DRAFT

Liberty Version 1.0 Errata

Edition 00

11 October 2002

Document Description: draft-liberty-version-1-errata-00

Notice

This Errata document refers to the Liberty Version 1.0 documents Architecture Overview, Protocols and Schemas Specification, Liberty Bindings and Profiles Specification, and Liberty Protocols and Schemas Specification. This Errata document has been prepared by Sponsors of the Liberty Alliance. Permission is hereby granted to use the Errata solely for the purpose of implementing the Specification. No rights are granted to prepare derivative works of this Errata. 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 the Specifications this Errata references may involve the use of one or more of the following United States Patents claimed by AOL Time Warner, Inc.: No.5,774,670, No.6,134,592, No.5,826,242, No. 5,825,890, and No.5,671,279. The Sponsors of the Specification take no position concerning the evidence, validity or scope of the claimed subject matter of the aforementioned patents. Implementation of certain elements of this Specification may also require licenses under third party intellectual property rights other than those identified above, including without limitation, patent rights. The Sponsors of the Specification are not and shall not be held responsible in any manner for identifying or failing to identify any or all such intellectual property rights that may be involved in the implementation of the Specification.

This Specification Errata 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 or third party intellectual property rights, and fitness for a particular purpose.

Liberty Alliance Project
Licensing Administrator
c/o IEEE-ISTO
445 Hoes Lane, P.O. Box 1331
Piscataway, NJ 08855-1331, USA

Editor

Jeff Hodges, Sun Microsystems, Jeff.Hodges@sun.com

Contributors

The following Liberty Alliance Project Sponsor companies contributed to the development of this specification:

ActivCard
American Express Travel Related Services
America Online, Inc.
Bank of America
Bell Canada
Cingular Wireless
Cisco Systems, Inc.
Citigroup
Communicator, Inc.
Consignia
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
Netegrity
NeuStar
Nextel Communications
Nippon Telegraph and Telephone Company
Nokia Corporation
Novell, Inc.
NTT DoCoMo, Inc.
OneName Corporation
Openwave Systems Inc.
PricewaterhouseCoopers LLP
Register.com
RSA Security Inc
Sabre Holdings Corporation
SAP AG
SchlumbergerSema
SK Telecom
Sony Corporation
Sun Microsystems, Inc.
United Airlines
VeriSign, Inc.
Visa International
Vodafone Group Plc
Wave Systems

Document History

Edition #	Date	Editor	Scope of changes
00	11-Oct-02	Jeff Hodges	Change Requests (CR numbers are included for Liberty Alliance internal reference only): 1103: In [1], 5.4.3.2 Liberty Browser POST Profile, argument of HTML and URLs is inversed. 1107: In [1], 5.7.1.3 Login via Embedded Form, incomplete policy/security note. 1122: In [3], 4.4.1 Common Threats for All Profiles, add security consideration statement correlating authentication requests with session holders 1129, 1130: In [2], [3], LEC open to a man-in-the-middle attack. Solution supplied.

Table of Contents

1 Introduction

This document lists errata in the Liberty v1.0 specification set. This specification set is listed in section 2 below. This is not an authoritative document, nor a final version, but a precursor for changes that will likely be included in a next revision of the Liberty v1 specification set.

Liberty v1.0 protocols as initially specified contained certain material and editorial errors, collectively referred to as *errata*. Readers of the Liberty v1.0 Specification Set should note the errata in this document and incorporate it into their reading of the specification set. Also, implementers of the Liberty v1.0 specification set should use the Liberty XSD contained in the file:

Filename: liberty-architecture-protocols-schemas-v1.0-errata-00.xsd

Location: http://www.projectliberty.org/specs/liberty-architecture-protocols-schemas-v1.0-errata-00.xsd

2 Target Specifications

The following specifications and XSD file are the targets of this errata document, and are referred to by the numbers in square brackets in the remainder of this document:

[1] Liberty Architecture Overview
http://www.projectliberty.org/specs/liberty-architecture-overview-v1.0.pdf

[2] Liberty Protocols and Schemas Specification
http://www.projectliberty.org/specs/liberty-architecture-protocols-schemas-v1.0.pdf

[3] Liberty Bindings and Profiles Specification
http://www.projectliberty.org/specs/liberty-architecture-bindings-and-profiles-v1.0.pdf

[4] Liberty Authentication Context Specification
http://www.projectliberty.org/specs/liberty-architecture-authentication-context-v1.0.pdf

[5] Liberty Glossary
http://www.projectliberty.org/specs/liberty-tech-glossary-v1.0.pdf

[6] Liberty Architecture Implementation Guidelines
http://www.projectliberty.org/specs/liberty-architecture-impl-guidelines-v1.0.pdf

[7] Liberty Protocols and Schemas Specification XSD file
http://www.projectliberty.org/specs/liberty-architecture-protocols-schemas-v1.0.xsd

3 Abbreviations

The following abbreviations are used in this document:

SE - Substantive Errata designator

AO - Architecture Overview [1] editorial errata designator

BP - Bindings and profiles [3] editorial errata designator

CR - Change Request entry number (CR numbers are included for Liberty Alliance internal reference only)

4 Substantive Errata (SE)

This section details *substantive* errata in the Liberty v1.0 specification set. "Substantive" means that the resolution of any of these errata causes a material change to the protocol specification. Because the Liberty v1.0 protocols are specified using a set of discrete specifications, the resolution of a given substantive erratum may affect more than one of the specification documents. See erratum SE1 for an example.

Erratum Designator	*Erratum Title*	*CRs*	*Summary and Resolution*
SE1	**LECP Security Vulnerability**	**1129, 1130**	

Summary:

Affected specifications and XSD file: [2], [3], [7].

The specifications, as they are written, leave the Liberty-enabled Client/Proxy (LECP) open to a man-in-the-middle attack where it can unknowingly enable a spurious site to access its account(s) at any service provider which implements the browser post, WML post, or LECP profiles.

The LECP profile allows the service provider to include its assertion consumer service URL in the <lib:AuthnRequestEnvelope> that it sends to the LECP. The LECP gets an assertion from the identity provider and then sends it to the assertion consumer service URL. As currently specified, there is no provision for validation of the assertion consumer service URL as the legitimate place to send the assertion; therefore, a spurious site can interpose itself between the user and the SP. This enables it to change this URL so that it obtains the authentication assertion and thus can impersonate the user at the SP.

Resolution:

1) lines 560-562 of [2]: Change to:

In some profiles, an intermediary is active between the service provider's authentication request and the identity provider's authentication response. Examples of an active intermediary are a user agent or client proxy that implement the "Liberty-Enabled Client and Proxy Profile" described in [LibertyBindProf].

NOTE: an active intermediary has the capability to return status codes to the service provider it interacts with. For example, the intermediary may be unable to contact an identity provider identified by the service provider, and the intermediary may return a status code to the service provider indicating that an error occured. Status codes MUST be conveyed within `<AuthnResponse>` messages using the `<samlp:Status>` element. Specific values for specific cases are defined below.

For all profiles specifying an active intermediary, the profile specification must:

- Specify whether the `<AuthnRequest>` element sent from the service provider to the identity provider via the intermediary is wrapped in an `<AuthnRequestEnvelope>`. See section 3.2.4.
- Specify whether the `<AuthnResponse>` element sent from the identity provider to the service provider via the intermediary is wrapped in an `<AuthnResponseEnvelope>`. See section 3.2.5.

3.2.3.1.1 Processing Rules for Active Intermediaries

For all profiles specifying an active intermediary, the intermediary MUST follow these processing rules:

Erratum Designator	*Erratum Title*	*CRs*	*Summary and Resolution*
SE1	**LECP Security Vulnerability**	**1129, 1130**	

- If the profile specifies that the message sent from the service provider to the identity provider, via the intermediary, is wrapped in an `<AuthnRequestEnvelope>`:
  - The intermediary MUST remove the enveloping `<AuthnRequestEnvelope>` before forwarding the `<AuthnRequest>` element to the identity provider.
- The intermediary MAY locally generate `<AuthnResponse>` elements and send them to the service provider using the `<AssertionConsumerServiceURL>` contained within the `<AuthnRequestEnvelope>`. Such `<AuthnResponse>` elements MUST NOT contain any `<lib:Assertion>` elements. These messages MAY be generated as a result of local errors on the intermediary, and should indicate the underlying reasons in the <samlp:Status> element in the `<AuthnResponse>`. The following are error conditions for which `<samlp:Status>` values are defined in section 3.2.3.1.2:
  - The identity provider cannot be reached
  - There is no identity provider in common between the intermediary and the service provider
- If the profile specifies that the message from the identity provider to the service provider, via the intermediary, is wrapped in an `<AuthnResponseEnvelope>`:
  - The intermediary MUST remove the enveloping `<AuthnResponseEnvelope>` before forwarding the `<AuthnResponse>` element to the service provider.
  - The intermediary MUST send `<AuthnResponse>` messages received from the identity provider to the service provider using the `<AssertionConsumerServiceURL>` contained within the `<AuthnResponseEnvelope>` ***sent by the identity provider***.

3.2.3.1.2 Status Code Values for Error Conditions

If an error occurs in the processing at the intermediary, the following status code values are defined for the `<samlp:Status>` element:

2) lines 568-570 (section 3.2.4) of [2]: Change to:

Some profiles MAY wrap the `<AuthnRequest>` element in an envelope. This envelope allows for extra processing by an intermediary between the service provider and the identity provider. An example of an intermediary is a user agent or proxy. Processing rules are given in section 3..23.1.1. Note that the envelope is for consumption by the intermediary and is removed before the enveloped `<AuthnRequest>` element is forwarded to the identity provider.

3) lines 674-676 (section 3.2.5) of [2]: change to:

As with the `<AuthnRequest>` element, some profiles MAY wrap the `<AuthnResponse>` element in an envelope. This envelope allows for extra processing by an intermediary between the identity provider and the service provider. An example of an intermediary is a user agent or proxy. Processing rules are given in section 3.2.3.1.1. Note that the envelope is for consumption by the intermediary and is removed before the enveloped `<AuthnResponse>` element is forwarded to the service provider.

4) line 580 of [2]: Change to:

The service provider's URL specifying where `<AuthnResponse>` elements, locally generated by the intermediary, are to be sent. See the processing rules for active intermediaries specified in section 3.2.3.1.1.

Erratum Designator	*Erratum Title*	*CRs*	*Summary and Resolution*
SE1	**LECP Security Vulnerability**	**1129, 1130**	

5) lines 678-679 of [2]: Change to:

The authentication response envelope contains the following elements:

AuthnResponse [Required]

The enveloped authentication response.

AssertionConsumerServiceURL [Required]

The service provider's URL where the authentication response should be sent. This element's value SHOULD be obtained from the element of the same name in the service provider's Provider Metadata.

6) insert after line 685 of [2]:

```
<element name="AssertionConsumerServiceURL" type="anyURI"/>
```

7) insert after line 697 of [2]:

```
<AssertionConsumerServiceURL>
     http://ServiceProvider.com/lecp_assertion_consumer
</AssertionConsumerServiceURL>
```

8) insert after line 1098 of [2]:

```
<element name="AssertionConsumerServiceURL" type="anyURI"/>
```

9) lines 876-877 of [3]: Change to:

The service provider MUST specify a URL for receiving `<AuthnResponse>` elements, locally generated by the intermediary, by including the `<lib:AssertionConsumerServiceURL>` element in the `<lib:AuthnRequestEnvelope>`.

10) lines 938-941 of [3]: Change to:

The `<lib:AuthnResponse>` MUST be sent using a POST to the service provider's assertion consumer service URL identified by the `<lib:AssertionConsumerServiceURL>` element within the `<lib:AuthnResponseEnvelope>` ***obtained from the identity provider*** in step 6.

11) These changes are required in liberty-architecture-protocols-schemas-v1.0.xsd [4]:

A. add these lines to the "### IMPORTANT NOTICE ##" comment, after the "11 July 2002" line in the large comment within the file..

as-modified by the "DRAFT Liberty Version 1.0 Errata" document,
(draft-liberty-version-1-errata-00)
11-Oct-2002

B. add this line..

```
<element name="AssertionConsumerServiceURL" type="anyURI"/>
```

..to the `<sequence>` within the `AuthnResponseEnvelopeType` complextype, after the `<element ref="lib:AuthnResponse"/>` line.

NOTE: the XSD file, liberty-architecture-protocols-schemas-v1.0-errata-00.xsd, identified in section 1 of this document contains these changes.

Erratum Designator	*Erratum Title*	*CRs*	*Summary and Resolution*
SE1	**LECP Security Vulnerability**	**1129, 1130**	

12) insert after line 1863 of [3] at end of section 4.4.2.1:

4.4.2.2 Liberty-Enabled Client and Proxy Profile

Threat: Intercepted `<lib:AuthnRequestEnvelope>` and `<lib:AuthnResponse>` and subsequent Principal impersonation

Description: A spurious system entity can interject itself as a man-in-the-middle (MITM) between the user agent (LECP) and a legitimate serviceprovider, where it acts in the service provider role in interactions with the LECP, and in the user agent role in interactions with the legitimate service provider. In this way, as a first step, the MITM is able to intercept the service provider's `<lib:AuthnRequestEnvelope>` (step 3 of section 3.2.5) and substitute any URL of its choosing for the `<lib:AssertionConsumerServiceURL>` value before forwarding the `<lib:AuthnRequestEnvelope>` on to the LECP. Typically, the MITM will insert a URL value that points back to itself. Then, if the LECP subsequently receives a `<lib:AuthnResponseEnvelope>` from the identity provider (step 6 in section 3.2.5) and subsequently sends the contained `<lib:AuthnResponse>` to the `<lib:AssertionConsumerServiceURL>` received from the MITM, the MITM will be able to masquerade as the Principal at the legitimate service provider.

Countermeasure: The identity provider specifies to the LECP the address to which the LECP must send the `<lib:AuthnResponse>`. The `<lib:AssertionConsumerServiceURL>` in the `<lib:AuthnResponseEnvelope>` element is for this purpose. This URL value is among the metadata which identity and service providers must exchange in the process of establishing their operational relationship, see sections 3.1 and 3.1.3.

5 Editorial Errata

This section details *editorial* errata in the Liberty v1.0 specification set. "Editorial" means that the resolution of any of these errata does not cause a material change to the specified protocol. Typically, the resolution of an editorial erratum will affect only one specification at a time, thus the editorial errata for each specification in the Liberty v1.0 specification set are divided into the below separate subsections.

5.1 Architecture Overview

The erratum designator for Architectural Overview [1] editorial errata is **AO**.

Erratum Designator	*Erratum Title*	*CRs*	*Summary and Resolution*
AO1	**login via embedded form only "may" reveal users' credentials to SP**	**1107**	

Summary:

The policy/security note at line 1199 of the Architecture Overview [1] says in line 1201

"...the user is revealing his identity provider credentials to the service provider..."

This is only true if there are provisions in the code implementing the webpage containing the embedded form and/or the embedded form itself that captures users' credentials (eg such could occur if the SP is rogue, or if it had been hacked).

Resolution:

1) lines 1199-1205 of [1]: Change to:

POLICY/SECURITY NOTE: Although users may like the seamlessness of this embedded form mechanism and deployers will like that the user does not leave their Website, it has serious policy and security considerations. In this mechanism, the user may be revealing his identity provider credentials to the service provider in cleartext. This is because the service provider controls the actual code implementing both the page and the embedded form and thus can conceivably capture users' credentials. In this way, privacy surrounding the user's identity provider account may be compromised by such a rogue service provider, who could then wield those credentials and impersonate the user. Because of this, when using authentication via embedded form, deployers may want to consider appropriate contract terms between identity providers and service providers to address this risk.

Erratum Designator	*Erratum Title*	*CRs*	*Summary and Resolution*
AO2	**Argument in line 949 transposed..**	**1103**	

Summary:

Affected line numbers are actually: 956-958

The text therein says:

> Because the size limitation is greater when using HTML forms than URLs, a full authentication assertion can be included.

The CR submitter commented:

> Argument in line 949 is inversed. It says available space in ULR larger than HTML form

Resolution:

1) Lines 956-958 of [1]: Change to:

> An entire authentication assertion can be included in the posted HTML form because the size allowances for HTML forms are great enough to accomodate one.

116

5.2 Bindings and Profiles Specification

The erratum designator for Bindings and Profiles [3] editorial errata is **BP**.

Erratum Designator	*Erratum Title*	*CRs*	*Summary and Resolution*
BP1	**Security consideration for state checking by IdP**	**1122**	

Summary:

The normative Liberty specifications don't contain language concerning the need to correlate authentication requests with session holders. There should be a security considerations item relating to this.

Resolution:

1) insert after line 1863 in [3]:

Threat: Rogue user attempts to impersonate currently logged-in legitimate Principal and thereby gain access to protected resources.

Description: Once a Principal is successfully logged into an identity provider, subsequent `<lib:AuthnRequest>` messages from different service providers concerning that Principal will not necessarily cause the Principal to be reauthenticated. Principals must, however, be authenticated unless the identity provider can determine that an `<lib:AuthnRequest>` is associated not only with the Principal's identity, but also with a validly authenticated identity provider session for that Principal.

Countermeasure: In implementations where this threat is a concern, identity providers MUST maintain state information concerning active sessions, and MUST validate the correspondence between an `<lib:AuthnRequest>` and an active session before issuing an `<lib:AuthnResponse>` without first authenticating the Principal. Cookies posted by identity providers MAY be used to support this validation process, though this specification does not mandate or specify such an approach.