Liberty ID-WSF 2.0 Static Conformance Requirements

Version: 1.0-errata-v1.0

Editors:
Greg Whitehead, Hewlett-Packard

Contributors:
Robert Aarts, Hewlett-Packard
John Kemp, Nokia Corporation
Rob Lockhart, IEEE-ISTO
Paul Madsen, Nippon Telegraph and Telephone Corporation
Jonathan Sergent, Sun Microsystems, Inc.
Eric Tiffany, IEEE-ISTO

Abstract:

Defines the static conformance requirements for the Liberty Alliance ID-WSF 2.0 specifications.

Filename: liberty-idwsf-2.0-scr-1.0-errata-v1.0.pdf

₁ **Notice**

₂ This document has been prepared by Sponsors of the Liberty Alliance. Permission is hereby granted to use the
₃ document solely for the purpose of implementing the Specification. No rights are granted to prepare derivative works
₄ of this Specification. Entities seeking permission to reproduce portions of this document for other uses must contact
₅ the Liberty Alliance to determine whether an appropriate license for such use is available.

₆ Implementation of certain elements of this document may require licenses under third party intellectual property
₇ rights, including without limitation, patent rights. The Sponsors of and any other contributors to the Specification are
₈ not and shall not be held responsible in any manner for identifying or failing to identify any or all such third party
₉ intellectual property rights. **This Specification is provided "AS IS", and no participant in the Liberty Alliance**
₁₀ **makes any warranty of any kind, express or implied, including any implied warranties of merchantability,**
₁₁ **non-infringement of third party intellectual property rights, and fitness for a particular purpose.** Implementers
₁₂ of this Specification are advised to review the Liberty Alliance Project's website (http://www.projectliberty.org/) for
₁₃ information concerning any Necessary Claims Disclosure Notices that have been received by the Liberty Alliance
₁₄ Management Board.

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

Contents

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 (v2.0)

- LibertySecMech (v2.0)

- LibertySecMech20SAML (v2.0)

- LibertyDisco (v2.0)

- LibertyInteract (v2.0)

- LibertyPAOS (v2.0)

- LibertyAuthn (v2.0)

- LibertyClientProfiles (v2.0)

- LibertyPeopleService (v1.0)

This document defines these requirements. This is a normative document with several non-normative explanatory sections.

1.1. Framework Version

This specification defines framework version 2.0 (see SOAP Binding Framework header, as described in [LibertySOAPBinding]).

1.2. 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), Identity Provider (IdP), Discovery Service (DS), Interaction Service (IS), and People Service (PS).

- 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.

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

1.3. Notation

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

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

134 **EXAMPLE**   This is an example of the format of the normative requirements. Each requirement is identified
135   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

Feature	WSC Common	WSP Common
Basic SOAP Binding	MUST	MUST
Basic Security Mechanisms	MUST	MUST

Table 2. Concrete Profile Matrix

Feature	SAML SP WSC	LUAD WSC	SAML SP WSP	LUAD WSP	SAML IdP	ID-WSF IdP	DS	PS	IS
WSC Common	MUST	MUST							
WSP Common			MUST	MUST			MUST	MUST	MUST
SAML SP WSC SOAP Binding	MUST								
SAML SP WSC Security Mechanisms	MUST								
LUAD		MUST		MUST			OPT	OPT	OPT
SAML DS Bootstrap	MUST				MUST				
Authentication Service		MUST				MUST			
SSO Service	OPT	OPT				MUST			
Identity Mapping Service						MUST			
Service Registration			OPT	OPT			MUST		
Service Discovery	MUST	MUST					MUST		
Service Invocation	MUST	MUST							
Group & User Management	OPT	OPT						MUST	
Invitations	OPT	OPT						OPT	
Interaction Service									MUST

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

wsc-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 all required headers, and for failing if any unsupported Header is received with a `mustUnderstand` attribute set to true.

wsc-soapbind-002   The WSC MUST support processing of the EndpointUpdate Header, as described in [LibertySOAPBinding]. Specifically, the WSC MUST (a) be able to retry an operation as specified by a EndpointUpdate 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 EndpointUpdate 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 (at a minimum)

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

- urn:liberty:security:2005-02:null:Bearer

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

- urn:liberty:security:2005-02:TLS:Bearer

as described in section 6 of [LibertySecMech].

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 all required headers, and for failing if any unsupported Header is received with a `mustUnderstand` attribute set to true.

wsp-soapbind-002   The WSP MUST process the UserInteraction Header, as described in [LibertySOAPBinding].

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 (at a minimum)

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

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

177   or

178   • urn:liberty:security:2005-02:null:Bearer

179   • urn:liberty:security:2005-02:TLS:Bearer

180   or

181   • urn:liberty:security:2006-08:null:SAMLV2

182   • urn:liberty:security:2006-08:TLS:SAMLV2

183   • urn:liberty:security:2006-08:ClientTLS:peerSAMLV2

184   as described in section 6 of [LibertySecMech] and section 4 of [LibertySecMech20SAML].

2.4. SAML Service Provider (SP) Web Service Consumer (WSC) Conformance Profile

This section defines the requirements for the SAML SP Web Service Consumer Profile.

2.4.1. WSC Common

Conforming SAML SP WSCs MUST support the Common WSC Profile

2.4.2. SAML SP WSC SOAP Binding

Conforming SAML SP WSCs MUST support the following additional SOAP Binding features:

samlsp-wsc-soapbind-001   The SAML SP WSC MUST send the SOAP Binding Sender Header, as described in [LibertySOAPBinding].

samlsp-wsc-soapbind-002   SAML SP WSCs MUST support redirect based user interaction, as described in section 7 of [LibertySOAPBinding].

2.4.3. SAML SP WSC Security Mechanisms

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

samlsp-wsc-secmech-001   The WSC MUST be able to constuct and send ID-WSF messages using

                    • urn:liberty:security:2006-08:null:SAMLV2

                    • urn:liberty:security:2006-08:TLS:SAMLV2

                    • urn:liberty:security:2006-08:ClientTLS:peerSAMLV2

          as described in section 6 of [LibertySecMech] and section 4 of [LibertySecMech20SAML].

2.4.4. SAML DS Bootstrap

Conforming SAML SP WSCs MUST support Discovery Service Bootstrap:

samlsp-wsc-bootstrap-001 The SAML SP WSC MUST support extraction of the Principal's's Discovery Service EPR from the SAML assertion authenticating the Principal, as described in section 4 of [LibertyDisco].

2.4.5. SSO Service

Conforming SAML SP WSCs MAY support obtaining SAML tokens from an IdP:

samlsp-wsc-ssosvc-001 The SAML SP WSC MAY support invocation of an SSO Service using the SAML Token Service Profile, as described in section 6.4 of [LibertyAuthn].

2.4.6. Service Discovery and Service Invocation

Conforming SAML SP WSCs MUST support discovery and invocation of at least one ID-WSF service:

samlsp-wsc-discinvk-001 The SAML SP WSC MUST support querying and invocation of at least one ID-WSF service registered in a Principal's Discovery Service (samlsp-wsc-bootstrap-001), as described in [LibertyDisco].

samlsp-wsc-discinvk-002 The SAML SP WSC MAY support discovery and invocation of PAOS services, as described in [LibertyPAOS].

2.4.7. Group & User Management and Invitations

Conforming SAML SP WSCs MAY support management of groups & users and invitations in a People Service:

samlsp-wsc-people-001 The SAML SP WSC MAY support management of groups and users, as described in sections 3.9-3.20 of [LibertyPeopleService].

samlsp-wsc-people-002 The SAML SP WSC MAY support invitations, as described in section 4 of [LibertyPeopleService].

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. LUAD

Conforming LUAD 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].

2.5.3. 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].

2.5.4. SSO Service

Conforming LUAD WSCs MAY support obtaining SAML tokens from an IdP:

luad-wsc-ssosvc-001   The LUAD WSC MAY support invocation of an SSO Service using the SAML Token Service Profile, as described in section 6 of [LibertyAuthn].

luad-wsc-ssosvc-002   The LUAD WSC MAY support invocation of an SSO Service using the Enhanced Client or Proxy Profile, as described in section 6 of [LibertyAuthn].

2.5.5. 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 EPR for at least one ID-WSF service, as described in section 3.3 of [LibertyDisco].

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

2.5.6. Group & User Management and Invitations

Conforming LUAD WSCs MAY support management of groups & users and invitations in a People Service:

luad-wsc-people-001   The LUAD WSC MAY support management of groups and users, as described in sections 3.9-3.20 of [LibertyPeopleService].

luad-wsc-people-002   The LUAD WSC MAY support invitations, as described in section 4 of [LibertyPeopleService].

2.6. SAML Service Provider (SP) Web Service Provider (WSP) Conformance Profile

This section defines the requirements for the SAML SP Web Service Provider Profile.

2.6.1. WSP Common

Conforming SAML SP WSPs MUST support the Common WSP Profile

2.6.2. Service Registration

Conforming SAML SP WSPs MAY support registration with a Principal's Discovery Service:

samlsp-wsp-registration-001   The SAML SP WSP MAY invoke the DS at a Principal's Discovery Service to register itself, as described in [LibertyDisco]. Note that the SAML 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.

2.7. 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. 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].

2.7.3. Service Registration

Conforming LUAD WSPs MAY support registration with a Principal's Discovery Service or advertisement and invocation via PAOS:

luad-wsp-registration-001   The LUAD WSP MAY invoke a Principal's Discovery Service to register itself, as described in [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.

luad-wsp-registration-002   The LUAD WSP MAY support advertisement and invocation via PAOS, as described in [LibertyPAOS].

2.8. SAML Identity Provider (IdP) Conformance Profile

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

2.8.1. SAML DS Bootstrap

Conforming SAML IdPs MUST support Discovery Service Bootstrap:

samlidp-bootstrap-001   The SAML IdP MUST include the Principal's Discovery Service EPR in SAML assertions, as described in section 4 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 MUST support sso requests:

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

2.9.3. Identity Mapping Service

Conforming IdPs MUST support identity mapping requests:

idwsfidp-imsvc-001   The IdP MUST respond to identity mapping requests, as described in section 7 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. LUAD

Conforming DSs MAY support the LUAD-DS profile:

318   **ds-luad-001**   The DS MAY support LUAD-DS profile, as described in section 5 of [LibertyClientProfiles].

2.10.3. Service Registration and Discovery

320 Conforming DSs MUST support discovery service requests:

321 **ds-discovery-001**   The DS MUST respond to discovery service requests, as described in section 3 of [Liberty-
322   Disco].

2.11. People Service (PS) Conformance Profile

324 This section defines the conformance requirements for the People Service Profile.

2.11.1. WSP Common

326 Conforming PSs MUST support the Common WSP Profile

2.11.2. LUAD

328 Conforming PSs MAY support the LUAD-WSP profile:

329   **ps-luad-001**   The PS MAY support LUAD-WSP profile, as described in section 4 of [LibertyClientProfiles].

2.11.3. Group & User Management and Invitations

331 Conforming PSs MUST support the following group & user management features:

332   **ps-people-001**   The PS MUST support group and user management, as described in sections 3.9-3.20 of
333   [LibertyPeopleService]

334 Conforming PSs MAY support the following invitation features:

335   **ps-people-002**   The PS MAY support user invitations as described in section 4 of [LibertyPeopleService].

2.12. Interaction Service (IS) Conformance Profile

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

2.12.1. WSP Common

339 Conforming ISs MUST support the Common WSP Profile

2.12.2. LUAD

341 Conforming ISs MAY support the LUAD-WSP profile:

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

2.12.3. Interaction Service

344 Conforming ISs MUST support interaction service requests:

345 **is-interaction-001**   The IS MUST respond to interaction requests, as described in [LibertyInteract].

References

Normative

[LibertySOAPBinding] Hodges, Jeff, Kemp, John, Aarts, Robert, Whitehead, Greg, Madsen, Paul, eds. "Liberty ID-WSF SOAP Binding Specification," Version 2.0-errata-v1.0, Liberty Alliance Project (21 April, 2007). *http://www.projectliberty.org/specs*

[LibertySecMech] Hirsch, Frederick, eds. "Liberty ID-WSF Security Mechanisms Core," Version 2.0-errata-v1.0, Liberty Alliance Project (21 April, 2007). *http://www.projectliberty.org/specs*

[LibertySecMech20SAML] Hirsch, Frederick, eds. "ID-WSF 2.0 SecMech SAML Profile," Version 2.0-errata-v1.0, Liberty Alliance Project (08 November, 2006). *http://www.projectliberty.org/specs*

[LibertyDisco] Cahill, Conor, Hodges, Jeff, eds. "Liberty ID-WSF Discovery Service Specification," Version 2.0-errata-v1.0, Liberty Alliance Project (29 November, 2006). *http://www.projectliberty.org/specs*

[LibertyInteract] Aarts, Robert, Madsen, Paul, eds. "Liberty ID-WSF Interaction Service Specification," Version 2.0-errata-v1.0, Liberty Alliance Project (21 April, 2007). *http://www.projectliberty.org/specs*

[LibertyPAOS] Aarts, Robert, Kemp, John, eds. "Liberty Reverse HTTP Binding for SOAP Specification," Version 2.0, Liberty Alliance Project (30 July, 2006). *http://www.projectliberty.org/specs*

[LibertyAuthn] Hodges, Jeff, Aarts, Robert, Madsen, Paul, Cantor, Scott, eds. " Liberty ID-WSF Authentication, Single Sign-On, and Identity Mapping Services Specification ," Version 2.0-errata-v1.0, Liberty Alliance Project (28 November, 2006). *http://www.projectliberty.org/specs*

[LibertyClientProfiles] Aarts, Robert, Kainulainen, Jukka, Kemp, John, eds. "Liberty ID-WSF Profiles for Liberty-Enabled User Agents and Devices," Version 2.0-errata-v1.0, Liberty Alliance Project (22 January, 2007). *http://www.projectliberty.org/specs*

[LibertyPeopleService] Koga, Yuzo, Madsen, Paul, eds. "Liberty ID-WSF People Service Specification," Version 1.0-errata-v1.0, Liberty Alliance Project (06 March, 2007). *http://www.projectliberty.org/specs*

[LibertyIDWSFv20Errata] Champagne, Darryl, Lockhart, Rob, Tiffany, Eric, eds. "Liberty ID-WSF 2.0 Errata," Version 1.0, Liberty Alliance Project (13 April, 2007). *http://www.projectliberty.org/specs*

Informative

[LibertyIDWSFGuide] Weitzel, David, eds. "Liberty ID-WSF Implementation Guide," Version 2.0-02, Liberty Alliance Project (13 January, 2005). *http://www.projectliberty.org/specs*

[LibertyGlossary] Hodges, Jeff, eds. "Liberty Technical Glossary," Version v2.0, Liberty Alliance Project (30 July, 2006). *http://www.projectliberty.org/specs*