Liberty Version 1.1 Errata

Version 01

15 April 2003

Document Description: draft-liberty-architecture-1.1-errata-01

Notice

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

Editors

John Kemp, IEEE-ISTO

Contributors

Scott Cantor, Internet2 / Ohio State University
Jonathan Sergent, Sun Microsystems
Xavier Serret, Gemplus

Document History

Revision	Date	Log
00	10-Mar-2003	Crs implemented: 6, 7

Table of Contents

1 Introduction

This document lists errata in the Liberty v1.1 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 v1.1 protocols as initially specified contained certain material errors, collectively referred to as *errata*. Readers of the Liberty v1.1 Specification Set should note the errata in this document and incorporate it into their reading of the specification set. Also, implementers of the Liberty v1.1 specification set should use the Liberty schemata contained in the files:

Filename: liberty-architecture-protocols-schema-v1.1-errata-01.xsd
Location: http://www.projectliberty.org/specs/liberty-architecture-protocols-schemas-v1.1-errata-01.xsd

Filename: liberty-architecture-authentication-context-v1.1-errata-00.xsd
Location: http://www.projectliberty.org/specs/liberty-architecture-authentication-context-v1.1-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 Protocols and Schemas Specification
http://www.projectliberty.org/specs/liberty-architecture-protocols-schemas-v1.1.pdf
[2] Liberty Protocols and Schemas Specification XSD file
http://www.projectliberty.org/specs/liberty-architecture-protocols-schemas-v1.1.xsd
[3] Liberty Authentication Context Specification
http://www.projectliberty.org/specs/liberty-architecture-authentication-context-v1.1.pdf
[4] Liberty Authentication Context Specification XSD file
http://www.projectliberty.org/specs/liberty-architecture-authentication-context-v1.1.xsd

3 Abbreviations

The following abbreviations are used in this document:

SE - Substantive 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 v1.1 specification set. "Substantive" means that the resolution of any of these errata causes a material change to the protocol specification. Because the Liberty v1.1 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.

4.1 [SE1] AuthnRequestEnvelopeType instances fail validation

4.1.1 Summary

The **AuthnRequestEnvelopeType** schema was written by derivation from the **RequestEnvelopeType**. The **RequestEnvelopeType** allows the addition of extra non-Liberty content into the `<AuthnRequestEnvelope>` message. Due to the way in which this portion of the schema was written, using an `<any>` element that allows elements from the core Liberty namespace to be used, we have created a non-deterministic content model. In addition, the derivation of **AuthnRequestEnvelopeType** does not actually allow this extra content to be introduced.

4.1.2 Resolution

1) Insert after line 724 in [1]:

In addition to the above elements, a wildcard `<any>` element is provided to allow arbitrary extensions to the **<**`AuthnRequestEnvelope`**>**. Use of this element is not normatively defined in this specification, and the element MUST be from a namespace other than the core `lib:` namespace.

2) Insert after line 736 in [1]:

```
<any namespace="##other" processContents="skip" minOccurs="0"
maxOccurs="unbounded"/>
```

3) Change line 743 of [1] to read:

```
<any namespace="##other" processContents="skip" minOccurs="0"
maxOccurs="unbounded"/>
```

4) Insert after line 1396 in [1]:

```
<any namespace="##other" processContents="skip" minOccurs="0"
maxOccurs="unbounded"/>
```

5) Change line 1403 of [1] to read:

```
<any namespace="##other" processContents="skip" minOccurs="0"
maxOccurs="unbounded"/>
```

6) Insert after line 78 in [2]:

```
<any namespace="##other" processContents="skip" minOccurs="0"
maxOccurs="unbounded"/>
```

7) Change line 85 of [2] to read:

```
<any namespace="##other" processContents="skip" minOccurs="0"
maxOccurs="unbounded"/>
```

4.2 [SE2] AuthnResponseEnvelopeType instances fail validation

4.2.1 Summary

The **AuthnResponseEnvelopeType** schema was written by derivation from the **ResponseEnvelopeType**. The **ResponseEnvelopeType** allows the addition of extra non-Liberty content into the `<AuthnResponseEnvelope>` message. Due to the way in which this portion of the schema was written, using an `<any>` element that allows elements from the core Liberty namespace to be used, we have created a non-deterministic content model. In addition, the derivation of **AuthnResponseEnvelopeType** does not actually allow this extra content to be introduced.

4.2.2 Resolution

1) Insert after line 824 in [1]:

In addition to the above elements, a wildcard `<any>` element is provided to allow arbitrary extensions to the **<**`AuthnResponseEnvelope`**>**. Use of this element is not normatively defined in this specification, and the element MUST be from a namespace other than the core `lib:` namespace.

2) Insert after line 832 in [1]:

```
<any namespace="##other" processContents="skip" minOccurs="0"
maxOccurs="unbounded"/>
```

3) Change line 839 of [1] to read:

```
<any namespace="##other" processContents="skip" minOccurs="0"
maxOccurs="unbounded"/>
```

4) Insert after line 1412 in [1]:

```
<any namespace="##other" processContents="skip" minOccurs="0"
maxOccurs="unbounded"/>
```

5) Change line 1419 of [1] to read:

```
<any namespace="##other" processContents="skip" minOccurs="0"
maxOccurs="unbounded"/>
```

6) Insert after line 94 in [2]:

```
<any namespace="##other" processContents="skip" minOccurs="0"
maxOccurs="unbounded"/>
```

7) Change line 101 of [2] to read:

```
<any namespace="##other" processContents="skip" minOccurs="0"
maxOccurs="unbounded"/>
```

4.3 [SE3] Authentication Context instances fail validation

4.3.1 Summary

There are a number of elements in the Authentication Context schema that contain an <any> element, used to permit arbitrary content to be added to those elements. This causes validation of instances that reference such elements to fail, due to the non-deterministic nature of the content model expressed in this schema.

4.3.2 Resolution

The general resolution is to disallow content from the `lib:` namespace in these extension elements, by changing the namespace allowed from "##any" to "##other". This affects **all** lines in both [3] and [4] that currently read:

```
<xs:any namespace="##any" minOccurs="0" maxOccurs="unbounded"
processContents="lax" />
```

These should now read:

```
<xs:any namespace="##other" minOccurs="0" maxOccurs="unbounded"
processContents="lax" />
```

In [4] the following lines are affected:

42,57,93,105,128,138,151,200,212,254,306,343,354,365,376,401,412,423,434,445,457,465,472,479

A list of line numbers for [3] is not provided due to the large number of affected lines, and the widespread use of global search and replace technologies that allow this change to be made in all affected lines without regard to specific line numbers.