Liberty Alliance Project:

Liberty ID-FF 1.1 Static Conformance Requirements
Version: 1.0

Editors:
Eric Tiffany, IEEE-ISTO

Abstract:
Defines the Static Conformance Requirements for the Liberty Alliance version 1.1 specifications.

Filename: liberty-idff-1.1-scr-v1.0.pdf
Copyright © 2003 America Online, Inc.; American Express Travel Related Services; Bank of America; Bell Canada; Cingular Wireless; Cisco Systems, Inc.; Communicator, Inc.; Deloitte & Touche LLP; Earthlink, Inc.; Electronic Data Systems, Inc.; Entrust, Inc.; Ericsson; Fidelity Investments; France Telecom; Gemplus; General Motors; Hewlett-Packard Company; i2 Technologies, Inc.; Intuit Inc.; MasterCard International; NEC Corporation; Netegrity; NeuStar; Nextel Communications; Nippon Telegraph and Telephone Corporation; Nokia Corporation; Novell, Inc.; NTT DoCoMo, Inc.; OneName Corporation; Openwave Systems Inc.; PricewaterhouseCoopers LLP; Register.com; Royal Mail; RSA Security Inc; Sabre Holdings Corporation; SAP AG; SchlumbergerSema; SK Telecom; Sony Corporation; Sun Microsystems, Inc.; Symlabs, Inc.; Trustgenix; United Airlines; VeriSign, Inc.; Visa International; Vodafone Group Plc; Wave Systems; All rights reserved.

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

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

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

31 1. Overview ................................................................. 4
32 2. Conformance Profiles .................................................. 5
33 References ................................................................. 23
1. Overview

Static conformance requirements (SCR) describe features that are mandatory and optional for implementations conforming to the Liberty Alliance Specifications (version 1.1). This document defines these requirements. This is a normative document with several non-normative explanatory sections.

1.1. Definitions and Motivation

The Liberty specifications define a large number of features and variations. Applications often do not require all the features within a specification. It is also possible that implementations may not be able to implement all the features. In these cases, it may be desirable to partition the specifications into subsets of functionality. A profile is a subset of the overall specifications that includes all of the functionality necessary to satisfy the requirements of a particular community of users. This document identifies several Liberty conformance profiles based on subsets of these specifications according to the following guidelines:

- The number of profiles should be kept small.
- The profiles should correspond to the major roles within the specifications: Identity Provider (IdP), Service Provider (SP), and Liberty Enabled Client/Proxy (LECP).
- The SCR should distinguish between software implementations and deployments. Allow deployments to optionally configure features that are mandatory in the conformance profiles.
- The SCR should place more stringent requirements on IDPs as compared with SPs to promote interoperability.
- Implementations conforming to one (or more) profiles should be able to interoperate with another conforming implementation of a complementary profile.

The resulting profiles are described below by means of tables indicating mandatory and optional features, with references to the appropriate sections of the specification documents.

1.2. Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in [RFC2119]: "they MUST only be used where it is actually required for interoperation or to limit behavior which has potential for causing harm (e.g., limiting retransmissions)."

The normative sections of this document are identified with special formatting as indicated here:

EXAMPLE This is an example of the format of the normative requirements. Each requirement is identified by a requirement identifier ("EXAMPLE" in this example).
2. Conformance Profiles

2.1. Profile Matrix

The following table summarizes the features that comprise the four profiles. The detailed specifications for each profile follow in subsequent sections.

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

2.2. Identity Provider Profile

This section defines the conformance requirements for an identity provider. These requirements are derived from the steps defined in the [LibertyBindProf1.1, Section 3], which describe the interactions between the user agent, the service provider, and the identity provider.

2.2.1. Single Sign-On and Federation

This section defines how an identity provider facilitates single sign-on by processing incoming and outgoing requests. The steps indicated refer to the interaction diagram in [LibertyBindProf1.1, 3.2.1] which illustrates the general single sign-on framework.

2.2.1.1. Common Interaction and Processing

The single sign-on requirements specified here assume that the user agent has already authenticated with the identity provider, and that a valid session exists for the user agent at the identity provider.

There are only two actions required of the identity provider, as noted here:

**IDP-SSO-001** In step 5, the identity provider MUST process the `<lib:AuthnRequest>` message according to the rules specified in [LibertyProtSchema1.1].
In step 6, the identity provider MUST respond to the user agent with a
<lib:AuthnResponse>, a SAML artifact, or an error. The form of this response is
contingent on the specific interaction method employed by the identity provider.

2.2.1.2. Single Sign-on Using Browser Artifact

This section describes the identity provider actions necessary to perform single sign-on using browser artifact. The requirements in this section are derived primarily from Liberty Bindings and Profiles, Section 3.2.2, with additional references to Step 8 in Section 3.1.

Single Sign-on using Browser Artifact is a mandatory supported feature of the identity provider conformance profile. The requirements in this section MUST be implemented according to the relevant sections of [LibertyBindProf1.1].

The identity provider must complete two processing steps to implement this feature: processing an authentication request, and processing a SAML assertion. The authentication interaction proceeds as follows:

The identity provider MUST process the <lib:AuthnRequest> message as specified in [LibertyBindProf1.1, 3.2.1, Step 5].

In response to the <lib:AuthnRequest> the identity provider MUST perform a redirection as specified in [LibertyBindProf1.1, 3.2.2.1, Step 6]

The identity provider MUST process the <samlp:Request> produced by the service provider in Step 8 of the single sign-on interaction, and produce a <samlp:Response> as specified in [LibertyBindProf1.1, 3.2.1, Step 9].

The artifact produced by the identity provider MUST be be formatted as specified in [LibertyBindProf1.1, 3.2.2.2, Artifact Format].

2.2.1.3. Single Sign-on using Liberty Browser POST

This section describes the identity provider requirements for performing single sign-on using Liberty Browser POST.

Single Sign-on using Liberty Browser POST is a mandatory supported feature of the identity provider conformance profile. The requirements in this section MUST be implemented according to the relevant sections of [LibertyBindProf1.1].

The identity provider MUST process the <lib:AuthnRequest> message as specified in [LibertyBindProf1.1, 3.2.1, Step 5]. (Same as [IDP-SSO-004]).

The identity provider generates an HTML 200 OK response containing an authentication request. This response MUST conform to the specification in [LibertyBindProf1.1, 3.2.3, Step 6]
2.2.1.4. Single Sign-on using Liberty WML POST

The Liberty WML POST is deprecated.

2.2.1.5. Single Sign-on using Liberty-Enabled Client and Proxy

This section specifies the identity provider requirements for performing single sign-on using the Liberty-Enabled Client and Proxy (LECP) interaction.

IDP-SSO-011  Single Sign-on using LECP is a mandatory supported feature of the identity provider conformance profile. The requirements in this section MUST be implemented according the the relevant sections of [LibertyBindProf1.1].

IDP-SSO-012  The identity provider MUST process the <lib:AuthnRequest> in the body of the SOAP POST message from the LECP as specified in [LibertyBindProf1.1, 3.2.1, Step 5]. (See [IDP-SSO-004]).

IDP-SSO-013  The identity provider MUST respond to the <lib:AuthnRequest> with a HTTP 200 OK response as specified in [LibertyBindProf1.1, 3.2.5.2, Step 6], with the correct MIME type (application/vnd.liberty-response+xml) and Liberty-Enabled HTTP header (see [LibertyBindProf1.1, 3.2.5.1]).

2.2.2. Register Name Identifier

This section specifies the required and optional features used by an identity provider to register or change a name identifier for a Principal. There are four variations of the register name identifier protocol: the name registration interaction can be initiated by either the identity provider or the service provider, and the protocol can be either HTTP-Redirect based, or SOAP/HTTP based [LibertyBindProf1.1, 3.3].

Note that while the name registration features are optional interactions in a deployment, some of these features are required for a implementation to be conformant. The following sections describe the mandatory and optional conformance requirements for an identity provider implementing the register name identifier feature.

2.2.2.1. Register Name Identifier Initiated at Identity Provider

2.2.2.1.1. HTTP-Redirect Based

IDP-RNI-001  The identity provider MUST redirect the user agent to the register name identifier service at the service provider as specified in [LibertyBindProf1.1, 3.3.1.1, Step 2].

2.2.2.1.2. SOAP/HTTP Based

IDP-RNI-002  The identity provider MUST only initiate SOAP/HTTP-based register name identifier when the service provider metadata specifies the appropriate URI identifier as specified in [LibertyBindProf1.1, 3.3.1.2].
The SOAP/HTTP-based Register Name Identifier transactions must use the SOAP binding for Liberty as defined in [LibertyBindProf1.1, 2.1].

The identity provider MUST initiate the Register Name Identifier transaction by sending a <lib:RegisterNameIdentifierRequest> message to the service provider’s SOAP endpoint as specified in [LibertyBindProf1.1, 3.3.1.2, Step 1].

The identity provider MUST process the <lib:RegisterNameIdentifierResponse> from the service provider as specified in [LibertyProtSchema1.1, 3.3.3].

2.2.2.2. Register Name Identifier Initiated at Service Provider

The following sections describe the interactions for an identity provider implementing the Register Name Identifier initiated at the service provider.

Register Name Identifier initiated at service provider is a REQUIRED feature of the Identity Provider Conformance Profile. Both the HTTP-Redirect and the SOAP/HTTP interaction MUST be implemented.

Note that this section refers to [LibertyBindProf1.1] Register Name Identifier interactions initiated at the identity provider. The steps associated with the service provider in those interactions are used here as if they were associated with the identity provider. All references to to service provider and identity provider have been interchanged as indicated in [LibertyBindProf1.1, 3.3.2.1] and [LibertyBindProf1.1, 3.3.2.2].

2.2.2.2.1. HTTP-Redirect Based

The identity provider MUST process the <lib:RegisterNameIdentifierRequest> from the service provider as specified in [LibertyProtSchema1.1, 3.3.3]. See [LibertyBindProf1.1, 3.3.1.1, Step 4].

The identity provider MUST respond to the service provider with a redirection URL as specified in the RegisterNameIdentifierServiceReturnURL metadata element. The redirection MUST adhere to the rules specified in [LibertyBindProf1.1, 3.3.1.1, Step 5].

2.2.2.2.2. SOAP/HTTP Based

[Liberty-RNI-003] is a requirement for this interaction.

The service provider will send a <lib:RegisterNameIdentifierRequest> protocol message to the identity provider. The identity provider MUST record the new <lib:SPProvidedNameIdentifier>.

After a successful registration of the <lib:SPProvidedNameIdentifier>, the identity provider MUST respond with a <lib:RegisterNameIdentifierResponse> according to the processing rules in [LibertyProtSchema1.1, 3.3.3].
2.2.3. Identity Federation Termination Notification

Liberty identity federation termination notification specifies how service providers and identity providers are notified of federation termination. There are four variations of the federation termination notification interaction: the federation termination notification interaction can be initiated by either the identity provider or the service provider, and the protocol can be based on either HTTP-Redirect or SOAP/HTTP.

IDP-FTN-001 This section specifies the conformance requirements for an identity provider to support identity federation termination notification. All four interactions specified in [LibertyBindProf1.1, 3.4] MUST be implemented.

2.2.3.1. Federation Termination Notification Initiated at the Identity Provider

2.2.3.1.1. HTTP-Redirect

IDP-FTN-002 This interaction MUST NOT be used unless the service provider metadata element FederationTerminationNotificationProtocolProfile specifies the URI http://projectliberty.org/profiles/fedterm-idp-http.

IDP-FTN-003 This interaction REQUIRES certain preconditions specified in [LibertyBindProf1.1, 3.4.1.1] are met.

IDP-FTN-004 In response to a request to the identity provider’s federation termination service URL, the identity provider MUST redirect the user agent to the federation termination service at the service provider. This redirection MUST adhere to the rules specified in [LibertyBindProf1.1, 3.4.1.1, Step 2].

2.2.3.1.2. SOAP/HTTP

IDP-FTN-005 This interaction MUST NOT be used unless the service provider metadata element FederationTerminationNotificationProtocolProfile specifies the URI http://projectliberty.org/profiles/fedterm-idp-soap.

IDP-FTN-006 This interaction REQUIRES certain preconditions specified in [LibertyBindProf1.1, 3.4.1.2] are met.

IDP-FTN-007 In response to a request from the user agent to the identity provider’s federation termination service URL, the identity provider MUST send an asynchronous SOAP over HTTP notification message to the service provider’s SOAP endpoint. The SOAP message MUST adhere to the rules specified in [LibertyBindProf1.1, 3.4.1.2, Step 2].

The service provider will respond to termination notification with a HTTP 204 No Content response.

IDP-FTN-008 The identity provider MUST process the HTTP 204 No Content response from the service provider and send an HTTP response confirming the requested action of federation termination with the specified service provider.
2.2.3.2. Federation Termination Initiated at the Service Provider

The following sections describe the interactions for an identity provider implementing federation termination notification initiated at the service provider.

Note that this section refers to [LibertyBindProf1.1] federation termination notifications interactions initiated at the identity provider. The steps associated with the service provider in those interactions are used here as if they were associated with the identity provider. All references to to service provider and identity provider have been interchanged as indicated in [LibertyBindProf1.1, 3.4.2.1] and [LibertyBindProf1.1, 3.4.2.2].

2.2.3.2.1. HTTP-Redirect

IDP-FTN-009 The identity provider MUST process the `<lib:FederationTerminationNotification>` received from the user agent according to the rules defined in [LibertyProtSchema1.1, 3.4.2] and in [LibertyBindProf1.1, 3.4.1.1, Step 4].

IDP-FTN-010 The identity provider’s federation termination service MUST respond by redirecting the user agent as specified in [LibertyBindProf1.1, 3.4.1.1, Step 5].

2.2.3.2.2. SOAP/HTTP

IDP-FTN-011 The identity provider MUST process the `<lib:FederationTerminationNotification>` in the SOAP message received from the service provider according to the rules defined in [LibertyProtSchema1.1, 3.4.2] and in [LibertyBindProf1.1, 3.4.1.2, Step 3].

IDP-FTN-012 The identity provider MUST respond to the `<lib:FederationTerminationNotification>` with a HTTP 204 OK response [LibertyBindProf1.1, 3.4.1.2, Step 4].

2.2.4. Single Logout

Liberty single logout specifies how service providers and identity providers synchronize logout across all sessions authenticated by a particular identity provider. There are five variations of the single logout interaction: the single logout can be initiated by either the identity provider or the service provider, and the protocol can be based on either HTTP-Redirect, HTTP-GET (only when initiated at the identity provider), or SOAP/HTTP.

IDP-SLO-001 This section specifies the conformance requirements for an identity provider to support Single Logout. All five interactions specified in [LibertyBindProf1.1, 3.5] MUST be implemented.

2.2.4.1. Single Logout Initiated at the Identity Provider

The following sections specify the requirements for single logout when initiated by a user agent at the identity provider.

2.2.4.1.1. HTTP-Redirect

IDP-SLO-002 This interaction MUST NOT be used unless the service provider metadata element SingleLogOutProtocolProfile specifies the URI http://projectliberty.org/profiles/slo-idp-http.
IDP-SLO-003  In response to the user agent request, the identity provider MUST redirect the user agent to the single logout service URL at each service provider for which the identity provider has provided an authentication assertion during the Principal’s current session. Each redirection MUST adhere to the rules specified in [LibertyBindProf1.1, 3.5.1.1.1, Step 2].

IDP-SLO-004  After receiving the request from the user agent to the SingleLogoutServiceReturnURL as specified in the identity provider metadata, the identity provider MUST process the request and send an HTTP response to the user agent confirming that the requested action of a single logout has been completed.

2.2.4.1.2. HTTP-GET

IDP-SLO-005  This interaction MUST NOT be used unless the service provider metadata element SingleLogOutProtocolProfile specifies the URI http://projectliberty.org/profiles/slo-idp-http.

IDP-SLO-006  In response to the user agent request, the identity provider MUST respond with a standard HTTP 200 OK response containing image tags referencing the logout service URL for each of the service providers for which the identity provider has provided an authentication assertion during the Principal’s current session. Each image tag MUST adhere to the rules specified in [LibertyBindProf1.1, 3.5.1.1.2, Step 2].

IDP-SLO-007  After receiving the request from the user agent to the SingleLogoutServiceReturnURL as specified in the identity provider metadata, the identity provider MUST process the request and send an HTTP response to the user agent confirming that the requested action of a single logout has been completed.

2.2.4.1.3. SOAP/HTTP

IDP-SLO-008  This interaction MUST NOT be used unless the service provider metadata element SingleLogOutProtocolProfile specifies the URI http://projectliberty.org/profiles/slo-idp-soap .

IDP-SLO-009  In response to a SOAP 200 OK <lib:LogoutRequest> message from the service provider, the identity provider MUST send an HTTP response confirming the requested action of single logout has completed.

2.2.4.2. Single Logout Initiated at the Service Provider

2.2.4.2.1. HTTP-Redirect

IDP-SLO-010  The user agent will access the identity provider’s single logout service URL. The identity provider MUST process the <lib:LogoutRequest> according to the rules defined in [LibertyProtSchema1.1, 3.5.1]
The identity provider MUST notify each service provider for which the identity provider provides authentication assertions of the logout request via the service provider’s preferred profile [LibertyBindProf1.1, 3.5.2.1, Step 4].

The identity provider MUST terminate the Principal’s current session, and no more authentication assertions for the Principal are to be given to service providers.

The identity provider MUST respond and redirect the user agent back to the service provider using the return URL location obtained from the SingleLogoutServiceReturnURL metadata element as specified in [LibertyBindProf1.1, 3.5.2.1, Step 5].

After receiving a <lib:LogoutRequest> from the service provider, the identity provider MUST process it according to the rules in [LibertyProtSchema1.1, 3.5.1].

The identity provider MUST submit to each service provider for which the identity provider has provided authentication assertions during the Principal’s current session a request to logout the Principal as specified in [LibertyBindProf1.1, 3.5.2.2, Step 3].

The identity provider MUST respond to the <lib:LogoutRequest> with a SOAP 200 OK <lib:LogoutResponse> message [LibertyBindProf1.1, 3.5.2.2, Step 4].

This section describes the conformance requirements for an identity provider implementing the identity provider introduction feature. The identity provider introduction feature is intended to allow service providers to discover which identity providers a Principal is using.

The identity provider introduction feature is a REQUIRED element of identity provider conformance profile.

Although a deployment may choose not to enable the identity provider introduction feature, an identity provider implementation must provide the feature in order to be conformant.

The identity provider introduction relies on the use of a common domain cookie.

The common domain cookie MUST be constructed as specified in [LibertyBindProf1.1, 3.6.1].

Creating and updating the common domain cookie is the responsibility of the identity provider.

After authenticating a Principal, the identity provider MUST attempt to set the common domain cookie, subject to cookie-setting restrictions of the user-agent.
The details of this procedure are implementation-dependent, and are not normatively specified. However, one possible strategy is described in [LibertyBindProf1.1, 3.6.2].

### 2.3. Liberty Enabled Client/Proxy (LECP)

This section contains detailed specifications of the LECP Profile.

#### 2.3.1. General LECP Requirements

**LCP-SSO-001** All HTTP requests made by a LECP MUST include a Liberty-Enabled indication. A Liberty-Enabled indication is either a Liberty-Enabled header or User-Agent header containing a Liberty-Enabled value as defined in [LibertyBindProf1.1, 3.2.5.1].

The preferred Liberty-Enabled indication is the Liberty-Enabled header.

**LCP-SSO-002** A LECP SHOULD add the Liberty-Enabled header to each HTTP request. This header MUST be constructed as specified in [LibertyBindProf1.1, 3.2.5.1].

**LCP-SSO-003** A LECP MAY add a Liberty-Enabled entry in the HTTP User-Agent request header, as specified in [LibertyBindProf1.1, 3.2.5.1].

#### 2.3.2. Single Sign-On

The single sign-on interaction is the only LECP interaction specified. This interaction assumes that the user agent has authenticated at the identity provider and that a valid session exists for the user agent at the identity provider.

**LCP-SSO-004** To initiate single sign-on, the user agent MUST contain at most one Liberty-Enabled header. If a proxy receives a HTTP request that contains a Liberty-Enabled header, it MUST NOT add another Liberty-Enabled header.

**LCP-SSO-005** A proxy MAY replace the Liberty-Enabled header, but this replacement MUST adhere to the specifications in [LibertyBindProf1.1, 3.2.5.2, Step 1].

After receiving the HTTP 200 OK response (containing a `<lib:AuthnRequestEnvelope>` from the service provider), the LECP will determine the correct identity provider to use.

**LCP-SSO-006** The LECP MUST issue an HTTP POST of the `<lib:AuthnRequest>` in the body of a SOAP message to the identity provider’s single sign-on service URL. This MUST be the same `<lib:AuthnRequest>` as was received in the service provider’s `<lib:AuthnRequestEnvelope>`. See [LibertyBindProf1.1, 3.2.5.2, Step 4].

**LCP-SSO-007** In case of any error, the LECP MUST return a `<lib:AuthnResponse>` to the service provider as specified in [LibertyBindProf1.1, 3.2.5.2, Step 4].

After receiving a HTTP response from the identity provider, the LECP will issue an HTTP POST to the service provider.

**LCP-SSO-008** The HTTP POST from the LECP MUST be composed as specified in [LibertyBindProf1.1, 3.2.5.2, Step 7].
In case of any error, the LECP MUST return a `<lib:AuthnResponse>` to the service provider as specified in [LibertyBindProf1.1, 3.2.5.2, Step 7].

### 2.4. Service Provider Basic Profile

This section defines the minimal conformance requirements for a Service Provider. These requirements are derived from the steps defined in the [LibertyBindProf1.1, Section 3], which describe the interactions between the user agent, the service provider, and the identity provider.

#### 2.4.1. Single Sign-On and Federation

##### 2.4.1.1. Common Interaction and Processing

The single sign-on requirements specified here assume that the user agent has already authenticated with the identity provider, and that a valid session exists for the user agent at the identity provider.

##### 2.4.1.2. Single Sign-on using Browser Artifact

This section describes the service provider actions necessary to perform single sign-on using browser artifact.

**SP-SSO-001** Single sign-on using browser artifact is a mandatory feature of the service provider basic conformance profile. The requirements in this section MUST be implemented as specified in [LibertyBindProf1.1, Section 3.2.2] and [LibertyBindProf1.1, 3.2.1, Steps 8 and 10].

The user agent initiates the single sign-on by making an HTTP request to the service provider, as indicated in [LibertyBindProf1.1, 3.2.1, Step 1]. The service provider then obtains the address of the appropriate identity provider in an implementation-dependent way (not normatively specified).

**SP-SSO-002** The service provider MAY use the Liberty identity provider introduction interaction while processing the user agent request.

**SP-SSO-003** The HTTP redirection response MUST adhere to the specifications in [LibertyBindProf1.1, 3.2.2.1, Step 3].

**SP-SSO-004** The service provider MUST send a `<samlp:Request>` SOAP message to the identity provider’s SOAP endpoint as specified in [LibertyBindProf1.1, 3.2.2.1, Step 8].

**SP-SSO-005** The service provider MUST process the `<saml:Assertion>` returned by the identity provider as specified in [LibertyBindProf1.1, 3.2.2.1, Step 10].
2.4.1.3. Single Sign-on using Liberty Browser POST

This section describes the service provider requirements for performing single sign-on using Liberty browser POST.

SP-SSO-006 Single sign-on using Liberty browser POST is a mandatory supported feature of the service provider Basic conformance profile. The requirements in this section MUST be implemented according to the relevant sections of [LibertyBindProf1.1, 3.2.3].

The user agent initiates the single sign-on by making an HTTP request to the service provider’s intersite transfer service as indicated in [LibertyBindProf1.1, 3.2.1, Step 1]. The service provider then obtains the address of the appropriate identity provider in an implementation-dependent way (not normatively specified).

The service provider’s responds to the user agent request by redirecting the user agent to the single sign-on service URL at the identity provider.

SP-SSO-007 The redirection MUST adhere to the rules specified in [LibertyBindProf1.1, 3.2.3, Step 3].

After obtaining an authentication assertion, the user agent will issue an HTTP POST request containing the 
<lib:AuthnResponse> to the service provider.

SP-SSO-008 The service provider MUST process the <lib:AuthnResponse> in the HTTP POST from the user agent as specified in [LibertyBindProf1.1, 3.2.2.1, Step 10]

2.4.1.4. Single Sign-on using Liberty WML POST

The Liberty WML POST is deprecated.

2.4.1.5. Single Sign-on using Liberty-Enabled Client and Proxy

This section specifies the service provider requirements for performing single sign-on using the Liberty-Enabled Client and Proxy (LECP) interaction.

SP-SSO-009 Single sign-on using LECP is a mandatory supported feature of the service provider basic conformance profile. The requirements in this section MUST be implemented according to [LibertyBindProf1.1, 3.2.5].

The user agent will submit request to the service provider which contains the requisite Liberty-Enabled indications.

SP-SSO-010 The service provider MUST NOT obtain an identity provider address or perform identity provider introduction.

SP-SSO-011 The service provider MUST issue an HTTP 200 OK response to the user agent. The response MUST adhere to the specifications of [LibertyBindProf1.1, 3.2.5.2, Step 3].

SP-SSO-012 If the service provider does not support Liberty version advertised by the LECP, the service provider MUST return an HTTP 501 Not Implemented response to the LECP with the reason phrase "Unsupported Liberty Version."

SP-SSO-013 The service provider SHOULD place appropriate headers in the response to ensure the response is not cached as specified in [LibertyBindProf1.1, 3.2.5.2, Step 3].
After obtaining an authentication assertion, the user agent will issue an HTTP POST request containing the
<lib:AuthnResponse> to the service provider.

SP-SSO-014 The service provider MUST process the <lib:AuthnResponse> in the HTTP POST from the
user agent as specified in [LibertyBindProf1.1, 3.2.2.1, Step 10]

2.4.2. Register Name Identifier

2.4.2.1. Register Name Identifier Initiated at Identity Provider

The following sections describe the interactions for a service provider implementing the register name identifier
initiated at the identity provider.

2.4.2.1.1. HTTP-Redirect Based

SP-RNI-001 The HTTP-Redirect based register name identifier (initiated at the identity provider) is a
REQUIRED feature of the service provider basic profile.

SP-RNI-002 The service provider MUST process the <lib:RegisterNameIdentifierRequest> from
the identity provider as specified in [LibertyProtSchema1.1, 3.3.3]. See [LibertyBindProf1.1,
3.3.1.1, Step 4].

SP-RNI-003 The service provider MUST respond to the identity provider with a redirection URL as specified
in the RegisterNameIdentifierServiceReturnURL metadata element. The redirection
MUST adhere to the rules specified in [LibertyBindProf1.1, 3.3.1.1, Step 5].

2.4.2.1.2. SOAP/HTTP Based

SP-RNI-004 The SOAP/HTTP based register name identifier (initiated at the identity provider) is an OP-
TIONAL feature of the service provider basic profile.

SP-RNI-005 The SOAP/HTTP-based register name identifier transactions MUST use the SOAP binding for
Liberty as defined in [LibertyBindProf1.1, 2.1].

SP-RNI-006 The identity provider will send a <lib:RegisterNameIdentifierRequest> proto-
col message to the service provider. The service provider MUST record the new
<lib:IDPProvidedNameIdentifier>.

SP-RNI-007 After a successful registration of the <lib:IDPProvidedNameIdentifier>, the service
provider MUST respond with a <lib:RegisterNameIdentifierResponse> according to
the processing rules in [LibertyProtSchema1.1, 3.3.3].
2.4.2.2. Register Name Identifier Initiated at Service Provider

Note that this section refers to LibertyBindProf1.1 register name identifier interactions initiated at the identity provider. The steps associated with the service provider in those interactions are used here as if they were associated with the identity provider. All references to service provider and identity provider have been interchanged as indicated in LibertyBindProf1.1, 3.3.2.2.

2.4.2.2.1. HTTP-Redirect Based

The HTTP-Redirect based register name identifier (initiated at the service provider) is a REQUIRED feature of the service provider basic profile. The service provider can initiate the register name identifier interaction, though the circumstances of this initiation are not normatively specified.

The service provider MUST redirect the user agent to the register name identifier service at the identity provider as specified in LibertyBindProf1.1, 3.3.1.1, Step 2.

2.4.2.2.2. SOAP/HTTP Based

The SOAP/HTTP based register name identifier (initiated at the service provider) is an OPTIONAL feature of the service provider basic profile. The service provider MUST only initiate SOAP/HTTP-based register name identifier when the identity provider metadata specifies the appropriate URI identifier as specified in LibertyBindProf1.1, 3.3.1.2.

The SOAP/HTTP-based register name identifier transactions MUST use the SOAP binding for Liberty as defined in LibertyBindProf1.1, 2.1.

The service provider MUST initiate the register name identifier transaction by sending a <lib:RegisterNameIdentifierRequest> message to the identity provider’s SOAP endpoint as specified in LibertyBindProf1.1, 3.3.1.2, Step 1.

The service provider MUST process the <lib:RegisterNameIdentifierResponse> from the identity provider as specified in LibertyProtSchematic1.1, 3.3.3.

2.4.3. Identity Federation Termination Notification

Liberty identity federation termination notification specifies how service providers and identity providers are notified of federation termination. There are four variations of the federation termination notification interaction: the federation termination notification interaction can be initiated by either the identity provider or the service provider, and the protocol can be based on either HTTP-Redirect or SOAP/HTTP.

2.4.3.1. Federation Termination Notification Initiated at the Identity Provider

2.4.3.1.1. HTTP-Redirect

The HTTP-Redirect based federation termination notification (initiated at the identity provider) is a REQUIRED feature of the service provider basic profile.
The service provider MUST process the `<lib:FederationTerminationNotification>` received from the user agent according to the rules defined in [LibertyProtSchema1.1, 3.4.2] and in [LibertyBindProf1.1, 3.4.1.1, Step 4].

The service provider’s federation termination service MUST respond by redirecting the user agent as specified in [LibertyBindProf1.1, 3.4.1.1, Step 5].

The SOAP/HTTP based federation termination notification (initiated at the identity provider) is an OPTIONAL feature of the service provider basic profile.

The service provider MUST process the `<lib:FederationTerminationNotification>` in the SOAP message received from the identity provider according to the rules defined in [LibertyProtSchema1.1, 3.4.2] and in [LibertyBindProf1.1, 3.4.1.2, Step 3].

The service provider MUST respond to the `<lib:FederationTerminationNotification>` with a HTTP 204 OK response [LibertyBindProf1.1, 3.4.1.2, Step 4].

The HTTP-Redirect based federation termination notification (initiated at the service provider) is a REQUIRED feature of the service provider basic profile.

This interaction MUST NOT be used unless the identity provider metadata element `FederationTerminationNotificationProtocolProfile` specifies the URI http://projectliberty.org/profiles/fedterm-sp-http.

This interaction REQUIRES certain preconditions specified in [LibertyBindProf1.1, 3.4.1.1] are met.

In response to a request to the service provider’s federation termination service URL, the service provider MUST redirect the user agent to the federation termination service at the identity provider. This redirection MUST adhere to the rules specified in [LibertyBindProf1.1, 3.4.1.1, Step 2].

The SOAP/HTTP based federation termination notification (initiated at the service provider) is an OPTIONAL feature of the service provider basic profile.
This interaction MUST NOT be used unless the identity provider metadata element FederationTerminationNotificationProtocolProfile specifies the URI http://projectliberty.org/profiles/fedterm-sp-soap.

This interaction REQUIRES certain preconditions specified in [LibertyBindProf1.1, 3.4.1.2] are met.

In response to a request from the user agent to the service provider’s federation termination service URL, the service provider MUST send an asynchronous SOAP over HTTP notification message to the identity provider’s SOAP endpoint. The SOAP message MUST adhere to the rules specified in [LibertyBindProf1.1, 3.4.1.2, Step 2].

The identity provider will respond to termination notification with a HTTP 204 No Content response.

The service provider MUST process the HTTP 204 No Content response from the identity provider and send an HTTP response confirming the requested action of federation termination with the specified identity provider.

2.4.4. Single Logout

Liberty single logout specifies how service providers and identity providers synchronize logout across all sessions authenticated by a particular identity provider. There are five variations of the single logout interaction: the single logout can be initiated by either the identity provider or the service provider, and the protocol can be based on either HTTP-Redirect, HTTP-GET (only when initiated at the identity provider), or SOAP/HTTP.

Note that Single Logout, in the general case, is an iterative process from the perspective of an identity provider since the identity provider must contact each service provider to which it has issued authentication assertions. However, for a service provider, the single logout interaction is a single event.

2.4.4.1. Single Logout Initiated at the Identity Provider

2.4.4.1. HTTP-Redirect

The HTTP-Redirect based single logout interaction (initiated at the identity provider) is a REQUIRED feature of the service provider basic profile.

The user agent will access the service provider’s single logout service URL via a redirect from the identity provider. The service provider MUST process the <lib:LogoutRequest> according to the rules defined in [LibertyProtSchema1.1, 3.5.1]

The service provider MUST invalidate the session(s) of the Principal referred to in the name identifier received from the identity provider in the <lib:LogoutRequest>.

The service provider MUST respond and redirect the user agent back to the identity provider using the return URL location obtained from the SingleLogoutServiceReturnURL metadata element as specified in [LibertyBindProf1.1, 3.5.1.1.1, Step 5].
2.4.4.1.2. HTTP-GET

SP-SLO-005 The HTTP-GET based single logout interaction (initiated at the identity provider) is a REQUIRED feature of the service provider basic profile.

The user agent will access the single logout service URL of the service provider as a result of an image tag load generated by the identity provider.

SP-SLO-006 The service provider MUST process the \(<lib:LogoutRequest>\) according to the rules defined in [LibertyProtSchema1.1, 3.5.1].

SP-SLO-007 The service provider MUST invalidate the session(s) of the Principal referred to in the name identifier received from the identity provider in the \(<lib:LogoutRequest>\).

SP-SLO-008 The service provider MUST respond and redirect the user agent image load back to the identity provider’s logout completion URL obtained from the SingleLogoutServiceReturnURL metadata element. The HTTP response MUST be formed as specified in [LibertyBindProf1.1, 3.5.1.2, Step 5].

2.4.4.1.3. SOAP/HTTP

SP-SLO-009 The SOAP/HTTP based single logout interaction (initiated at the identity provider) is an OPTIONAL feature of the service provider basic profile.

SP-SLO-010 After receiving a \(<lib:LogoutRequest>\) from the identity provider, the service provider MUST process it according to the rules in [LibertyProtSchema1.1, 3.5.1].

SP-SLO-011 The service provider MUST invalidate the session(s) of the Principal referred to in the name identifier received from the identity provider in the \(<lib:LogoutRequest>\).

SP-SLO-012 The service provider MUST respond to the \(<lib:LogoutRequest>\) with a SOAP 200 OK \(<lib:LogoutResponse>\) message [LibertyBindProf1.1, 3.5.1.2, Step 4].

2.4.4.2. Single Logout Initiated at the Service Provider

2.4.4.2.1. HTTP-Redirect

SP-SLO-013 The HTTP-Redirect based single logout interaction (initiated at the service provider) is a REQUIRED feature of the service provider basic profile.

The user agent will access the single logout service URL at the service provider.

SP-SLO-014 The service provider’s single logout service responds and redirects the user agent to the single logout service at the identity provider. The HTTP redirect MUST adhere to the rules specified in [LibertyBindProf1.1, 3.5.2.1, Step 2].
After the identity provider has processed the single logout request and contacted the appropriate service providers, the user agent will be redirected back to the service provider contacted originally.

SP-SLO-015 The service provider SHOULD send an HTTP 200 OK response to the user agent with confirmation of the logout.

2.4.4.2.2. SOAP/HTTP

SP-SLO-016 The SOAP/HTTP based single logout interaction (initiated at the service provider) is an OPTIONAL feature of the service provider basic profile.

The user agent will initiate single logout by accessing the single logout service URL at the service provider via an HTTP request.

SP-SLO-017 In response to the single logout request, the service provider sends a SOAP over HTTP request to the identity provider’s SOAP endpoint. The SOAP request MUST be constructed and processed as specified in [LibertyBindProf1.1, 3.5.2.2, Step 2].

The identity provider will contact all service providers to which it has issued assertions for the Principal to request a logout action. The identity provider may determine that one or more of the service providers do not support the SOAP single logout interaction. The identity provider will return a <lib:LogoutResponse> containing a status code of <lib:UnsupportedProfile>

SP-SLO-018 If the identity provider responds to the single logout request with <lib:UnsupportedProfile>, the service provider MUST re-submit its <lib:LogoutRequest> via the HTTP interaction specified above.

SP-SLO-019 If the identity provider responds to the logout request with a SOAP 200 OK <lib:LogoutResponse>, indicating successful single logout, the service provider SHOULD send a HTTP response to the user agent confirming the single logout.

2.4.5. Identity Provider Introduction

This section describes the conformance requirements for a service provider implementing the identity provider introduction feature. The identity provider introduction feature is intended to allow service providers to discover which identity providers a Principal is using.

SP-IPI-001 The identity provider introduction feature is an OPTIONAL element of the service provider basic conformance profile.

2.4.5.1. Common Domain Cookie

The identity provider introduction relies on the use of a common domain cookie.

SP-IPI-002 The common domain cookie MUST be constructed as specified in [LibertyBindProf1.1, 3.6.1].
2.4.5.2. Obtaining the Common Domain Cookie

The service provider uses the common domain cookie to determine which identity providers a Principal uses. The common domain cookie is presented to the service provider after being read by an HTTP server in the common domain; the details of this interaction are outside the scope of this document.

SP-IPI-003 If the HTTP server in the common domain is operated by the service provider, the service provider MAY redirect the user agent to an identity provider for single sign-on.

The details of this procedure are implementation-dependent, and are not normatively specified. However, one possible strategy is described in [LibertyBindProf1.1, 3.6.3].

2.5. Service Provider Complete Profile

This section defines the conformance requirements for the SP complete Profile.

SP-COMPLETE The service provider complete profile is defined to be the service provider basic profile with all optional interactions changed to REQUIRED except for the identity provider introduction interaction.
References

Normative


Informative
