?>
2661 <S:Envelope>
2662   xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
2663   xmlns:aol="http://schemas.corp.aol.com/soap/sif-2004-02"
2664   xmlns:disco="urn:liberty:disco:2003-08"
2665   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
2666   xmlns:sb="urn:liberty:wsf:soap-bind:1.0"
2667   xmlns:sa="urn:liberty:wsf:soap-auth:1.0" >
2668   <S:Header>
2669     <sb:Correlation S:mustUnderstand="1"
2670       messageID="uuid:234235-993209787-099087238923"
2671       timestamp="2003-06-07T12:00:00Z" />
2672   <wsse:Security>
2673     <saml:Assertion MajorVersion="1" MinorVersion="1"
2674       AssertionID="e06e5a28-bc80-4ba6-9ecb-712949db686e"
2675       Issuer="http://idp.aol.com"
2676       IssueInstant="2003-06-06T12:10:11Z"
2677       InResponseTo="uuid:0023923-28329023-238239026" >
2678     <saml:Conditions NotOnOrAfter="2003-06-07T12:10:10Z" >
2679       <saml:AudienceRestrictionCondition>
2680         <saml:Audience>http://discovery.aol.com</saml:Audience>
2681       </saml:AudienceRestrictionCondition>
2682     </saml:Conditions>
2683     <lib:AuthenticationStatement
2684       AuthenticationInstant="2003-06-06:12:10:11Z"
2685       SessionIndex="1" >
2686     <lib:AuthnContext>
2687       <lib:AuthnContextClassRef>
2688         http://schemas.aol.com/authctx/classes/DeviceProtectedTransport
2689       </lib:AuthnContextClassRef>
2690     </lib:AuthnContext>
2691     <saml:Subject>
2692       <saml:NameIdentifier>
2693         <saml:NameQualifier>http://aol.com</saml:NameQualifier >
2694         <saml:Format>urn:liberty:iff:nameid:federated</saml:Format>
2695         AOLScreenname
2696       </saml:NameIdentifier>
2697     <saml:SubjectConfirmation>
2698       <saml:ConfirmationMethod>
2699         urn:oasis:names:tc:SAML:1.0:cm:Bearer
2700       </saml:ConfirmationMethod>
2701     </saml:SubjectConfirmation>
2702   </saml:Subject>
2703 </lib:AuthenticationStatement>
2704 <saml:AttributeStatement>
2705   <saml:Subject>
2706     <saml:NameIdentifier>
2707       <saml:NameQualifier>http://aol.com</saml:NameQualifier>
2708       <saml:Format>urn:liberty:iff:nameid:federated</saml:Format>
2709       AOLScreenname
2710     </saml:NameIdentifier>
2711   </saml:Subject>
2712   <saml:Attribute AttributeName="devUPC"
2713     AttributeNamespace="http://schemas.corp.aol.com">
2714     <saml:AttributeValue>123456789012</saml:AttributeValue>
2715   </saml:Attribute>
2716 </saml:AttributeStatement>
2717 <ds:Signature>
2718   Signature data goes here
    
```

```

2719         </ds:Signature>
2720     </saml:Assertion>
2721 </wsse:Security>
2722 </S:Header>
2723 <S:Body>
2724     <sa:SASLRequest advisoryAuthnID="123456789012:10023923"
2725         mechanism="CRAM-MD5" />
2726 </S:Body>
2727 </S:Envelope>
2728

```

2729 Notes:

2730 1. The previously-returned security token is presented back to the authentication service.

2731 2. The "renewal" attribute is all that is needed on this authentication request.

## 2732 8.17. The Authentication Server Returns New Token

2733 The server processes the request and returns the renewed security token to the caller.

```

2734 <?xml version="1.0" encoding="utf-8" ?>
2735 <S:Envelope>
2736     xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
2737     xmlns:aol="http://schemas.corp.aol.com/soap/sif-2004-02"
2738     xmlns:disco="urn:liberty:disco:2003-08"
2739     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
2740     xmlns:sb="urn:liberty:wsf:soap-bind:1.0"
2741     xmlns:sa="urn:liberty:wsf:soap-auth:1.0" >
2742 <S:Header>
2743     <sb:Correlation S:mustUnderstand="1"
2744         messageID="uuid:87432-79234723-072347893"
2745         refToMessageID="uuid:234235-993209787-099087238923"
2746         timestamp="2003-06-07T12:00:00Z" />
2747 </S:Header>
2748 <S:Body>
2749     <sa:SASLResponse>
2750     <sa:Status code="success" />
2751     <sa:Credential>
2752     <saml:Assertion MajorVersion="1" MinorVersion="1"
2753         AssertionID="9fe4357-df43-b902-9123-da8082fe7"
2754         Issuer="http://idp.aol.com"
2755         IssueInstant="2003-06-07T12:00:00Z"
2756         InResponseTo=" uuid:234235-993209787-099087238923">
2757     <saml:Conditions NotOnOrAfter="2003-06-08T12:00:00Z" >
2758         <saml:AudienceRestrictionCondition>
2759             <saml:Audience>http://discovery.aol.com</saml:Audience>
2760         </saml:AudienceRestrictionCondition>
2761     </saml:Conditions>
2762     <lib:AuthenticationStatement
2763         AuthenticationInstant="2003-06-06T12:10:11Z"
2764         SessionIndex="1" >
2765     <lib:AuthnContext>
2766     <lib:AuthnContextClassRef>
2767         http://schemas.corp.aol.com/authctx/classes/DeviceProtectedTransport
2768     </lib:AuthnContextClassRef>
2769     </lib:AuthnContext>
2770     <saml:Subject>
2771     <saml:NameIdentifier>
2772         <saml:NameQualifier>http://aol.com</saml:NameQualifier>
2773         <saml:Format>urn:liberty:iff:nameid:federated</saml:Format>
2774         AOLScreenname
2775     </saml:NameIdentifier>
2776     <saml:SubjectConfirmation>
2777     <saml:ConfirmationMethod>

```

```
2778         urn:oasis:names:tc:SAML:1.0:cm:Bearer
2779     </saml:ConfirmationMethod>
2780 </saml:SubjectConfirmation>
2781 </saml:Subject>
2782 </lib:AuthenticationStatement>
2783 <saml:AttributeStatement>
2784     <saml:Subject>
2785         <saml:NameIdentifier>
2786             <saml:NameQualifier>http://aol.com</saml:NameQualifier>
2787             <saml:Format>urn:liberty:iff:nameid:federated</saml:Format>
2788             AOLScreenname
2789         </saml:NameIdentifier>
2790     </saml:Subject>
2791     <saml:Attribute AttributeName="devUPC"
2792         AttributeNamespace="http://schemas.corp.aol.com">
2793         <saml:AttributeValue>123456789012</saml:AttributeValue>
2794     </saml:Attribute>
2795 </saml:AttributeStatement>
2796 <ds:Signature>
2797     Signature data goes here
2798 </ds:Signature>
2799 </saml:Assertion>
2800 </sa:Credential>
2801 </sa:SASLResponse>
2802 </S:Body>
2803 </S:Envelope>
2804
```

2805 Notes:

2806 1. The discovery service bootstrap information is not included since it was sent previously.

2807 2. The renewed token still has the same "AuthenticationInstant" since this is a renewal, not a re-  
2808 authentication.

## 2809 References

### 2810 Normative

- 2811 [LibertyAuthnContext] Madsen, Paul, eds. "Liberty ID-FF Authentication Context Specification," Version 2.0-01,  
2812 Liberty Alliance Project (21 November 2004). <http://www.projectliberty.org/specs>
- 2813 [LibertyBindProf] Cantor, Scott, Kemp, John, Champagne, Darryl, eds. "Liberty ID-FF Bindings and  
2814 Profiles Specification," Version 1.2-errata-v2.0, Liberty Alliance Project (12 September 2004).  
2815 <http://www.projectliberty.org/specs>
- 2816 [LibertyDisco] Beatty, John, Sergent, Jonathan, Hodges, Jeff, eds. "Liberty ID-WSF Discovery Service Specification,"  
2817 Version 2.0-12, Liberty Alliance Project (21 Sep 2005). <http://www.projectliberty.org/specs>
- 2818 [LibertyDST] Kellomäki, Sampo, Kainulainen, Jukka, eds. "Liberty ID-WSF Data Services Template," Version 2.1-  
2819 08, Liberty Alliance Project (21 Sep 2005). <http://www.projectliberty.org/specs>
- 2820 [LibertyIDEP] Kellomäki, Sampo, eds. "Liberty ID-SIS Employee Profile Service Specification," Version 1.1-02,  
2821 Liberty Alliance Project (13 September, 2005). <http://www.projectliberty.org/specs>
- 2822 [LibertyIDFFOverview] Wason, Thomas, eds. "Liberty ID-FF Architecture Overview," Version 1.2-errata-v1.0,  
2823 Liberty Alliance Project (12 September 2004). <http://www.projectliberty.org/specs>
- 2824 [LibertyIDPPP] Kellomäki, Sampo, eds. "Liberty Identity Personal Profile Service Specification," Version 1.1-02,  
2825 Liberty Alliance Project (13 September, 2005). <http://www.projectliberty.org/specs>
- 2826 [LibertyIDWSFSecurityPrivacyGuidelines] Landau, Susan, eds. "Liberty ID-WSF Security and Privacy Overview,"  
2827 Version 1.0, Liberty Alliance Project (8 October 2003). <http://www.projectliberty.org/specs>
- 2828 [LibertyImplGuide] "Liberty ID-FF Implementation Guidelines," Version 1.2, Liberty Alliance Project (18 April  
2829 2004). <http://www.projectliberty.org/specs> Thompson, Peter, Champagne, Darryl, eds.
- 2830 [LibertyInteract] Aarts, Robert, Madsen, Paul, eds. "Liberty ID-WSF Interaction Service Specification," Version 2.0-  
2831 04, Liberty Alliance Project (21 Sep 2005). <http://www.projectliberty.org/specs>
- 2832 [LibertyMetadata] Davis, Peter, eds. "Liberty Metadata Description and Discovery Specification," Version 2.0-02,  
2833 Liberty Alliance Project (25 November 2004). <http://www.projectliberty.org/specs>
- 2834 [LibertyPAOS] Aarts, Robert, eds. "Liberty Reverse HTTP Binding for SOAP Specification," Version 2.0-01, Liberty  
2835 Alliance Project (22 November 2004). <http://www.projectliberty.org/specs>
- 2836 [LibertySecMech] Ellison, Gary, Hirsch, Frederick, Madsen, Paul, eds. "Liberty ID-WSF Security Mechanisms Core,"  
2837 Version v2.0-12, Liberty Alliance Project (22 September 2005). <http://www.projectliberty.org/specs>
- 2838 [LibertySOAPBinding] Hodges, Jeff, Kemp, John, Aarts, Robert, Whitehead, Greg, eds. "Liberty ID-  
2839 WSF SOAP Binding Specification," Version 2.0-09, Liberty Alliance Project (22 September, 2005).  
2840 <http://www.projectliberty.org/specs>
- 2841 [OASISGloss] Hodges, Jeff, eds. (2003). "OASIS Security Services TC: Glossary," Organization for the Advancement  
2842 of Structured Information Standards <http://www.oasis-open.org/committees/security/#documents>
- 2843 [RFC2119] Bradner, S., eds. "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119, The Internet  
2844 Engineering Task Force (March 1997). <http://www.ietf.org/rfc/rfc2119.txt> [March 1997].
- 2845 [RFC2222] "Simple Authentication and Security Layer (SASL)," John G. Myers (October 1997). RFC 2222, Internet  
2846 Engineering Task Force <http://www.ietf.org/rfc/rfc2222.txt> [October 1997].

- 2847 [SAMLCore11] Maler, Eve, Mishra, Prateek, Philpott, Rob, eds. (2 September 2003). "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1," SAML v1.1, OASIS Standard, Organization for the Advancement of Structured Information Standards <http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf>
- 2848
- 2849
- 2850
- 2851 [SAMLCore2] Cantor, Scott, Kemp, John, Philpott, Rob, Maler, Eve, eds. (15 March 2005). "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0," SAML V2.0, OASIS Standard, Organization for the Advancement of Structured Information Standards <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- 2852
- 2853
- 2854
- 2855 [SAMLGloss] Hodges, Jeff, Maler, Eve, eds. (05 November 2002). "Glossary for the OASIS Security Assertion Markup Language (SAML)," SAML V1.0, OASIS Standard, Organization for the Advancement of Structured Information Standards <http://www.oasis-open.org/specs/index.php#samlv1.0>
- 2856
- 2857
- 2858 [SASLCram] Nerneberg, L., eds. (June, 2003). Internet Engineering Task Force "The CRAM-MD5 SASL Mechanism," <http://www.ietf.org/proceedings/03nov/1-D/draft-ietf-sasl-crammd5-00.txt>
- 2859
- 2860 [WSScore] Nadalin, Anthony, Kaler, Chris, Hallam-Baker, Phillip, Monzillo, Ronald, eds. (March, 2004). "Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)," Organization for the Advancement of Structured Information Standards <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf>
- 2861
- 2862
- 2863
- 2864 [X.509] "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks," ITU-T (2000). ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2000,
- 2865

## 2866 Informative

- 2867 [LibertyGlossary] Hodges, Jeff, eds. "Liberty Technical Glossary," Version v2.0-03, Liberty Alliance Project (29 Aug 2005). <http://www.projectliberty.org/specs>
- 2868
- 2869 [LibertyIDWSFOverview] Tourzan, Jonathan, Koga, Yuzo, eds. "Liberty ID-WSF Web Services Framework Overview," Version 1.0-errata-v1.0, Liberty Alliance Project (12 September 2004). <http://www.projectliberty.org/specs>
- 2870
- 2871