



1

2 **Liberty ID-FF 1.2 Interoperability Conformance Testing**
3 **Procedures**

4 **Version 1.0-05**

5 **6 April 2004**

6 **Editors:**

7 Jeff Smith, Nippon Telegraph and Telephone Corporation

8 **Contributors:**

9 John Kemp, IEEE-ISTO
10 Jonathan Sergent, Sun Microsystems
11 Roger Sullivan, Phaos
12 Eric Tiffany, IEEE-ISTO

13 **Abstract:**

14
15 The conformance program is designed to validate core functionality via interoperability testing so that
16 purchasers of Liberty-based technology can focus on other details specific to their market and/or
17 deployment. This document describes the process and procedures for conducting interoperability testing
18 for conformance. The goal of this document, combined with the SCR and the Liberty Conformance Process
19 and Administration document is to unambiguously define the process and procedures that will be followed
20 at conformance interoperability testing events. The procedures in this document are intended to streamline
21 testing events, shorten testing times, and minimize disputes that could result in requests for arbitration.

22
23 File: lib-ceg-id-ff-1.2-conformance-testing-v1.0-02.pdf

24
25 Change log (to be deleted when published publicly):

26 1.0-01 2/9/04 JS Initial changes for ID-FF 1.2, separate doc for administrative process

27	1.0-02	3/1/04	JS	Updates based on email and conf call feedback. Baseline of tests for all profiles.
28	1.0.03	4/6/04	ET	Updated testing scripts and checklists for ID-FF 1.2. Other editorial cleanup.
29	1.0.04	5/5/04	ET	Modify guidance around IDP-Proxy interactions with SP for logout.
30	1.0.05	5/20/04	ET	Added steps to Extended profiles for Affiliation testing and IDP Proxy. Also added
31				guidance to Name ID Mapping section for post-interaction testing of decryption of
32				Name ID values.
33	1.0.06	6/14/04	ET	Update to order of Extended Test sequence. Corrected out-of-sequence repeated SSO
34				step in IDP sequence. Changed estimated time for basic profile to 30 minutes based
35				on empirical evidence.

36

37 **Contents**

38	1. Introduction	4
39	2. Overview of Conformance Process	6
40	3. Test Procedures.....	7
41	4. Checklists	18
42	5. Sample Testing Procedures (Reference)	22
43	6. References.....	26
44		

45 **1. Introduction**

46 This document currently refers only to ID-FF 1.2 and the conformance profiles described in the ID-FF 1.2 SCR
47 [LibertyIDFF12SCR].

48
49 The conformance program is designed to validate core functionality via interoperability testing so that
50 purchasers of Liberty-based technology can focus on other details specific to their market and/or deployment.
51 This document describes the process and procedures for conducting interoperability testing for conformance.
52 (Note: The interoperability testing described in this document is specific to testing conducted for the
53 conformance process i.e., “validation of implementations”. Other interoperability testing focused on validation of
54 specifications is to be considered separately from testing described here.)

55
56 The goal of this document, combined with the SCR and the Liberty Conformance Process and Administration
57 document is to unambiguously define the procedures that will be followed at conformance interoperability
58 testing events. The procedures in this document are intended to streamline testing events, shorten testing
59 times, and minimize disputes that could result in requests for arbitration.

60
61 The SCR describes a total of six conformance profiles and the specific features that are required or optional for
62 each profile. There are four core profiles derived from the original ID-FF 1.1 SCR (IDP, SP Basic, SP, LECP)
63 and two additional extended profiles specific to ID-FF 1.2 (IDP Extended, SP Extended). [Take text from SCR
64 regarding “core” profile + extended profile... implementation that claims extended profile conformance must
65 complete the appropriate core profile first.] The tables below summarizes the features that comprise the
66 profiles. A vendor can participate in conformance interoperability testing in the role of any one or more of these
67 conformance profiles.

68
69 This document is maintained by the Conformance Expert Group (CEG). Testing events are organized and
70 managed by the CEG. The Liberty Conformance Review Team (LCRT) is a sub-team of the Liberty Alliance
71 management board and will arbitrate any claims arising from testing events and shall act as an official observer
72 of testing events.

73 Table 1: Core Profiles Matrix

Feature	IDP	SP Basic	SP	LECP
Single Sign-On using Artifact Profile	MUST	MUST	MUST	
Single Sign-On using Browser POST Profile	MUST	MUST	MUST	
Single Sign-On using LECP Profile	MUST	MUST	MUST	MUST
Register Name Identifier (IdP Initiated) HTTP Redirect	OPTIONAL	MUST	MUST	
Register Name Identifier (IdP Initiated) SOAP/HTTP	OPTIONAL	OPTIONAL	MUST	
Register Name Identifier (SP Initiated) HTTP Redirect	MUST	MUST	MUST	
Register Name Identifier (SP Initiated) SOAP/HTTP	MUST	OPTIONAL	MUST	
Federation Termination Notification (IdP Initiated) HTTP Redirect	MUST	MUST	MUST	
Federation Termination Notification (IdP Initiated) SOAP/HTTP	MUST	OPTIONAL	MUST	
Federation Termination Notification (SP Initiated) HTTP Redirect	MUST	MUST	MUST	
Federation Termination Notification (SP Initiated) SOAP/HTTP	MUST	OPTIONAL	MUST	
Single Logout (IdP Initiated) - HTTP Redirect	MUST	MUST	MUST	
Single Logout (IdP Initiated) - HTTP GET	MUST	MUST	MUST	
Single Logout (IdP Initiated) – SOAP	MUST	OPTIONAL	MUST	
Single Logout (SP Initiated) - HTTP Redirect	MUST	MUST	MUST	
Single Logout (SP Initiated) - SOAP	MUST	OPTIONAL	MUST	
Identity Provider Introduction	MUST	OPTIONAL	OPTIONAL	
Backward Compatibility	OPTIONAL	OPTIONAL	OPTIONAL	

74
 75 Table 2: Extended Profile Matrix

Feature	IDP Extended	SP Extended
One-Time (Anonymous) Name Identifiers	MUST	MUST
Affiliations	MUST	MUST
Identity Provider Proxy	MUST	MUST
Name Identifier Mapping	MUST	MUST

76 **2. Overview of Conformance Process**

77 See [LibConfProc]

78 **3. Test Procedures**

79 Testing will follow a simple scenario based approach with multiple passes that test required features, and
80 optional features when support is indicated by the vendor in the Static Conformance Checklist. The basic
81 scenario is intended to simulate a full life-cycle of establishing and using a federated identity:

- 82 1. Metadata exchange for IdPs and SPs
- 83 2. Single Sign-On and Federation
- 84 3. Single logout
- 85 4. Single Sign-On already federated
- 86 5. Single logout
- 87 6. Federation termination

88
89 It will be necessary to repeat this scenario through several passes in order to test each of the profiles specified in
90 the SCR and the test process is designed to avoid repeating unnecessary steps to the extent possible.

91
92 In addition, for the extended profiles (IDP Extended, SP Extended) and also for implementations supporting the
93 optional backwards compatibility the above steps will be repeated as appropriate.

94
95 Each test item is indicated by an item number in the table below and the test procedure tables for each
96 conformance profile indicate the test item and the order in which the tests are to be performed.

97
98 Note: Even though test procedure tables for each conformance profile are listed in practice testing is
99 bidirectional (e.g. IDP \leftrightarrow SP) and both the IDP and SP being tested should be able to complete one of the two
100 minimum test runs simultaneously. **A full test run of a core profile takes approximately 30 minutes to complete**
101 **if everything goes smoothly.**

102
 103

Table 2. Test items

MTD	Metadata exchange	
SSO	Single Sign On	
SSO-1	<i>Artifact profile</i>	
SSO-1.1		New Federation
SSO-1.2		Federated
SSO-1.3		One-time/Anonymous
SSO-1.4		Affiliations
SSO-1.5		IDP Proxy
SSO-2	<i>Browser POST profile</i>	
SSO-2.1		New Federation
SSO-2.2		Federated
SSO-2.3		One-time/Anonymous
SSO-2.4		Affiliations
SSO-2.5		IDP Proxy
SSO-3	<i>LECP profile</i>	
SSO-3.1		New Federation
SSO-3.2		Federated
SLO	Single Logout	
SLO-1	<i>IDP initiated HTTP-Redirect</i>	
SLO-2	<i>IDP initiated HTTP-GET</i>	
SLO-3	<i>IDP initiated SOAP</i>	
SLO-4	<i>SP initiated HTTP-Redirect</i>	
SLO-5	<i>SP initiated SOAP</i>	
SLO-6	<i>SLO with Affiliation, SP initiated</i>	<i>(Do we need all variations above?)</i>
SLO-7	<i>SP initiated SOAP with IDP Proxy</i>	<i>(Does IDP init make sense?)</i>
FTN	Federation Termination	
FTN-1	<i>IDP initiated HTTP-Redirect</i>	
FTN-2	<i>IDP initiated SOAP/HTTP</i>	
FTN-3	<i>SP initiated HTTP-Redirect</i>	
FTN-4	<i>SP initiated SOAP/HTTP</i>	
FTN-5	<i>FTN with Affiliation</i>	<i>(Variations?)</i>
RNI	Register Name Identifier	
RNI-1	<i>IDP initiated HTTP-Redirect</i>	
RNI-2	<i>IDP initiated SOAP/HTTP</i>	
RNI-3	<i>SP initiated HTTP-Redirect</i>	
RNI-4	<i>SP initiated SOAP/http</i>	
RNI-5	<i>RNI with Affiliation</i>	
IPI	Identity Provider Introduction	
BCK	Backward Compatibility[†]	
ANN	One-time/Anonymous[†]	
AFF	Affiliations[†]	
IPP	Identity Provider Proxy[†]	

[†] These profiles are not associated with distinct test items or protocol messages. Instead, other test items (e.g. SSO and SLO) are constructed with optional parameters enabled or modified to achieve the test objective.

NIM	Name Identifier Mapping (do we need to repeat for all 3 crypto methods?)
NIM-1	<i>Name ID Mapping</i>
NIM-2	<i>Mapped Identifier Confirmation</i>

104

105 **3.1. IDP Profile test procedure**

106 An IDP is required to test each test item against (a minimum of) two SP and two LECP (for the LECP profile)
 107 implementations. Principal should have accounts at the SPs and IDP and be authenticated at the IDP in
 108 advance. Steps in grey are optional profiles.
 109

Step	Test item	Description
1	MTD	Metadata exchange (in-band not required)
2	SSO-1.1	SSO Artifact – new federation
3	SLO-1	SLO IDP-initiated HTTP-Redirect
4	SSO-1.2	SSO Artifact - federated
5	SLO-2	SLO IDP-initiated HTTP-GET
6	SSO any profile	SSO any profile
7	FTN-1	Federation Termination IDP-initiated HTTP-Redirect
8	SSO-2.1	SSO POST – new federation
9	SLO-3	SLO IDP-initiated SOAP
10	SSO-2.2	SSO POST - federated
11	SLO-4	SLO SP-initiated HTTP-Redirect
12	SSO any profile	SSO any profile
13	FTN-2	Federation Termination IDP-initiated SOAP/HTTP
14	SSO any profile	SSO any profile + federate
15	SLO-5	SLO SP-initiated SOAP
16	SSO any profile	SSO any profile
17	FTN-3	Federation Termination SP-initiated HTTP-Redirect
18	SSO any profile	SSO any profile + federate
19	FTN-4	Federation Termination SP-initiated SOAP/HTTP
20	SSO any profile	SSO any profile + federate
21	RNI-3	Name Registration SP-initiated HTTP-Redirect
22	SLO any profile	SLO any profile
23	SSO any profile	SSO any profile
24	SLO any profile	SLO any profile
25	SSO any profile	SSO any profile
26	RNI-4	Name Registration SP-initiated SOAP/HTTP
27	SLO any profile	SLO any profile
28	SSO any profile	SSO any profile
29	SLO any profile	SLO any profile
30	Login to IDP	IDP login w/cookie
31	IP	Identity Provider Introduction
32	SSO any profile	SSO any profile
33	RNI-1	Name Registration IDP-initiated HTTP-Redirect
34	SLO any profile	SLO any profile (SP-initiated)
35	SSO any profile	SSO any profile (confirm assertion has new name identifier)
36	SLO any profile	SLO any profile (IDP-initiated)
37	SSO any profile	SSO any profile
38	RNI-2	Name Registration IDP-initiated SOAP/HTTP
39	SLO any profile	SLO any profile (SP-initiated)
40	SSO any profile	SSO any profile (confirm assertion has new name identifier)
41	SLO any profile	SLO any profile (IDP-initiated)
42	SSO any profile	SSO any profile
43	FTN any profile	Federation Termination any profile
44	SSO 3.1	SSO LECP – new federation
45	SSO 3.2	SSO LECP – federated
Backwards Compatibility		
46	SSO any profile	SSO any profile – new federation using ID-FF 1.1

47	SLO any profile	SLO any profile
48	SSO any profile	SSO any profile – federated using ID-FF 1.2
49	FTN any profile	Federation Termination any profile
50	SSO any profile	SSO any profile + federate
51	RNI-3 or RNI-4	Name Registration SP-initiated HTTP-Redirect or SOAP/HTTP
52	SLO any profile	SLO any profile
53	SSO any profile	SSO any profile
54	SLO any profile	SLO any profile

110

111 **3.2. SP Basic Conformance Profile**

112 An SP Basic is required to test each test item against (a minimum of) two IDP and two LECP implementations.
 113 Principal should have accounts at the SP and IDPs and be authenticated at the IDP in advance. Steps in grey
 114 are optional profiles.

Step	Test item	Description
1	MTD	Metadata exchange (in-band not required)
2	SSO-1.1	SSO Artifact – new federation
3	SLO-1	SLO IDP-initiated HTTP-Redirect
4	SSO-1.2	SSO Artifact – federated
5	SLO-2	SLO IDP-initiated HTTP-GET
6	SSO any profile	SSO any profile
7	FTN-1	Federation Termination IDP-initiated HTTP-Redirect
8	SSO-2.1	SSO POST – new federation
9	SLO-4	SLO SP-initiated HTTP-Redirect
10	SSO-2.2	SSO POST - federated
11	SLO any profile	SLO any profile
12	SSO any profile	SSO any profile
13	FTN-3	Federation Termination SP-initiated HTTP-Redirect
14	SSO any profile	SSO any profile + federate
15	RNI-1	Name Registration IDP-initiated HTTP-Redirect
16	SLO any profile	SLO any profile (SP-initiated)
17	SSO any profile	SSO any profile
18	SLO any profile	SLO any profile (IDP-initiated)
19	SSO any profile	SSO any profile
20	RNI-3	Name Registration SP-initiated HTTP-Redirect
21	SLO any profile	SLO any profile (SP-initiated)
22	SSO any profile	SSO any profile
23	SLO any profile	SLO any profile (IDP-initiated)
24	RNI-2	Name Registration IDP-initiated SOAP/HTTP
25	SLO any profile	SLO any profile (SP-initiated)
26	SSO any profile	SSO any profile
27	SLO any profile	SLO any profile (IDP-initiated)
28	SSO any profile	SSO any profile
29	RNI-4	Name Registration SP-initiated SOAP/HTTP
30	SLO any profile	SLO any profile (SP-initiated)
31	SSO any profile	SSO any profile
32	SLO any profile	SLO any profile (IDP-initiated)
33	Login to IDP	IDP login w/cookie
34	IP	Identity Provider Introduction
35	SSO any profile	SSO any profile
36	FTN any profile	Federation Termination any profile
37	SSO 3.1	SSO LECP – new federation
38	SSO 3.2	SSO LECP – federated
Backwards compatibility		
39	SSO any profile	SSO any profile – new federation using ID-FF 1.1
40	SLO any profile	SLO any profile
41	SSO any profile	SSO any profile – federated using ID-FF 1.2
42	FTN any profile	Federation Termination any profile
43	SSO any profile	SSO any profile + federate
44	RNI-1 or RNI-3	Name Registration IDP-initiated or SP-initiated HTTP-Redirect
45	SLO any profile	SLO any profile (SP-initiated)
46	SSO any profile	SSO any profile
47	SLO any profile	SLO any profile (IDP-initiated)

115 **3.3. SP Complete Conformance Profile**

116 An SP Complete is required to test each test item against (a minimum of) two IDP and two LECP
 117 implementations. Principal should have accounts at the SP and IDPs and be authenticated at the IDP in
 118 advance. Steps in grey are optional profiles.
 119

Step	Test item	Description
1	MTD	Metadata exchange
2	SSO-1.1	SSO Artifact – new federation
3	SLO-1	SLO IDP-initiated HTTP-Redirect
4	SSO-1.2	SSO Artifact
5	SLO-2	SLO IDP-initiated HTTP-GET
6	SSO any profile	SSO any profile
7	FTN-1	Federation Termination IDP-initiated HTTP-Redirect
8	SSO-2.1	SSO POST – new federation
9	SLO-3	SLO IDP-initiated SOAP
10	SSO-2.2	SSO POST - federated
11	SLO-4	SLO SP-initiated HTTP-Redirect
12	SSO any profile	SSO any profile
13	FTN-2	Federation Termination IDP-initiated SOAP/HTTP
14	SSO any profile	SSO any profile + federate
15	SLO-5	SLO SP-initiated SOAP
16	SSO any profile	SSO any profile
17	FTN-3	Federation Termination SP-initiated HTTP-Redirect
18	SSO any profile	SSO any profile + federate
19	FTN-4	Federation Termination SP-initiated SOAP/HTTP
20	SSO any profile	SSO any profile + federate
21	RNI-1	Name Registration IDP-initiated HTTP-Redirect
22	SLO any profile	SLO any profile (SP-initiated)
23	SSO any profile	SSO any profile
24	SLO any profile	SLO any profile (IDP-initiated)
25	SSO any profile	SSO any profile
26	RNI-2	Name Registration IDP-initiated SOAP/HTTP
27	SLO any profile	SLO any profile (SP-initiated)
28	SSO any profile	SSO any profile
29	SLO any profile	SLO any profile (IDP-initiated)
30	SSO any profile	SSO any profile
31	RNI-3	Name Registration SP-initiated HTTP-Redirect
32	SLO any profile	SLO any profile (SP-initiated)
33	SSO any profile	SSO any profile
34	SLO any profile	SLO any profile (IDP-initiated)
35	SSO any profile	SSO any profile
36	RNI-4	Name Registration SP-initiated SOAP/HTTP
37	SLO any profile	SLO any profile (SP-initiated)
38	SSO any profile	SSO any profile
39	SLO any profile	SLO any profile (IDP-initiated)
40	Login to IDP	IDP login w/cookie
41	IP	Identity Provider Introduction
42	SSO any profile	SSO any profile
43	FTN any profile	Federation Termination any profile
44	SSO 3.1	SSO LECP – new federation
45	SSO 3.2	SSO LECP – federated
Backwards compatibility		
46	SSO any profile	SSO any profile – new federation using ID-FF 1.1

47	SLO any profile	SLO any profile
48	SSO any profile	SSO any profile – federated using ID-FF 1.2
49	FTN any profile	Federation Termination any profile
50	SSO any profile	SSO any profile + federate
51	RNI any profile	Name Registration any profile
52	SLO any profile	SLO any profile (SP-initiated)
53	SSO any profile	SSO any profile
54	SLO any profile	SLO any profile (IDP-initiated)

120

121 **3.4. LECP Conformance Profile**

122 A LECP is required to test each test item against (a minimum of) two IDP and two SP implementations.
123 Principal should have accounts at the SP and IDPs and must be authenticated at the IDP in advance.
124

Step	Test item	Description
1	SSO 3.1	SSO LECP – new federation
2	SSO 3.2	SSO LECP - federation

125
126

127 **3.5. IDP Extended Conformance Profile**

128 An IDP is required to test each test item against (a minimum of) two SP implementations. Principal should have
 129 accounts at the SPs and IDP and be authenticated at the IDP in advance. Successful completion of the IDP
 130 conformance profile is a prerequisite for the IDP Extended conformance profile.

Step	Test item	Description
1	SSO 1.3 or 2.3	SSO Artifact or POST with one-time/anonymous
2	SLO any profile	SLO any profile
3	SSO any profile	SSO any profile
4	NMI-1	Encrypted Name ID Mapping (initiated at SPa)
5	NMI-2	SP partner checks encryption validity at SPb
6	SSO-1.5 or 2.5	SSO Artifact or POST with IDP Proxy (Test IDP is relay)
7	SLO-7	SLO SP initiated SOAP with IDP Proxy (Test IDP is relay)
8	SSO 1.4 or 2.4	SSO Artifact or POST with affiliations – new federation (SPa)
9	SLO-6	SLO any profile with affiliation
10	SSO 1.4 or 2.4	SSO Artifact or POST with affiliations – federated (SPb)
11	RNI-5	RNI with affiliation
12	FTN-5	FTN with affiliation

131 **3.5.1. One-Time/Anonymous**

132 Requires SPa, IDP from different vendors.

133 **3.5.2. Affiliations**

134 Requires SPa, SPb, and IDP. SPa and SPb provided by single vendor because Liberty does not specify how
 135 affiliations are established between service providers.

136 **3.5.3. IDP Proxy**

137 Requires IDPa (relaying IDP), IDPb (authenticating IDP), and SP. To properly test an IDP a vendor will be
 138 required to test as IDPa (other vendor is IDPb and SP).

139 Note that due to an omission in the protocol spec, the Proxying IDP interaction with the SP during single logout
 140 MUST be conducted using the SOAP profile. The Proxying IDP interacts with the Target IDP using SOAP, and
 141 there is no mechanism to indicate that the SP only supports the http profiles.

142 [“Will” and “will not” proxy not tested. Also RNI, and combination of IDP Proxy with affiliations and
 143 anonymous/one-time will not be tested. Enforcement of proxy-count not tested.]

144 **3.5.4. Name Identifier Mapping**

145 Requires SPa, SPb, and IDP. To properly test SPa and IDP are from different vendors (SPa and SPb must be
 146 from same vendor). SPa and SPb should already be federated with the IDP

147 Though encryption is not required by the specifications, the SCR requires that encryption be demonstrated for
 148 conformance. The XML Encryption standard referenced in the SCR requires that three encryption standards be
 149 supported: Triple-DES, AES 128 and AES 256. At least one of these must be supported by both vendors

150 The testing requires that the IDP correctly map and encrypt a name identifier from SPb so it can be used by
 151 SPa to interact with SPb. For purposes of testing, the encrypted Name ID obtained at SPa should be decrypted
 152 at SPb to demonstrate that the identifier is correct. The method for transferring, decrypting, and comparing the
 153 identifier is not specified by Liberty.

154 **3.6. SP Extended Conformance Profile**

155 An SP is required to test each test item against (a minimum of) two IDP implementations. Principal should have
 156 accounts at the SPs and IDP and be authenticated at the IDP in advance. Successful completion of one of the
 157 SP conformance profiles (SP or SP Basic) is a prerequisite for the SP Extended conformance profile. It is
 158 unlikely that an SP Basic will qualify for SP Extended as SOAP/HTTP is required in some portions of the SP
 159 Extended conformance profile

Step	Test item	Description
1	SSO 1.3 or 2.3	SSO Artifact or POST with one-time/anonymous
2	SLO any profile	SLO any profile
3	SSO any profile	SSO any profile
4	NMI-1	Encrypted Name ID Mapping (initiated at SPa)
5	NMI-2	SP partner checks encryption validity at SPb
6	SSO-1.5 or 2.5	SSO Artifact or POST with IDP Proxy (Test IDP is relay)
7	SLO-7	SLO SP initiated SOAP with IDP Proxy (Test IDP is relay)
8	SSO 1.4 or 2.4	SSO Artifact or POST with affiliations – new federation (SPa)
9	SLO-6	SLO any profile with affiliation
10	SSO 1.4 or 2.4	SSO Artifact or POST with affiliations – federated (SPb)
11	RNI-5	RNI with affiliation
12	FTN-5	FTN with affiliation

160 **3.6.1. One-time/Anonymous**

161 Requires SPa and IDP from different vendors.

162 **3.6.2. Affiliations**

163 Requires SPa, SPb, and IDP. SPa and SPb provided by single vendor.

164 **3.6.3. IDP Proxy (IPP)**

165 Requires IDPa (relaying IDP), IDPb (authenticating IDP), and SP. To properly test an SP a vendor will be
 166 required to test as SP (other vendor is IDPa and IDPb).

167 Note that due to an omission in the protocol spec, the Proxying IDP interaction with the SP during single logout
 168 MUST be conducted using the SOAP profile. The Proxying IDP interacts with the Target IDP using SOAP, and
 169 there is no mechanism to indicate that the SP only supports the http profiles.

170 [“Will” and “will not” proxy not tested. Also RNI, and combination of IDP Proxy with affiliations and
 171 anonymous/one-time will not be tested. Enforcement of proxy-count not tested]

172 **3.6.4. Name Identifier Mapping (NIM)**

173 Encryption is required in SCR (even though it is SHOULD encrypt in the specification).

174 Requires SPa (initiating SP), SPb (target SP), and IDP. To properly test SPa and IDP must be from different
 175 vendors (SPb should be from same vendor as SPa – to properly test encryption).

176 The testing requires that the IDP correctly map and encrypt a name identifier from SPb so it can be used by
 177 SPa to interact with SPb. For purposes of testing, the encrypted Name ID obtained at SPa should be decrypted
 178 at SPb to demonstrate that the identifier is correct. The method for transferring, decrypting, and comparing the
 179 identifier is not specified by Liberty.

180 **4. Checklists**

181 **4.1. Static Conformance Checklist**

182 The product name is simply an identifier; it does not have to be the public name of the product.

Product Name			
Version (major.minor)			
Implementation Type(s)	SP Basic	SP Complete	SP Extended
	IDP	IDP Extended	LECP
Company			
Contact Name			
Contact Phone			
Contact Email			

183 Please indicate in the any optional features to be tested by circling OPTIONAL as appropriate.

Feature	IDP	SP Basic	SP	LECP
Single Sign-On using Artifact Profile	MUST	MUST	MUST	
Single Sign-On using Browser POST Profile	MUST	MUST	MUST	
Single Sign-On using LECP Profile	MUST	MUST	MUST	MUST
Register Name Identifier (IdP Initiated) HTTP Redirect	OPTIONAL	MUST	MUST	
Register Name Identifier (IdP Initiated) SOAP/HTTP	OPTIONAL	OPTIONAL	MUST	
Register Name Identifier (SP Initiated) HTTP Redirect	MUST	MUST	MUST	
Register Name Identifier (SP Initiated) SOAP/HTTP	MUST	OPTIONAL	MUST	
Federation Termination Notification (IdP Initiated) HTTP Redirect	MUST	MUST	MUST	
Federation Termination Notification (IdP Initiated) SOAP/HTTP	MUST	OPTIONAL	MUST	
Federation Termination Notification (SP Initiated) HTTP Redirect	MUST	MUST	MUST	
Federation Termination Notification (SP Initiated) SOAP/HTTP	MUST	OPTIONAL	MUST	
Single Logout (IdP Initiated) - HTTP Redirect	MUST	MUST	MUST	
Single Logout (IdP Initiated) - HTTP GET	MUST	MUST	MUST	
Single Logout (IdP Initiated) – SOAP	MUST	OPTIONAL	MUST	
Single Logout (SP Initiated) - HTTP Redirect	MUST	MUST	MUST	
Single Logout (SP Initiated) - SOAP	MUST	OPTIONAL	MUST	
Identity Provider Introduction	MUST	OPTIONAL	OPTIONAL	

Backward Compatibility	OPTIONAL	OPTIONAL	OPTIONAL	
------------------------	----------	----------	----------	--

184 There are no optional features in the extended profiles, but the required features are indicated below. Note that
 185 IDP Extended and SP Extended profiles implicitly included one of the corresponding IDP or SP profiles above.

Feature	IDP Extended	SP Extended
One-Time (Anonymous) Name Identifiers	MUST	MUST
Affiliations	MUST	MUST
Identity Provider Proxy	MUST	MUST
Name Identifier Mapping	MUST	MUST

186 **4.2. Testing Checklist**

187 This form must be completed for each complete test run. Both parties to the test must agree to the indication of
 188 pass/fail for each feature tested and sign each copy of the form. A copy of the form will go to each testing party
 189 and the original will be kept on record by LCRT/ISTO.

190 The product name is simply an identifier; it does not have to be the public name of the product.

IDP Tester	
Product Name	
Version (major.minor)	
Implementation Type(s)	IDP IDP Extended
Company	
Contact Name	
Contact Phone	
Contact Email	
Signature (after testing)	

191

SP Tester	
Product Name	
Version (major.minor)	
Implementation Type(s)	SP Basic SP Complete SP Extended
Company	
Contact Name	
Contact Phone	
Contact Email	
Signature (after testing)	

192

LECP Tester	
Product Name	
Version (major.minor)	
Company	
Contact Name	
Contact Phone	
Contact Email	
Signature (after testing)	

193

LCRT Representative	
Contact Name	
Signature (after testing)	

194

Date of testing	
-----------------	--

195 Testing Checklist page 2
 196

Profile/Description	Test item	Pass/Fail
Metadata Exchange		
Exchange metadata	MTD	
Single Sign-On		
Artifact Profile	SSO-1.1	
	SSO-1.2	
Browser POST Profile	SSO-2.1	
	SSO-2.2	
LECP Profile	SSO-3.1	
	SSO-3.2	
Register Name Identifier		
IDP initiated HTTP-Redirect	RNI-1	optional (IDP)
IDP initiated SOAP/HTTP	RNI-2	optional (IDP and SP Basic)
SP initiated HTTP-Redirect	RNI-3	
SP initiated SOAP/HTTP	RNI-4	optional (SP Basic)
Federation Termination Notification		
IDP initiated HTTP-Redirect	FTN-1	
IDP initiated SOAP/HTTP	FTN-2	optional (SP Basic)
SP initiated HTTP-Redirect	FTN-3	
SP initiated SOAP/HTTP	FTN-4	optional (SP Basic)
Single Logout		
IDP initiated HTTP-Redirect	SLO-1	
IDP initiated HTTP-GET	SLO-2	
IDP initiated SOAP	SLO-3	optional (SP Basic)
SP initiated HTTP-Redirect	SLO-4	
SP initiated SOAP	SLO-5	optional (SP Basic)
Identity Provider Introduction		
IDP Introduction Cookie	IPI	optional (SP)
Backward Compatibility		
Backward Compatibility Sequence	BCK	optional (all)
One-Time/Anonymous		
Anonymous login sequence	ANN	
Affiliations		
Affiliation SSO/SLO/RNI/FTN sequence	AFF	
IDP Proxy		
Proxy SSO/SLO Sequence	IPP	
Name Identifier Mapping		
Name ID Mapping Sequence	NIM	

197

IDP Tester Signature	SP Tester Signature	LECP Tester Signature	LCRT Signature
Date			

198 **5. Sample Testing Procedures (Reference)**

199 *Note: This section has not been updated to include the changes for IDFF 1.2 or the extended profiles*
200

201 **5.1. Introduction**

202 Below are sample testing procedures taken. This content is provided as reference only and may not be
203 appropriate for all implementations.
204

205 **5.2. Metadata and configuration**

206 The service provider and identity provider under test should exchange Liberty metadata in the form of XML files.
207 The service provider should provide a file containing an SPDescriptor element, and the identity provider should
208 provide a file containing an IDPDescriptor element. The files should be validated using a test tool to conform
209 with the schema and the rules outlined in the protocols and schemas document. The files should include X.509
210 certificates containing the public keys which are used by the providers to sign messages. It is not a
211 requirement that the implementations automatically generate or parse these files; the human associated with
212 the implementation may generate or process the XML file by hand if necessary.
213

214 The test environment should include:

215 The service provider under test.

216 The identity provider under test.

217 A known good service provider which supports all of the single logout profiles to be tested.

218 A known good identity provider which supports the identity provider introduction protocol.

219 DNS infrastructure to establish a common introduction domain for at least the two identity providers and the
220 service provider under test.

221 One or more clients which the service provider and identity provider under test claim to support for the profiles
222 under test.

223 Network sniffing tool which can capture all traffic between the providers and between the client and the
224 providers. The tool must be capable of decrypting SSL conversations given the private keys of the providers'
225 HTTP servers.
226

227 **5.3. Single sign-on and federation protocol**

228 **5.3.1. Common steps**

229 The following steps apply for several profiles and are provided here for reference.

230 Create accounts offline on IDP and SP, initialized without federations.

231 Start "clean" browser (without pre-existing cookies)

232 Log in to SP and access user interface for federating with an identity provider.

233 Choose to federate the identity provider under test.

234 SP should send a valid AuthnRequest to the IDP. Capture this request using profile-specific means and log it.

235 Navigate through IDP user interface to authenticate to the IDP and consent to the federation, if necessary.

236 IDP should redirect browser back to SP and send response back to SP. Capture this profile-specific data
237 exchange and log it.

238 User should be successfully federated with SP now. Use SP user interface and IDP user interface to verify that
239 the federation is known by both sides, if possible.

240 (Single sign-on test procedure starts here.) Start a new "clean" browser.

241 Log in to the IDP site.

242 Visit SP site and access user interface for single sign-on with the IDP, complete sign-on. SP should have
243 redirected the browser using a valid AuthnRequest URL (capture and log); IDP should have responded with
244 valid profile-specific response data (capture and log).

245 Verify that the user is signed in to the SP.

246 Start a new "clean" browser.

247 Visit SP site and access user interface for single sign-on with the IDP.

248 Browser should redirect using valid AuthnRequest URL (capture and log).
249 Authenticate to IDP.
250 IDP should send response to SP (capture and log).
251 Verify that the user is signed in to the SP.

252 **5.3.2. Browser artifact profile**

253 Follow common steps as in 3.1.

254 **5.3.3. Browser post profile**

255 Follow common steps as in 3.1.

256 **5.3.4. Liberty-enabled client/proxy profile**

257 Follow common steps as in 3.1. (Note that some of the identity provider selection and authentication user
258 interface may come from the client instead of from the identity provider.)

259 **5.4. Single log-out**

260 **5.4.1. Common steps for SP-initiated single log-out**

261 The following steps apply for several profiles and are provided here for reference.

262
263 Prerequisite: successfully test single sign-on with at least one profile.
264 Log in to the IDP.
265 Use the single sign-on protocol, in any profile, to sign in to the service provider via the IDP.
266 Use the single sign-on protocol to sign in to one other known good service provider.
267 Access the single log-out UI at the service provider under test and initiate logout.
268 The service provider sends a logout message to the IDP. The IDP forwards the logout message to the other
269 service provider. Capture and log these messages.
270 Verify that the user is no longer signed in at the IDP or at either of the service providers.

271 **5.4.2. SOAP-based SP-initiated single log-out**

272 Follow common steps as in 4.1.

273 **5.4.3. HTTP-redirect-based SP-initiated single log-out**

274 Follow common steps as in 4.1.

275 **5.4.4. Common steps for IDP-initiated single logout**

276 The following steps apply for several profiles and are provided here for reference.

277
278 Prerequisite: successfully test single sign-on with at least one profile.
279 Log in to the IDP.
280 Use the single sign-on protocol, in any profile, to sign in to the service provider via the IDP.
281 Access the single log-out UI at the identity provider under test and initiate logout.
282 The IDP sends a logout message to the SP. Capture and log this message.
283 Verify that the user is no longer signed in at the IDP or at the service provider.
284

285 **5.4.5. SOAP-based IDP-initiated single log-out**

286 Follow common steps as in 4.4.

287 **5.4.6. HTTP-redirect-based IDP-initiated single log-out**

288 Follow common steps as in 4.4.

289 **5.4.7. HTTP-GET-based IDP-initiated single log-out**

290 Follow common steps as in 4.4.

291 **5.5. Federation termination**

292 **5.5.1. Common steps**

293 The following steps apply for several profiles and are provided here for reference.

294
295 Prerequisite: successfully test single sign-on with at least one profile.
296 Use the single sign-on protocol, in any profile, to sign in to the service provider via the IDP.
297 Access the federation termination UI at the provider to initiate federation termination.
298 The provider sends a federation termination message to the remote provider. Capture and log this message.
299 Start a clean browser. Verify that attempts to perform single sign-on from the IDP under test to the SP under
300 test now fail.

301 **5.5.2. SP-initiated SOAP-based federation termination**

302 Follow common steps as in 5.1.

303 **5.5.3. SP-initiated HTTP-redirect-based federation termination**

304 Follow common steps as in 5.1.

305 **5.5.4. IDP-initiated SOAP-based federation termination**

306 Follow common steps as in 5.1.

307 **5.5.5. IDP-initiated HTTP-redirect-based federation termination**

308 Follow common steps as in 5.1.

309 **5.6. Identity provider introduction**

310 If possible, configure the service provider so that it knows of more than one identity provider.
311 Start a clean browser.
312 Log into another identity provider (not the one under test) which uses the same common domain and sets the
313 introduction cookie.
314 Log into the IDP under test.
315 Examine the browser's cookie file or cookie manager to verify that the cookie was set correctly. Validate the
316 format of the cookie. Verify that the IDP under test is listed in the correct order.
317 Access the service provider. Verify that the introduction cookie was successfully read by examining the user
318 interface for evidence that the identity provider under test was selected.
319

320 **5.7. Name registration**

321 **5.7.1. Common steps for SP-initiated name registration**

322 Prerequisite: successfully test single sign-on with at least one profile.
323
324 The following steps apply for several profiles and are provided here for reference.
325 Create accounts offline on IDP and SP, initialized without federations.
326 Start "clean" browser (without pre-existing cookies)

327 Log in to SP and access user interface for federating with an identity provider.
328 Choose to federate the identity provider under test.
329 SP should send a valid AuthnRequest to the IDP.
330 Navigate through IDP user interface to authenticate to the IDP and consent to the federation, if necessary.
331 IDP should redirect browser back to SP and send response back to SP.
332 If the SP automatically initiates name registration upon federation, the SP should now send a
333 RegisterNameIdentifierRequest to the IDP. In this case, capture this request and validate it.
334 The IDP should register the new name and return a successful RegisterNameIdentifierResponse. Capture
335 this response and validate it.
336 User should be successfully federated with SP now. Use SP user interface and IDP user interface to verify that
337 the federation is known by both sides, if possible.
338 If the SP did not automatically initiates name registration upon federation, access the user interface to cause
339 the SP to now send a RegisterNameIdentifierRequest to the IDP. In this case, capture this request and validate
340 it.
341 Start a clean browser.
342 Use the single sign-on protocol, in any profile, to sign in to the service provider via the IDP.
343 If supported, test single log-out in any profile.
344 If supported, test federation termination in any profile.

345 **5.7.2. SOAP-based SP-initiated profile**

346 Follow common steps as in 7.1.

347 **5.7.3. HTTP-redirect-based SP-initiated profile**

348 Follow common steps as in 7.1.

349 **5.7.4. Common steps for IDP-initiated name registration**

350 Prerequisite: successfully test single sign-on with at least one profile.
351
352 The following steps apply for several profiles and are provided here for reference.
353 Log in to the IDP.
354 Use the single sign-on protocol, in any profile, to sign in to the service provider via the IDP.
355 Cause the IDP to initiate a name registration request to the SP. Capture and log this request.
356 The SP should response with a successful name registration response. Capture and log this response.
357 Start a clean browser.
358 Log in to the IDP.
359 Use the single sign-on protocol, in any profile, to sign in to the service provider via the IDP.
360 If supported, test single log-out in any profile.
361 If supported, test federation termination in any profile.
362

363 **5.7.5. SOAP-based IDP-initiated profile**

364 Follow common steps as in 7.4.

365 **5.7.6. HTTP-redirect-based IDP-initiated profile**

366 Follow common steps as in 7.4.

367 **6. References**

368 [LibertyIDFF12SCR] Tiffany, Eric. "Liberty ID-FF 1.2 Static Conformance Requirements," Version 1.0-09,
369 Liberty Alliance Project (March 2004). <http://www.projectliberty/specs>

370
371 [LibConfProc] Smith, Jeff. "Liberty Conformance Process and Administration," Version 1.0-05, Liberty Alliance
372 Project (April 2004), <http://www.projectliberty.org/conformance/>