Liberty Alliance Project:

Liberty Alliance Project

Liberty ID-WSF 1.1 Static Conformance Requirements
Version: 1.0

Editors:
Greg Whitehead, Trustgenix, Inc.

Contributors:
Eric Tiffany, IEEE-ISTO
John Kemp, Nokia Corporation
Jonathan Sergent, Sun Microsystems, Inc.
Robert Aarts, Nokia Corporation

Abstract:
Defines the static conformance requirements for the Liberty Alliance ID-WSF 1.1 specifications.

Filename: liberty-idwsf-1.1-scr-v1.0.pdf
Notice

This 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 document 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.

Copyright © 2004 America Online, Inc.; American Express Travel Related Services; Axalto; Bank of America Corporation; Communicator, Inc.; Computer Associates International, Inc.; Deloitte & Touche LLP; Electronic Data Systems, Inc.; Entrust, Inc.; Epok, Inc.; Ericsson; Fidelity Investments; France Telecom; Gamefederation; Gemplus; General Motors; Giesecke & Devrient GmbH; Hewlett-Packard Company; Indentrus; Infospace; Intuit Inc.; Kayak Interactive; MasterCard International; NEC Corporation; Netegrity, Inc.; NeuStar, Inc.; Nippon Telegraph and Telephone Corporation; Nokia Corporation; Novell, Inc.; NTT DoCoMo, Inc.; Openwave Systems Inc.; Oracle Corporation; Phaos Technology; Ping Identity Corporation; PricewaterhouseCoopers LLP; RegistryPro, Inc.; Royal Mail Group plc; RSA Security Inc.; Sabre Holdings Corporation; SAP AG; Sharp Laboratories of America; Sigaba; Sony Corporation; Sun Microsystems, Inc.; Trustgenix; VeriSign, Inc.; Visa International; Vodafone Group Plc. All rights reserved.
Contents

1. Overview ................................................................. 4
2. Conformance Profiles .................................................. 6
References ................................................................. 16
1. Overview

Static conformance requirements (SCR) describe features that are mandatory and optional for implementations conforming to the Liberty Alliance Identity Web Service Framework (ID-WSF) Specifications:

- LibertySOAPBinding (v1.2)
- LibertySecMech (v1.2)
- LibertyDisco (v1.2)
- LibertyInteract (v1.1)
- LibertyPAOS (v1.1)
- LibertyAuthn (v1.1)
- LibertyClientProfiles (v1.1)
- LibertyMetadata (v1.1)
- LibertyProtSchema (v1.2-errata-v3.0)
- LibertyBindProf (v1.2-errata-v2.0)
- LibertyAuthnContext (v1.3)

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 conformance profiles should be kept small.
- The profiles should correspond to the major roles within the specifications: Web Service Consumer (WSC), Web Service Provider (WSP), Discovery Service (DS), Interaction Service (IS), and Identity Provider (IdP).
- 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 service providers as compared with service consumers 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 interoperability 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 tables summarize the features that comprise the conformance profiles. The detailed specifications for each profile follow in subsequent sections.

Table 1. Abstract Profile Matrix

<table>
<thead>
<tr>
<th>Feature</th>
<th>WSC Common</th>
<th>WSP Common</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic SOAP Binding</td>
<td>MUST</td>
<td>MUST</td>
</tr>
<tr>
<td>Basic Security Mechanisms</td>
<td>MUST</td>
<td>MUST</td>
</tr>
<tr>
<td>Interaction Header</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2. Concrete Profile Matrix

<table>
<thead>
<tr>
<th>Feature</th>
<th>ID-FF SP WSC</th>
<th>LUAD WSC</th>
<th>ID-FF SP WSP</th>
<th>LUAD WSP</th>
<th>ID-FF IdP</th>
<th>ID-WSF IdP</th>
<th>DS</th>
<th>IS</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSC Common</td>
<td>MUST</td>
<td>MUST</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WSP Common</td>
<td>MUST</td>
<td>MUST</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID-FF SP WSC SOAP Binding</td>
<td>MUST</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID-FF SP WSC Security Mechanisms</td>
<td>MUST</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interaction Redirect</td>
<td>MUST</td>
<td>OPT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interaction Service</td>
<td>OPT</td>
<td>OPT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID-FF DS Bootstrap</td>
<td>MUST</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSO Service</td>
<td>MUST</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>MUST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Registration</td>
<td></td>
<td>OPT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Discovery</td>
<td>MUST</td>
<td>MUST</td>
<td></td>
<td></td>
<td></td>
<td>MUST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Invocation</td>
<td>MUST</td>
<td>MUST</td>
<td></td>
<td></td>
<td></td>
<td>MUST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAOS</td>
<td>OPT</td>
<td>OPT</td>
<td></td>
<td></td>
<td>OPT</td>
<td>OPT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LUAD</td>
<td>MUST</td>
<td>MUST</td>
<td></td>
<td></td>
<td>OPT</td>
<td>OPT</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.2. Web Service Consumer (WSC) Common Conformance Profile

This section defines the common conformance requirements for all Web Service Consumer Profiles.

2.2.1. Basic SOAP Binding

Conforming WSCs MUST support the following SOAP Binding features

**wsd-soapbind-001** The WSC MUST conform to the requirements for sending SOAP-bound ID-* messages and receiving their responses, as described in sections 4 and 5 of [LibertySOAPBinding]. This includes support for sending and processing the Correlation Header, and for failing if any unsupported Header is received with a mustUnderstand attribute set to true.
Liberty Alliance Project: Version: 1.0
Liberty ID-WSF 1.1 Static Conformance Requirements

wsc-soapbind-002 The WSC MUST support processing of the ServiceInstanceUpdate Header, as described in section 6.4 of [LibertySOAPBinding]. Specifically, the WSC MUST (a) be able to retry an operation as specified by a ServiceInstanceUpdate Header received in combination with an EndpointMoved Fault and (b) be able to accept new credentials for use in subsequent operations as specified by a ServiceInstanceUpdate Header received in combination with a normal response Body.

2.2.2. Basic Security Mechanisms
Conforming WSCs MUST be able to construct and send ID-WSF messages using the following Security Mechanisms:

wsc-secmech-001 The WSC MUST be able to construct and send ID-WSF messages using null and TLS peer entity authentication mechanisms, as described in section 6.2 of [LibertySecMech].

wsc-secmech-002 The WSC MUST be able to construct and send ID-WSF messages using null and Bearer message authentication mechanisms, as described in section 6.3 of [LibertySecMech].

Combined, these requirements correspond to the following set of Security Mechanism URIs:

- urn:liberty:security:2003-08:TLS:null

2.3. Web Service Provider (WSP) Common Conformance Profile
This section defines the common conformance requirements for all Web Service Provider Profiles.

2.3.1. Basic SOAP Binding
Conforming WSPs MUST support the following SOAP Binding features

wsp-soapbind-001 The WSP MUST conform to the requirements for receiving SOAP-bound ID-* messages and sending their responses, as described in sections 4 and 5 of [LibertySOAPBinding]. This includes support for sending and processing the Correlation Header, and for failing if any unsupported Header is received with a mustUnderstand attribute set to true.

2.3.2. Basic Security Mechanisms
Conforming WSPs MUST be able to receive and process ID-WSF messages using the following Security Mechanisms

wsp-secmech-001 The WSP MUST be able to receive and process ID-WSF messages using null and TLS peer entity authentication mechanisms, as described in section 6.2 of [LibertySecMech].

wsp-secmech-002 The WSP MUST be able to receive and process ID-WSF messages using either null or Bearer or both x509 and SAML message authentication mechanisms, as described in section 6.3 of [LibertySecMech].
Combined, these requirements correspond to the following sets of Security Mechanism URIs:

- `urn:liberty:security:2003-08:TLS:null`

or


or

- `urn:liberty:security:2003-08:TLS:X509`

### 2.3.3. Interaction Header

Conforming WSPs MUST support the following Interaction features:

- `wsp-interact-001` The WSP MUST process the UserInteraction Header, as described in section 3 of [LibertyInteract].

### 2.4. ID-FF Service Provider (SP) Web Service Consumer (WSC) Conformance Profile

This section defines the requirements for the ID-FF SP Web Service Consumer Profile.

#### 2.4.1. WSC Common

Conforming ID-FF SP WSCs MUST support the Common WSC Profile

#### 2.4.2. ID-FF SP WSC SOAP Binding

Conforming ID-FF SP WSCs MUST support the following additional SOAP Binding features:

- `idffsp-wsc-soapbind-001` The ID-FF SP WSC MUST send the SOAP Binding Provider Header, as described in section 5.2 of [LibertySOAPBinding].
2.4.3. Interaction Redirect

Conforming ID-FF SP WSCs MUST support the following Interaction features:

idffsp-wsc-interact-001 ID-FF SP WSCs MUST support redirect based user interaction, as described in section 4 of [LibertyInteract].

2.4.4. ID-FF SP WSC Security Mechanisms

Conforming ID-FF SP WSCs MUST be able to construct and send ID-WSF messages using the following additional Security Mechanisms:

idffsp-wsc-secmech-001 The WSC MUST be able to construct and send ID-WSF messages using x509 and SAML message authentication mechanisms, as described in section 6.3 of [LibertySecMech].

Combined with the peer entity authentication mechanisms required by the WSC Common Profile, this requirement corresponds to the following additional Security Mechanism URIs:

• urn:liberty:security:2003-08:null:X509
• urn:liberty:security:2003-08:null:SAML
• urn:liberty:security:2003-08:TLS:X509
• urn:liberty:security:2003-08:TLS:SAML

2.4.5. ID-FF DS Bootstrap

Conforming ID-FF SP WSCs MUST support Discovery Service Bootstrap:

idffsp-wsc-bootstrap-001 The ID-FF SP WSC MUST support extraction of the Principal’s’s Discovery Service Resource Offering and any Credentials from the ID-FF assertion authenticating the Principal, as described in section 6 of [LibertyDisco].

2.4.6. Service Discovery and Service Invocation

Conforming ID-FF SP WSCs MUST support discovery and invocation of at least one ID-WSF service registered in a Principal’s Discovery Service (see idffsp-wsc-bootstrap-001):

idffsp-wsc-discinvk-001 The ID-FF SP WSC MUST support querying the Principal’s Discovery Service to obtain the Resource Offering and any Credentials for at least one ID-WSF service, as described in section 6 of [LibertyDisco].

idffsp-wsc-discinvk-002 The ID-FF SP WSC MUST support invocation of at least one discovered ID-WSF service.
2.4.7. PAOS

Conforming ID-FF SP WSCs MAY support discovery and invocation of PAOS services:

idffsp-wsc-paos-001   The ID-FF SP WSC MAY support discovery and invocation of PAOS services, as described in [LibertyPAOS].

2.5. Liberty User Agent or Device (LUAD) Web Service Consumer (WSC) Conformance Profile

This section defines the requirements for the LUAD Web Service Consumer Profile.

2.5.1. WSC Common

Conforming LUAD WSCs MUST support the Common WSC Profile

2.5.2. Authentication Service

Conforming LUAD WSCs MUST support authentication via an IdP:

luad-wsc-authsvc-001   The LUAD WSC MUST support invocation of an authentication service, as described in section 5 of [LibertyAuthn].

luad-wsc-authsvc-002   The LUAD WSC MUST support the PLAIN and CRAM-MD5 authentication mechanisms, as referenced in appendix A of [LibertyAuthn].

luad-wsc-authsvc-003   The LUAD WSC MUST support the password transforms Truncation, Lowercase, Uppercase, and Select, as described in appendix B of [LibertyAuthn].

2.5.3. SSO Service

Conforming LUAD WSCs MAY support SSO via an IdP:

luad-wsc-ssosvc-001   The LUAD WSC MAY support invocation of an sso service, as described in section 6 of [LibertyAuthn].

2.5.4. Service Discovery and Service Invocation

Conforming LUAD WSCs MUST support discovery and invocation of at least one ID-WSF service registered in a Principal’s Discovery Service:

luad-wsc-discinvk-001   The LUAD WSC MUST support querying the Principal’s Discovery Service to obtain the Resource Offering and any Credentials for at least one ID-WSF service, as described in section 6 of [LibertyDisco].

luad-wsc-discinvk-002   The LUAD WSC MUST support invocation of at least one discovered ID-WSF service.
2.5.5. LUAD

Conforming WSCs MUST support the LUAD-WSC profile:

luad-wsc-luad-001 The WSC MUST support LUAD-WSC profile, as described in section 3 of [LibertyClientProfiles].

2.6. ID-FF Service Provider (SP) Web Service Provider (WSP) Conformance Profile

This section defines the requirements for the ID-FF SP Web Service Provider Profile.

2.6.1. WSP Common

Conforming ID-FF SP WSPs MUST support the Common WSP Profile

2.6.2. Interaction Redirect and Interaction Service

Conforming ID-FF SP WSPs MAY optionally support the following Interaction features:

idffsp-wsp-interact-001 The ID-FF SP WSP MAY support redirect based user interaction, as described in section 4 of [LibertyInteract].

idffsp-wsp-interact-002 The ID-FF SP WSP MAY support invocation of a user interaction service, as described in section 5 of [LibertyInteract]. Note that the ID-FF SP WSP takes on the role of a WSC in making interaction service calls, and so is bound by all of the requirements of the applicable WSC profile.

2.6.3. Service Registration

Conforming ID-FF SP WSPs MAY support registration with a Principal’s Discovery Service using DS Modify InsertEntry:

idffsp-wsp-registration-001 The ID-FF SP WSP MAY invoke DS Modify InsertEntry at a Principal’s Discovery Service to register itself, as described in section 5.2 of [LibertyDisco]. Note that the ID-FF SP WSP takes on the role of a WSC in making DS calls, and so is bound by all of the requirements specified in the applicable WSC profile.

2.6.4. Service Invocation

Conforming ID-FF SP WSPs MUST support invocation by a WSC based on a resource offering and credentials discovered by WSC in a Principal’s Discovery Service:

idffsp-wsp-discinvk-001 The ID-FF SP WSP MUST support invocation by a WSC as a discovered ID-WSF service.
2.7. Liberty User Agent or Device (LUAD) Web Service Provider (WSP) Conformance Profile

This section defines the requirements for the LUAD Web Service Provider Profile.

2.7.1. WSP Common

Conforming LUAD WSPs MUST support the Common WSP Profile

2.7.2. Interaction Redirect and Interaction Service

Conforming LUAD WSPs MAY optionally support the following Interaction features:

luad-wsp-interact-001 The LUAD WSP MAY support invocation of a user interaction service, as described in section 5 of [LibertyInteract]. Note that the LUAD WSP takes on the role of a WSC in making interaction service calls, and so is bound by all of the requirements specified in the applicable WSC profile.

2.7.3. Service Registration

Conforming LUAD WSPs MAY support registration with a Principal’s Discovery Service using DS Modify InsertEntry:

luad-wsp-registration-001 The LUAD WSP MAY invoke DS Modify InsertEntry at a Principal’s Discovery Service to register itself, as described in section 5.2 of [LibertyDisco]. Note that the LUAD WSP takes on the role of a WSC in making DS calls, and so is bound by all of the requirements specified in the applicable WSC profile.

2.7.4. Service Invocation

Conforming LUAD WSPs MUST support invocation by a WSC based on a resource offering and credentials discovered by the WSC in a Principal’s Discovery Service:

luad-wsp-discinvk-001 The LUAD WSP MUST support invocation by a WSC as a discovered ID-WSF service.

2.7.5. PAOS

Conforming LUAD WSPs MAY support advertisement and invocation via PAOS:

luad-wsp-paos-001 The LUAD WSP MAY support advertisement and invocation via PAOS, as described in [LibertyPAOS].

2.7.6. LUAD

Conforming LUAD WSPs MUST support the LUAD-WSP profile:

luad-wsp-luad-001 The LUAD WSP MUST support the LUAD-WSP profile, as described in section 4 of [LibertyClientProfiles].
2.8. ID-FF Identity Provider (IdP) Conformance Profile

This section defines the conformance requirements for the ID-FF Identity Provider Profile. By supporting this profile, ID-FF IdPs enable ID-FF SP WSCs.

2.8.1. ID-FF DS Bootstrap

Conforming ID-FF IdPs MUST support Discovery Service Bootstrap:

`idffidp-bootstrap-001` The ID-FF IdP MUST include the Principal’s Discovery Service Resource Offering in ID-FF assertions, as described in section 6 of [LibertyDisco].

2.9. ID-WSF Identity Provider (IdP) Conformance Profile

This section defines the conformance requirements for the ID-WSF Identity Provider Profile. By supporting this profile, IdPs enable LUAD WSCs.

2.9.1. Authentication Service

Conforming IdPs MUST support authentication requests:

`idwsfidp-authsvc-001` The IdP MUST respond to authentication requests, as described in section 5 of [LibertyAuthn].

`idwsfidp-authsvc-002` The IdP MUST support the PLAIN and CRAM-MD5 authentication mechanisms, as referenced in appendix A of [LibertyAuthn].

2.9.2. SSO Service

Conforming IdPs MAY support sso requests:

`idwsfidp-ssosvc-001` The IdP MAY respond to sso requests, as described in section 6 of [LibertyAuthn].

2.10. Discovery Service (DS) Conformance Profile

This section defines the conformance requirements for the Discovery Service Profile.

2.10.1. WSP Common

Conforming DSs MUST support the Common WSP Profile

2.10.2. Interaction Redirect and Interaction Service

Conforming DSs MAY optionally support the following Interaction features:

`ds-interact-001` The DS MAY support redirect based user interaction, as described in section 4 of [LibertyInteract].
The DS MAY support invocation of a user interaction service, as described in section 5 of [LibertyInteract]. Note that the DS takes on the role of a WSC in making interaction service calls, and so is bound by all of the requirements specified in the applicable WSC profile.

### 2.10.3. Service Registration

Conforming DSs MUST support Discovery Service Modify:

The DS MUST process DS Modify InsertEntry requests, as described in section 5.2 of [LibertyDisco].

The DS MUST process DS Modify RemoveEntry requests, as described in section 5.2 of [LibertyDisco].

Conforming DSs MUST support the following Discovery Service Modify Directives:

The DS MUST support the EncryptResourceID directive, as described in section 5.2.1.1 of [LibertyDisco].

The DS MAY support the AuthenticateRequester, AuthorizeRequester and AuthenticateSessionContext directives, as described in section 5.2.1.1 of [LibertyDisco].

### 2.10.4. Service Discovery

Conforming DSs MUST support Discovery Service Queries:

The DS MUST process DS Query requests, as described in section 5.1 of [LibertyDisco].

### 2.10.5. PAOS

Conforming DSs MAY support advertisement and invocation via PAOS:

The DS MAY support advertisement and invocation via PAOS, as described in [LibertyPAOS].

### 2.10.6. LUAD

Conforming DSs MAY support the LUAD-DS profile:

The DS MAY support LUAD-DS profile, as described in section 5 of [LibertyClientProfiles].
2.11. Interaction Service (IS) Conformance Profile

This section defines the conformance requirements for the Interaction Service Profile.

2.11.1. WSP Common

Conforming ISs MUST support the Common WSP Profile

2.11.2. Interaction Service

Conforming ISs MUST support interaction requests:

is-interaction-001 The IS MUST respond to interaction requests, as described in section 5 of [LibertyInteract].

2.11.3. Service Registration

Conforming ISs MAY support registration with a Principal’s Discovery Service using DS Modify InsertEntry:

is-registration-001 The IS MAY invoke DS Modify InsertEntry at a Principal’s Discovery Service to register itself, as described in section 5.2 of [LibertyDisco]. Note that the LUAD WSP takes on the role of a WSC in making DS calls, and so is bound by all of the requirements specified in the applicable WSC profile.

2.11.4. PAOS

Conforming ISs MAY support advertisement and invocation via PAOS:

is-paos-001 The IS MAY support advertisement and invocation via PAOS, as described in [LibertyPAOS].

2.11.5. LUAD

Conforming ISs MAY support the LUAD-WSP profile:

is-luad-001 The IS MAY support LUAD-WSP profile, as described in section 4 of [LibertyClientProfiles].
References

Normative


Informative
