Liberty Interoperability Testing Procedures

(ID-FF 1.1)

Version 1.0-10

09 December 2003

Editors:

Jeff Smith, Nippon Telegraph and Telephone Corporation

Contributors:

John Kemp, IEEE-ISTO
Jonathan Sergent, Sun Microsystems
Roger Sullivan, Phaos
Eric Tiffany, IEEE-ISTO

Abstract:

This document describes the process and procedures for conducting interoperability testing for conformance. The goal of this document, combined with the SCR, is to unambiguously define the process and procedures that will be followed at conformance interoperability testing events. The procedures in this document are intended to streamline testing events, shorten testing times, and minimize disputes that could result in requests for arbitration.

File: lib-ceg-conformance-testing-v1.0-10.pdf

Contents

1. Introduction

This document currently refers only to ID-FF 1.1 and the conformance profiles described in the ID-FF 1.1 SCR [LibertyIDFF11SCR].

This document describes the process and procedures for conducting interoperability testing for conformance. (Note: The interoperability testing described in this document is specific to testing conducted for the conformance process i.e., "validation of implementations". Other interoperability testing focused on validation of specifications is to be considered separately from testing described here.)

The goal of this document, combined with the SCR, is to unambiguously define the process and procedures that will be followed at conformance interoperability testing events. The procedures in this document are intended to streamline testing events, shorten testing times, and minimize disputes that could result in requests for arbitration.

The SCR describes four conformance profiles (IDP, SP Basic, SP Complete, LECP) and the specific features that are required or optional for each profile. The table below summarizes the features that comprise the four profiles. A vendor can participate in conformance interoperability testing in the role of any one or more of these conformance profiles.

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

52 Table 1: Conformance Profile Matrix

Feature	IDP Profile	SP Basic	SP Complete	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	

2. Overview of Conformance Process

1. Non-disclosure Agreement for the interoperability testing must be signed and returned to Liberty/ISTO.
2. Fees for events will be determined based on an annual break-even budget. Fees for the first event (November 11-14 in Madrid, Spain) are $1500 per vendor. Fees for 2004 events are projected at $3000 per event per vendor. A vendor may send up to three people to an event.
3. Vendors intending to participate in a conformance interoperability testing event will be required to provide information as to which conformance profiles and any optional features are supported in an implementation. The Static Conformance Checklist (see appendix for sample) is used for this purpose. This information is used for building a test matrix for the interoperability testing event and determining whether or not complete testing is possible given the number of type of participants. This information will not be published by Liberty, but a vendor may indicate in their own literature, website, etc. what conformance profiles they have implemented, but may make no claim of conformance or interoperability.
4. After signing and returning the NDA, payment of fees, and completion of the Static Conformance Checklist form the vendor will be registered for regularly scheduled interoperability testing events
5. Vendor attends interoperability testing event
    a. A testing schedule (including setup time), assigned IP addresses, certificates, etc. necessary for testing will be provided in advance of the testing event. Vendors will be required to provide metadata (in the XML doc format required in the specifications) in advance of the testing event so that metadata for all implementations can be posted on a common server that will be setup at the testing location.
    b. Testing for each profile follows the procedures described in this document. A vendor will be required to pass testing with a minimum of two, and when time permits, with all implementations at a testing event. Vendors must stay for entire testing event – i.e. a vendor cannot just leave when their own tests are complete. The vendor does not determine with whom they will test. Testing partners will be determined by the Liberty Conformance Review Team (LCRT) and/or ISTO.
    c. In the case where a vendor "fails" on a given feature within a profile, minor fixes to problems that can be completed quickly during testing will be allowed. Testing should continue from the point of failure, but upon successful completion of the remaining test the vendor will be required to retest from beginning (to make sure bug fixes didn't break something else). Vendors will be required to remedy any problems and complete testing by the end of the scheduled event. Vendors who cannot retest within the scheduled time will be required to wait until the next testing event.
    d. A complete log of all traffic between testing partners will be captured. Currently, capture is performed by 'ssldump.' The test results log file will be an electronic file that ISTO will digitally sign and archive. This file is intended as a record of the event and the results of each test and is NOT for public release.
    e. A checklist, based on the testing procedures defined in this document is included in the Appendix. Testing vendors will sign-off on each other's checklist ("grade the other guy's test") in addition to sign-off from an LCRT member/observer.
    f. The LCRT shall be the arbiter in the case of disputed interoperability, but vendors and observers are encouraged to resolve such issues while at the event.
6. Upon successful completion of interoperability testing
    a. Results of testing event will be reported to the LCRT which will review the documentation and make the recommendation to the management board that successful vendors be licensed for use of the "Liberty Interopable" logo and that the results be publicly announced (per the details specified in the NDA and License Agreement).
    b. Vendor must sign license agreement for "Liberty Interoperable" logo if they wish to use the logo and publicly claim interoperability.
    c. Usage guidelines (e.g., size, color, placement, proximity to other logos, edge of page, etc.) will be included with the license agreement.
    d. Listing on Liberty website
        i. Liberty will host on the projectliberty.org website a master list of vendor implementations that have achieved conformance (specific Implementation version numbers – e.g. Liberty Alliance SCR1.1 Specification Interoperable Products: AcmeProducts LibertyFederator version 1.2, IDP conformance profile, etc.
        ii. The logo license agreement requires that 1) for print use of logo the certified product major.minor version number and SCR version and conformance profile be listed wherever

the logo is used 2) in addition for web use the logo be clickable and point to the Liberty website listed information for that vendor's product conformance.

e. Follow-up testing for future revisions to specs and revisions of vendor's implementation(s)
The conformance is tied to specific versions of the specification and specific versions of the vendor's implementation as noted above. The license agreement carries the obligation to repair product defects in a timely manner. If the vendor chooses not to continue certifying future versions of the product family the permission to continue use of the logo is revoked. Retesting for updated versions of a vendor's implementation is optional for minor versions (x.1, x.2, etc.) and mandatory for major revisions 1.x, 2.x, etc.

f. Requirement to participate in future conformance events (as part of reference pool)
A vendor must keep major.minor software version available as part of a reference pool for next 2 test events or for 6 months – which ever comes first. It is likely that a vendor will come with a new version also for testing at future events, and the reference pool requirement does not imply that the vendor is required to continue to sell and support an older version of their software, just that they must make the major.minor version available at test events for the specified period of time in order to maintain consistency in the reference pool.

3. Test Procedures

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

1. Metadata exchange for IdPs and SPs
2. Single Sign-On and Federation
3. Single logout
4. Single Sign-On already federated
5. Single logout
6. Federation termination

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

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

Note: Even though test procedure tables for each conformance profile are listed in practice testing is bidirectional (e.g. IDP ←→SP) and both the IDP and SP being tested should be able to complete one of the two minimum test runs simultaneously. A full test run takes approximately 1-1.5 hours to complete.

146 Table 2. Test items
147

MTD	**Metadata exchange**		
SSO	**Single Sign On**		
SSO-1		*Artifact profile*	
SSO-1.1			New Federation
SSO-1.2			Federated
SSO-2		*Browser POST profile*	
SSO-2.1			New Federation
SSO-2.2			Federated
SSO-3		*LECP profile*	
SSO-3.1			New Federation
SSO-3.2			Federated
SLO	**Single Logout**		
SLO-1		*IDP initiated HTTP-Redirect*	
SLO-2		*IDP initiated HTTP-GET*	
SLO-3		*IDP initiated SOAP*	
SLO-4		*SP initiated HTTP-Redirect*	
SLO-5		*SP initiated SOAP*	
FTN	**Federation Termination**		
FTN-1		*IDP initiated HTTP-Redirect*	
FTN-2		*IDP initiated SOAP/HTTP*	
FTN-3		**SP initiated HTTP-Redirect**	
FTN-4		*SP initiated SOAP/HTTP*	
RNI	**Register Name Identifier**		
RNI-1		*IDP initiated HTTP-Redirect*	
RNI-2		*IDP initiated SOAP/HTTP*	
RNI-3		*SP initiated HTTP-Redirect*	
RNI-4		*SP initiated SOAP/HTTP*	
IPI	**Identity Provider Introduction**		

148

3.1. IDP Profile test procedure

An IDP is required to test each test item against (a minimum of) two SP and two LECP (for the LECP profile) implementations. Principal should have accounts at the SPs and IDP and be authenticated at the IDP in advance. Steps in grey 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-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
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	SSO any profile	SSO any profile
34	RNI-1	Name Registration IDP-initiated HTTP-Redirect
35	SLO any profile	SLO any profile (SP-initiated)
36	SSO any profile	SSO any profile (confirm assertion has new name identifier)
37	SLO any profile	SLO any profile (IDP-initiated)
38	SSO any profile	SSO any profile
39	RNI-2	Name Registration IDP-initiated SOAP/HTTP
40	SLO any profile	SLO any profile (SP-initiated)
41	SSO any profile	SSO any profile (confirm assertion has new name identifier)
42	SLO any profile	SLO any profile (IDP-initiated)
43	FTN any profile	Federation Termination any profile
44	SSO 3.1	SSO LECP – new federation
45	SSO 3.2	SSO LECP – federated

3.2. SP Basic Conformance Profile

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

3.3. SP Complete Conformance Profile

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

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

3.4. LECP Conformance Profile

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

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

4. Checklists

4.1. Static Conformance Checklist

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)	IDP SP Basic SP Complete LECP
Company	
Contact Name	
Contact Phone	
Contact Email	

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

Feature	IDP Profile	SP Basic	SP Complete	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	

177 ## 4.2. Testing Checklist

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

181 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)	
Company	
Contact Name	
Contact Phone	
Contact Email	
Signature (after testing)	

182

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

183

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

184

LCRT Representative	
Contact Name	
Signature (after testing)	

185

Date of testing	

186 Testing Checklist page 2
187

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 inititiated 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 inititiated 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 initated SOAP	SLO-3	optional (SP Basic)
SP initated HTTP-Redirect	SLO-4	
SP initiated SOAP	SLO-5	optional (SP Basic)
Identity Provider Introduction		
IDP Introduction Cookie	IPI	optional (SP)

188

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

5. Sample Testing Procedures (Reference)

1. Introduction

Below are sample testing procedures taken from “Liberty interoperability testing procedures” dated 11/26/02 and authored by Jonathan Sergent, Sun Microsystems. This content is provided as reference only and may not be appropriate for all implementations.

2. Metadata and configuration

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

The test environment should include:
The service provider under test.
The identity provider under test.
A known good service provider which supports all of the single logout profiles to be tested.
A known good identity provider which supports the identity provider introduction protocol.
DNS infrastructure to establish a common introduction domain for at least the two identity providers and the service provider under test.
One or more clients which the service provider and identity provider under test claim to support for the profiles under test.
Network sniffing tool which can capture all traffic between the providers and between the client and the providers. The tool must be capable of decrypting SSL conversations given the private keys of the providers' HTTP servers.

3. Single sign-on and federation protocol

3.1. Common steps

The following steps apply for several profiles and are provided here for reference.
Create accounts offline on IDP and SP, initialized without federations.
Start "clean" browser (without pre-existing cookies)
Log in to SP and access user interface for federating with an identity provider.
Choose to federate the identity provider under test.
SP should send a valid AuthnRequest to the IDP. Capture this request using profile-specific means and log it.
Navigate through IDP user interface to authenticate to the IDP and consent to the federation, if necessary.
IDP should redirect browser back to SP and send response back to SP. Capture this profile-specific data exchange and log it.
User should be successfully federated with SP now. Use SP user interface and IDP user interface to verify that the federation is known by both sides, if possible.
(Single sign-on test procedure starts here.) Start a new "clean" browser.
Log in to the IDP site.
Visit SP site and access user interface for single sign-on with the IDP, complete sign-on. SP should have redirected the browser using a valid AuthnRequest URL (capture and log); IDP should have responded with valid profile-specific response data (capture and log).
Verify that the user is signed in to the SP.
Start a new "clean" browser.

Visit SP site and access user interface for single sign-on with the IDP.
Browser should redirect using valid AuthnRequest URL (capture and log).
Authenticate to IDP.
IDP should send response to SP (capture and log).
Verify that the user is signed in to the SP.

3.2. Browser artifact profile

Follow common steps as in 3.1.

3.3. Browser post profile

Follow common steps as in 3.1.

3.5. Liberty-enabled client/proxy profile

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

4. Single log-out

4.1. Common steps for SP-initiated single log-out

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

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

4.2. SOAP-based SP-initiated single log-out

Follow common steps as in 4.1.

4.3. HTTP-redirect-based SP-initiated single log-out

Follow common steps as in 4.1.

4.4. Common steps for IDP-initiated single logout

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

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

4.5. SOAP-based IDP-initiated single log-out

Follow common steps as in 4.4.

4.6. HTTP-redirect-based IDP-initiated single log-out

Follow common steps as in 4.4.

4.7. HTTP-GET-based IDP-initiated single log-out

Follow common steps as in 4.4.

5. Federation termination

5.1. Common steps

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

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

5.2. SP-initiated SOAP-based federation termination

Follow common steps as in 5.1.

5.3. SP-initiated HTTP-redirect-based federation termination

Follow common steps as in 5.1.

5.4. IDP-initiated SOAP-based federation termination

Follow common steps as in 5.1.

5.5. IDP-initiated HTTP-redirect-based federation termination

Follow common steps as in 5.1.

6. Identity provider introduction

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

7. Name registration

7.1. Common steps for SP-initiated name registration

Prerequisite: successfully test single sign-on with at least one profile.

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

Create accounts offline on IDP and SP, initialized without federations.
Start "clean" browser (without pre-existing cookies)
Log in to SP and access user interface for federating with an identity provider.
Choose to federate the identity provider under test.
SP should send a valid AuthnRequest to the IDP.
Navigate through IDP user interface to authenticate to the IDP and consent to the federation, if necessary.
IDP should redirect browser back to SP and send response back to SP.
If the SP automatically initiates name registration upon federation, the SP should now send a RegisterNameIdentifierRequest to the IDP. In this case, capture this request and validate it.
The IDP should register the new name and return a successful RegisterNameIdentifierResponse. Capture this response and validate it.
User should be successfully federated with SP now. Use SP user interface and IDP user interface to verify that the federation is known by both sides, if possible.
If the SP did not automatically initiates name registration upon federation, access the user interface to cause the SP to now send a RegisterNameIdentifierRequest to the IDP. In this case, capture this request and validate it.
Start a clean browser.
Use the single sign-on protocol, in any profile, to sign in to the service provider via the IDP.
If supported, test single log-out in any profile.
If supported, test federation termination in any profile.

7.2. SOAP-based SP-initiated profile

Follow common steps as in 7.1.

7.3. HTTP-redirect-based SP-initiated profile

Follow common steps as in 7.1.

7.4. Common steps for IDP-initiated name registration

Prerequisite: successfully test single sign-on with at least one profile.

The following steps apply for several profiles and are provided here for reference.
Log in to the IDP.
Use the single sign-on protocol, in any profile, to sign in to the service provider via the IDP.
Cause the IDP to initiate a name registration request to the SP. Capture and log this request.
The SP should response with a successful name registration response. Capture and log this response.
Start a clean browser.
Log in to the IDP.
Use the single sign-on protocol, in any profile, to sign in to the service provider via the IDP.
If supported, test single log-out in any profile.
If supported, test federation termination in any profile.

7.5. SOAP-based IDP-initiated profile

Follow common steps as in 7.4.

7.6. HTTP-redirect-based IDP-initiated profile

Follow common steps as in 7.4.

References

[LibertyIDFF11SCR] Tiffany, Eric. "Liberty ID-FF 1.1 Static Conformance Requirements," Version 1.0, Liberty Alliance Project (November 2003). *http://www.projectliberty/specs*