



# Cross Operation of Single Sign-On, Federation, and Identity Web Services Frameworks

Version: 1.1

**Editors:**

Sampo Kellomäki, Symlabs, Inc.

**Contributors:**

Conor Cahill, Intel

Rob Lockhart, IEEE-ISTO

Guillermo Lorenzo, Symlabs, Inc.

Paul Madsen, NTT

Greg Whitehead, Hewlett-Packard

**Abstract:**

As standards evolve, both in versions and in scope, it is necessary to adopt newer technologies. This poses problems in terms of already-provisioned federations as well as in using combinations of frameworks that were not foreseen at the time when the specifications were written.

This technote provides pragmatic solutions for these situations, providing equivalence or interoperability of Name IDs as well as specifying how all known combinations of SSO assertions and bootstraps are represented.

**Filename:** liberty-cross-framework-v1.1.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.** Implementers  
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 © 2006 2FA Technology; Adobe Systems; Agencia Catalana De Certificacio; America Online, Inc.;  
16 American Express Company; Amssoft Systems Pvt Ltd.; Avatier Corporation; BIPAC; BMC Software, Inc.; Bank of  
17 America Corporation; Beta Systems Software AG; British Telecommunications plc; Computer Associates  
18 International, Inc.; Credentica; DataPower Technology, Inc.; Deutsche Telekom AG, T-Com; Diamelle Technologies,  
19 Inc.; Diversinet Corp.; Drummond Group Inc.; Enosis Group LLC; Entrust, Inc.; Epok, Inc.; Ericsson; Falkin  
20 Systems LLC; Fidelity Investments; Forum Systems, Inc.; France Télécom; French Government Agence pour le  
21 développement de l'administration électronique (ADAE); Fugen Solutions, Inc; Fulvens Ltd.; GSA Office of  
22 Governmentwide Policy; Gamefederation; Gemalto; General Motors; GeoFederation; Giesecke & Devrient GmbH;  
23 Hewlett-Packard Company; Hochhauser & Co., LLC; IBM Corporation; Intel Corporation; Intuit Inc.; Kantega;  
24 Kayak Interactive; Livo Technologies; Luminance Consulting Services; MasterCard International; MedCommons  
25 Inc.; Mobile Telephone Networks (Pty) Ltd; NEC Corporation; NTT DoCoMo, Inc.; Netegrity, Inc.; Neustar, Inc.;  
26 New Zealand Government State Services Commission; Nippon Telegraph and Telephone Corporation; Nokia  
27 Corporation; Novell, Inc.; OpenNetwork; Oracle Corporation; Ping Identity Corporation; RSA Security Inc.;  
28 Reactivity Inc.; Royal Mail Group plc; SAP AG; Senforce; Sharp Laboratories of America; Sigaba; SmartTrust; Sony  
29 Corporation; Sun Microsystems, Inc.; Supremacy Financial Corporation; Symlabs, Inc.; Telecom Italia S.p.A.;  
30 Telefónica Móviles, S.A.; Telenor R&D; Thales e-Security; Trusted Network Technologies; UNINETT AS; UTI;  
31 VeriSign, Inc.; Vodafone Group Plc.; Wave Systems Corp. All rights reserved.

32 Liberty Alliance Project  
33 Licensing Administrator  
34 c/o IEEE-ISTO  
35 445 Hoes Lane  
36 Piscataway, NJ 08855-1331, USA  
37 info@projectliberty.org

---

## Contents

38		
39	1. Introduction	4
40	1.1. Notational Conventions	4
41	2. Name ID Compatibility Between SAML 1.x, ID-FF 1.x, and SAML 2.0	5
42	2.1. An Introduction to Name IDs	5
43	2.2. NameQualifiers Across Versions	5
44	2.3. Name ID Formats	6
45	3. Independence of SSO (a.k.a. Federation) Framework from WS Framework	7
46	3.1. Guidance for Cross Use of SSO and WS Frameworks	7
47	3.2. Trivial Interoperability	7
48	3.3. Interoperability Between SAML 2.0 SSO and Liberty ID-WSF 1.1	7
49	3.4. General Interoperability Between SSO and ID-WSF	8
50	4. Using ID-WSF 1.x Service Specifications with ID-WSF 2.0	9
51	4.1. ResourceIDs	9
52	4.2. Action URIs	9
53	4.3. DST 2.0 Subscriptions	9
54	4.4. Example – Personal Profile Service	9
55	5. Examples	11
56	5.1. SAML 2.0 SSO with ID-WSF 1.1 and 2.0 Bootstraps	11
57	5.2. ID-FF 1.2 SSO with ID-WSF 1.1 and 2.0 Bootstraps	13
58	References	16

## 59 1. Introduction

60 As standards evolve, both in versions and in scope, it is necessary to adopt newer technologies. This poses problems  
61 in terms of already-provisioned federations as well as in using combinations of frameworks that were not foreseen at  
62 the time when the specifications were written.

63 This technote provides specific solutions to these advanced problems. For introductory material, see [[LibertyIDWS-  
64 FGuide10](#)].

### 65 1.1. Notational Conventions

66 In case of disagreement between the present document and any guidelines or [[XML](#)] schema descriptions, this  
67 document is prescriptive. Any published errata is hereby incorporated to this document by reference and as such  
68 is normative.

69 The key words "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT,"  
70 "RECOMMENDED," "MAY," and "OPTIONAL" in this specification are to be interpreted as described in IETF  
71 [[RFC2119](#)].

## 2. Name ID Compatibility Between SAML 1.x, ID-FF 1.x, and SAML 2.0

SAML assertions are the basis of most modern Single Sign-On (SSO) and Federation Frameworks. There is a frequent need to migrate already-existing federations between the different versions of SAML assertions or, indeed, serve from the same federation database, both SAML 2.0 [SAMLCore2] and SAML 1.1 [SAMLCore] assertions, simultaneously, as would be necessary in heterogeneous environments of partners supporting different versions of SAML.

Historically, Liberty ID-FF and, lately, SAML 2.0 have evolved towards a better understood and more coherent Name ID, or *pseudonym*, format and management system. The SAML 2.0 incarnation represents the current culmination of this evolution. While the Name ID format varies between SAML versions and while the additional semantics attached by various Liberty ID-FF versions vary, as well, it is possible to define a least common denominator format. In this discussion, we are mainly concerned with pseudonyms because they are characteristically used in federation databases. Other formats, such as temporary Name IDs, do not present similar problems.

By adopting the conventions described below, it is possible to support many types of federation protocols from one federation database.

### 2.1. An Introduction to Name IDs

A SAML 1.1 `<NameIdentifier>` carries `NameQualifier` and `Format` [XML] attributes. See [SAMLCore] Section 2.4.2.2 "Element `<NameIdentifier>`," p. 18.

A SAML 2.0 `<NameID>`, which is of XSD type `NameIDType`, carries `NameQualifier`, `SPNameQualifier`, `Format`, and `SPProvidedID` [XML] attributes. See [SAMLCore2], Section 2.2.2 "Complex Type `NameIDType`," p. 13.

Liberty ID-FF 1.2 [LibertyProtSchema], Section 3.1.11.1 "Deprecation of ID-FF 1.1 Name Identifier Practices," discusses some problems that older versions of the specifications have with respect to Name IDs.

### 2.2. NameQualifiers Across Versions

For each federation, the IdP always assigns a Name ID for the Principal, but it is qualified by the namespace of the SP towards which the Principal is federated. By convention, the namespace qualification is expressed by carrying the Provider ID or Entity ID of the SP, or the *affiliation* to which the SP belongs, in the `NameQualifier`. Both versions of SAML assertions work the same in this regard.

Versions of ID-FF prior to 1.2 did not support affiliations and did not require any *NameQualifier* to be specified, but, unfortunately, allowed it to be specified without specifying what the allowable values were. If an old federation has a nonstandard `NameQualifier`, then that should be kept in a database and reproduced when using Liberty ID-FF 1.0 or 1.1 protocols. However, when talking Liberty ID-FF 1.2 or SAML 2.0 protocol, the old `NameQualifier` MUST be ignored and the Provider ID or Entity ID used instead.

For each federation, it is possible for the SP to register an additional Name ID, which will be sent back to the SP whenever the IdP talks to the SP about the given federation. However, Liberty ID-FF 1.2 and SAML 2.0 behave differently in this regard. In SAML 2.0, the SP Name ID is always carried in `SPProvidedID`, which can be namespace-qualified using `SPNameQualifier`, which contains the affiliation ID of the SP, if any, or, otherwise, the entity ID of the SP.

ID-FF 1.x extended the SAML Subject to add an `IDPProvidedNameIdentifier` element in addition to `<NameIdentifier>`. In the case where there is no SP-provided Name ID, then both `Subject/NameIdentifier` and `Subject/IDPProvidedNameIdentifier` are the IdP-provided Name ID. In the case where there is an SP-provided Name ID, it goes in `Subject/NameIdentifier` and `Subject/IDPProvidedNameIdentifier` is the IdP-provided Name ID.

114 In SAML 1.1, there is no special way to express the SP-registered Name ID. By convention, in communications  
115 towards the SP, the <NameIdentifier> contains (properly namespace-qualified) the SP-registered Name ID, if any, or,  
116 otherwise, the IdP-assigned Name ID. In communications towards the IdP, the <NameIdentifier> always carries the  
117 IdP-assigned Name ID.

118 NameQualifier and Format in an ID-FF SP-provided Name ID is discarded when translating to SAML 2.0 unless  
119 they happen to correspond to the SAML 2.0-specified values. Clearly, this could be problematic and, practically, it  
120 restricts interoperability to the cases where implementations are not dependent on these values being preserved. ID-FF  
121 1.x deployments that are using these features may need to take the step of updating their federations to be SAML  
122 2.0-compatible before attempting migration or interoperability.

123 In various versions of Liberty ID-FF, different rules, which may or may not differ from the base convention, apply to  
124 what is appropriate to carry in the <NameIdentifier> when using the Name ID Registration protocol. Understanding  
125 these is left as an exercise to the reader.

126 **Conclusion:** NameQualifiers are interoperable between SAML 2.0, Liberty ID-FF 1.2, and SAML  
127 1.1. Earlier versions of Liberty ID-FF require special case treatment.

## 128 2.3. Name ID Formats

129 In SAML, a Name ID may have different formats. Of interest here is the *pseudonymous* format, a.k.a. *persistent*  
130 format. SAML 1.1 [SAMLCore], Section 7.3 "NameIdentifier Format Identifiers," p. 49, does not specify  
131 this format, but Liberty ID-FF 1.2 [LibertyProtSchema], Section 3.2.2.3 "SubjectType and Related Types," p. 18,  
132 specifies urn:liberty:iff:nameid:federated and, in Section 3.2.1.1 "Element <AuthnRequest>," p. 14,  
133 a corresponding <NameIDPolicy> enumerator federated. SAML 2.0 [SAMLCore2], Section 8.3.7 "Persistent  
134 Identifier," p. 79, specifies urn:oasis:names:tc:SAML:2.0:nameid-format:persistent and also specifies,  
135 in Section 3.4.1.1 "Element <NameIDPolicy>," p. 50, that the same enumerator is used as NameIDPolicy.

136 We adopt the convention that urn:liberty:iff:nameid:federated and urn:oasis:names:tc:SAML:2.0:  
137 nameid-format:persistent are treated synonymously such that if a federation database has a Name ID in the  
138 former format, it MUST be reported in SAML 2.0 transactions as the latter format, and if a database has a Name ID in  
139 the latter format, it MUST be reported in SAML 1.1 or Liberty ID-FF transactions as the former format.

140 We also adopt the convention that ID-FF 1.2 urn:liberty:iff:nameid:one-time is mapped to  
141 urn:oasis:names:tc:SAML:2.0:nameid-format:transient and vice versa, as needed.

142 Both versions of SAML specify the Name ID as xs:string, thus, the actual value of the Name ID does NOT  
143 have compatibility issues. However, we RECOMMEND that Name IDs be URIs for improved compatibility and be  
144 restricted to the character set of safe base 64 encoding [RFC3548] for maximum compatibility.

145 **Conclusion:** Name ID Formats are interoperable by treating *federated* (ID-FF) and *persistent*  
146 (SAML 2.0) as equivalent.

## 3. Independence of SSO (a.k.a. Federation) Framework from WS Framework

### 3.1. Guidance for Cross Use of SSO and WS Frameworks

Single Sign-On (SSO) frameworks (often referred to as Federation Frameworks), such as SAML 2.0 [SAMLCore2] and Liberty ID-FF 1.2 [LibertyProtSchema], are nearly entirely disjoint from Identity Web Services frameworks such as Liberty ID-WSF 1.0, ID-WSF 1.1 [LibertyIDWSFGuide10], and ID-WSF 2.0 [LibertyIDWSFGuide]. The only connection occurs when, as part of an SSO, a *discovery bootstrap* is conveyed. Therefore, it is desirable to decouple the choice of SSO framework from the choice of Identity Web Services frameworks.

Each framework makes an independent choice of the version of SAML assertions that is used within its own sphere. A different version can be profitably used in each sphere, thus all combinations in the accompanying table are valid. However, Liberty ID-FF 1.2 with ID-WSF 2.0, but only using SAML 1.1 assertions for both, is NOT valid. Similarly, SAML 2.0 with ID-WSF 1.1, but only using SAML 2.0 assertions for both, is not valid.

**Table 1. Valid Combinations of Frameworks and SAML versions: SSO Assertion Version (Bootstrap Assertion Version)**

	ID-WSF 1.1	ID-WSF 2.0
SAML 2.0 protocol	SAML 2.0 ( SAML 1.1 )	SAML 2.0 ( SAML 2.0 )
Liberty ID-FF 1.2	SAML 1.1 ( SAML 1.1 )	SAML 1.1 ( SAML 2.0 )

The SSO operation results in a Federation framework-dependent version of a SAML assertion that carries an ID-WSF version-dependent SAML assertion. All versions of SAML assertions support attribute statements and an attribute statement<sup>1</sup> is capable of carrying an arbitrary payload. There is no problem in the inner assertion being of a different version than the assertion carrying the attribute statement. Implementations wishing to support cross operation will simply need to support multiple versions of SAML.

### 3.2. Trivial Interoperability

Interoperability of Liberty ID-FF 1.2 with Liberty ID-WSF 1.1 is described in [LibertyDisco12], Section 6 "SAML AttributeDesignator for Discovery ResourceOffering."

Interoperability of Liberty ID-FF 1.2 and SAML 2.0 with Liberty ID-WSF 2.0 is described in [LibertyDisco].

### 3.3. Interoperability Between SAML 2.0 SSO and Liberty ID-WSF 1.1

It turns out that Liberty ID-WSF 1.1 in [LibertyDisco12], Section 6 "SAML AttributeDesignator for Discovery ResourceOffering," p. 23, appears to have an unnecessary restriction hampering interoperability in that the namespace prefix `saml`: actually is bound to SAML 1.1. There is no need to make this restriction.

To carry a Liberty ID-WSF 1.1 bootstrap in a SAML 2.0 SSO assertion, the following convention is adopted.

- The `Attribute/@Name` MUST be "urn:liberty:disco:2003-08:DiscoveryResourceOffering."
- The `Attribute/@NameFormat` MUST be "urn:oasis:names:tc:SAML:2.0:attrname-format:uri."
- One or more `<AttributeValue>` elements MUST be included and each of them MUST contain a single `<ResourceOffering>` (usually referring to a Discovery Service).

<sup>1</sup>For ID-WSF 1.x, the security token is carried in `Advice`, not in the attribute value.

- 178 • The **<ResourceOffering>** that is inside the **<AttributeStatement>** may contain **<CredentialRef>** elements  
179 referring to credentials that are necessary to access the service. These IDs SHOULD resolve to an [\[XML\]](#)  
180 element contained within the `Advice` element of the SSO assertion.

### 181 Example

```
182 <saml2:Attribute  
183   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
184   Name="urn:liberty:disco:2003-08:DiscoveryResourceOffering">  
185   <sb1:ResourceOffering> ... </sb1:ResourceOffering>  
186 </saml2:Attribute>  
187  
188
```

189 **Conclusion:** Interoperability is achieved by treating SAML 1.1 `AttributeName` and  
190 `AttributeNameSpace` fields as SAML 2.0 `Attribute/@Name` and `Attribute/@NameFormat`  
191 fields, respectively. The bootstrap attribute name value and format value are determined by the  
192 respective Liberty ID-WSF specifications.

## 193 3.4. General Interoperability Between SSO and ID-WSF

194 In general, any SSO protocol that can carry generic attributes can be used with ID-WSF by embedding the bootstrap  
195 as an attribute. The attribute name and name format should respect what is defined in respective ID-WSF bootstrap  
196 specifications.

197 For the specific case of ID-WSF 1.x, where the credential is not carried in an attribute but rather in the `Advice`, the  
198 putative SSO - ID-WSF cross operation scheme needs to specify a specific solution such as a special `credential`  
199 attribute.

200 For those developing new such mappings, please keep the Liberty Alliance up to date on such through Liberty's  
201 [\[LibertyFeedback\]](#) process. Such submissions will be reviewed in light of adding them here.

---

## 202 4. Using ID-WSF 1.x Service Specifications with ID-WSF 2.0

203 ID-WSF 1.x service specifications may be readily adapted for use within the ID-WSF 2.0 framework by following the  
204 guidelines in this chapter.

### 205 4.1. ResourceIDs

206 When constructing messages according to the ID-WSF 1.x service specification, use urn:liberty:isf:implied-  
207 resource for the ResourceID. In the case that the service specification makes ResourceID optional, and defaults to  
208 urn:liberty:isf:implied-resource, then the ResourceID element should be omitted.

### 209 4.2. Action URIs

210 For each message defined by the service specification, construct the action URI for that message by taking the  
211 namespace qualified name of the message element (i.e., the element that will be placed in the SOAP Body) and  
212 concatenating the namespace with the element name, separated by ":".

### 213 4.3. DST 2.0 Subscriptions

214 DST 2.0 Subscription elements use the ID-WSF 1.1 ServiceInstanceUpdate structure to describe NotifyTo and  
215 NotifyEndedTo endpoints. When using DST 2.0 Subscription elements within the ID-WSF 2.0 framework, use the  
216 following mapping to/from the ID-WSF 2.0 EndpointReference representation of the endpoints:

- 217 • EPR/Address = ServiceInstanceUpdate/Endpoint
- 218 • EPR/Metadata/SecurityContext/SecurityMechID = ServiceInstanceUpdate/SecurityMechID
- 219 • EPR/Metadata/SecurityContext/Token = ServiceInstanceUpdate/Credential

### 220 4.4. Example – Personal Profile Service

221 For the ID-WSF 1.x Personal Profile service, the action URIs would be:

- 222 • urn:liberty:id-sis-pp:2003-08:Query
- 223 • urn:liberty:id-sis-pp:2003-08:QueryResponse
- 224 • urn:liberty:id-sis-pp:2003-08:Modify
- 225 • urn:liberty:id-sis-pp:2003-08:ModifyResponse

226 and a Query request might look like:

```
227 <S:Envelope xmlns:S="...">
228   <S:Header>
229     <sbf:Framework version="2.0"/>
230     <wsa:MessageID xmlns:wsa="...">...</wsa:MessageID>
231     <wsa:Action xmlns:wsa="...">urn:liberty:id-sis-pp:2003-08:Query</wsa:Action>
232     <sb:Sender xmlns:sb="..." providerID="http://wsc.com"/>
233     <wsse:Security>
234       ...
235     </wsse:Security>
236   </S:Header>
237   <S:Body>
238     <pp:Query xmlns:pp="urn:liberty:id-sis-pp:2003-08:Query">
239       <pp:QueryItem itemID="1">
240         <pp:Select>/pp:PP/pp:CommonName/pp:CN</pp:Select>
241       </pp:QueryItem>
242     </pp:Query>
243   </S:Body>
244 </S:Envelope>
245
```

## 5. Examples

The following two examples illustrate different combinations of Federation Frameworks and ID Web Services Frameworks. They also show how a Federation Frameworks can simultaneously support both ID Web Services Frameworks by simply returning two bootstraps.

### 5.1. SAML 2.0 SSO with ID-WSF 1.1 and 2.0 Bootstraps

```

251 <sa:Assertion
252   xmlns:sa="urn:oasis:names:tc:SAML:2.0:assertion"
253   ID="ARFamaI5TXCcPKchcZ_R"
254   IssueInstant="2006-03-10T01:31:12Z"
255   Version="2.0">
256   <sa:Issuer
257     Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
258     https://s-ps.liberty-iop.org:8881/idp.xml
259   </sa:Issuer>
260   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
261     <ds:SignedInfo>
262       <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
263       <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
264       <ds:Reference URI="#ARFamaI5TXCcPKchcZ_R">
265         <ds:Transforms>
266           <ds:Transform Algorithm="w3:xmldsig#enveloped-signature" />
267           <ds:Transform Algorithm="w3:xml-exc-c14n#" />
268         </ds:Transforms>
269       </ds:Reference>
270       <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
271       <ds:DigestValue>2siB09gKiQ3b9CimyCt8uHgxFXM=</ds:DigestValue>
272     </ds:SignedInfo>
273     <ds:SignatureValue>ZI0Vz...HrUu2o=</ds:SignatureValue>
274   </ds:Signature>
275   <sa:Subject>
276     <sa:NameID
277       Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
278       NameQualifier="https://s-ps.liberty-iop.org:8881/idp.xml">
279       PGCTWDFZmWApzRT_ZeOB4</sa:NameID>
280     <sa:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
281       <sa:SubjectConfirmationData
282         NotOnOrAfter="2006-03-10T01:41:11Z"
283         Recipient="https://s-ps.liberty-iop.org:8843/SP-A" />
284     </sa:SubjectConfirmation>
285   </sa:Subject>
286   <sa:Conditions NotBefore="2006-03-10T01:26:12Z" NotOnOrAfter="2006-03-10T01:41:12Z">
287     <sa:AudienceRestriction>
288       <sa:Audience>https://s-ps.liberty-iop.org:8843/sp.xml</sa:Audience>
289     </sa:AudienceRestriction>
290   </sa:Conditions>
291   <sa:AuthnStatement AuthnInstant="2006-03-10T01:31:12Z" SessionIndex="1141954271-1">
292     <sa:AuthnContext>
293       <sa:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password
294     </sa:AuthnContextClassRef>
295   </sa:AuthnContext>
296 </sa:AuthnStatement>
297 <sa:AttributeStatement>
298
299 <!-- ID-WSF 1.1 Bootstrap -->
300
301   <sa:Attribute
302     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
303     Name="urn:liberty:disco:2003-08:DiscoveryResourceOffering">
304     <sa:AttributeValue>
305       <disco:ResourceOffering
306         xmlns:disco="urn:liberty:disco:2003-08"
307         entryID="2">
308         <disco:ResourceID>

```

```

309         https://s-ps.liberty-iop.org/profiles/WSF1.1/RID-DISCO-sue
310     </disco:ResourceID>
311     <disco:ServiceInstance>
312         <disco:ServiceType>urn:liberty:disco:2003-08</disco:ServiceType>
313         <disco:ProviderID>https://s-ps.liberty-iop.org:8881/idp.xml</disco:ProviderID>
314         <disco:Description>
315             <disco:SecurityMechID>
316                 urn:liberty:security:2005-02:TLS:Bearer
317             </disco:SecurityMechID>
318             <disco:Endpoint>https://s-ps.liberty-iop.org:8881/DISCO-S</disco:Endpoint>
319         </disco:Description>
320     </disco:ServiceInstance>
321     <disco:Abstract>Symlabs Discovery Service Team G</disco:Abstract>
322 </disco:ResourceOffering>
323 </sa:AttributeValue>
324 </sa:Attribute>
325
326 <!-- ID-WSF 2.0 Bootstrap -->
327
328     <sa:Attribute
329         Name="urn:liberty:disco:2005-11:DiscoveryEPR"
330         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
331         <sa:AttributeValue>
332             <wsa:EndpointReference xmlns:wsa="http://www.w3.org/2005/08/addressing" entryID="2">
333                 <wsa:Address>https://s-ps.liberty-iop.org:8881/DISCO-S</wsa:Address>
334                 <wsa:Metadata>
335                     <disco:Abstract xmlns:disco="urn:liberty:disco:2005-11">
336                         Symlabs Discovery Service Team G
337                     </disco:Abstract>
338                     <disco:ProviderID xmlns:disco="urn:liberty:disco:2005-11">
339                         https://s-ps.liberty-iop.org:8881/idp.xml
340                     </disco:ProviderID>
341                     <disco:ServiceType xmlns:disco="urn:liberty:disco:2005-11">
342                         urn:liberty:disco:2005-11
343                     </disco:ServiceType>
344                     <disco:SecurityContext xmlns:disco="urn:liberty:disco:2005-11">
345                         <disco:SecurityMechID>
346                             urn:liberty:security:2005-02:TLS:Bearer
347                         </disco:SecurityMechID>
348                         <sec:Token>
349                             <sa:Assertion
350                                 ID="CREDJjxfYtEabJY0VD5Mbf42"
351                                 IssueInstant="2006-03-10T01:31:12Z"
352                                 Version="2.0">
353                                 <sa:Issuer
354                                     Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
355                                     https://s-ps.liberty-iop.org:8881/idp.xml
356                                 </sa:Issuer>
357                                 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" >
358                                     <ds:SignedInfo>
359                                         <ds:CanonicalizationMethod
360                                             Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
361                                         <ds:SignatureMethod
362                                             Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
363                                         <ds:Reference URI="#CREDJjxfYtEabJY0VD5Mbf42">
364                                             <ds:Transforms>
365                                                 <ds:Transform Algorithm="w3:xmldsig#enveloped-signature" />
366                                                 <ds:Transform
367                                                     Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
368                                             </ds:Transforms>
369                                         <ds:DigestMethod
370                                             Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
371                                         <ds:DigestValue>AHzzZvqRH/su5755Tb30GmE8M4=</ds:DigestValue>
372                                     </ds:Reference>
373                                 </ds:SignedInfo>
374                                 <ds:SignatureValue>rABK91+1...N/CuiM=</ds:SignatureValue>
375                             </ds:Signature>

```

```

376         <sa:Subject>
377             <sa:NameID
378                 NameQualifier="https://s-ps.liberty-iop.org:8881/idp.xml" >
379                 915YxgPo2hrUzzq_hPtOzGSJ9StANPPCh5YweHbxxCE=
380             </sa:NameID>
381             <sa:SubjectConfirmation
382                 Method="urn:oasis:names:tc:SAML:2.0:cm: bearer" />
383         </sa:Subject>
384         <sa:Conditions
385             NotBefore="2006-03-10T01:26:12Z" NotOnOrAfter="2006-03-10T01:41:12Z">
386             <sa:AudienceRestriction>
387                 <sa:Audience>
388                     https://s-ps.liberty-iop.org:8843/sp.xml
389                 </sa:Audience>
390             </sa:AudienceRestriction>
391         </sa:Conditions>
392     </sa:Assertion>
393 </sec:Token>
394 </disco:SecurityContext>
395 </wsa:Metadata>
396 </wsa:EndpointReference>
397 </sa:AttributeValue>
398 </sa:Attribute>
399
400 </sa:AttributeStatement>
401 </sa:Assertion>
402
    
```

## 5.2. ID-FF 1.2 SSO with ID-WSF 1.1 and 2.0 Bootstraps

```

404 <saml:Assertion
405     xmlns:lib="urn:liberty:iff:2003-08"
406     xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
407     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
408     AssertionID="ARFAHo2R6kXmv9W9XrQM"
409     InResponseTo="RaUb5vfg_19khwnR4F0mW"
410     IssueInstant="2006-03-10T02:41:05Z"
411     Issuer="https://s-ps.liberty-iop.org:8881/idp.xml "
412     MajorVersion="1"
413     MinorVersion="2"
414     xsi:type="lib:AssertionType">
415     <saml:Conditions
416         NotBefore="2006-03-10T02:39:05Z"
417         NotOnOrAfter="2006-03-11T02:41:05Z">
418         <saml:AudienceRestrictionCondition>
419             <saml:Audience>
420                 https://s-ps.liberty-iop.org:8843/sp.xml
421             </saml:Audience>
422         </saml:AudienceRestrictionCondition>
423     </saml:Conditions>
424     <saml:AuthenticationStatement
425         AuthenticationInstant="2006-03-10T02:41:05Z"
426         AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password"
427         SessionIndex="1141958463-1"
428         xsi:type="lib:AuthenticationStatementType">
429         <saml:Subject
430             xsi:type="lib:SubjectType">
431             <saml:NameIdentifier
432                 Format="urn:liberty:iff:nameid:federated"
433                 NameQualifier="https://s-ps.liberty-iop.org:8843/sp.xml">PFAXR79p6NFy72j_nS7Xt
434             </saml:NameIdentifier>
435             <saml:SubjectConfirmation>
436                 <saml:ConfirmationMethod>
437                     urn:oasis:names:tc:SAML:1.0:cm: bearer</saml:ConfirmationMethod>
438             </saml:SubjectConfirmation>
439         </lib:IDPProvidedNameIdentifier
    
```

```

440         Format="urn:liberty:iff:nameid:federated"
441         NameQualifier="https://s-ps.liberty-iop.org:8843/sp.xml">
442         PFAXR79p6NFy72j_nS7Xt
443     </lib:IDPProvidedNameIdentifier>
444 </saml:Subject>
445 </saml:AuthenticationStatement>
446 <saml:AttributeStatement xsi:type="lib:AttributeStatementType" >
447     <saml:Subject xsi:type="lib:SubjectType">
448         <saml:NameIdentifier
449             Format="urn:liberty:iff:nameid:federated"
450             NameQualifier="https://s-ps.liberty-iop.org:8843/sp.xml">PFAXR79p6NFy72j_nS7Xt
451         </saml:NameIdentifier>
452         <saml:SubjectConfirmation>
453             <saml:ConfirmationMethod>
454                 urn:oasis:names:tc:SAML:1.0:cm:bearer</saml:ConfirmationMethod>
455             </saml:SubjectConfirmation>
456             <lib:IDPProvidedNameIdentifier
457                 Format="urn:liberty:iff:nameid:federated"
458                 NameQualifier="https://s-ps.liberty-iop.org:8843/sp.xml">PFAXR79p6NFy72j_nS7Xt
459             </lib:IDPProvidedNameIdentifier>
460         </saml:Subject>
461
462 <!-- ID-WSF 1.1 Bootstrap -->
463
464     <saml:Attribute
465         AttributeName="DiscoveryResourceOffering"
466         AttributeNamespace="urn:liberty:disco:2003-08">
467         <saml:AttributeValue>
468             <disco:ResourceOffering
469                 xmlns:disco="urn:liberty:disco:2003-08" entryID="2">
470                 <disco:ResourceID>
471                     https://s-ps.liberty-iop.org/profiles/WSF1.1/RID-DISCO-sue
472                 </disco:ResourceID>
473                 <disco:ServiceInstance>
474                     <disco:ServiceType>
475                         urn:liberty:disco:2003-08</disco:ServiceType>
476                     <disco:ProviderID>
477                         https://s-ps.liberty-iop.org:8881/idp.xml</disco:ProviderID>
478                     <disco:Description>
479                         <disco:SecurityMechID>urn:liberty:security:2005-02:TLS:Bearer
480                         </disco:SecurityMechID>
481                         <disco:Endpoint>
482                             https://s-ps.liberty-iop.org:8881/DISCO-S
483                         </disco:Endpoint>
484                     </disco:Description>
485                 </disco:ServiceInstance>
486                 <disco:Abstract>Symlabs Discovery Service Team G</disco:Abstract>
487             </disco:ResourceOffering>
488         </saml:AttributeValue>
489     </saml:Attribute>
490
491 <!-- ID-WSF 2.0 Bootstrap -->
492
493     <saml:Attribute
494         AttributeName="urn:liberty:disco:2005-11:DiscoveryEPR"
495         AttributeNamespace="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
496         <saml:AttributeValue>
497             <wsa:EndpointReference
498                 xmlns:wsa="http://www.w3.org/2005/08/addressing" entryID="2">
499                 <wsa:Address>
500                     https://s-ps.liberty-iop.org:8881/DISCO-S</wsa:Address>
501                 <wsa:Metadata>
502                     <disco:Abstract
503                         xmlns:disco="urn:liberty:disco:2005-11">
504                         Symlabs Discovery Service Team G</disco:Abstract>
505                     <disco:ProviderID
506                         xmlns:disco="urn:liberty:disco:2005-11">

```

```

507         https://s-ps.liberty-iop.org:8881/idp.xml</disco:ProviderID>
508     <disco:ServiceType
509         xmlns:disco="urn:liberty:disco:2005-11">urn:liberty:disco:2005-11
510     </disco:ServiceType>
511     <disco:SecurityContext xmlns:disco="urn:liberty:disco:2005-11">
512         <disco:SecurityMechID>urn:liberty:security:2005-02:TLS:Bearer
513         </disco:SecurityMechID>
514         <sec:Token>
515             <sa:Assertion
516                 xmlns:sa="urn:oasis:names:tc:SAML:2.0:assertion"
517                 ID="CRED7I6vzj8rGuoATD1QAYZG"
518                 IssueInstant="2006-03-10T02:41:04Z"
519                 Version="2.0">
520                 <sa:Issuer
521                     Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
522                     https://s-ps.liberty-iop.org:8881/idp.xml
523                 </sa:Issuer>
524                 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
525                     <ds:SignedInfo>
526                         <ds:CanonicalizationMethod
527                             Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
528                         <ds:SignatureMethod
529                             Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
530                         <ds:Reference URI="#CRED7I6vzj8rGuoATD1QAYZG">
531                             <ds:Transforms>
532                                 <ds:Transform
533                                     Algorithm="http://www.w3.org/2000/09/xmldsig
534 #enveloped-signature" />
535                                 <ds:Transform
536                                     Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
537                             </ds:Transforms>
538                             <ds:DigestMethod
539                                 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
540                             <ds:DigestValue>SQhsTDCK24L7QIqePR7va4BX4z4=</ds:DigestValue>
541                             </ds:Reference>
542                             <ds:SignatureValue>kmlM...N/F2Y=</ds:SignatureValue>
543                         </ds:SignedInfo>
544                         <sa:Subject>
545                             <sa:NameID
546                                 NameQualifier="https://s-ps.liberty-iop.org:8881/idp.xml">
547                                 gXw_-3PgHN7cTS4cxli17vFEGngSmfULfFHqJZnr_0Q=
548                             </sa:NameID>
549                             <sa:SubjectConfirmation
550                                 Method="urn:oasis:names:tc:SAML:2.0:cm:bearer" />
551                             </sa:Subject>
552                             <sa:Conditions
553                                 NotBefore="2006-03-10T02:36:04Z"
554                                 NotOnOrAfter="2006-03-10T02:51:04Z">
555                                 <sa:AudienceRestriction>
556                                     <sa:Audience>
557                                         https://s-ps.liberty-iop.org:8843/sp.xml
558                                     </sa:Audience>
559                                 </sa:AudienceRestriction>
560                             </sa:Conditions>
561                         </ds:Signature>
562                     </sa:Assertion>
563                 </sec:Token>
564             </disco:SecurityContext>
565         </wsa:Metadata>
566     </wsa:EndpointReference>
567 </saml:AttributeValue>
568 </saml:Attribute>
569
570 </saml:AttributeStatement>
571 </saml:Assertion>
572

```

---

## References

### Normative

- 575 [LibertyDisco] Hodges, Jeff, Cahill, Conor, eds. "Liberty ID-WSF Discovery Service Specification," Version 2.0,  
576 Liberty Alliance Project (30 July, 2006). <http://www.projectliberty.org/specs>
- 577 [LibertyDisco12] Sergent, Jonathan, eds. "Liberty ID-WSF Discovery Service Specification," Version 1.2, Liberty  
578 Alliance Project (12 December 2004). <http://www.projectliberty.org/specs/>
- 579 [LibertyProtSchema] Cantor, Scott, Kemp, John, eds. "Liberty ID-FF Protocols and Schema Specification," Version  
580 1.2-errata-v3.0, Liberty Alliance Project (14 December 2004). <http://www.projectliberty.org/specs>
- 581 [RFC2119] S. Bradner "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119, The Internet  
582 Engineering Task Force (March 1997). <http://www.ietf.org/rfc/rfc2119.txt>
- 583 [RFC3548] Josefsson, S., eds. (July 2003). "The Base16, Base32, and Base64 Data Encodings," RFC 3548, The  
584 Internet Engineering Task Force <http://www.ietf.org/rfc/rfc3548.txt>
- 585 [SAMLCore] Hallam-Baker, Phillip, Maler, Eve, eds. (05 November 2002). "SAML Core Assertions and Protocols,"  
586 SAML V1.0, OASIS Standard, Organization for the Advancement of Structured Information Standards  
587 <http://www.oasis-open.org/specs/index.php#samlv1.0>
- 588 [SAMLCore2] Cantor, Scott, Kemp, John, Philpott, Rob, Maler, Eve, eds. (15 March 2005). "Assertions  
589 and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0," SAML V2.0, OA-  
590 SIS Standard, Organization for the Advancement of Structured Information Standards [http://docs.oasis-  
open.org/security/saml/v2.0/saml-core-2.0-os.pdf](http://docs.oasis-<br/>591 open.org/security/saml/v2.0/saml-core-2.0-os.pdf)
- 592 [XML] Bray, Tim, Paoli, Jean, Sperberg-McQueen, C. M., Maler, Eve, Yergeau, Francois, eds. (04 February 2004).  
593 "Extensible Markup Language (XML) 1.0 (Third Edition)," Recommendation, World Wide Web Consortium  
594 <http://www.w3.org/TR/2004/REC-xml-20040204>

### Informative

- 596 [LibertyFeedback] Champagne, Darryl, Lockhart, Rob, eds. (2003). "Provide Comments and Questions about Liberty  
597 Specifications," Release 1.0, Liberty Alliance Project [http://www.projectliberty.org/specs/specs\\_comments\\_questions.asp](http://www.projectliberty.org/specs/specs_comments_questions.asp)
- 598 [LibertyIDWSFGuide10] Weitzel, David, eds. (22 May 2005). "Liberty ID-WSF Implementation Guideline," Draft  
599 v1.0-12, Liberty Alliance Project <http://www.projectliberty.org/specs/>
- 600 [LibertyIDWSFGuide] Weitzel, David, eds. "Liberty ID-WSF Implementation Guide," Version 2.0-02, Liberty  
601 Alliance Project (13 January, 2005). <http://www.projectliberty.org/specs>