Liberty ID-FF Implementation Guidelines

Draft Version 1.2-02

14 April 2003

Editor:

Tom Wason, IEEE-ISTO

Abstract:

This document defines the recommended implementation guidelines and checklists for the Liberty architecture focused on deployments for the service-providing entities: service providers, identity providers, and Liberty-enabled clients or proxies (LECPs). It is intended to provide recommended implementation guidelines to Liberty component developers to help them decide what they need to implement to meet their business needs. Because Liberty Phase 1 does not provide formal compliance, this document does not contain any conformance requirements — only recommendations.

Notice

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

Document History

Rev	Date	By Whom	Description
1.2	27-Mar-03	Tom Wason	• Addition of Name Identifier Mapping profiles to Identity Provider and Service Provider.
1.2	27-Mar-03	Tom Wason	• Addition of Introduction Notification to Identity Provider
1.2	27-Mar-03	Tom Wason	• Addition of Provider Relationship Termination to Identity Provider, Services Provider
1.2	12-Apr-03	Tom Wason	• Abstract added.

Table of Contents

1 Introduction

This document defines the recommended implementation guidelines and checklists for the Liberty architecture focused on deployments for the service-providing entities: service providers, identity providers, and Liberty-enabled clients or proxies (LECPs). It is intended to provide recommended implementation guidelines to Liberty component developers to help them decide what they need to implement to meet their business needs. Because Liberty Phase 1 does not provide formal compliance, this document does not contain any conformance requirements — only recommendations. A recommended profile tailored according to the high-level Liberty features is provided for different Liberty service-providing entities. Implementers facing specific needs can decide to implement what they need and claim support for each specific feature separately.

The document also provides a checklist of requirements based on the following Liberty architecture specification categories that implementers can use to advertise their supported feature set:

- Functionality in the Liberty protocols and schemas described
- Bindings and profiles defined for each Liberty protocol type (specific interactions between identity providers, service providers, and LECPs)
- The authentication request and reply context-specific information

Definitions for Liberty-specific terms can be found in [LibertyGloss]. Note: Phrases and numbers in brackets [ ] refer to other documents; details of these references can be found in Section 4 (at the end of this document).

Policy/Security and Technical notes related to implementations are covered by Liberty Architecture Overview document associated with this Implementation Guidelines document specified by [LibertyArchOverview].

2 Recommended Liberty Architecture Implementation Guidelines

The recommended implementation guidelines for identity providers, service providers, and LECPs are listed in the tables in 2.1 through 2.3. The guidelines refer to front-channel-based and back-channel-based mechanisms. *Front channel* is described as a communication channel where HTTP redirect-, GET-, and POST-based request and response protocol messages between the identity provider and the service provider flow through the Web browser. *Back channel* is a SOAP/HTTP-based direct communication channel between the identity provider and the service provider. A service provider with SOAP client support is considered to be a "back-channel-capable SP" whereas a "basic SP" is not back-channel-capable.

2.1 Identity Provider Implementation Guidelines

Liberty Feature	Recommendations
Single Sign-On	It is strongly recommended that identity providers support the LECP single sign-on profile to ensure forward compatibility. The LECP profile is intended for future clients of all kinds (thin and thick) as well as existing wireless thin clients (WML, HDML, etc) when used with a LEP. Identity providers that want to support existing HTML client environments should implement the browser artifact and the browser POST single sign-on profiles. To support existing WML client in environments that do not contain any LEP, identity providers should support the WML single sign-on profile.
Identity Federation	Identity providers that want to support permanent identity linking between service providers and identity providers (beyond the stateless single sign-on association) should support the `<Federate>` element of the `<AuthnRequest>` for all the supported single sign-on profiles.
Federation Termination Notification	Identity providers that support identity federation should also support the Federation Termination Notification Protocol. When supported, both service-provider-initiated and identity-provider-initiated federation termination notification should be supported. Liberty offers two federation termination notification mechanisms: • Front channel, or HTTP-redirect-based • Back channel, or SOAP-based As a minimum, identity providers should support the front-channel-based mechanism. Identity providers that want to support back-channel-capable SPs should implement both mechanisms.
Name Registration	The Name Registration Protocol allows the service provider to use its own opaque handle to identify the Principal when communicating with the identity provider (rather than using the identity provider's opaque handle generated during federation). This protocol also allows the identity provider to register a new name identifier with the service provider at any time after federation. When supported, both service-provider-initiated and identity-provider-initiated Name Registration should be supported. Liberty offers two Name Registration mechanisms: • Front channel, or HTTP-redirect-based

Liberty Feature	Recommendations
	• Back channel, or SOAP-based At a minimum, identity providers should support the front-channel-based mechanism. Identity providers that want to support back-channel-capable SPs should implement both mechanisms.
Single Logout	The Single Logout Protocol allows logging out a Principal from all its active sessions to service providers, linked to an identity provider. Identity providers keeping trace of the Principal's service provider sessions should implement this feature. When supported, both service-provider-initiated and identity-provider-initiated single logout should be supported. Liberty offers two single logout mechanisms: • Front channel, or HTTP-redirect-based • Back channel, or SOAP-based As a minimum, identity providers supporting this feature should support the front-channel-based mechanism. Identity providers that want to support back-channel-capable SPs should implement both mechanisms.
Identity Provider Introduction	Identity providers that want to support more than a single circle of trust simultaneously should support the Identity Provider Introduction Protocol.
Name Identifier Mapping	Identify providers that want to enable service providers to communicate with each other about the Principal, in the absence of a federation between them, should support the Name Identifier Mapping SAML profile. The Name Identifier may be obfuscated to protect the Principal's privacy.
Introduction Notification	One identity provider may introduce another identity provider to a service provider. Identity providers that need to notify, or be notified of, the federation of a Principal between a service provider and the introduced identity provider should support the SOAP-based Introduction Notification.
Provider Relationship Termination	An identity provider that wants to introduce service providers to new identity providers should support the SOAP-based Provider Relationship Termination protocol in order to notify those service providers when it severs a relationship with another identity provider.

91
92

2.2 Service Provider Implementation Guidelines

In general service providers are divided in two categories: the back-channel-capable SPs and the basic SPs (that are not back-channel-capable).

Liberty Feature	Recommendations
Single Sign-On	It is strongly recommended that service providers support the LECP single sign-on profile to ensure forward compatibility. The LECP profile is intended for future clients of all kinds (thin and thick) as well as existing wireless thin clients (WML, HDML, etc) when used with a LEP. Service providers that want to support existing HTML client environments should implement the browser artifact and the browser POST single sign-on profiles. To support existing WML client in environments that do not contain any LEP, service providers should support the WML single sign-on profile.
Identity Federation	Service providers that want to support permanent identity linking between service providers and identity providers (beyond the stateless single sign-on association) should support the `<Federate>` element of the `<AuthnRequest>` for all the supported single sign-on profiles.
Federation Termination Notification	Service providers that support identity federation should also support the Federation Termination Notification Protocol. When supported, both service-provider-initiated and identity-provider-initiated federation termination notification should be supported. Service providers should support either the front-channel or back-channel federation termination notification mechanisms depending on their respective capabilities although nothing prevents them from supporting both mechanisms if desired.
Name Registration	The Name Registration Protocol allows the service provider to use its own opaque handle to identify the Principal when communicating with the identity provider (rather than using the identity provider's opaque handle generated during federation). This protocol also allows the service provider to register a new name identifier with the identity provider at any time after federation. Service providers should support either the front-channel or back-channel Name Registration mechanisms depending on their respective capabilities although nothing prevents them from supporting both mechanisms if desired.
Single Logout	The Single Logout Protocol allows logging out a Principal from all its active sessions to service providers, linked to an identity provider. When supported, both service-provider-initiated and identity-provider-initiated single logout should be supported. Service providers should support either the front-channel or back-channel single logout mechanisms depending on their respective capabilities although nothing prevents them from supporting both mechanisms if desired.
Identity Provider Introduction	Service providers that want to support networks with more than a single circle of trust simultaneously should support the Identity Provider Introduction Protocol.
Name Identifier Mapping	Service providers that want to communicate with other service

Liberty Feature	Recommendations
	providers about a Principal that has not federated between them should support the Name Identifier Mapping SAML profile.
Provider Relationship Termination	A service provider that wants to allow itself to be introduced to new identity providers should support the SOAP-based Provider Relationship Termination protocol in order to be notified when identity providers involved in introduction transactions sever their relationships.

2.3 LECP Implementation Guidelines

Liberty Feature	Recommendations
Single Sign-On	Support for LECP single sign-on profile.

100 # 3 Liberty Architecture Specifications Checklist

101 ## 3.1 Liberty Bindings and Profiles Requirements — Identity Provider

102

Req ID#	Description	Ref	Y/N
IDP-FED-1	Identity Federation	Section 3.2.1 [LibertyBindProf]	
IDP-SSO-1	Single Sign-On using Browser Artifact	Section 3.2.2 [LibertyBindProf]	
IDP-SSO-2	Single Sign-On using Browser POST	Section 3.2.3 [LibertyBindProf]	
IDP-SSO-3	Single Sign-On using WML POST	Section 3.2.4 [LibertyBindProf]	
IDP-SSO-4	Single Sign-On using LECP	Section 3.2.5 [LibertyBindProf]	
IDP-REG-1	Register Name Identifier — Front Channel	Section 3.3 [LibertyBindProf]	
IDP-REG-2	Register Name Identifier — Back Channel	Section 3.3 [LibertyBindProf]	
IDP-REG-3	Register Name Identifier (Identity Provider initiated) — Front Channel	Section 3.3.1.1 [LibertyBindProf]	
IDP-REG-4	Register Name Identifier (Identity Provider initiated) — Back Channel	Section 3.3.1.2 [LibertyBindProf]	
IDP-REG-5	Register Name Identifier (Service Provider initiated) — Front Channel	Section 3.3.2.1 [LibertyBindProf]	
IDP-REG-6	Register Name Identifier (Service Provider initiated) — Back Channel	Section 3.3.2.2 [LibertyBindProf]	
IDP-FED-2	Identity Federation Termination — Front Channel	Section 3.4 [LibertyBindProf]	
IDP-FED-3	Identity Federation Termination — Back Channel	Section 3.4 [LibertyBindProf]	
IDP-FED-4	Federation Termination Notification (Identity Provider Initiated) — Front Channel	Section 3.4.1.1 [LibertyBindProf]	
IDP-FED-5	Federation Termination Notification (Identity Provider Initiated) — Back Channel	Section 3.4.1.2 [LibertyBindProf]	
IDP-FED-6	Federation Termination Notification (Service Provider Initiated) — Front Channel	Section 3.4.2.1 [LibertyBindProf]	
IDP-FED-7	Federation Termination Notification (Service Provider Initiated) — Back Channel	Section 3.4.2.2 [LibertyBindProf]	
IDP-SLO-1	Single Logout	Section 3.5 [LibertyBindProf]	
IDP-SLO-2	Single Logout Initiated by Identity Provider: Redirect	Section 3.5.1.1 [LibertyBindProf]	
IDP-SLO-3	Single Logout Initiated by Identity Provider: SOAP	Section 3.5.1.2	

Req ID#	Description	Ref	Y/N
		[LibertyBindProf]	
IDP-SLO-4	Single Logout Initiated by Service Provider: Redirect	Section 3.5.2.1 [LibertyBindProf]	
IDP-SLO-5	Single Logout Initiated by Service Provider: SOAP	Section 3.5.2.2 [LibertyBindProf]	
IDP-INT-1	Identity Provider Introduction	Section 3.6 [LibertyBindProf]	
IDP-COM-1	HTTP Connection over SSL3.0 or TLS1.0 [RFC2246], WTLS	[SSLv3], [RFC2246], [WTLS]	
IDP-COM-2	Support for Minimum URL length of 256 bytes	[RFC2965]	
IDP-COM-3	Support for Session Cookies	[RFC2965]	
IDP-NIM-1	Name Identifier Mapping request Initiated by Service Provider: SOAP	Section 3.7 [LibertyBindProf]	
IDP-IN-1	Introduction Notification initiated by an Identity Provider: SOAP	Section 3.8 [LibertyBindProf]	
IDP-PRT-1	Provider Relationship Termination initiated by an Identity Provider: SOAP/HTTP	Section 3.9 [LibertyBindProf]	

3.2 Liberty Bindings and Profiles Requirements — Service Provider

Req ID#	Description	Ref	Y/N
SP-FED-1	Identity Federation	Section 3.2.1 [LibertyBindProf]	
SP-SSO-1	Single Sign-On using Browser Artifact	Section 3.2.2 [LibertyBindProf]	
SP-SSO-2	Single Sign-On using Browser POST	Section 3.2.3 [LibertyBindProf]	
SP-SSO-3	Single Sign-On using WML	Section 3.2.4 [LibertyBindProf]	
SP-SSO-4	Single Sign-On using LECP	Section 3.2.5 [LibertyBindProf]	
SP-REG-1	Register Name Identifier — Front Channel	Section 3.3 [LibertyBindProf]	
SP-REG-2	Register Name Identifier — Back Channel	Section 3.3 [LibertyBindProf]	
SP-REG-3	Register Name Identifier (Identity Provider initiated) — Front Channel	Section 3.3.1.1 [LibertyBindProf]	
SP-REG-4	Register Name Identifier (Identity Provider initiated) — Back Channel	Section 3.3.1.2 [LibertyBindProf]	
SP-REG-5	Register Name Identifier (Service Provider initiated) — Front Channel	Section 3.3.2.1 [LibertyBindProf]	
SP-REG-6	Register Name Identifier (Service Provider initiated) — Back Channel	Section 3.3.2.2 [LibertyBindProf]	
SP-FED-2	Identity Federation Termination — Front Channel	Section 3.4 [LibertyBindProf]	

Req ID#	Description	Ref	Y/N
SP-FED-3	Identity Federation Termination — Back Channel	Section 3.4 [LibertyBindProf]	
SP-FED-4	Federation Termination Notification (Identity Provider Initiated) — Front Channel	Section 3.4.1.1 [LibertyBindProf]	
SP-FED-5	Federation Termination Notification (Identity Provider Initiated) — Back Channel	Section 3.4.1.2 [LibertyBindProf]	
SP-FED-6	Federation Termination Notification (Service Provider Initiated) — Front Channel	Section 3.4.2.1 [LibertyBindProf]	
SP-FED-7	Federation Termination Notification (Service Provider Initiated) — Back Channel	Section 3.4.2.2 [LibertyBindProf]	
SP-SLO-1	Single Logout	Section 3.5 [LibertyBindProf]	
SP-SLO-2	Single Logout Initiated by Identity Provider: Redirect	Section 3.5.1.1 [LibertyBindProf]	
SP-SLO-3	Single Logout Initiated by Identity Provider: SOAP	Section 3.5.1.2 [LibertyBindProf]	
SP-SLO-4	Single Logout Initiated by Service Provider: Redirect	Section 3.5.2.1 [LibertyBindProf]	
SP-SLO-5	Single Logout Initiated by Service Provider: SOAP	Section 3.5.2.2 [LibertyBindProf]	
SP-INT-1	Identity Provider Introduction	Section 3.6 [LibertyBindProf]	
SP-COM-1	HTTP Connection over SSL3.0 or TLS1.0 [RFC2246], WTLS	[SSLv3], [RFC2246], [WTLS]	
SP-COM-2	Support for Minimum URL Length of 256 bytes	[RFC2965]	
SP-COM-3	Support for Session Cookies	[RFC2965]	
IDP-NIM-1	Name Identifier Mapping request Initiated by Service Provider: SOAP	Section 3.7 [LibertyBindProf]	
IDP-PRT-1	Provider Relationship Termination initiated by an Identity Provider: SOAP/HTTP	Section 3.9 [LibertyBindProf]	

3.3 Liberty Bindings and Profiles Requirements — LECP

Req ID#	Description	Ref	Y/N
LECP-SSO-1	Single Sign-On using LECP	Section 3.2.5 [LibertyBindProf]	
LECP-COM-1	Support for Minimum URL Length of 256 bytes	[RFC2965]	
LECP-COM-2	Support for Session Cookies	[RFC2965]	

3.4 Authentication Context Requirements — Identity Provider

Req ID#	Description	Ref	Y/N
IDP-AUTHN-01	MobileContract	Section 5.1.1 [LibertyAuthnContext]	
IDP-AUTHN-02	MobileDigitalID	Section 5.1.2 [LibertyAuthnContext]	
IDP-AUTHN-03	MobileUnregistered	Section 5.1.3 [LibertyAuthnContext]	
IDP-AUTHN-04	Password	Section 5.1.4 [LibertyAuthnContext]	
IDP-AUTHN-05	Password-ProtectedTransport	Section 5.1.5 [LibertyAuthnContext]	
IDP-AUTHN-06	Previous-Session	Section 5.1.6 [LibertyAuthnContext]	
IDP-AUTHN-07	Smartcard	Section 5.1.7 [LibertyAuthnContext]	
IDP-AUTHN-08	Smartcard-PKI	Section 5.1.8 [LibertyAuthnContext]	
IDP-AUTHN-09	Software-PKI	Section 5.1.9 [LibertyAuthnContext]	
IDP-AUTHN-10	Time-Sync-Token	Section 5.1.10 [LibertyAuthnContext]	

3.5 Authentication Context Requirements — Service Provider

Req ID#	Description	Ref	Y/N
SP-AUTHN-01	MobileContract	Section 5.1.1 [LibertyAuthnContext]	
SP-AUTHN-02	MobileDigitalID	Section 5.1.2 [LibertyAuthnContext]	
SP-AUTHN-03	MobileUnregistered	Section 5.1.3 [LibertyAuthnContext]	
SP-AUTHN-04	Password	Section 5.1.4 [LibertyAuthnContext]	
SP-AUTHN-05	Password-ProtectedTransport	Section 5.1.5 [LibertyAuthnContext]	
SP-AUTHN-06	Previous-Session	Section 5.1.6 [LibertyAuthnContext]	
SP-AUTHN-07	Smartcard	Section 5.1.7 [LibertyAuthnContext]	
SP-AUTHN-08	Smartcard-PKI	Section 5.1.8 [LibertyAuthnContext]	
SP-AUTHN-09	Software-PKI	Section 5.1.9	

Req ID#	Description	Ref	Y/N
		[LibertyAuthnContext]	
SP-AUTHN-10	Time-Sync-Token	Section 5.1.10 [LibertyAuthnContext]	

115

116 3.6 Authentication Context Requirements — LECP

117

Req ID#	Description	Ref	Y/N
LECP-AUTHN-01	MobileContract	Section 5.1.1 [LibertyAuthnContext]	
LECP-AUTHN-02	MobileDigitalID	Section 5.1.2 [LibertyAuthnContext]	
LECP-AUTHN-03	MobileUnregistered	Section 5.1.3 [LibertyAuthnContext]	
LECP-AUTHN-04	Password	Section 5.1.4 [LibertyAuthnContext]	
LECP-AUTHN-05	Password-ProtectedTransport	Section 5.1.5 [LibertyAuthnContext]	
LECP-AUTHN-06	Previous-Session	Section 5.1.6 [LibertyAuthnContext]	
LECP-AUTHN-07	Smartcard	Section 5.1.7 [LibertyAuthnContext]	
LECP-AUTHN-08	Smartcard-PKI	Section 5.1.8 [LibertyAuthnContext]	
LECP-AUTHN-09	Software-PKI	Section 5.1.9 [LibertyAuthnContext]	
LECP-AUTHN-10	Time-Sync-Token	Section 5.1.10 [LibertyAuthnContext]	

118

119

4 References

[LibertyArchOverview] Hodges, J., & Wason, T., eds. (January 2003) "Liberty Architecture Overview," Version 1.1. Liberty Alliance Project, <http://www.projectliberty.org/specs/>.

[LibertyAuthnContext] Madsen, P., & Kemp, J., eds. (January 2003). "Liberty Authentication Context Specification," Version 1.1. Liberty Alliance Project, <http://www.projectliberty.org/specs/>.

[LibertyBindProf] Rouault, J., & Wason, T., eds. (January 2003). "Liberty Bindings and Profiles Specification," Version 1.1. Liberty Alliance Project, <http://www.projectliberty.org/specs/>.

[LibertyGloss] Mauldin, H., & Wason, T., eds. (January 2003). "Liberty Architecture Glossary," Version 1.1. Liberty Alliance Project, <http://www.projectliberty.org/specs/>.

[LibertyProtSchema] Beatty, J., & Kemp, J., eds. (January 2003). "Liberty Protocols and Schema Specification," Version 1.1. Liberty Alliance Project, <http://www.projectliberty.org/specs/>.

[RFC2246] Dierks, T.,& Allen, C. (January 1999). "The TLS Protocol Version 1.0," RFC 2246. The Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc2246.txt> [18 December 2002]

[RFC2965] Kristol, D., & Montulli, L. (October 2000). "HTTP State Management Mechanism," RFC 2965. The Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc2965.txt> [18 December 2002].

[SAMLBind] Mishra, P., ed. (05 Nov. 2002). "Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML)," Version 1.0, OASIS Standard. Organization for the Advancement of Structured Information Standards, <http://www.oasis-open.org/committees/security/#documents> [18 December 2002].

[SAMLCore] Hallam-Baker, P., Maler, E., eds. (05 Nov. 2002). "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)," Version 1.0, OASIS Standard. Organization for the Advancement of Structured Information Standards, <http://www.oasis-open.org/committees/security/#documents> [18 December 2002].

[SOAP1.1] D. Box et al. (May 2000). "Simple Object Access Protocol (SOAP) 1.1," Note. World Wide Web Consortium, <http://www.w3.org/TR/SOAP> [18 December 2002].

[SSLv3] Freier, A. O., Karlton, P., & Kocher, P. (November 1996). "The SSL Protocol," Version 3.0, Internet Draft 02. Internet Engineering Task Force, <http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt> [18 December 2002].

[WML1.3] (February 2000). "Wireless Application Protocol Wireless Markup Language Specification" Version 1.3. Wireless Application Protocol Forum, Ltd., <http://www.wapforum.org/what/technical.htm> [18 December 2002].

[WTLS] (September 2001). "Wireless Transport Layer Security" Wireless Application Forum, Ltd., <http://www.wapforum.org/what/technical.htm> [18 December 2002].

[XMLSig] Eastlake, D., Reagle, J., Solo, D., et al. (February 2002). "XML-Signature Syntax and Processing," Recommendation. World Wide Web Consortium, <http://www.w3.org/TR/xmldsig-core/> [18 December 2002].