Liberty Bindings and Profiles Specification

Version 1.1

15 January 2003

Document Description: **liberty-architecture-bindings-profiles-v1.1**

Notice

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

40

41 ## Editors

42 Jason Rouault, Hewlett-Packard Company
43 Tom Wason. IEEE-ISTO

44 ## Contributors

45

ActivCard
American Express Travel Related Services
America Online, Inc.
Bank of America
Bell Canada
Catavault
Cingular Wireless
Cisco Systems, Inc.
Citigroup
Communicator, Inc.
Consignia
Cyberun Corporation
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
NEC Corporation
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

46

47 **Document History**

Version #	Date	Editor	Scope of changes
1.0	14-Mar-02	Jason Rouault	Initial Draft Based on Liberty V1.0
1.1	04-Nov-02	Jason Rouault, Tom Wason	CR1097: Typo corrections. CR1098: collapse the HTTP-GET-Based and HTTP-Redirect-Based profiles into the same profile CR1106: prescriptive alternative for countermeasure to Unsigned `<lib:AuthnRequest>` message. Section 4.4.2.1. CR1118: Added rogue participant threat notice. Section 4.4.2.3. CR1122: Describe rogue impersonation threat and countermeasure. Section 4.4.2.1. CR1130: Resolution of LEC vulnerability to a man-in-the-middle attack. Section 3.2.5.1. CR1138: Changed namespace notation "http://projectliberty.org/schemas/core/2002/08 to "http://projectliberty.org/schemas/core/2002/12. Section 1.1, Section 3.2.5.2 step 3. CR1139: Change cookie constraints. In Section 3.6.1 changed “identity provider ID” to “identity provider succinct ID”. Restricted Path prefix. In Section 3.6.2 removed figure and steps, added text describing setting common domain cookie. In section 3.6.3 removed steps and figure, inserted text describing reading the common domain cookie. CR1140: Clarification of construction of ProviderSuccinctID. Section 3.2.2.2 CR1147: Correct typo. CR1148: Remove use of element samlp:RespondWith. Section 3.1.2.1.2. CR1150: Added note on escaping base64-encoded signature values. Section 3.1.2.1. CR1151: Added “The service URL provided by the provider (the URL to which <query> parameters are added) MUST NOT contain any pre-existing <query> parameter values.” Section 3.1.2.1

			CR1156: URI specified in the service provider metadata element FederationTerminationNotificationProtocolProfile. Section 3.4.1. CR1157: Session persistence at federation termination notification. Section 3.4.2 CR1159: Changed "…SAML artifact on success or empty on failure." To "…SAML artifact on success or on failure." Added following sentence: "In the case of failure, the status information will be communicated in the `<samlp:Response>` returned." in step 9. Section 3.2.2.1 CR1160, CR1161: Generalizing Register Name Identifier Profile. Register name identifier profile is changed to support NameIdentifier changes by both Identity Provider and Service Provider. Section 3.3. Change Name Registration Profile description to reflect the bi-directional nature of the profile for establishing or changing a Principal's name identifier. Section 3. CR1162: Change "Name" to "NameIdentifier". Sections 3.1.2.1.3, 3.1.2.1.4 CR1166: Changed example to provide correct content type. Section 2.2. CR1167: Change header from "Liberty-LECP" to "Liberty-Enabled". Section 3.2.5.1. CR1168: Delete requirement for base64 encoding in Section 3.2.5.2, Step 3. CR1169: Change "…transfer service responds and redirects…" to "…transfer service responds and sends…", delete redirection rules from Step 3. Added, "The form and contents of the HTTP response in this step are profile-dependent." in following line. Removed "attached to the URL fulfilling the redirect request" from step 4. Section 3.2.1. Added step 3 to Sections 3.2.2.1 and 3.2.3. CR1178: Changed "Maximum URL length of 256 bytes." To "Minimum maximum URL length of 256 bytes." Section 3.1.1. CR1180: Modified Step 5: Processing `<AuthnRequest>`, Section 3.2.1. CR1181: Modified Step 6: HTTP Response with `<AuthnResponse>` or Artifact, Section

			3.2.1. CR1182: Changed common requirements 3, 4 &6, deleted #12. Section 3.1. CR1219: Changed references to Name Registration Profiles, now plural. Sections 3, 3.3. CR1220: Specify algorithms and identifiers, Section 3.1.2.1 CR1221: Added encodings for RegisterNameIdentifierRequest, Section 3.1.2.1.6 and RegisterNameIdentifierResponse, Section 3.1.2.1.7. CR1223: Correct typos. Sections 3.2.1, 3.3, 3.5, 3.5.2.2. CR1224: Replaced <lib:Assertion> with <saml:Assertion> 8 places. CR1225: Corrected contents of `<saml:assertion>`, Section 3.2.1, Step 9. CR1228: Removed “asynchronous”, Section 3.3.2.2. CR1229: Revised code for the original `<lib:AuthnRequest>` message, Section 3.1.2.1.2. CR1230: Changed Liberty-LECP to Liberty-Enabled, 2 places in Section 3.2.5.1. CR1231: Added URI-based identifiers to Register Name Identifier profiles, Sections 3.3.2.1, 3.3.2.2 CR1232: Typo CR1233: Added 2 metadata elements to Register Name Identifier profiles, Section 3.3. CR1242: Corrected error in implementing CR 1181, Steps 6 in both Sections 3.2.5.2 and 3.2.1. CR1243: Replace RELAYSTATE and LRURL with RelayState throughout. CR1244: Removed references to ProviderSuccinctID in Section 3.2.2.2. CR1245: RegisterNameIdentifierReturnURL is changed to RegisterNameIdentifierServiceReturnURL, Section 3.3. CR1253: Changed all instances of

			LogoutNotification to LogoutRequest, Section 3.5. CR1255: Revised Single Logout LogoutRequest profiles to be similar to other requests by adding LogoutResponse. Substantive changes to all of Section 3.5 CR1256: Correct element order in XML example, Section 3.2.5.2, Step 3. CR1259: Change AuthnContextComparisonType to AuthnContextComparison, Section 3.1.2.1.2. CR1260: Remove extraneous RegisterNameIdentifierReturnURL, Section 3.3. CR1261: Added LogoutResponse encoding, Section 3.1.2.1.5. CR1262: Added mechanism for extending the sampl:Request type in Section 3.2.1. SOAP example modified in Section 2.2. CR1263: Editorial adjustments.
1.1 - 18	12-Dec-02	Jason Rouault, Tom Wason	CR1179: Divided references into normative and informative categories, Section 5. CR1264: Add RelayState to LogoutRequest example Section 3.1.2.1.4. CR1266: See CR1282. CR1268: Replaced SOAP over HTTP example. Section 2.2. CR1269: Change OLDProvidedNameIdentifier to OldProvidedNameIdentifier, Section 3.1.2.1.6. CR1271: Clarify POST error reporting, step 4, Section 3.2.5.2 CR1273: Corrected typo. CR1274: Reference “Minimum maximum”. Section 3.1.1. CR1275: Re-entered cookie writing instruction for appending IDP Succinct ID. Section 3.6.1. CR1278: Notes for implementing multilevel status codes. Sections 3.1.2.1, 3.1.2.1.5, 3.1.2.1.7. CR1282: Removed requirement that `<query>` parameter name MUST be an XML attribute name, Section 3.1.2.1. Differentiated

			NameQualifier values for RegisterNameIdentifierRequest, Section 3.1.2.1.6. CR1283: Added instruction for use of predefined xmlns:prefixes for status codes in URL-encoded responses. Section 3.1.2.1. CR1284: Add RelayState to FederationTerminationNotification URL-Encoding, Section 3.1.2.1.3. CR1285: URL-Encoding templates updated, corrected, consistently formatted Section 3.1.2.1. CR1289: delete note on addition of RelayState element in step 2 of sections 3.3.1.1, 3.4.1.1, 3.5.1.1.1, 3.5.1.1.2 and 3.5.2.1
1.1 Final	15-Jan-03	John Kemp	Corrected SLO profiles for LogoutResponse. Regenerated TOC Typos

48

Table of Contents

1 Introduction

This specification defines the bindings and profiles of the Liberty protocols and messages to HTTP-based communication frameworks. This specification relies on the SAML core framework in [SAMLCore] and makes use of adaptations of the SAML profiles in [SAMLBind]. A separate specification, [LibertyProtSchema], is used to define the Liberty protocols and messages used within the profiles. Definitions for Liberty-specific terms can be found in [LibertyGloss].

1.1 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 interoperation or to limit behavior which has potential for causing harm (e.g., limiting retransmissions)."

These keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

```
Listings of productions or other normative code appear like this.
```

```
Example code listings appear like this.
```

Note: Non-normative notes and explanations appear like this.

Conventional XML namespace prefixes are used throughout this specification to stand for their respective namespaces as follows, regardless of whether a namespace declaration is present in the example:

- The prefix `lib:` stands for the Liberty namespace `http://projectliberty.org/schemas/core/2002/12`
- The prefix `saml:` stands for the SAML assertion namespace (see [SAMLCore]).
- The prefix `samlp:` stands for the SAML request-response protocol namespace (see [SAMLCore]).
- The prefix `ds:` stands for the W3C XML signature namespace, `http://www.w3.org/2000/09/xmldsig#` (see [XMLSig]).
- The prefix `SOAP-ENV:` stands for the SOAP 1.1 namespace, `http://schemas.xmlsoap.org/soap/envelope` (see [SOAP1.1]).

Terminology from [RFC2396] is used to describe components of an HTTP URL. An HTTP URL has the following form:

```
<scheme>://<authority><path>?<query>
```

Sections in this document specify certain portions of the <query> component of the URL. Ellipses are used to indicate additional, but unspecified, portions of the <query> component.

2 Protocol Bindings

The Liberty protocol bindings are defined in this section.

2.1 SOAP Binding for Liberty

Because the Liberty protocols are an extension of the SAML protocol (see [SAMLCore]) and a SOAP protocol binding for SAML has been defined, the SOAP binding for Liberty MUST adhere to the processing rules for the "SOAP binding for SAML" as specified in [SAMLBind] unless otherwise noted. Just like SAML, the SOAP binding for Liberty uses HTTP as the transport mechanism.

2.2 Example of Message Exchange Using SOAP over HTTP

The following is an example of the SOAP exchange for the single sign-on browser artifact profile requesting an authentication assertion (the left margin whitespace added for legibility invalidates the signature).

```
POST /authn HTTP/1.1
Host: idp.example.com
Content-type: text/xml
Content-length: nnnn
<soap-env:Envelope
  xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/">
  <soap-env:Header/>
  <soap-env:Body>
  <samlp:Request xmlns="urn:oasis:names:tc:SAML:1.0:protocol"
    xmlns:lib="http://projectliberty.org/schemas/core/2002/12"
    xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
    xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    IssueInstant="2002-12-12T10:08:56Z"
    MajorVersion="1"
    MinorVersion="0"
    RequestID="e4d71c43-c89a-426b-853e-a2b0c14a5ed8"
    id="ericssonb6dc3636-f2ad-42d1-9427-220f2cf70ec1"
    xsi:type="lib:SignedSAMLRequestType">
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod
            Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
          </ds:CanonicalizationMethod>
          <ds:SignatureMethod
            Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
          </ds:SignatureMethod>
          <ds:Reference URI="#ericssonb6dc3636-f2ad-42d1-9427-220f2cf70ec1">
            <ds:Transforms>
              <ds:Transform
                Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature">
              </ds:Transform>
              <ds:Transform
                Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod
              Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
            </ds:DigestMethod>
            <ds:DigestValue>+k6TnolGkIPKZlpUQVyok8dwkuE=</ds:DigestValue>
          </ds:Reference>
```

```
        </ds:SignedInfo>
        <ds:SignatureValue>
          wXJMVoPO1V1jFnWJPyOWqP5Gqm8A1+/2b5gNzF4L4LMu4yEcRtttLdPPT3bvhwkwHXjL9NuOFumQ
          5YEyiVzlNcjAxX0LfgwutvEdJb748IU4L+8obXPXfqTZLiBK1RbHCRmRvjlPIu22oGCV6EwuiWRv
          OD6Ox9svtSgFJ+iXkZQ
        </ds:SignatureValue>
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>
              MIIDMTCCApqgAwIBAgIBHDANBgkqhkiG9w0BAQQFADCBlTELMAkGA1UEBhMCVVMxCzAJBgNVBAcT
              AlNGMRkwFwYDVQQKExBMaWJlcnR5IEFsbGlhbmNlMRQwEgYDVQQLEwtJT1AgVGVzdGVyczEiMCAG
              A1UEAxMZTGliZXJ0eSBUZXN0ZXJzIENlcnRpZmllcjEkMCIGCSqGSIb3DQEJARYVcnJvZHJpZ3Vl
              ekBuZW9zb2wubmV0MB4XDTAyMTIwNDE1NTg0NFoXDTEyMTIwMTE1NTg0NFowgasxCzAJBgNVBAYT
              AlVTMQswCQYDVQQHEwJTRjEkMCIGA1UEChMbTGliZXJ0eSBBbGxpYW5jZSBlcmljc3Nvbi1hMSYw
              JAYDVQQLEx1JT1AgVGVzdGVycyBlcmljc3Nvbi1hIHNpZ25lcjEXMBUGA1UEAxMOZXJpY3Nzb24t
              YS5pb3AxKDAmBgkqhkiG9w0BCQEWGXJyb2RyaWd1ZXpAZXJpY3Nzb24tYS5pb3AwgZ8wDQYJKoZI
              hvcNAQEBBQADgY0AMIGJAoGBAPUoGYvJxQc5jzDnJ14TV6TaTbB3fH95ju24Z0y6HQxm6gXdJSAo
              Wh7/AIes4UcV09DC2kKS6Vow2YoXt2LIyH9HWH2tEUt1jS/PUeBHEWcW3tFezM6jh5GG5rCuVPZa
              W9eoGUbFPSzOPFKUAwdHUXSDWufY1KZ93IxhOBeZgg6VAgMBAAGjeTB3MEoGCWCGSAGG+EIBDQQ9
              FjtUaGlzIHNpZ25pbmcgY2VydCB3YXMgY3JlYXRlZCBmb3IgdGVzdGluZy4gRG8gbm90IHRydXN0
              IGl0LjAJBgNVHRMEAjAAMBEGCWCGSAGG+EIBAQQEAwIEMDALBgNVHQ8EBAMCBsAwDQYJKoZIhvcN
              AQEEBQADgYEAR/HSgBpAprQwQVyWDE9pCaiduKv4/W/+hrdpXlVKSr6TIlg4ouDCQJNos7tNuG9Z
              AbfWtHvCss51N2cfAzfns/DKqxRqcsxzL5ZUBksPpmsDoboopUv6Xm8RFsi7yB9AGaVuqObeY/+m
              70nOu03O+FlMN3U1k2E3rOKXlU1noC0</ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
        </ds:Signature>
      <samlp:AssertionArtifact>
        AAM1uXw6+f+jyA/4XuFHqPl7QDvc/LIQL9+t7YQtG1Gwk9bph0Adl+o+
      </samlp:AssertionArtifact>
    </samlp:Request>
  </soap-env:Body>
</soap-env:Envelope>
```

The following is an example of a response, which supplies an assertion containing an authentication statement.

```
HTTP/1.1 200 OK
Content-Type: text/xml
Content-Length: nnnn
<soap-env:Envelope
  xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/">
  <soap-env:Header/>
  <soap-env:Body>
    <samlp:Response
      xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
      InResponseTo="RPCUk2ll+GVz+t1lLURp51oFvJXk"
      IssueInstant="2002-10-31T21:42:13Z" MajorVersion="1" MinorVersion="0"
      Recipient="http://localhost:8080/sp"
      ResponseID="LANWfL2xLybnc+BCwgY+p1/vIVAj">
      <samlp:Status>
        <samlp:StatusCode
          xmlns:qns="urn:oasis:names:tc:SAML:1.0:protocol"
          Value="qns:Success">
        </samlp:StatusCode>
      </samlp:Status>
      <saml:Assertion
        xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
        xmlns:lib="http://projectliberty.org/schemas/core/2002/12"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        AssertionID="SqMC8Hs2vJ7Z+t4UiLSmhKOSUO0U"
        InResponseTo="RPCUk2ll+GVz+t1lLURp51oFvJXk"
        IssueInstant="2002-10-31T21:42:13Z" Issuer="http://localhost:8080/idp"
        MajorVersion="1" MinorVersion="0"
        xsi:type="lib:AssertionType">
        <saml:Conditions
          NotBefore="2002-10-31T21:42:12Z"
          NotOnOrAfter="2002-10-31T21:42:43Z">
          <saml:AudienceRestrictionCondition>
```

```
            <saml:Audience>http://localhost:8080/sp</saml:Audience>
          </saml:AudienceRestrictionCondition>
        </saml:Conditions>
        <saml:AuthenticationStatement
          AuthenticationInstant="2002-10-31T21:42:13Z"
          AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password"
          xsi:type="lib:AuthenticationStatementType">
          <saml:Subject xsi:type="lib:SubjectType">
            <saml:NameIdentifier>C9FfGouQdBJ7bpkismYgd8ygeVb3PlWK</saml:NameIdentifier>
            <saml:SubjectConfirmation>
              <saml:ConfirmationMethod>
                urn:oasis:names:tc:SAML:1.0:cm:artifact-01
              </saml:ConfirmationMethod>
            </saml:SubjectConfirmation>
            <lib:IDPProvidedNameIdentifier>
              C9FfGouQdBJ7bpkismYgd8ygeVb3PlWK
            </lib:IDPProvidedNameIdentifier>
          </saml:Subject>
        </saml:AuthenticationStatement>
        <ds:Signature>
          <ds:SignedInfo>
            <ds:CanonicalizationMethod
              Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            </ds:CanonicalizationMethod>
           <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
           </ds:SignatureMethod>
           <ds:Reference URI="">
             <ds:Transforms>
               <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature">
               </ds:Transform>
               <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
               </ds:Transform>
             </ds:Transforms>
             <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
             </ds:DigestMethod>
             <ds:DigestValue>ZbscbqHTX9H8bBftRIWlG4Epv1A=</ds:DigestValue>
             </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>
            H+q3nC3jUalj1uKUVkcC4iTFClxeZQIFF0nvHqPS5oZhtkBaDb9qITA7gIkotaB584wXqTXwsfsu
            IrwT5uL3r85Rj7IF6NeCeiy3K0+z3uewxyeZPz8wna449VNm0qNHYkgNak9ViNCp0/ks5MAttoPo
            2iLOfaKu3wWG6d1G+DM=
          </ds:SignatureValue>
        </ds:Signature>
      </saml:Assertion>
    </samlp:Response>
  </soap-env:Body>
</soap-env:Envelope>
```

3 Profiles

This section defines the Liberty profiles for the use of request and response messages defined in [LibertyProtSchema]. The combination of message content specification and message transport mechanisms for a single client type (that is, user agent) is termed a *Liberty profile*. The profiles have been grouped into categories, according to the Liberty protocol message intent.

The following profile categories are defined in this document:

- **Single Sign-On and Federation**: The profiles by which a service provider obtains an authentication assertion from an identity provider facilitating single sign-on and identity federation.
- **Name Registration**: The profiles by which service providers and identity providers specify the name identifier to be used when communicating with each other about the Principal.

- **Identity Termination Notification**: The profiles by which service providers and identity providers are notified of federation termination.
- **Single Logout**: The profiles by which service providers and identity providers are notified of authenticated session termination.
- **Identity Provider Introduction**: The profile by which a service provider discovers which identity providers a Principal may be using.

3.1 Common Requirements

The following rules apply to all profiles in this specification, unless otherwise noted by the individual profile.

1 All HTTP requests and responses MUST be drawn from either HTTP 1.1 (see [RFC2616]) or HTTP 1.0 (see [RFC1945]). When an HTTP redirect is specified, the HTTP response MUST have a status code of "302." According to HTTP 1.1 and HTTP 1.0, the use of status code 302 is recommended to indicate "the requested resource resides temporarily under a different URI." The response may also include additional headers and an optional message.

2 When `https` is specified as the `<scheme>` for a URL, the HTTP connection MUST be made over either SSL 3.0 (see [SSLv3]) or TLS 1.0 (see [RFC2246]) or any subsequent protocols that are backwards compatible with SSL 3.0 and/or TLS 1.0. Other security protocols MAY be used as long as they implement equivalent security measures.

3 Messages between providers MUST have their integrity protected, confidentiality MUST be ensured and the recipient MUST authenticate the sender.

4 Providers MUST use secure transport (https) to achieve confidentiality and integrity protection. The initiator of the secure connection MUST authenticate the server using server-side X.509 certificates.

5 The authenticated identity of an identity provider MUST be securely available to a Principal before the Principal presents his/her personal authentication data to that identity provider.

6 For signing and verification of protocol messages, identity and service providers SHOULD use certificates and private keys that are distinct from the certificates and private keys applied for SSL or TLS channel protection. Certificates and private keys MUST be suitable for long-term signatures. See [LibertyProtSchema] for guidelines on signature verification.

7 In transactions between service providers and identity providers, requests MUST be protected against replay, and received responses MUST be checked for correct correspondence with issued requests. (Note: Other steps may intervene between the issuance of a request and its eventual response within a multistep transaction involving redirections.) Additionally, time-based assurance of freshness MAY be provided.

8 Each service provider within a circle of trust MUST be configured to enable identification of the identity providers whose authentications it will accept, and each identity provider MUST be configured to enable identification of the service providers it intends to serve. (Note: The format of this configuration is a local matter and could, for example, be represented as lists of names or as sets of X.509 certificates of other circle of trust members).

9 Circle of trust bilateral agreements on selecting certificate authorities, obtaining X.509 credentials, establishing and managing trusted public keys, and tracking lifecycles of corresponding credentials are assumed and not in scope for this specification.

10 The `<scheme>` of the URL for SOAP endpoints MUST be `https`.

11 All SOAP message exchanges MUST adhere to the SOAP protocol binding for Liberty (see 2.1).

3.1.1 User Agent

A user agent, unless otherwise noted in the specific profile, MUST support the following features to be interoperable with the protocols in [LibertyProtSchema] and Liberty profiles in this document:

- HTTP 1.0 (see [RFC1945]) or HTTP 1.1 (see [RFC2616]).
- SSL 3.0 (see [SSLv3]) or TLS 1.0 (see [RFC2246]) or any subsequent protocols which are backwards compatible with SSL 3.0 and/or TLS 1.0 either directly or via a proxy (for example, a WAP gateway).
- Minimum maximum URL length of 256 bytes. See [LibertyGloss] for definition.

Additionally, to support the optional identity provider introduction profile, either the user agent or a proxy must support session cookies (see [RFC2109]). Support for persistent cookies will yield a more seamless user experience.

3.1.2 Formatting and Encoding of Protocol Messages

All Liberty protocol messages that are indicated by the profile as being communicated in the `<query>` component of the URL MUST adhere to the formatting and encoding rules in 3.1.2.1.

3.1.2.1 Encoding URL-embedded Messages

URL-embedded messages are encoded using the `application/x-www-form-urlencoded` MIME type as if they were generated from HTML forms with method of GET as defined in [HTML4].

The original Liberty XML protocol message MUST be encoded as follows:

- The `<query>` component parameter value MUST be the value of the Liberty XML protocol message element or attribute value.
- When the original message element has multiple values, the value of the `<query>` component parameter MUST be a space-delimited list.
- Some of the referenced protocol message elements and attributes are optional. If an optional element or attribute does not appear in the original Liberty XML protocol message, then the corresponding data item MUST be omitted from the URL encoded message.
- URLs appearing in the URL-encoded message SHOULD NOT exceed 80 bytes in length (including %-escaping overhead). Likewise, the `<lib:RelayState>` data value SHOULD NOT exceed 80 bytes in length.
- The URL-encoding of status codes in the responses `RegisterNameIdentifierResponse` and `LogoutResponse` may be taken from several sources. The top level codes MUST be from SAML. Other codes (including Liberty-defined values) MAY be used at the second or lower levels. The URL parameter

value should be interpreted as a QName with the "lib", "saml", and "samlp" namespaces pre-defined to their respective namespace URIs. Query parameters with the name "xmlns:prefix" can be used to map additional namespace prefixes for the purpose of QName resolution, so long as the xmlns:prefix URL parameter appears before the URL parameter containing the QName which needs the prefix definition.

As <samlp:StatusCode> elements may be nested hierarchically (see [SAMLCore]), there may exist multiple values for <samlp:StatusCode> in the response messages. These multiple values MUST be encoded by producing a URL-encoded space-separated string as the value of this query parameter. An example is shown below:

```
Value=samlp%3AResponder%20lib%3AFederationDoesNotExist
```

XML digital signatures are not directly URL-encoded due to space concerns. If the Liberty XML protocol message is signed with an XML signature, the encoded URL form of the message MUST be signed as follows:

- Include the signature algorithm identifier as a new <query> component parameter named SigAlg, but omitting the signature.
- Sign the string containing the URL-encoded message. The string to be signed MUST include only the <query> part of the URL (that is, everything after ? and before &Signature=). Any required URL-escaping MUST be done before signing.
- Encode the signature using base64 (see [RFC2045]).
- Add the base64-encoded signature to the encoded message as a new data item named Signature.

Note that some characters in the base64-encoded signature value may require URL escaping before insertion into the URL <query> part, as is the case for any other data item value.

Any items added after the Signature <query> component parameter are implicitly unsigned.

The service URL provided by the provider (the URL to which <query> parameters are added) MUST NOT contain any pre-existing <query> parameter values.

The following signature algorithms (i.e., DSAwithSHA1, RSAwithSHA1) and their identifiers (the URIs) MUST be supported:

- DSAwithSHA1 — http://www.w3.org/2000/09/xmldsig#dsa-sha1
- RSAwithSHA1 — http://www.w3.org/2000/09/xmldsig#rsa-sha1

3.1.2.1.1 Size Limitations

When the request initiator detects that the user agent cannot process the full URL-encoded message in the URL due to size considerations, the requestor MAY send the Liberty XML protocol message using a form POST. The form MUST be constructed with contents that contain the field LAREQ or LARES with the respective value being the Liberty XML protocol request or response message (e.g., <lib:AuthnRequest> or <lib:AuthnResponse>) as defined in [LibertyProtSchema]. The Liberty XML protocol message MUST be encoded by applying a base64 transformation (refer to [RFC2045]) to the XML message and all its elements.

3.1.2.1.2 URL-encoded <lib:AuthnRequest>

The original `<lib:AuthnRequest>` message:

```
<lib:AuthnRequest
  RequestID="[RequestID]"
  MajorVersion="[MajorVersion]"
  MinorVersion="[MinorVersion]"
  IssueInstant="[IssueInstant]">
    <lib:ProviderID>[ProviderID]</lib:ProviderID>
    <lib:ForceAuthn>[ForceAuthn]</lib:ForceAuthn>
    <lib:IsPassive>[IsPassive]</lib:IsPassive>
    <lib:Federate>[Federate]</lib:Federate>
    <lib:ProtocolProfile>[ProtocolProfile]</lib:ProtocolProfile>
    <lib:AuthnContext>
      <lib:AuthnContextStatementRef>[AuthnContextStatementRef]
        </lib:AuthnContextStatementRef>
    </lib:AuthnContext>
    <lib:RelayState>[RelayState]</lib:RelayState>
    <lib:AuthnContextComparison>[AuthnContextComparison]
      </lib:AuthnContextComparison>
</lib:AuthnRequest>
```

- Data elements that MUST be included in the encoded data with their values as indicated in brackets above if present in the original message:

  `RequestID, MajorVersion, MinorVersion, IssueInstant, ProviderID, ForceAuthn, IsPassive, Federate, ProtocolProfile, AuthnContextStatementRef, AuthnContextClassRef, AuthnContextComparison, RelayState.`

- Maximum size: 748 bytes + 81 * number of `AuthnContextClassRef` or `AuthnContextStatementRefs`

- Example of `<lib:AuthnRequest>` message URL-encoded and signed `(772 bytes)`:

```
http://idp.example.com/authn?RequestID=RMvY34pg%2FV9aGJ5yw0HL0AcjcqQF&MajorVersion=1&MinorVersi
on=0&IssueInstant=2002-05
15T00%3A58%3A19&ProviderID=http%3A%2F%2Fsp.example.com%2Fliberty%2F&ForceAuthn=true&IsPassive=f
alse&Federate=true&ProtocolProfile=http%3A%2F%2Fprojectliberty.org%2Fprofiles%2Fbrws-
post&AuthnContextClassRef=http%3A%2F%2Fprojectliberty.org%2Fauthnctx%2Fprofiles%2FPassword-
over-
HTTP&RelayState=03mhakSms5tMQ0WRDCEzpF7BNcywZa75FwIcSSEPvbkoFxaQHCuNnc5yChIdDlWc7JBV9Xbw3avRBK7
VFsPl2X&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-
sha1&Signature=EoD8bNr2jEOe%2Fumon6oU%2FZGIIF7gbJAe4MLUUMrD%2BPP7P8Yf3gfdZG2qPJdNAJkzVHGfO8W8Dz
pQ%0D%0AsDTTd5VP9MLPcvxbFQoF0CJJmvL26cPsuc54q7ourcH0jJ%2F2UkDq4DAlYlZ5kPIg%2BtrykgLz0U%2BS%0D%0
ANqpNHkjh6W3YkGv7RBs%3D
```

3.1.2.1.3 URL-Encoded <lib:FederationTerminationNotification>

The original `<lib:FederationTerminationNotification>` message:

```
<lib:FederationTerminationNotification ...
  RequestID="[RequestID]"
  MajorVersion="[MajorVersion]"
  MinorVersion="[MinorVersion]"
  IssueInstant="[IssueInstant]">
        <lib:ProviderID>[ProviderID]</lib:ProviderID>
          <saml:NameIdentifier
            NameQualifier="[NameQualifier]"
            Format="[NameFormat]">[NameIdentifier]</saml:NameIdentifier>
        <lib:RelayState>[RelayState]</lib:RelayState>
</lib:FederationTerminationNotification>
```

- Data elements that MUST be included in the encoded data with their values as indicated in brackets above if present in the original message:

  `RequestID, MajorVersion, MinorVersion, IssueInstant, ProviderID, NameQualifier, NameFormat, NameIdentifier, RelayState.`

3.1.2.1.4 URL-Encoded <lib:LogoutRequest>

The original `<lib:LogoutRequest>` message:

```
<lib:LogoutRequest ...
  RequestID="[RequestID]"
  MajorVersion="[MajorVersion]"
  MinorVersion="[MinorVersion]"
  IssueInstant="[IssueInstant]">
        <lib:ProviderID>[ProviderID]</lib:ProviderID>
        <saml:NameIdentifier
          NameQualifier="[NameQualifier]"
          Format="[NameFormat]">
                [NameIdentifier]
        </saml:NameIdentifier>
        <lib:SessionIndex>[SessionIndex]</lib:SessionIndex>
        <lib:RelayState>[RelayState]</lib:RelayState>
</lib:LogoutRequest>
```

- Data elements that MUST be included in the encoded data with their values as indicated in brackets above if present in the original message:

  `RequestID, MajorVersion, MinorVersion, IssueInstant, ProviderID, NameQualifier, NameFormat, NameIdentifier, SessionIndex, RelayState.`

3.1.2.1.5 URL-Encoded <lib:LogoutResponse>

The `<lib:LogoutResponse>` response message:

```
<lib:LogoutResponse
  ResponseID="[ResponseID]"
  InResponseTo="[InResponseTo]"
  MajorVersion="[MajorVersion]"
  MinorVersion="[MinorVersion]"
  IssueInstant="[IssueInstant]"
  Recipient="[Recipient]">
        <lib:ProviderID>[ProviderID]</lib:ProviderID>
        <samlp:Status>
                <samlp:StatusCode Value="[Value]"/>
        </samlp:Status>
        <lib:RelayState>[RelayState]</lib:RelayState>
</lib:LogoutResponse>
```

- Data elements that MUST be included in the encoded data with their values as indicated in brackets above if present in the original message:

  `ResponseID, InResponseTo, MajorVersion, MinorVersion, IssueInstant, Recipient, ProviderID, Value, RelayState.`

- The `<lib:LogoutResponse>` message may contain nested status code information. Multiple values MUST be URL-encoded by creating a space-separated list (see general requirements at top of section 3.1.2.1.5).

3.1.2.1.6 URL-Encoded <lib:RegisterNameIdentifierRequest>

The original `<lib:RegisterNameIdentifierRequest>` message:

```
<lib:RegisterNameIdentifierRequest
  RequestID="[RequestID]"
  MajorVersion="[MajorVersion]"
  MinorVersion="[MinorVersion]"
  IssueInstant="[IssueInstant]">
        <lib:ProviderID>[ProviderID]</lib:ProviderID>
        <lib:IDPProvidedNameIdentifier
          NameQualifier="[IDPNameQualifier]"
          Format="[IDPNameFormat]">[IDPProvidedNameIdentifier]
        </lib:IDPProvidedNameIdentifier>
        <lib:SPProvidedNameIdentifier
          NameQualifier="[SPNameQualifier]"
          Format="[SPNameFormat]">[SPProvidedNameNameIdentifier]
        </lib:SPProvidedNameIdentifier>
        <lib:OldProvidedNameIdentifier
          NameQualifier="[OldNameQualifier]"
          Format="[OldNameFormat]">[OldProvidedNameIdentifier]
        </lib:OldProvidedNameIdentifier>
        <lib:RelayState>[RelayState]</lib:RelayState>
</lib:RegisterNameIdentifierRequest>
```

- Data elements that MUST be included in the encoded data with their values as indicated in brackets above if present in the original message:

  `RequestID, MajorVersion, MinorVersion, IssueInstant, ProviderID, IDPNameQualifier, IDPNameFormat, IDPProvidedNameIdentifier, SPNameQualifier, SPNameFormat, SPProvidedNameIdentifier, OldNameQualifier, OldNameFormat, OldProvidedNameIdentifier, RelayState`

3.1.2.1.7 URL-Encoded <lib:RegisterNameIdentifierResponse>

The `<lib:RegisterNameIdentifierResponse>` response message:

```
<lib:RegisterNameIdentifierResponse
  ResponseID="[ResponseID]"
  InResponseTo="[InResponseTo]"
  MajorVersion="[MajorVersion]"
  MinorVersion="[MinorVersion]"
  IssueInstant="[IssueInstant]"
  Recipient="[Recipient]">
        <lib:ProviderID>[ProviderID]</lib:ProviderID>
        <samlp:Status>
               <samlp:StatusCode Value="[Value]"/>
        </samlp:Status>
        <lib:RelayState>[RelayState]</lib:RelayState>
</lib:RegisterNameIdentifierResponse>
```

- Data elements that MUST be included in the encoded data with their values as indicated in brackets above if present in the original message:

  `ResponseID, InResponseTo, MajorVersion, MinorVersion, IssueInstant, Recipient, ProviderID, Value, RelayState`

- The `<lib:RegisterNameIdentifierResponse>` message may contain nested status code information. Multiple values MUST be URL-encoded by creating a space-separated list (see general requirements at top of section 3.1.2.1).

3.1.3 Provider Metadata

The majority of the Liberty profiles defined in this document rely on metadata that specify the policies that govern the behavior of the service provider or identity provider. These provider metadata are typically shared out of band between an identity provider and a service provider prior to the exchange of Liberty protocol messages. The provider metadata relevant to each profile are listed in this document at the beginning of the profile category. Refer to [LibertyProtSchema] for a complete enumeration of the Liberty provider metadata elements and their associated schema.

3.2 Single Sign-On and Federation Profiles

This section defines the profiles by which a service provider obtains an authentication assertion from an identity provider to facilitate single sign-on. Additionally, the single sign-on profiles can be used as a means of federating an identity from a service provider to an identity provider through the use of the `<Federate>` element in the `<lib:AuthnRequest>` protocol message as specified in [LibertyProtSchema].

The single sign-on profiles make use of the following metadata elements, as defined in [LibertyProtSchema].

- `ProviderID` — Used to uniquely identify the service provider to the identity provider and is documented in these profiles as "service provider ID."
- `SingleSignOnServiceURL` — The URL at the identity provider that the service provider should use when sending single sign-on and federation requests. It is documented in these profiles as "single sign-on service URL."
- `AssertionConsumerServiceURL` — The URL at the service provider that an identity provider should use when sending single sign-on or federation responses. It is documented in these profiles as "assertion consumer service URL."
- `SOAPEndpoint` — The SOAP endpoint location at the service provider or identity provider to which Liberty SOAP messages are sent.

3.2.1 Common Interactions and Processing Rules

This section defines the set of interactions and process rules that are common to all single sign-on profiles.

All single sign-on profiles can be described by one interaction diagram, provided that different messages are optional in different profiles and that the actual content of the messages may differ slightly. Where interactions and messages differ or are optional, they are called out and detailed within the specific single sign-on profiles. Figure 1 represents the basic template of interactions for achieving single sign-on and should be used as the baseline for all single sign-on profiles.

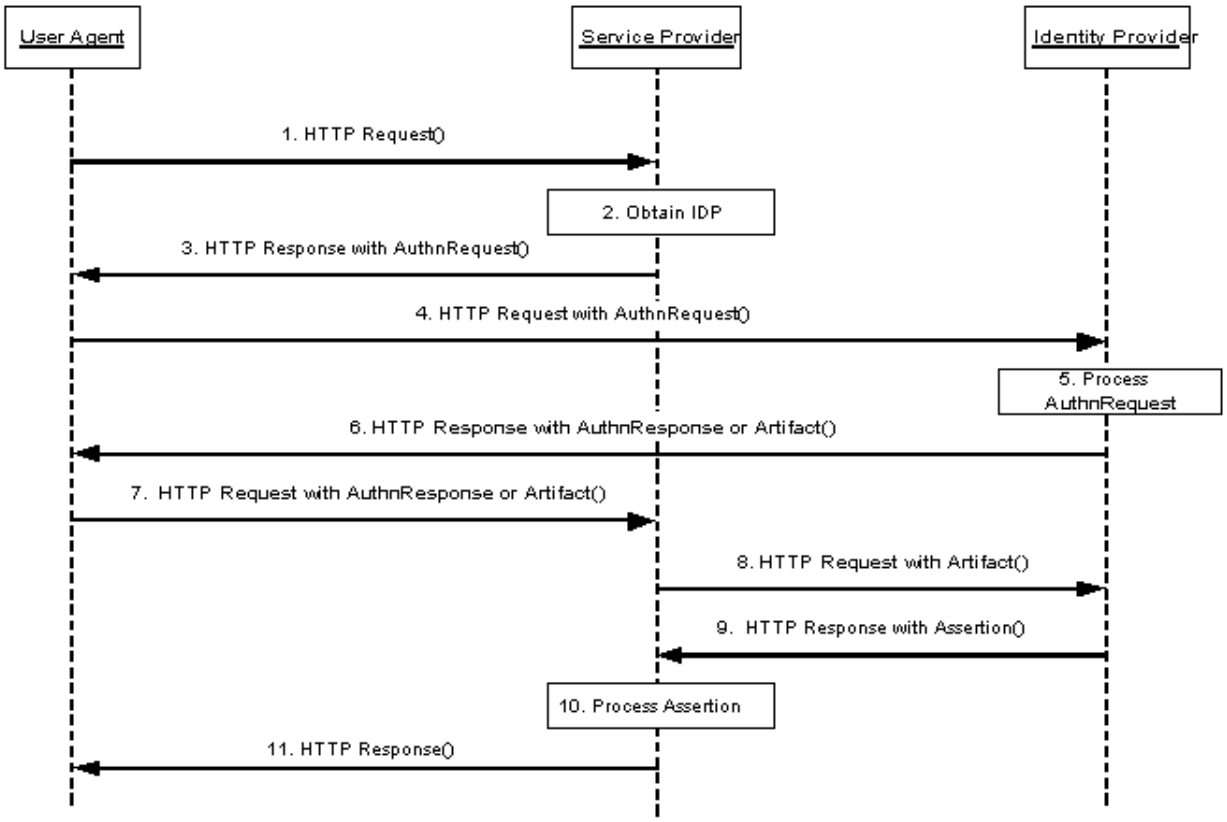


Figure 1: Basic single sign-on profile

Step 1: HTTP Request

In step 1, the user agent accesses the intersite transfer service at the service provider with information about the desired target attached to the URL. Typically, access to the intersite transfer service occurs via a redirection by the service provider in response to a user agent request for a restricted resource.

It is RECOMMENDED that the HTTP Request URI contain a `<query>` component at its end where

`<query>=…RelayState=<return URL>…`

The `<query>` component can be used to convey information about the originally requested resource at the service provider. It is RECOMMENDED that the `<query>` parameter be named `RelayState` and its value be the URL originally requested by the user agent.

It is RECOMMENDED that the HTTP request be made over either SSL 3.0 (see [SSLv3]) or TLS 1.0 (see [RFC2246]) to maintain confidentiality and message integrity in step 1.

Step 2: Obtain Identity Provider

In step 2, the service provider obtains the address of the appropriate identity provider to redirect the user agent to in step 3. The means by which the identity provider address is obtained is implementation-dependent and up to the service provider. The service provider MAY use the Liberty identity provider introduction profile in this step.

Step 3: HTTP Response with <AuthnRequest>

In step 3, the service provider's intersite transfer service responds and sends the user agent to the single sign-on service URL at the identity provider.

The form and contents of the HTTP response in this step are profile-dependent.

Step 4: HTTP Request with <AuthnRequest>

In step 4, the user agent accesses the identity provider's single sign-on service URL with the `<lib:AuthnRequest>` information.

Step 5: Processing <AuthnRequest>

In step 5, the identity provider MUST process the `<lib:AuthnRequest>` message according to the rules specified in [LibertyProtSchema].

If the Principal has not yet been authenticated with the identity provider, authentication at the identity provider MAY occur in this step. The identity provider MAY obtain consent from the Principal for federation, or otherwise consult the Principal. To this end the identify provider MAY return to the HTTP request any HTTP response; including but not limited to HTTP Authentication, HTTP redirect, or content. The identity provider SHOULD respect the HTTP User-Agent and Accept headers and SHOULD avoid responding with content-types that the User-Agent may not be able to accept. Authentication of the Principal by the identity provider is dependent upon the `<lib:AuthnRequest>` message content.

In case the identity provider responds to the user agent with a form, it is RECOMMENDED that the `<input>` parameters of the form be named according to [RFC3106] whenever possible.

Step 6: HTTP Response with <AuthnResponse> or Artifact

In step 6, the identity provider MUST respond to the user agent with a `<lib:AuthnResponse>`, a SAML artifact, or an error.

The form and contents of the HTTP response in this step are profile-dependent.

Step 7: HTTP Request with <AuthnResponse> or Artifact

In step 7, the user agent accesses the assertion consumer service URL at the service provider with a `<lib:AuthnResponse>` or a SAML artifact.

The form and contents of the HTTP request in this step are profile-dependent.

Step 8: HTTP Request with Artifact

Step 8 is required only for single sign-on profiles that use a SAML artifact.

In this step the service provider, in effect, dereferences the single SAML artifact in its possession to acquire the authentication assertion that corresponds to the artifact.

The service provider MUST send a `<samlp:Request>` SOAP message to the identity provider's SOAP endpoint, requesting the assertion by supplying the SAML assertion artifact in the `<samlp:AssertionArtifact>` element as specified in [SAMLBind].

The `<samlp:Request>` MUST be digitally signed by the service provider. The `<samlp:Request>` MUST be signed in accordance with Liberty signing guidelines (Sections 3.1.3 and 3.1.5 in [LibertyProtSchema]). An `id` attribute may be added to the `<samlp:Request>` by declaring an alternate type, `<lib:SignedSAMLRequestType>`. This `id` attribute may be used for signing. The use of the alternate type is as follows:

```
<soap-env:Envelope
  xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/">
  <soap-env:Header/>
  <soap-env:Body>
   <samlp:Request
        xsi:type="lib:SignedSAMLRequestType"
        id="x"
        xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
      IssueInstant="2002-10-31T21:42:14Z"
        MajorVersion="1"
        MinorVersion="0"
      RequestID="2H+PRhYSFYXozOD6r6PZ4YqyKfft">
        ...
   </samlp:Request>
  </soap-env:Body>
</soap-env:Envelope>
```

Step 9: HTTP Response with Assertion

Step 9 is required only for single sign-on profiles that use a SAML artifact.

In this step if the identity provider is able to find or construct the requested assertion, it responds with a `<samlp:Response>` SOAP message with the requested `<saml:Assertion>`. Otherwise, it returns an appropriate status code, as defined within the "SOAP binding for SAML" (see [SAMLBind]) and the [LibertyProtSchema].

The `<samlp:Response>` message MAY be digitally signed. The `<saml:Assertion>` contained in the message MUST be digitally signed by the identity provider.

The `<saml:Assertion>` elements contained within the `<samlp:Response>` message returned by the identity provider MUST include a `<saml:NameIdentifier>` element. If the service provider has registered a name identifier, *i.e.*, the `SPProvidedNameIdentifier`, that value will be used. If the service provider has not registered a name identifier, the name identifier provided by the identity provider will be used. When the identity provider returns multiple assertions within `<samlp:Response>`, it MUST return exactly one `<saml:Assertion>` for each SAML artifact found in the corresponding `<samlp:Request>` element. The case where fewer or greater number of assertions is returned within the `<samlp:Response>` element MUST be treated as an error state by the service provider. The identity provider MUST return a response with zero assertions if

a <samlp:Request> is received from any service provider other than the service provider for which the SAML artifact was originally issued.

The <saml:ConfirmationMethod> element of the assertion MUST be set to the value specified in [SAMLCore] for "SAML Artifact," and the <saml:SubjectConfirmationData> element MUST be present with its value being the SAML artifact supplied to obtain the assertion.

Step 10: Process Assertion

In step 10, the service provider processes the <saml:Assertion> returned in the <samlp:Response> or <lib:AuthnResponse> protocol message to determine its validity and how to respond to the Principal's original request. The signature on the <saml:Assertion> must be verified.

The service provider processing of the assertion MUST adhere to the rules defined in [SAMLCore] for things such as assertion <saml:Conditions> and <saml:Advice>.

The service provider MAY obtain authentication context information for the Principal's current session from the <lib:AuthnContext> element contained in the <saml:advice>. Similarly, the information in the <lib:RelayState> element MAY be obtained and used in further processing by the service provider.

Step 11: HTTP Response

In step 11, the user agent is sent an HTTP response that either allows or denies access to the originally requested resource.

3.2.2 Liberty Browser Artifact Profile

The Liberty browser artifact profile relies on a reference to the needed assertion traveling in a SAML artifact, which the service provider must dereference from the identity provider to determine whether the Principal is authenticated. This profile is an adaptation of the "Browser/artifact profile" for SAML as documented in [SAMLBind]. See Figure 2.

The following URI-based identifier MUST be used when referencing this specific profile (for example, <lib:ProtocolProfile> element of the <lib:AuthnRequest> message):

URI: `http://projectliberty.org/profiles/brws-art`

The Liberty browser artifact profile consists of a single interaction among three parties: a user agent, an identity provider, and a service provider, with a nested subinteraction between the identity provider and the service provider.

3.2.2.1 Interactions

Figure 2 illustrates the Liberty browser artifact profile for single sign-on.

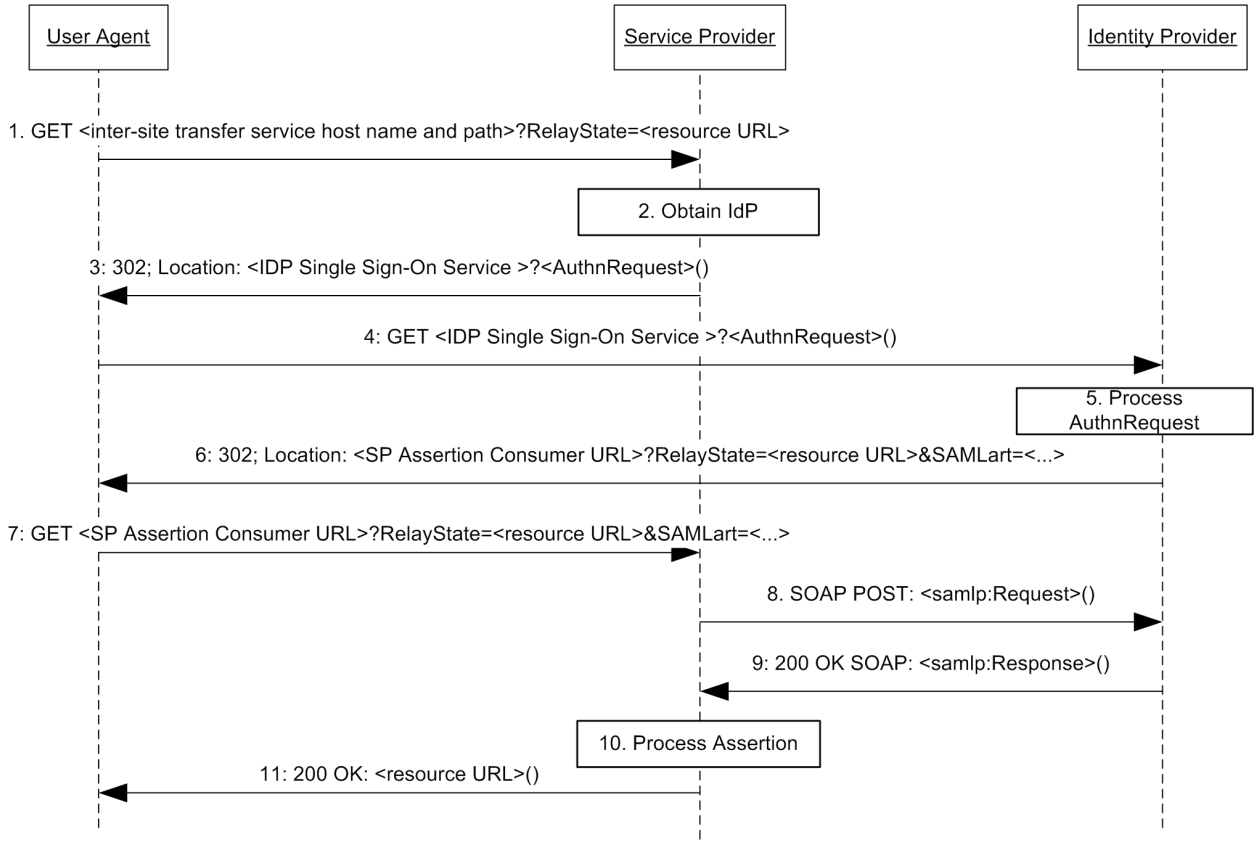


Figure 2: Liberty browser artifact profile for single sign-on

This profile description assumes that the user agent has already authenticated at the identity provider prior to step 1. Thus, a valid session exists for the user agent at the identity provider.

When implementing this profile, all processing rules defined in 3.2.1 for the single sign-on profiles MUST be followed. Additionally, the following rules MUST be observed as they relate to steps 3, 6 and 7:

Step 3: Single sign on Service with <AuthnRequest>

In step 3, the service provider's intersite transfer service responds and sends the user agent to the single sign-on service URL at the identity provider.

The redirection MUST adhere to the following rules:

- The Location HTTP header MUST be set to the identity provider's single sign-on service URL.
- The identity provider's single sign-on service URL MUST specify `https` as the URL scheme; if another scheme is specified, the service provider MUST NOT redirect to the identity provider.

  Note: Future protocols may be adopted and enabled to work within this framework. Therefore, implementers are encouraged to not hardcode a reliance on `https`.

- The Location HTTP header MUST include a `<query>` component containing the `<lib:AuthnRequest>` protocol message as defined in [LibertyProtSchema] with formatting as specified in 3.1.2.

  Note: The `<lib:RelayState>` element of the `<lib:AuthnRequest>` message can be used by the service provider to help maintain state information during the single sign-on and federation process. For example, the originally requested resource (that is, `RelayState` in step 1) could be stored as the value for the `<lib:RelayState>` element, which would then be returned to the service provider in the `<lib:AuthnResponse>` in step 7. The service provider could then use this information to know how to formulate the HTTP response to the user agent in step 11.

The HTTP response MUST take the following form:

```
<HTTP-Version> 302 <Reason Phrase>
<other headers>
Location: https://<Identity Provider Single Sign-On Service host name and path>?<query>
<other HTTP 1.0 or 1.1 components>
```

where

`<Identity Provider Single Sign-On service host name and path>`
: This element provides the host name, port number, and path components of the single sign-on service URL at the identity provider.

`<query>= …<URL-encoded AuthnRequest> …`
: A `<query>` component MUST contain a single authentication request.

Step 6: Redirecting to the Service Provider

In step 6, the identity provider performs a redirection to the service provider's assertion consumer service URL including a SAML artifact in the `<query>` component of the URL.

The redirection MUST adhere to the following rules:

- The Location HTTP header MUST be set to the service provider's assertion consumer service URL, the value of which was determined based upon the `<lib:ProviderID>` element of the `<lib:AuthnRequest>` message.
- The service provider's assertion consumer service URL MUST specify `https` as the URL scheme; if another scheme is specified, the identity provider MUST NOT redirect to the service provider.
- The Location HTTP header MUST include a `<query>` parameter `SAMLart`, the value of which is the SAML artifact on success or on failure. In the case of failure, the status information will be communicated in the `<samlp:Response>` returned in step 9. Additionally, if the `<lib:AuthnRequest>` processed in step 5 included a value for the `<lib:RelayState>` element, then a parameter named `RelayState` with a value set to the value of the `<lib:RelayState>` element MUST be included in the `<query>` component.

The HTTP response MUST take the following form:

```
<HTTP-Version> 302 <Reason Phrase>
<other headers>
Location: https://<Service Provider assertion consumer service URL>?<query>
```

```
<other HTTP 1.0 or 1.1 components>
```

where

`<Service Provider assertion consumer service URL>`

`This element provides the host name, port number, and path components of an assertion consumer service URL at the service provider.`

`<query>= …SAMLart=<SAML Artifact>…RelayState=<resource URL> …`

At least one SAML artifact MUST be included in the `<query>` component. A single `RelayState` MUST be included if a value for `<RelayState>` was provided in the `<lib:AuthnRequest>`. If more than one SAML artifact is included the `<query>` component, all artifacts MUST have the same `IdentityProviderID`.

Step 7: Accessing the Assertion Consumer Service

In step 7, the user agent accesses the assertion consumer service URL at the service provider, with a SAML artifact representing the Principal's authentication information attached to the URL.

3.2.2.2 Artifact Format

The artifact format includes a mandatory two-byte artifact type code, as follows:

```
SAML_artifact     := B64(TypeCode RemainingArtifact)
TypeCode          := Byte1Byte2
```

The notation `B64(TypeCode RemainingArtifact)` stands for the application of the base64 transformation to the catenation of the `TypeCode` and `RemainingArtifact`. This profile defines an artifact type of type code `0x0003`, which is REQUIRED (mandatory to implement) for any implementation of the Liberty browser artifact profile. This artifact type is defined as follows:

```
TypeCode          := 0x0003
RemainingArtifact := IdentityProviderSuccinctID AssertionHandle
IdentityProviderSuccinctID:= 20-byte_sequence
AssertionHandle   := 20-byte_sequence
```

`IdentityProviderSuccinctID` is a 20-byte sequence used by the service provider to determine identity provider identity and location. It is assumed that the service provider will maintain a table of `IdentityProviderSuccinctID` values as well as the URL (or address) for the corresponding SAML responder at the identity provider. This information is communicated between the identity provider and service provider out of band. On receiving the SAML artifact, the service provider determines whether the `IdentityProviderSuccinctID` belongs to a known identity provider and, if so, obtains the location before sending a SAML request.

Any two identity providers with a common service provider MUST use distinct `IdentityProviderSuccinctID` values. Construction of `AssertionHandle` values is governed by the principles that the values SHOULD have no predictable relationship to the contents of the referenced assertion at the identity provider and that constructing or guessing the value of a valid, outstanding assertion handle MUST be infeasible.

The following rules MUST be followed for the creation of SAML artifacts at identity providers:

- Each identity provider selects a single identification URL, corresponding to the provider metadata element `ProviderID` specified in [LibertyProtSchema].

- The identity provider constructs the IdentityProviderSuccinctID component of the artifact by taking the SHA-1 hash of the identification URL as a 20-byte binary value. Note that the `IdentityProviderSuccinctID` value, used to construct the artifact, is not encoded in hexadecimal.The `AssertionHandle` value is constructed from a cryptographically strong random or pseudo-random number sequence (see [RFC1750]) generated by the identity provider. The sequence consists of values of at least eight bytes in size. These values should be padded to a total length of 20 bytes.

3.2.3 Liberty Browser POST Profile

The Liberty browser POST profile allows authentication information to be supplied to an identity provider without the use of an artifact. Figure 3 diagrams the interactions between parties in the Liberty POST profile. This profile is an adaptation of the "Browser/post profile" for SAML as documented in [SAMLBind].

The following URI-based identifier MUST be used when referencing this specific profile (for example, `<lib:ProtocolProfile>` element of the `<lib:AuthnRequest>` message)

URI: `http://projectliberty.org/profiles/brws-post`

The Liberty POST profile consists of a series of two interactions, the first between a user agent and an identity provider, and the second directly between the user agent and the service provider.

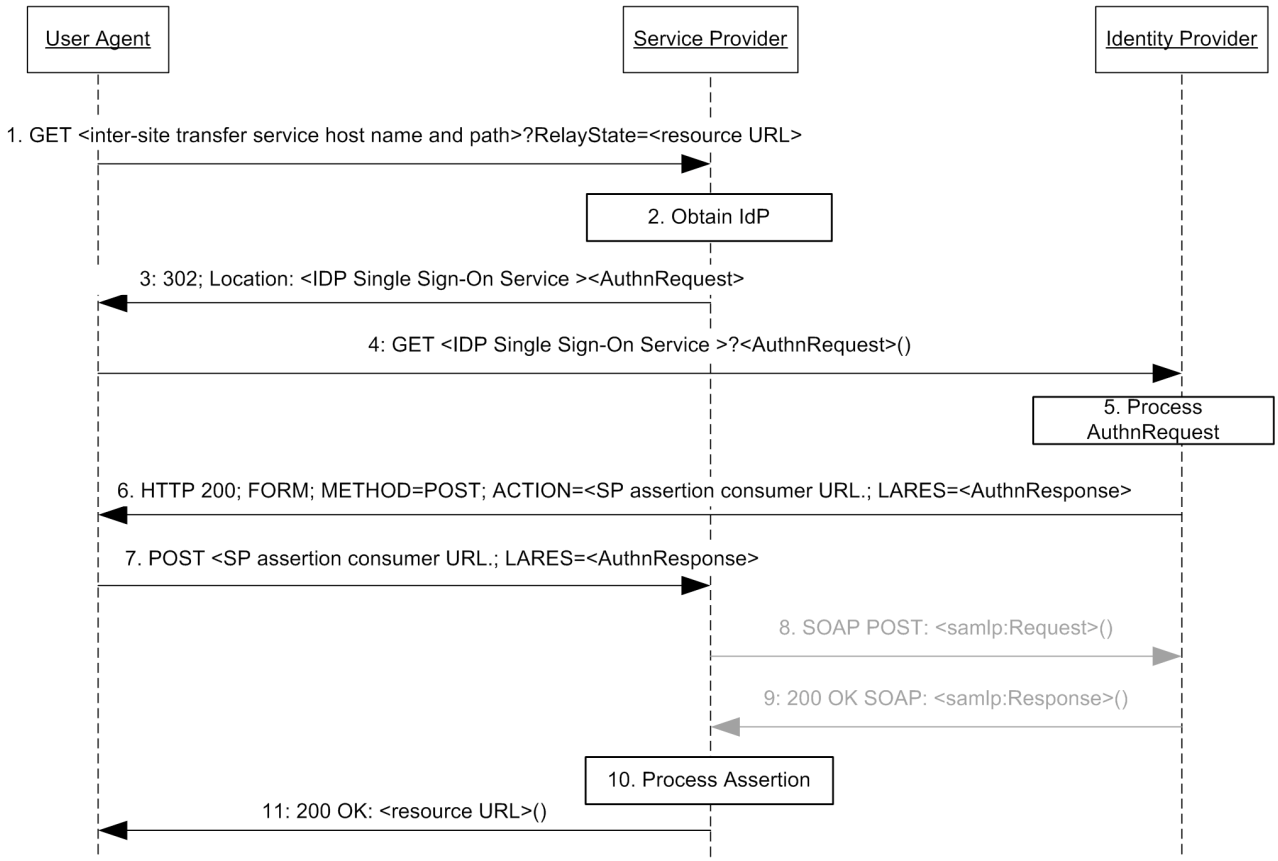


Figure 3: Liberty browser POST profile for single sign-on

This profile description assumes that the user agent has already authenticated at the identity provider prior to step 1. Thus, a valid session exists for the user agent at the identity provider.

When implementing this profile, all processing rules defined in 3.2.1 for single sign-on profiles MUST be followed with the exception that steps 8 and 9 MUST be omitted. Additionally, the following rules MUST be observed as they relate to steps 3, 6 and 7:

Step 3: Single Sign On Service with <AuthnRequest>:

In step 3, the service provider's intersite transfer service responds and sends the user agent to the single sign-on service URL at the identity provider.

The redirection MUST adhere to the following rules:

- The Location HTTP header MUST be set to the identity provider's single sign-on service URL.
- The identity provider's single sign-on service URL MUST specify `https` as the URL scheme; if another scheme is specified, the service provider MUST NOT redirect to the identity provider.

  Note: Future protocols may be adopted and enabled to work within this framework. Therefore, implementers are encouraged to not hardcode a reliance on `https`.

- The Location HTTP header MUST include a `<query>` component containing the `<lib:AuthnRequest>` protocol message as defined in [LibertyProtSchema] with formatting as specified in 3.1.2.

  Note: The `<lib:RelayState>` element of the `<lib:AuthnRequest>` message can be used by the service provider to help maintain state information during the single sign-on and federation process. For example, the originally requested resource (that is, `RelayState` in step 1) could be stored as the value for the `<lib:RelayState>` element, which would then be returned to the service provider in the `<lib:AuthnResponse>` in step 7. The service provider could then use this information to know how to formulate the HTTP response to the user agent in step 11.

The HTTP response MUST take the following form:

```
<HTTP-Version> 302 <Reason Phrase>
<other headers>
Location: https://<Identity Provider Single Sign-On Service host name and path>?<query>
<other HTTP 1.0 or 1.1 components>
```

where

`<Identity Provider Single Sign-On service host name and path>`
: This element provides the host name, port number, and path components of the single sign-on service URL at the identity provider.

`<query>= …<URL-encoded AuthnRequest> …`
: A `<query>` component MUST contain a single authentication request.

Step 6: Generating and Supplying the <AuthnResponse>

In step 6, the identity provider generates an HTML form containing an authentication assertion that MUST be sent in an HTTP 200 response to the user agent.

The form MUST be constructed so that it requests a POST to the service provider's assertion consumer URL with form contents that contain the field `LARES` with the value being the `<lib:AuthnResponse>` protocol message as defined in [LibertyProtSchema]. The `<lib:AuthnResponse>` MUST be encoded by applying a base64 transformation (refer to [RFC2045]) to the `<lib:AuthnResponse>` and all its elements. The service provider's assertion consumer service URL used as the target of the form POST MUST specify `https` as the URL scheme; if another scheme is specified, it MUST be treated as an error by the identity provider.

Multiple `<saml:Assertion>` elements MAY be included in the response. The identity provider MUST digitally sign all the assertions included in the response.

The `<saml:ConfirmationMethod>` element of the assertion MUST be set to the value specified in [SAMLCore] for "Assertion Bearer."

Step 7: Posting the Form Containing the <AuthnResponse>

In step 7, the user agent issues the HTTP POST request containing the `<lib:AuthnResponse>` to the service provider.

3.2.4 Liberty WML POST Profile

The Liberty WML POST profile relies on the use of WML events to instruct a WML browser to submit a HTTP form. This profile is an adaptation of the "Browser/form post profile" for SAML as documented in [SAMLBind]. See Figure 4

The following URI-based identifier MUST be used when referencing this specific profile (for example, `<lib:ProtocolProfile>` element of the `<lib:AuthnRequest>` message)

URI: `http://projectliberty.org/profiles/wml-post`

WML browsers are typical on mobile handsets. The browsers on such handsets communicate via a dedicated proxy, a WAP gateway. This proxy converts the Wireless Session Protocol of the handset into HTTP. Note: The service provider and identity provider will be contacted using only HTTP.

The WML profile described in this section allows for the transportation of signed Liberty messages that are up to approximately 1100 bytes; the length is limited by the overall size of the WML deck. Many WAP browsers do not accept WML decks that are larger than 1300 bytes (after WML tokenizing).

A user agent for this profile, typically a standard WAP browser on a mobile handset, MUST support WAP WML 1.0, 1.1, 1.2, or 1.3 (see [WML1.3]) in addition to the features listed in 3.1.

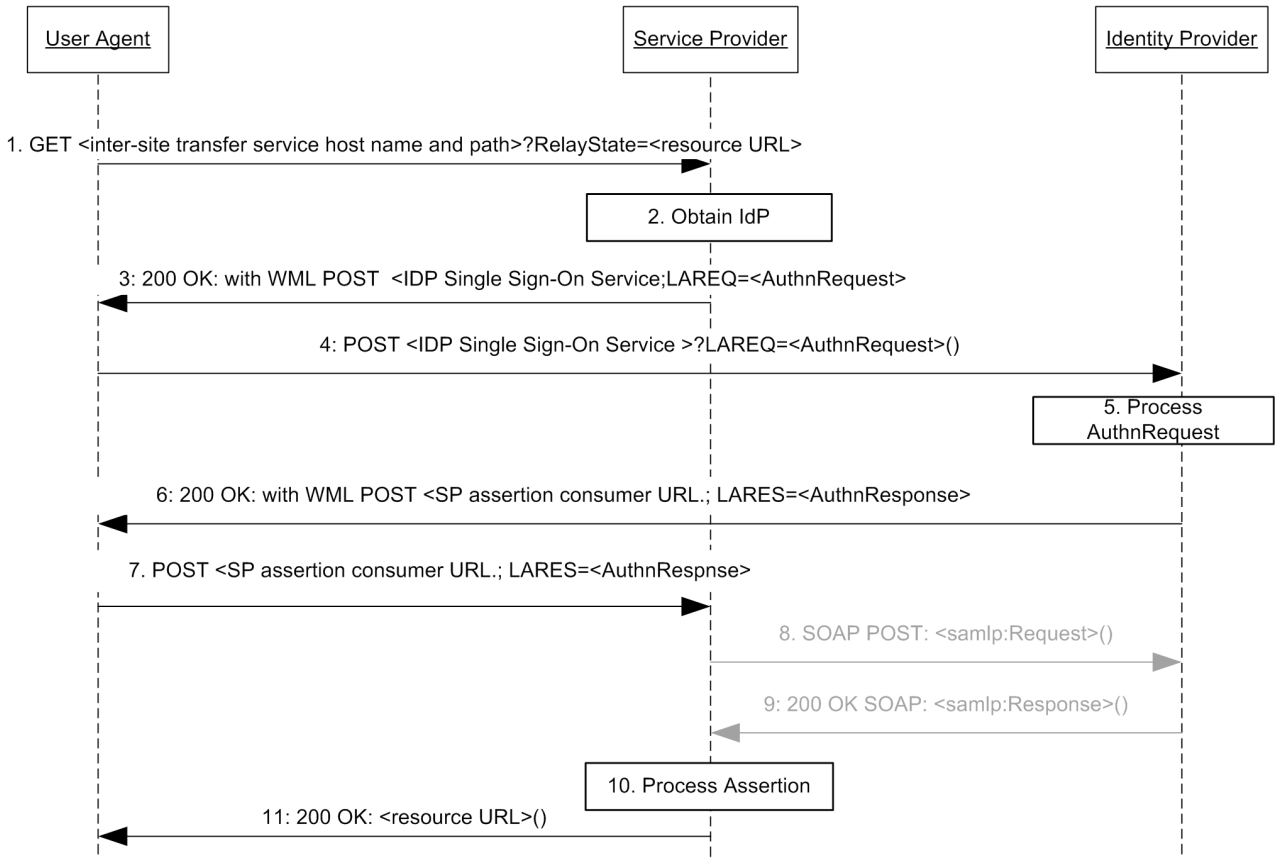


Figure 4: Liberty WML POST profile for single sign-on

This profile description assumes that the user agent has already authenticated at the identity provider prior to step 1. Thus, a valid session exists for the user agent at the identity provider.

When implementing this profile, all processing rules defined in 3.2.1 for single sign-on profiles MUST be followed with the exception that steps 8 and 9 MUST be omitted. Additionally, the following rules MUST be observed as they relate to steps 3, 4, 6, and 7:

Step 3: HTTP Response with <AuthnRequest>

In step 3, the service provider's intersite transfer service responds and instructs the user agent to POST an `<lib:AuthnRequest>` to the single sign-on service URL at the identity provider.

The form contents MUST contain the field `LAREQ` with the value of the `<lib:AuthnRequest>` protocol message as defined in [LibertyProtSchema]. The `<lib:AuthnRequest>` MUST be encoded by applying a base64 transformation (refer to [RFC2045]) to the `<lib:AuthnRequest>` and all its elements. The identity provider's single sign-on service URL used as the target of the form POST MUST specify `https` as the URL scheme; if another scheme is specified, the service provider MUST NOT issue the POST of the `<lib:AuthnRequest>` to the identity provider.

> Note: One method for seamlessly instructing the user agent to POST the `<lib:AuthnRequest>` is to include a WML deck (see Chapter 17 in [HTML4]) within the HTTP 200 response. The following is an example of how the WML code could be structured:

```
…
<wml>
<card id="redirect" title="Log In">
  <onenterforward>
    <go method="post" href="<Identity Provider Single Sign-On service URL>" >
  <postfield name="LAREQ" Value="(<lib:AuthnRequest>)" />
</go>
  </onenterforward>
  <onenterbackward>
    <prev/>
  </onenterbackward>
  <p>
    Contacting IdP. Please wait…
  </p>
…
</card>
…
</wml>
```

It is recommended that the `<go>` element be contained within a `<onenterforward>` element of the first `<card>` in the WML deck. The `<go>` element will ensure that the browser will post the authentication request as soon as the WML code is processed. In addition it is recommended to add an `<onenterbackward>` element to ensure that a Principal will not be presented with the redirect card when navigating backwards.

Step 4: HTTP Request with <AuthnRequest>

In step 4, the user agent issues the HTTP POST request containing the `<lib:AuthnRequest>` to the identity provider.

Step 6: HTTP Response with <AuthnResponse>

In step 6, the identity provider's single sign-on service instructs the user agent to POST a `<lib:AuthnResponse>` to the assertion consumer service URL at the service provider.

The form MUST be constructed so that it requests a POST to the service provider's assertion consumer service URL with the form contents that contain the field `LARES` with the value being the `<lib:AuthnResponse>` protocol message as defined in [LibertyProtSchema]. The `<lib:AuthnResponse>` MUST be encoded by applying a base64 transformation (refer to [RFC2045]) to the `<lib:AuthnResponse>` and all its elements. Multiple SAML assertions MAY be included in the response. The identity provider MUST digitally sign the assertions included in the response. The service provider's assertion consumer service URL used as the target of the form POST MUST specify `https` as the URL scheme; if another scheme is specified, it MUST be treated as an error by the identity provider.

The `<saml:ConfirmationMethod>` element of the assertion MUST be set to the value specified in [SAMLCore] for "Assertion Bearer."

Note: As in step 3, one way of achieving this step is to use a WML deck.

Step 7: HTTP POST with <AuthnResponse>

In step 7, the user agent issues the HTTP POST request containing the `<lib:AuthnResponse>` to the service provider.

3.2.5 Liberty-Enabled Client and Proxy Profile

The Liberty-enabled client and proxy profile specifies interactions between Liberty-enabled clients and/or proxies, service providers, and identity providers. See Figure 5. A Liberty-enabled client is a client that has, or knows how to obtain, knowledge about the identity provider that the Principal wishes to use with the service provider. In addition a Liberty-enabled client receives and sends Liberty messages in the body of HTTP requests and responses. Therefore, Liberty-enabled clients have no restrictions on the size of the Liberty protocol messages.

A Liberty-enabled proxy is a HTTP proxy (typically a WAP gateway) that emulates a Liberty-enabled client. Unless stated otherwise, all statements referring to LECP are to be understood as statements about both Liberty-enabled clients as well as Liberty-enabled proxies.

The following URI-based identifier must be used when referencing this specific profile (for example, `<lib:ProtocolProfile>` element of the `<lib:AuthnRequest>` message)

URI: `http://projectliberty.org/profiles/lecp`

All LECPs, in addition to meeting the common requirements for profiles in 3.1, MUST indicate that it is a LECP by including a Liberty-Enabled header or entry in the value of the HTTP User-Agent header for each HTTP request they make. The preferred method is the Liberty-Enabled header. The formats of the Liberty-Enabled header and User-Agent header entry are defined 3.2.5.1.

3.2.5.1 Liberty-Enabled Indications

A LECP SHOULD add the Liberty-Enabled header to each HTTP request. The Liberty-Enabled header MUST be named `Liberty-Enabled` and be defined as using Augmented BNF as specified in section 2 of [RFC 2616].

```
Liberty-Enabled = "Liberty-Enabled" ":" LIB_Version ["," 1#Extension]
LIB_Version = "LIBV" "=" 1*absoluteURI
; any spaces or commas in the absoluteURI MUST be escaped as defined
in section 2.4 of [RFC 2396]
Extension = ExtName "=" ExtValue
ExtName = ["." host] | <any field-value but ".", "," or "=">) <any
field-value but "=" or ",">
ExtValue = <any field-value but ",">)
```

The comment, field-value, and product productions are defined in [RFC 2616]. `LIB_Version` identifies the versions of the Liberty specifications that are supported by this LECP. Each version is identified by a URI. Service providers or identity providers receiving a Liberty-Enabled header MUST ignore any URIs listed in the `LIB_Version` production that they do not recognize. All LECPs compliant with this specification MUST send out, at minimum, the URI `http://projectliberty.org/specs/v1` as a value in the `LIB_Version` production. The ordering of the URIs in the `LIB_Version` header is meaningful; therefore, service providers and identity providers are encouraged to use the first version in the list that they support. Supported Liberty versions are not negotiated between the LECP and the service provider. The LECP simply advertises what version it does support, and the service provider MUST return the response for the corresponding version as defined in step 3 below.

Optional extensions MAY be added to the Liberty-Enabled header to indicate new information. The value of the `ExtName` production MUST use the "`host`" ";" prefixed form if the new

extension name has not been standardized and registered with Liberty or its designated registration authorities. The value of the `host` production MUST be an IP or DNS address that is owned by the issuer of the new name. By using the DNS/IP prefix, namespace collisions can be effectively prevented without having to introduce yet another centralized registration agency.

LECPs MAY include the Liberty-Agent header in their requests. This header provides information about the software implementing the LECP functionality and is similar to the User-Agent and Server headers in HTTP.

```
Liberty-Agent = "Liberty-Agent" ":" 1*( product | comment)
```

> Note: The reason for introducing the new header (that is, Liberty-Enabled) rather than just using User-Agent is that LECP may be a Liberty-enabled proxy. In that case the information about the Liberty-enabled proxy would not be in the User-Agent header. In theory the information could be in the VIA header. However, for security reasons, values in the VIA header can be collapsed, and comments (where software information would be recorded) can always be removed. As such, the VIA header is not suitable. Using the User-Agent header for a Liberty-enabled client and the Liberty-Agent header for a Liberty-enabled proxy was also discussed. However, this approach seemed too complex.
>
> Originally the Liberty-Agent header was going to be part of the Liberty-Enabled header. However, header lengths in HTTP implementations are limited; therefore, putting this information in its own header was considered the preferred approach.

A LECP MAY add a Liberty-Enabled entry in the HTTP User-Agent request header. The HTTP User-Agent header is specified in [RFC2616]. A LECP MAY include in the value of this header the `Liberty-Enabled` string as defined above for the Liberty-Enabled header.

> Note: The reason for adding information to the User-Agent header is to allow for Liberty-enabled client products that must rely on a platform that cannot be instructed to insert new headers in each HTTP request.
>
> The User-Agent header is often overloaded; therefore, the Liberty-Enabled header should be the first choice for any implementation of a LECP. The entry in the User-Agent header then remains as a last resort.

3.2.5.2 Interactions

Figure 5 illustrates the Liberty-enabled client and proxy profile for single sign-on.

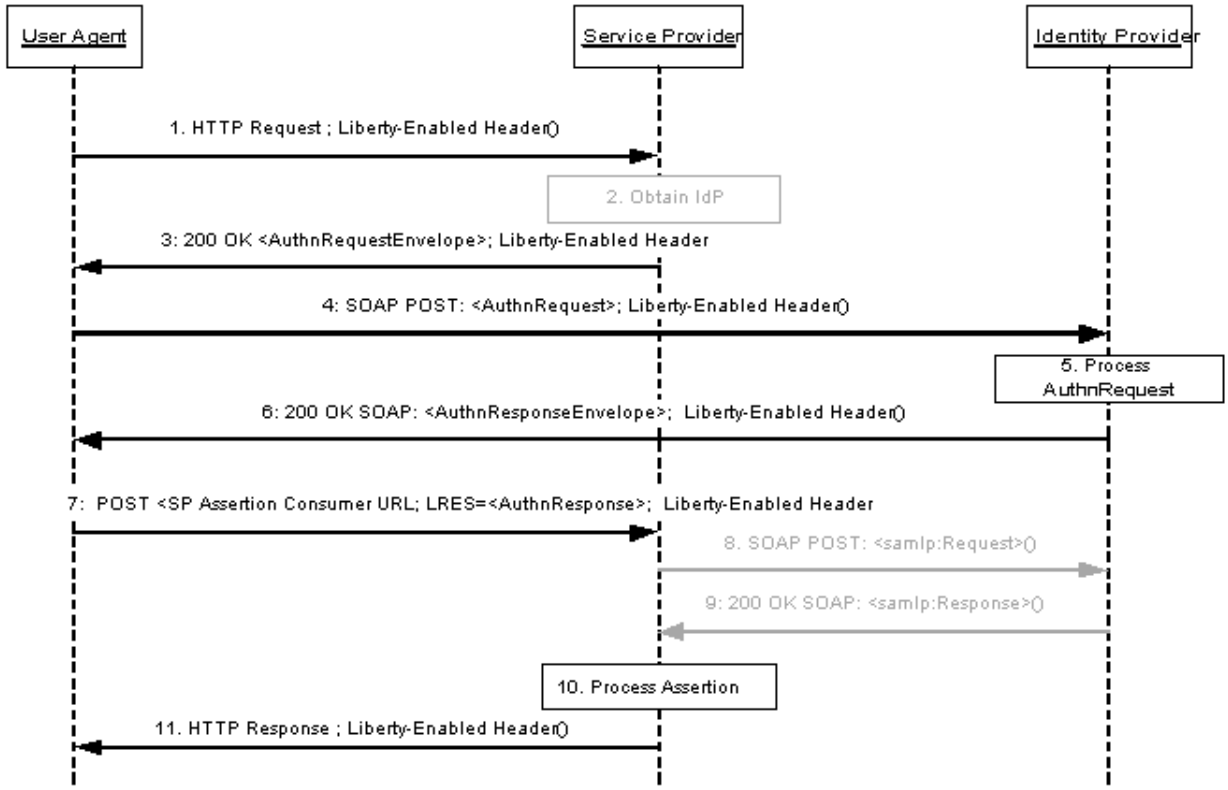


Figure 5: Liberty-enabled client and proxy profile for single sign-on

This profile description assumes that the user agent has already authenticated at the identity provider prior to step 1. Thus, a valid session exists for the user agent at the identity provider.

The LECP receives authentication requests from the service provider in the body of the HTTP response. The LECP submits this authentication request as a SOAP request to the identity provider. Because this SOAP request is between the LECP and the identity provider, TLS authentication cannot be performed between service provider and identity provider; therefore, service providers and identity providers MUST rely on the signature of the `<lib:AuthnRequest>` and the returned `<saml:Assertion>`, respectively, for mutual authentication.

When implementing this profile, processing rules for steps 5, 10, and 11 defined in 3.2.1 for single sign-on profiles MUST be followed, while steps 2, 8, and 9 MUST be omitted. Additionally, the following rules MUST be observed as they relate to steps 1, 3, 4, 6, and 7:

Step 1: Accessing the Service Provider

In step 1, the user agent accesses the service provider with the Liberty-Enabled header (or with the Liberty-Enabled entry in the User-Agent header) included in the HTTP request.

The HTTP request MUST contain only one Liberty-Enabled header. Hence if a proxy receives a HTTP request that contains a Liberty-Enabled header, it MUST NOT add another Liberty-Enabled header. However, a proxy MAY replace the Liberty-Enabled header. A proxy that replaces or adds

a Liberty-Enabled header MUST process <lib:AuthnRequest> messages as defined in steps 3 and 4 as well as <lib:AuthnResponse> messages as specified in steps 6 and 7.

It is RECOMMENDED that a LECP add "application/vnd.liberty-request+xml" as one of its supported content types to the Accept header.

Step 3: HTTP Response with <AuthnRequest>

In step 3, the service provider's intersite transfer service issues an HTTP 200 OK response to the user agent. The response MUST contain a single <lib:AuthnRequestEnvelope> with content as defined in [LibertyProtSchema]. If a service provider receives a Liberty-Enabled header, or a User-Agent header with the Liberty-Enabled entry, the service provider MUST respond according to the Liberty-enabled client and proxy profile and include a Liberty_Enabled header in its response. Hence service providers MUST support the Liberty-enabled client and proxy profile.

The processing rules and default values for the Liberty-Enabled indications are as defined in 3.2.5.1. The service provider MAY advertise any Liberty version supported in this header, not only the version used for the specific response.

The HTTP response MUST contain a Content-Type header with the value application/vnd.liberty-request+xml unless the LECP and service provider have negotiated a different format.

A service provider MAY provide a list of identity providers it recognizes by including the <lib:IDPList> element in the <lib:AuthnRequestEnvelope>. The format and processing rules for the identity provider list MUST be as defined in [LibertyProtSchema].

> Note: In cases where a value for the <lib:GetComplete> element is provided within <lib:IDPList>, the URI value for this element MUST specify https as the URL <scheme>.

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>.

The following example demonstrates the usage of the <lib:AuthnRequestEnvelope>:

```
<?xml version="1.0" ?>
 <lib:AuthnRequestEnvelope xmlns:lib="http://projectliberty.org/schemas/core/2002/12/">
   <lib:AuthnRequest >
     . . . AuthnRequest goes here . . .
   </lib:AuthnRequest>
   <lib:AssertionConsumerServiceURL>
       https://service-provider.com/LibertyLogin
   </lib:AssertionConsumerServiceURL>
   <lib:IDPList >
     . . . IdP list goes here . . .
   </lib:IDPList>
</lib:AuthnRequestEnvelope>
```

If the service provider does not support the LECP-advertised Liberty version, the service provider MUST return to the LECP an HTTP 501 response with the reason phrase "Unsupported Liberty Version."

The responses in step 3 and step 6 SHOULD NOT be cached. To this end service providers and identity providers SHOULD place both "Cache-Control: no-cache" and "Pragma: no-

1162 cache" on their responses to ensure that the LECP and any intervening proxies will not cache the
1163 response.

1164 Step 4: HTTP Request with <AuthnRequest>

1165 In step 4, the LECP determines the appropriate identity provider to use and then issues an HTTP
1166 POST of the <lib:AuthnRequest> in the body of a SOAP message to the identity provider's
1167 single sign-on service URL. The request MUST contain the same <lib:AuthnRequest> as was
1168 received in the <lib:AuthnRequestEnvelope> from the service provider in step 3.

1169 Note: The identity provider list can be used by the LECP to create a user identifier
1170 to be presented to the Principal. For example, the LECP could compare the list of
1171 the Principal's known identities (and the identities of the identity provider that
1172 provides those identities) against the list provided by the service provider and then
1173 only display the intersection.

1174 If the LECP discovers a syntax error due to the service provider or cannot proceed any further for
1175 other reasons (for example, cannot resolve identity provider, cannot reach the identity provider,
1176 etc), the LECP MUST return to the service provider a <lib:AuthnResponse> with a
1177 <samlp:Status> indicating the desired error element as defined in [LibertyProtSchema]. The
1178 <lib:AuthnResponse> containing the error status MUST be sent using a POST to the service
1179 provider's assertion consumer service URL obtained from the
1180 <lib:AssertionConsumerServiceURL> element of the <lib:AuthnRequestEnvelope>.
1181 The POST MUST be a form that contains the field LARES with the value being the
1182 <lib:AuthnResponse> protocol message as defined in [LibertyProtSchema], containing the
1183 <samlp:Status>. The <lib:AuthnResponse> MUST be encoded by applying a base64
1184 transformation (refer to
1185 [RFC2045]) to the <lib:AuthnResponse> and all its elements.

1186 Step 6: HTTP Response with <AuthnResponse>

1187 In step 6, the identity provider responds to the <lib:AuthnRequest> by issuing an HTTP 200
1188 OK response. The response MUST contain a single <lib:AuthnResponseEnvelope> in the
1189 body of a SOAP message with content as defined in [LibertyProtSchema].

1190 The identity provider MUST include the Liberty-Enabled HTTP header following the same
1191 processing rules as defined in 3.2.5.1.

1192 The Content-Type MUST be set to application/vnd.liberty-response+xml.

1193 If the identity provider discovers a syntax error due to the service provider or LECP or cannot
1194 proceed any further for other reasons (for example, unsupported Liberty version), the identity
1195 provider MUST return to the LECP a <lib:AuthnResponseEnvelope> containing a
1196 <lib:AuthnResponse> with a <samlp:Status> indicating the desired error element as
1197 defined in [LibertyProtSchema].

1198 Step 7: Posting the Form Containing the <AuthnResponse>

1199 In step 7, the LECP issues an HTTP POST of the <lib:AuthnResponse> that was received in
1200 the <lib:AuthnResonseEnvelope> SOAP response in step 6. The <lib:AuthnResponse>
1201 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*. The POST MUST be a form that contains the field LARES with the value being the <lib:AuthnResponse> protocol message as defined in [LibertyProtSchema]. The <lib:AuthnResponse> MUST be encoded by applying a base64 transformation (refer to [RFC2045]) to the <lib:AuthnResponse> and all its elements. The service provider's assertion consumer service URL used as the target of the form POST MUST specify https as the URL scheme; if another scheme is specified, it MUST be treated as an error by the identity provider.

If the LECP discovers an error (for example, syntax error in identity provider response), the LECP MUST return to the service provider a <lib:AuthnResponse> with a <samlp:Status> indicating the appropriate error element as defined in [LibertyProtSchema]. The <lib:AuthnResponse> containing the error status MUST be sent using a POST to the service provider's assertion consumer service URL. The POST MUST be a form that contains the field named LARES with its value being the <lib:AuthnResponse> protocol message as defined in [LibertyProtSchema] with formatting as specified 3.1.2. Any <lib:AuthnResponse> messages created by the identity provider MUST not be sent to the service provider.

3.3 Register Name Identifier Profiles

This section defines the profiles by which a provider may register or change a name identifier for a Principal. This message exchange is optional. During federation, the identity provider supplies an opaque handle identifying the Principle. This is the <lib:IDPProvidedNameIdentifier>. If neither provider involved in the federation opts to register any other name identifier, then this initial <lib:IDPProvidedNameIdentifier> is to be used by both providers.

An identity provider may choose to register a new <lib:IDPProvidedNameIdentifier> at any time subsequent to federation, using this protocol. Additionally, a service provider may choose to register an <lib:SPProvidedNameIdentifier>, which it expects the identity provider to use (instead of the <lib:IDPProvidedNameIdentifier>) when communicating with it about the Principal.

Two profiles are specified: HTTP-Redirect-Based and SOAP/HTTP-based.

Either the identity or service provider may initiate the register name identifier protocol. The available profiles are defined in 3.3.1 and 3.3.2, and vary slightly based on whether the protocol was initiated by the identity or service provider:

- Register Name Identifier Initiated at Identity Provider
  - **HTTP-Redirect-Based:** Relies on a HTTP 302 redirect to communicate between the identity provider and the service provider.
  - **SOAP/HTTP-Based:** Relies on a SOAP call from the identity provider to the service provider.
- Register Name Identifier Initiated at Service Provider
  - **HTTP-Redirect-Based:** Relies on a HTTP 302 redirect to communicate between the service provider and the identity provider.

- **SOAP/HTTP-Based:** Relies on a SOAP call from the service provider to the identity provider.

The interactions and processing rules for the SOAP/HTTP-based and HTTP-redirect-based profiles are essentially the same regardless of whether the profile was initiated at the service provider or at the identity provider, but the message flow directions are reversed.

The register name identifier profiles make use of the following metadata elements, as defined in [LibertyProtSchema]:

- `RegisterNameIdentifierProtocolProfile`: The service provider's preferred register name identifier profile, which should be used by the identity provider when registering a new identifier. This would specify the URI based identifier for one of the IDP Initiated register name identifier profiles.
- `RegisterNameIdentifierServiceURL`: The URL used for user-agent-based Register Name Identifier Protocol profiles.
- `RegisterNameIdentifierServiceReturnURL`: The provider's redirecting URL for use after HTTP name registration has taken place.
- `SOAPEndpoint`: The SOAP endpoint location at the service provider or identity provider to which Liberty SOAP messages are sent.

3.3.1 Register Name Identifier Initiated at Identity Provider

An identity provider MAY change the `<lib:IDPProvidedNameIdentifier>` it has assigned a Principal and transmit that information to a service provider. The `<lib:IDPProvidedNameIdentifier>` MAY be changed without changing any federations. The reasons an identity provider may wish to change the name identifier for a Principal are implementation dependent, and thus outside the scope of this specification. Changing the `<lib:IDPProvidedNameIdentifier>` MAY be accomplished in either an HTTP-Redirect-Based or SOAP/HTTP mode.

3.3.1.1 HTTP-Redirect-Based Profile

A HTTP-redirect-based register name identifier profile cannot be self-initiated by an identity provider, but must be a triggered by a message, such as an `<lib:AuthnRequest>`. We note that we do not normatively specify when and how the identity provider can initiate this profile—that is left to the discretion of the identity provider. As an example, it may be triggered by a message, such as an `<lib:AuthnRequest>`. When the identity provider decides to initiate the profile in this case, it will insert this profile between the `AuthnRequest/AuthnResponse` transactions.

The HTTP-redirect-based profile relies on using HTTP 302 redirects to communicate register name identifier messages from the identity provider to the service provider. The HTTP-Redirect Register Name Identifier Profile (Figure 6) illustrates this transaction.

The following URI-based identifier MUST be used when referencing this specific profile:

URI: `http://projectliberty.org/profiles/rni-idp-http`

This URI identifier MUST be specified in the service provider metadata element `RegisterNameIdentifierProtocolProfile` when the service provider intends to indicate to the identity provider a preference for receiving register name identifier messages via a HTTP 302 redirect.

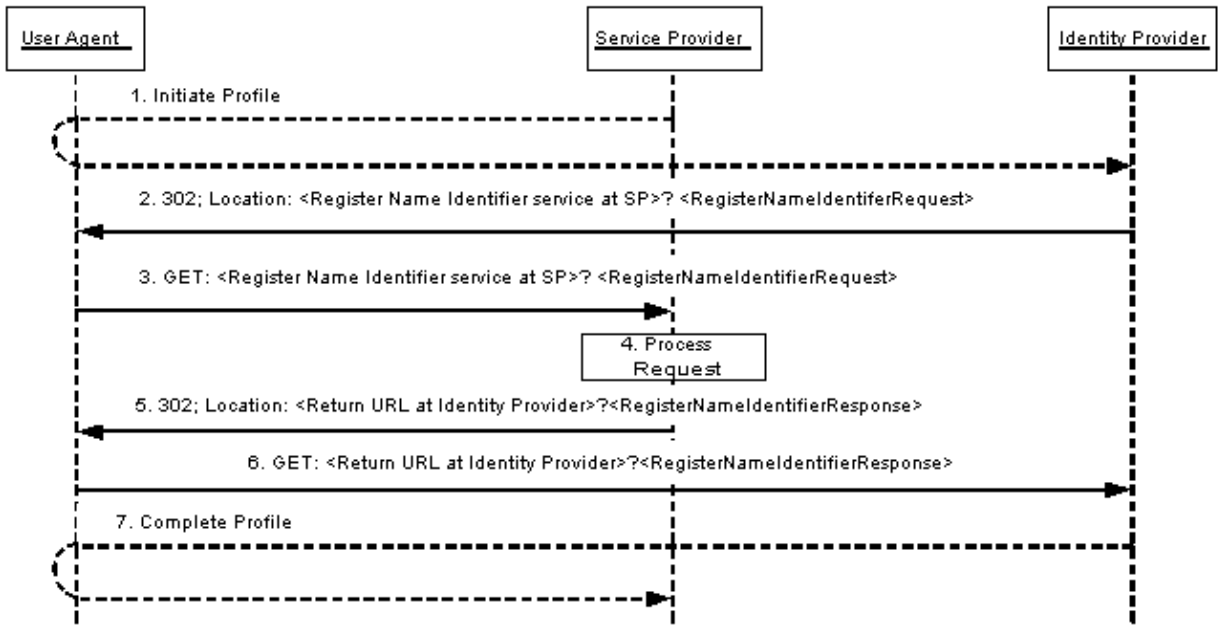


Figure 6. Register Name Identifier Profile.

In an example scenario, the service provider makes an `<lib:AuthnRequest>` to the identity provider for authentication of the Principal's User Agent (step 1). The identity provider effects an `<lib:IDPProvidedNameIdentifier>` change in the service provider via a URL redirection. The profile is as follows:

Step 1: Initiate Profile

This interaction is not normatively specified as part of the profile, but shown for illustrative purposes.

Step 2: Redirecting to the Service Provider Register Name Identifier Service

In step 2, the identity provider redirects the user agent to the register name identifier service at the service provider.

The redirection MUST adhere to the following rules:

- The Location HTTP header MUST be set to the service provider's register name identifier service URL.

- The service provider's register name identifier service URL MUST specify https as the URL scheme; if another scheme is specified, the identity provider MUST NOT redirect to the service provider.
- The Location HTTP header MUST include a `<query>` component containing the `<lib:RegisterNameIdentifierRequest>` protocol message as defined in [LibertyProtSchema] with formatting as specified in 3.1.2.

The HTTP response MUST take the following form:

```
<HTTP-Version> 302 <Reason Phrase>
<other headers>
Location : https://<Service Provider Register Name Identifier service URL>?<query>
<other HTTP 1.0 or 1.1 components>
```

where

`<Service Provider Register Name Identifier service URL>`
: This element provides the host name, port number, and path components of the register name identifier service URL at the service provider.

`<query>= …<URL-encoded RegisterNameIdentifierRequest>…`
: The `<query>` component MUST contain a single register name identifier request.

Step 3: Accessing the Service Provider Register Name Identifier Service

In step 3, the user agent accesses the service provider's register name identifier service URL with the `<lib:RegisterNameIdentifierRequest>` information attached to the URL fulfilling the redirect request.

Step 4: Processing the Register Name Identifier Request

In step 4, the service provider MUST process the `<lib:RegisterNameIdentifierRequest>` according to the rules defined in [LibertyProtSchema].

The service provider MAY remove the old name identifier after registering the new name identifier.

Step 5: Redirecting to the Identity Provider return URL with the Register Name Identifier Response

In step 5, the service provider's register name identifier service responds and redirects the user agent back to identity provider using a return URL location specified in the `RegisterNameIdentifierServiceReturnURL` metadata element. If the URL-encoded `<lib: RegisterNameIdentifierRequest>` message received in step 3 contains a parameter named `RelayState`, then the service provider MUST include a `<query>` component containing the same `RelayState` parameter and its value in its response to the identity provider.

The redirection MUST adhere to the following rules:

- The Location HTTP header MUST be set to the identity providers return URL specified in the `RegisterNameIdentifierServiceReturnURL` metadata element.

- The identity provider's return URL MUST specify https as the URL scheme; if another scheme is specified, the service provider MUST NOT redirect to the identity provider.
- The Location HTTP header MUST include a `<query>` component containing the `<lib:RegisterNameIdentifierResponse>` protocol message as defined in [LibertyProtSchema] with formatting as specified in 3.1.2.

The HTTP response MUST take the following form:

```
<HTTP-Version> 302 <Reason Phrase>
<other headers>
Location : https://<Identity Provider Service Return URL >?<query>
<other HTTP 1.0 or 1.1 components>
```

where:

`<Identity Provider Service Return URL>`
This element provides the host name, port number, and path components of the return URL at the identity provider.

`<query>= …<URL-encoded RegisterNameIdentifierResponse>…`
The `<query>` component MUST contain a single register name identifier response. The `<URL-encoded RegisterNameIdentifierResponse>` component MUST contain the identical `RelayState` parameter and its value that was received in the URL-encoded register name identifier message obtained in step 3. If no `RelayState` parameter was provided in the step 3 message, then a `RelayState` parameter MUST NOT be specified in the `<URL-encoded RegisterNameIdentifierResponse>`.

Step 6: Accessing the Identity Provider return URL with the Register Name Identifier Response

In step 6, the user agent accesses the identity provider's return URL location fulfilling the redirect request.

Step 7: Complete profile

This concludes the initial sequence, which triggered the initiation of this profile.

3.3.1.2 SOAP/HTTP-Based Profile

The following URI-based identifier MUST be used when referencing this specific profile:

URI: `http://projectliberty.org/profiles/rni-idp-soap`

This URI identifier MUST be specified in the service provider metadata element `RegisterNameIdentifierProtocolProfile` when the service provider intends to indicate to the identity provider a preference for receiving register name identifier messages via SOAP over HTTP.

The steps involved in the SOAP/HTTP-based profile MUST utilize the SOAP binding for Liberty as defined in 2.1. See Figure 7.

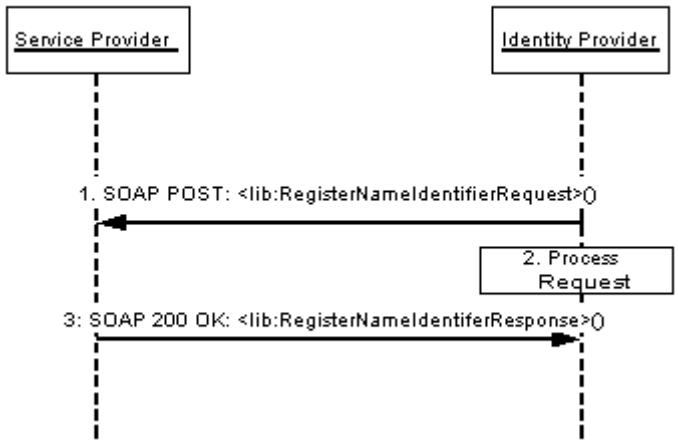


Figure 7: SOAP/HTTP-based profile for registering name identifiers

Step 1: Request to Register Name Identifier

In step 1, the identity provider sends a `<lib:RegisterNameIdentifierRequest>` protocol message to the service provider's SOAP endpoint specifying `<lib:SPProvidedNameIdentifier>` , `<lib:IDPProvidedNameIdentifier>`, and `<lib:OldProvidedNameIdentifier>` as defined in [LibertyProtSchema]. The `<lib:SPProvidedNameIdentifier>` will only contain a value if the service provider has previously used the register name identifier profile.

Step 2: Process Request

Service provider records new `<lib:IDPProvidedNameIdentifier>`.

Step 3: Response to Register Name Identifier

The service provider, after successfully registering the new `<lib:IDPProvidedNameIdentifier>` provided by the identity provider, MUST respond with a `<lib:RegisterNameIdentifierResponse>` according to the processing rules defined in [LibertyProtSchema].

3.3.2 Register Name Identifier Initiated at Service Provider

A service provider may register, or change a `<lib:SPProvidedNameIdentifier>` which is a name identifier it expects the identity provider to use when communicating with it about the Principal. Until it registers a `<lib:SPProvidedNameIdentifier>`, an identity provider will continue to use the current `<lib:IDPProvidedNameIdentifier>` when referring to the Principal.

3.3.2.1 HTTP-Redirect-Based Profile

The HTTP-redirect-based profile relies on the use of a HTTP 302 redirect to communicate a register name identifier message from the service provider to the identity provider.

The following URI-based identifier MUST be used when referencing this specific profile:

URI: `http://projectliberty.org/profiles/rni-sp-http`

A HTTP-redirect-based register name identifier profile can be self-initiated by a service provider to change the `<lib:SPProvidedNameIdentifier>`. We note that we do not normatively specify when and how the service provider can initiate this profile—that is left to the discretion of the service provider. The HTTP-redirect-based profile relies on using HTTP 302 redirects to communicate register name identifier messages from the service provider to the identity provider. The service provider effects a `<lib:SPProvidedNameIdentifier>` change in the identity provider via a URL redirection. For a discussion of the interactions and processing steps, refer to 3.3.1.1. When reviewing that profile, interchange all references to service provider and identity provider in the interaction diagram and processing steps 3-7.

3.3.2.2 SOAP/HTTP-Based Profile

The SOAP/HTTP-based profile relies on using SOAP over HTTP to communicate register name identifier messages from the service provider to the identity provider. For a discussion of the interactions and processing steps, refer to 3.3.1.2. When reviewing that profile, interchange all references to service provider and identity provider in the interaction diagram and processing steps.

The following URI-based identifier MUST be used when referencing this specific profile:

URI: `http://projectliberty.org/profiles/rni-sp-soap`

3.4 Identity Federation Termination Notification Profiles

The Liberty identity federation termination notification profiles specify how service providers and identity providers are notified of federation termination (also known as defederation). Note: Other means of federation termination are possible, such as federation expiration and termination of business agreements between service providers and identity providers. These means of federation termination are outside the scope of this specification.

Identity federation termination can be initiated at either the identity provider or the service provider. The Principal SHOULD have been authenticated by the provider at which identity federation termination is being initiated. The available profiles are defined in 3.4.1 and 3.4.2, depending on whether the identity federation termination notification process was initiated at the identity provider or service provider:

- **Federation Termination Notification Initiated at Identity Provider**
  - **HTTP-Redirect-Based:** Relies on a HTTP 302 redirect to communicate between the identity provider and the service provider.
  - **SOAP/HTTP-Based:** Relies on a SOAP call from the identity provider to the service provider.

- **Federation Termination Notification Initiated at Service Provider**
  - **HTTP-Redirect-Based:** Relies on a HTTP 302 redirect to communicate between the service provider and the identity provider.
  - **SOAP/HTTP-Based:** Relies on a SOAP call from the service provider to the identity provider.

The interactions and processing rules for the SOAP/HTTP-based and HTTP-redirect-based profiles are essentially the same regardless of whether federation termination notification was initiated at the service provider or at the identity provider.

The identity federation termination notification profiles make use of the following metadata elements, as defined in [LibertyProtSchema]:

- `FederationTerminationServiceURL` — The URL at the service provider or identity provider to which identity federation termination notifications are sent. It is documented in these profiles as "federation termination service URL."
- `FederationTerminationServiceReturnURL` — The URL used by the service provider or identity provider when redirecting the user agent at the end of the federation termination notification profile process.
- `FederationTerminationNotificationProtocolProfile` — Used by the identity provider to determine which federation termination notification profile MUST be used when communicating with the service provider.
- `SOAPEndpoint` — The SOAP endpoint location at the service provider or identity provider to which Liberty SOAP messages are sent.

3.4.1 Federation Termination Notification Initiated at Identity Provider

The profiles in 3.4.1.1 and 3.4.1.2 are specific to identity federation termination when initiated at the identity provider. Effectively, when using these profiles, the identity provider is stating to the service provider that it will no longer provide the Principal's identity information to the service provider and that the identity provider will no longer respond to any requests by the service provider on behalf of the Principal.

3.4.1.1 HTTP-Redirect-Based Profile

The HTTP-redirect-based profile relies on using HTTP 302 redirect to communicate federation termination notification messages from the identity provider to the service provider. See Figure 8.

The following URI-based identifier MUST be used when referencing this specific profile:

URI: `http://projectliberty.org/profiles/fedterm-idp-http`

This URI identifier MUST be specified in the service provider metadata element `FederationTerminationNotificationProtocolProfile` when the service provider intends to indicate to the identity provider a preference for receiving federation termination notifications via a HTTP 302 redirect.

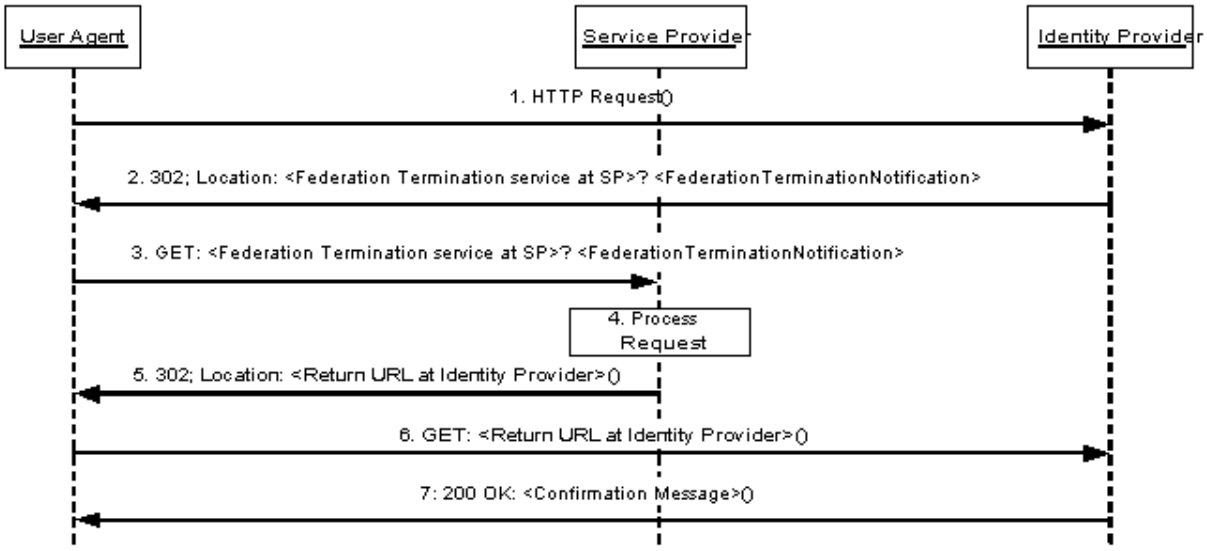


Figure 8: HTTP-redirect-based profile for federation termination

This profile description assumes the following preconditions:

- The Principal's identity at the service provider is federated with his/her identity at the identity provider.
- The Principal has requested to the identity provider that the federation be terminated.
- The Principal has authenticated with the identity provider.

Step 1: Accessing the Federation Termination Service

In step 1, the user agent accesses the identity federation termination service URL at the identity provider specifying the service provider with which identity federation termination should occur. How the service provider is specified is implementation-dependent and, as such, is out of the scope of this specification.

Step 2: Redirecting to the Service Provider

In step 2, the identity provider's federation termination service URL responds and redirects the user agent to the federation termination service at the service provider.

The redirection MUST adhere to the following rules:

- The Location HTTP header MUST be set to the service provider's federation termination service URL.
- The service provider's federation termination service URL MUST specify `https` as the URL scheme; if another scheme is specified, the identity provider MUST NOT redirect to the service provider.

- The Location HTTP header MUST include a `<query>` component containing the `<lib:FederationTerminationNotification>` protocol message as defined in [LibertyProtSchema] with formatting as specified in 3.1.2.

The HTTP response MUST take the following form:

```
<HTTP-Version> 302 <Reason Phrase>
<other headers>
Location : https://<Service Provider Federation Termination service URL>?<query>
<other HTTP 1.0 or 1.1 components>
```

where

`<Service Provider Federation Termination service URL>`
: This element provides the host name, port number, and path components of the federation termination service URL at the service provider.

`<query>= …<URL-encoded FederationTerminationNotification>…`
: The `<query>` component MUST contain a single terminate federation request.

Step 3: Accessing the Service Provider Federation Termination Service

In step 3, the user agent accesses the service provider's federation termination service URL with the `<lib:FederationTerminationNotification>` information attached to the URL fulfilling the redirect request.

Step 4: Processing the Notification

In step 4, the service provider MUST process the `<lib:FederationTerminationNotification>` according to the rules defined in [LibertyProtSchema].

The service provider MAY remove any locally stored references to the name identifier it received from the identity provider in the `<lib:FederationTerminationNotification>`.

Step 5: Redirecting to the Identity Provider Return URL

In step 5, the service provider's federation termination service responds and redirects the user agent back to identity provider using a return URL location specified in the `FederationTerminationServiceReturnURL` metadata element. If the URL-encoded `<lib:FederationTerminationNotification>` message received in step 3 contains a parameter named `RelayState`, then the service provider MUST include a `<query>` component containing the same `RelayState` parameter and its value in its response to the identity provider.

No success or failure message should be conveyed in this HTTP redirect. The sole purpose of this redirect is to return the user agent to the identity provider where the federation termination process began.

The HTTP response MUST take the following form:

```
<HTTP-Version> 302 <Reason Phrase>
<other headers>
Location : https://<Identity Provider Service Return URL >?<query>
<other HTTP 1.0 or 1.1 components>
```

where

`<Identity Provider Service Return URL>`
: This element provides the host name, port number, and path components of the return URL at the identity provider.

`<query>= …RelayState=<…>`
: The `<query>` component MUST contain the identical `RelayState` parameter and its value that was received in the URL-encoded federation termination message obtained in step 3. If no `RelayState` parameter was provided in the step 3 message, then a `RelayState` parameter MUST NOT be specified in the `<query>` component.

Step 6: Accessing the Identity Provider Return URL

In step 6, the user agent accesses the identity provider's return URL location fulfilling the redirect request.

Step 7: Confirmation

In step 7, the user agent is sent an HTTP response that confirms the requested action of identity federation termination with the specific service provider.

3.4.1.2 SOAP/HTTP-Based Profile

The SOAP/HTTP-based profile relies on using asynchronous SOAP over HTTP to communicate federation termination notification messages from the identity provider to the service provider. See Figure 9.

The following URI-based identifier MUST be used when referencing this specific profile:

URI: `http://projectliberty.org/profiles/fedterm-idp-soap`

This URI identifier MUST be specified in the service provider metadata element `FederationTerminationNotificationProtocolProfile` when the service provider intends to indicate to the identity provider a preference for receiving federation termination notifications via SOAP over HTTP.

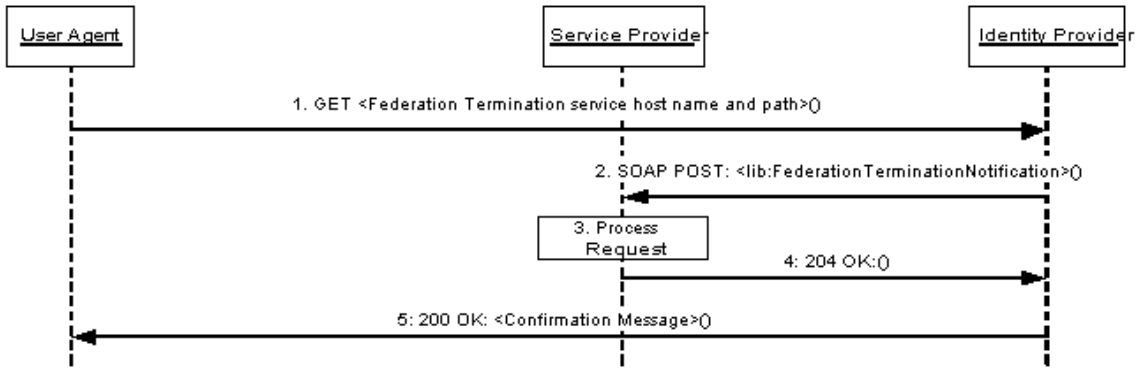


Figure 9: SOAP/HTTP-based profile for federation termination

This profile description assumes the following preconditions:

- The Principal's identity at the service provider is federated with his/her identity at the identity provider.
- The Principal has requested to the identity provider that the federation be terminated.
- The Principal has authenticated with the identity provider.

Step 1: Accessing the Federation Termination Service

In step 1, the user agent accesses the identity federation termination service URL at the identity provider specifying the service provider for with which identity federation termination should occur. How the service provider is specified is implementation-dependent and, as such, is out of the scope of this specification.

Step 2: Notification of Federation Termination

In step 2, the identity provider sends an asynchronous SOAP over HTTP notification message to the service provider's SOAP endpoint. The SOAP message MUST contain exactly one `<lib:FederationTerminationNotification>` element in the SOAP body and adhere to the construction rules defined in [LibertyProtSchema].

If a SOAP fault occurs, the identity provider SHOULD employ best effort to resolve the fault condition and resend the federation termination notification message to the service provider.

Step 3: Processing the Notification

In step 3, the service provider MUST process the `<lib:FederationTerminationNotification>` according to the rules defined in [LibertyProtSchema].

The service provider MAY remove any locally stored references to the name identifier it received from the identity provider in the `<lib:FederationTerminationNotification>`.

Step 4: Responding to the Notification

In step 4, the service provider MUST respond to the `<lib:FederationTerminationNotification>` with a HTTP 204 OK response.

Step 5: Confirmation

In step 5, the user agent is sent an HTTP response that confirms the requested action of identity federation termination with the specific service provider.

3.4.2 Federation Termination Notification Initiated at Service Provider

The profiles in 3.4.2.1 and 3.4.2.2 are specific to identity federation termination notification when initiated by a Principal at the service provider. Effectively, when using this profile, the service provider is stating to the identity provider that the Principal has requested that the identity provider no longer provide the Principal's identity information to the service provider and that service provider will no longer ask the identity provider to do anything on the behalf of the Principal.

It is RECOMMENDED that the service provider, after initiating or receiving a federation termination notification, invalidate the local session for the Principal that was authenticated at the

identity provider with which federation has been terminated. If the Principal was locally authenticated at the service provider, the service provider MAY continue to maintain a local session for the Principal. If the Principal wants to engage in a single sign-on session with identity provider again, the service provider MUST first federate with identity provider the given Principal.

3.4.2.1 HTTP-Redirect-Based Profile

The HTTP-redirect-based profile relies on the use of a HTTP 302 redirect to communicate a federation termination notification message from the service provider to the identity provider. For a discussion of the interactions and processing steps, refer to 3.4.1.1. When reviewing that profile, interchange all references to service provider and identity provider in the interaction diagram and processing steps.

The following URI-based identifier MUST be used when referencing this specific profile:

URI: `http://projectliberty.org/profiles/fedterm-sp-http`

This URI identifier is really only meant for service provider consumption and as such is not needed in any provider metadata.

3.4.2.2 SOAP/HTTP-Based Profile

The SOAP/HTTP-based profile relies on using asynchronous SOAP over HTTP to communicate federation termination notification messages from the service provider to the identity provider. For a discussion of the interactions and processing steps, refer to 3.4.1.2. When reviewing that profile, interchange all references to service provider and identity provider in the interaction diagram and processing steps.

The following URI-based identifier MUST be used when referencing this specific profile:

URI: `http://projectliberty.org/profiles/fedterm-sp-soap`

This URI identifier is really only meant for service provider consumption and as such is not needed in any provider metadata.

3.5 Single Logout Profiles

The single logout profiles synchronize session logout functionality across all sessions that were authenticated by a particular identity provider. The single logout can be initiated at either the identity provider or the service provider. In either case, the identity provider will then communicate a logout request to each service provider with which it has established a session for the Principal. The negotiation of which single logout profile the identity provider uses to communicate with each service provider is based upon the `SingleLogoutProtocolProfile` provider metadata element defined in [LibertyProtSchema].

The available profiles are defined in 3.5.1 and 3.5.2, depending on whether the single logout is initiated at the identity provider or service provider:

- **Single Logout Initiated at Identity Provider**
  - **HTTP-Based:** Relies on using either HTTP 302 redirects or HTTP GET requests to communicate logout requests from an identity provider to the service providers.
  - **SOAP/HTTP-Based:** Relies on SOAP over HTTP messaging to communicate logout requests from an identity provider to the service providers.

- **Single Logout Initiated at Service Provider**
  - **HTTP-Redirect-Based:** Relies on a HTTP 302 redirect to communicate a logout request with the identity provider.
  - **SOAP/HTTP-Based:** Relies on SOAP over HTTP messaging to communicate a logout request from a service provider to an identity provider.

The single logout profiles make use of the following metadata elements, as defined in [LibertyProtSchema].

- `SingleLogoutServiceURL` — The URL at the service provider or identity provider to which single logout requests are sent. It is described in these profiles as "single logout service URL."
- `SingleLogoutServiceReturnURL` — The URL used by the service provider when redirecting the user agent to the identity provider at the end of the single logout profile process.
- `SingleLogoutProtocolProfile` — Used by the identity provider to determine which single logout request profile MUST be used when communicating with the service provider.
- `SOAPEndpoint` — The SOAP endpoint location at the service provider or identity provider to which Liberty SOAP messages are sent.

3.5.1 Single Logout Initiated at Identity Provider

The profiles in 3.5.1.1 through 3.5.1.2 are specific to a single logout when initiated by a user agent at the identity provider.

3.5.1.1 HTTP-Based Profile

The HTTP-based profile defines two possible implementations that an identity provider may use. The first implementation relies on using HTTP 302 redirects, while the second uses HTTP GET requests. The choice of implementation is entirely dependent upon the type of user experience the identity provider provides.

The following URI-based identifier MUST be used when referencing either implementation for this specific profile:

URI: `http://projectliberty.org/profiles/slo-idp-http`

This URI identifier MUST be specified in the service provider metadata element `SingleLogOutProtocolProfile` when the service provider intends to indicate to the identity provider a preference for receiving logout requests via either a HTTP redirect or a HTTP GET.

3.5.1.1.1 HTTP-Redirect Implementation

The HTTP-Redirect implementation uses HTTP 302 redirects to communicate a logout request to each service provider for which the identity provider has provided authentication assertions during the Principal's current session if the service provider indicated a preference to receive logout requests via the HTTP based profile. See Figure 10.

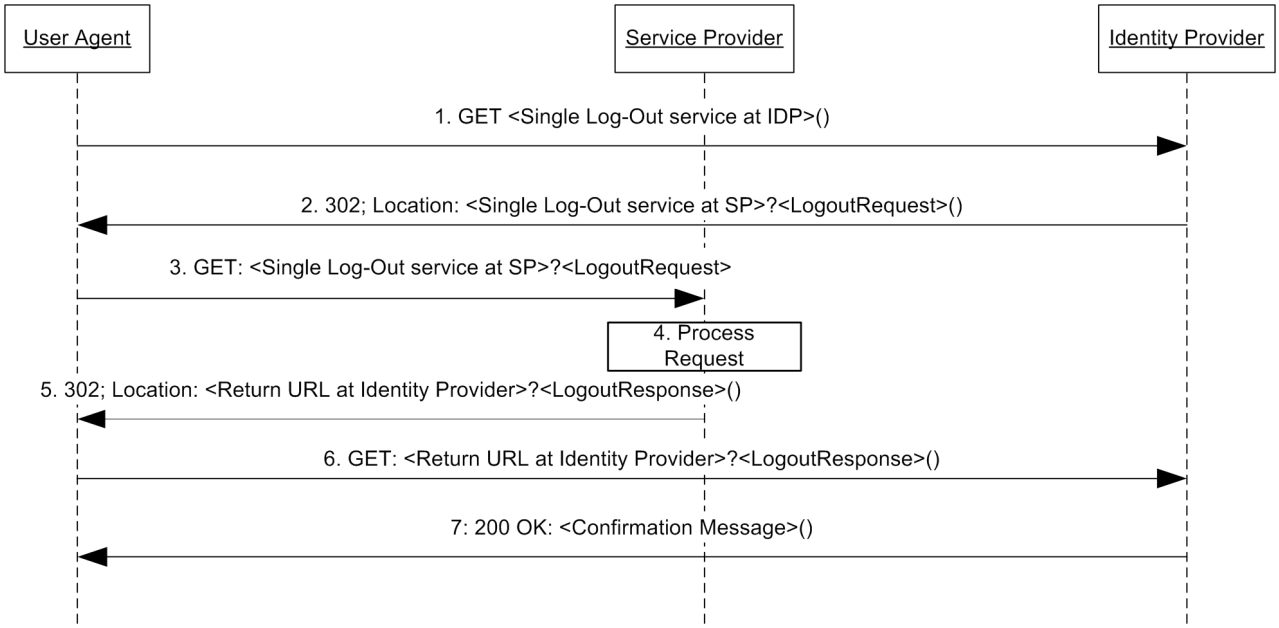


Figure 10: HTTP-Redirect implementation for single logout initiated at identity provider

Note: Steps 2 through 6 may be an iterative process for requesting logouts by each service provider that has been issued authentication assertions during the Principal's current session and has indicated a preference to receive logout requests via the HTTP based profile.

Note: [RFC 2616] indicates a client should detect infinite redirection loops because such loops generate network traffic for each redirection. This requirement was introduced because previous versions of the specification recommended a maximum of five redirections. Content developers should be aware that some clients might implement such a fixed limitation.

Step 1: Accessing the Single Logout Service at the Identity Provider

In step 1, the user agent accesses the single logout service URL at the identity provider indicating that all service providers for which this identity provider has provided authentication assertions during the Principal's current session must be notified of session termination.

Step 2: Redirecting to the Single Logout Service at the Service Provider

In step 2, the identity provider's single logout service responds and redirects the user agent to the single logout service URL at each service provider for which the identity provider has provided an authentication assertion during the Principal's current session with the identity provider.

The redirections MUST adhere to the following rules:

- The Location HTTP header MUST be set to the service provider's single logout service URL.

- The service provider's single logout service URL MUST specify `https` as the URL scheme; if another scheme is specified, the identity provider MUST NOT redirect to the service provider.
- The Location HTTP header MUST include a `<query>` component containing the `<lib:LogoutRequest>` protocol message as defined in [LibertyProtSchema] with formatting as specified in 3.1.2.

The HTTP response MUST take the following form:

```
<HTTP-Version> 302 <Reason Phrase>
<other headers>
Location : https://<Service Provider Single Log-Out service URL>?<query>
<other HTTP 1.0 or 1.1 components>
```

where

`<Service Provider Single Log-Out service URL>`
: This element provides the host name, port number, and path components of the single logout service URL at the service provider.

`<query>= …<URL-encoded LogoutRequest>…`
: The `<query>` MUST contain a single logout request.

Step 3: Accessing the Service Provider Single Logout Service

In step 3, the user agent accesses the service provider's single logout service URL with the `<lib:LogoutRequest>` information attached to the URL fulfilling the redirect request.

Step 4: Processing the Request

In step 4, the service provider MUST process the `<lib:LogoutRequest>` according to the rules defined in [LibertyProtSchema].

The service provider MUST invalidate the session(s) of the Principal referred to in the name identifier it received from the identity provider in the `<lib:LogoutRequest>`.

Step 5: Redirecting to the Identity Provider Return URL

In step 5, the service provider's single logout service responds and redirects the user agent back to the identity provider using the return URL location obtained from the `SingleLogoutServiceReturnURL` metadata element. If the URL-encoded `<lib:LogoutRequest>` message received in step 3 contains a parameter named `RelayState`, then the service provider MUST include a `<query>` component containing the same `RelayState` parameter and its value in its response to the identity provider.

The purpose of this redirect is to return the user agent to the identity provider so that the single logout process may continue in the same fashion with other service providers.

The HTTP response MUST take the following form:

```
<HTTP-Version> 302 <Reason Phrase>
<other headers>
Location : https://<Identity Provider Service Return URL>?<query>
<other HTTP 1.0 or 1.1 components>
```

where

`<Identity Provider Service Return URL>`
: This element provides the host name, port number, and path components of the return URL at the identity provider.

`<query>= …<URL-encoded LogoutResponse>`
: The `<query>` component MUST contain a single logout response. The `<URL-encoded LogoutResponse>` MUST contain the identical `RelayState` parameter and its value that was received in the URL-encoded logout request message obtained in step 3. If no `RelayState` parameter was provided in the step 3 message, then a `RelayState` parameter MUST NOT be specified in the `<URL-encoded LogoutResponse>`.

Step 6: Accessing the Identity Provider Return URL

In step 6, the user agent accesses the identity provider's return URL location fulfilling the redirect request.

Step 7: Confirmation

In step 7, the user agent is sent an HTTP response that confirms the requested action of a single logout has been completed.

3.5.1.1.2 HTTP-GET Implementation

The HTTP-GET implementation uses HTTP GET requests to communicate logout requests to each service provider for which the identity provider has provided authentication during the Principal's current session if the service provider indicated a preference to receive logout requests via the HTTP based profile. See Figure 11.

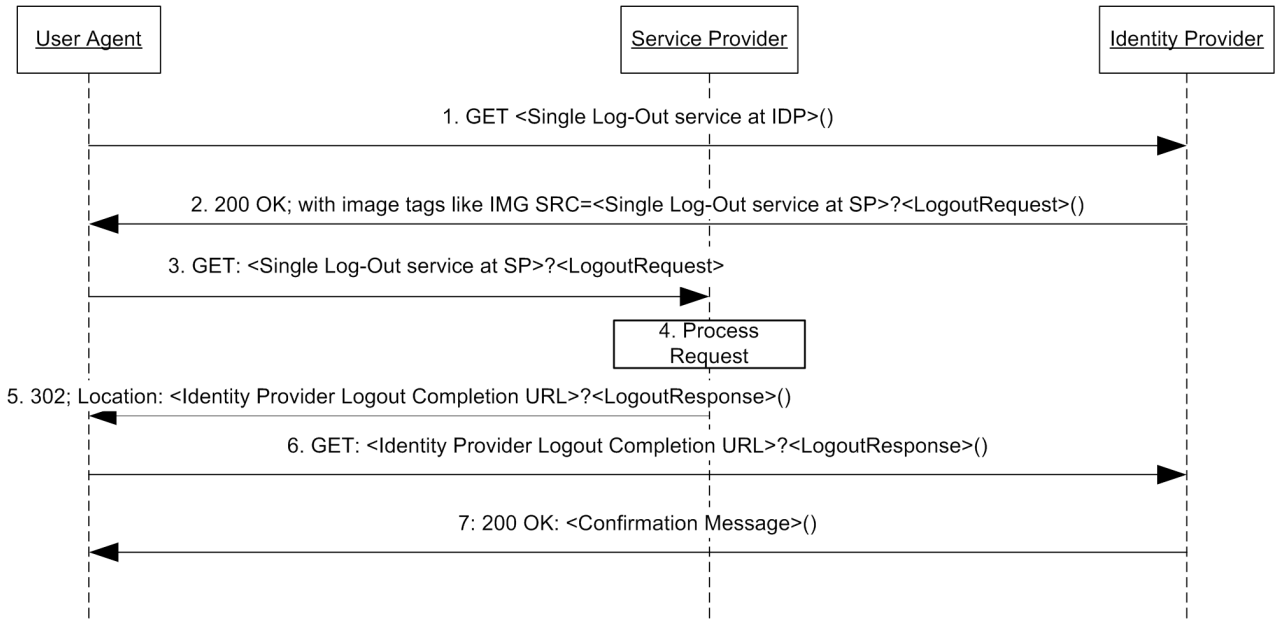


Figure 11: HTTP-GET implementation for single logout initiated at identity provider

Note: Steps 3 through 7 may be an iterative process for requesting logout of each service provider that has been issued authentication assertions during the

Principal's current session and has indicated a preference to receive logout requests via the HTTP based profile.

Step 1: Accessing the Single Logout Service at the Identity Provider

In step 1, the user agent accesses the single logout service URL at the identity provider indicating that all service providers for which this identity provider has provided authentication assertions during the Principal's current session must be notified of session termination and requested to logout the Principal.

Step 2: HTML Page Returned to User Agent with Image Tags

In step 2, the identity provider's single logout service responds with an HTML page that includes image tags referencing the logout service URL for each of the service providers for which the identity provider has provided an authentication assertion during the Principal's current session. The list of image tags MUST be sent in a standard HTTP 200 response to the user agent.

The image tag loads on the HTML page MUST adhere to the following rules:

- The `SRC` attribute MUST be set to the specific service provider's single logout service URL.
- The service provider's single logout service URL MUST specify `https` as the URL scheme.
- The service provider's single logout service URL MUST include a `<query>` component containing the `<lib:LogoutRequest>` protocol message as defined in [LibertyProtSchema] with formatting as specified in 3.1.2.

Step 3: Accessing the Service Provider Single Logout Service

In step 3, the user agent, as a result of each image load, accesses the service provider's single logout service URL with `<lib:LogoutRequest>` information attached to the URL. This step may occur multiple times if the HTTP response includes multiple image tag statements (one for each service provider that has been issued authentication assertions during the Principal's current session).

Step 4: Processing the Request

In step 4, the service provider MUST process the `<lib:LogoutRequest>` according to the rules defined in [LibertyProtSchema].

The service provider MUST invalidate the session of the Principal referred to in the name identifier it received from the identity provider in the `<lib:LogoutRequest>`.

Step 5: Redirecting to the Identity Provider Logout Completion URL

In step 5, the service provider's single logout service responds and redirects the image load back to the identity provider's logout completion URL. This location will typically point to an image that will be loaded by the user agent to indicate that the logout is complete (for example, a checkmark).

The logout completion URL is obtained from the `SingleLogoutServiceReturnURL` metadata element.

The HTTP response MUST take the following form:

```
<HTTP-Version> 302 <Reason Phrase>
<other headers>
Location : https://<Identity Provider Logout Completion URL>?<query>
<other HTTP 1.0 or 1.1 components>
```

where

`<Identity Provider Logout Completion URL>`
: This element provides the host name, port number, and path components of the identity provider logout completion URL at the identity provider.

`<query>=…<URL-encoded LogoutResponse>`
: The `<query>` component MUST contain a single logout response. The `<URL-encoded LogoutResponse>` component MUST contain the identical `RelayState` parameter and its value that was received in the URL-encoded logout request message obtained in step 3. If no `RelayState` parameter was provided in step 3 then a `RelayState` message NUST NOT be specified in the `<URL-encoded LogoutResponse>`.

Step 6: Accessing the Identity Provider Logout Completion URL

In step 6, the user agent accesses the identity provider's logout completion URL fulfilling the redirect request.

Step 7: Confirmation

In step 7, the user agent is sent an HTTP response that confirms the requested action of a single logout has been completed.

> Note: One method for seamlessly returning the user agent back to the identity provider is for the HTML page generated in step 2 to include a script that runs when the page is completely loaded (all logouts completed) that will initiate the redirect to the identity provider.

3.5.1.2 SOAP/HTTP-Based Profile

The SOAP/HTTP-based profile uses SOAP over HTTP messaging to communicate a logout request to each service provider for which the identity provider has provided authentication assertions during the Principal's current session if the service provider indicated a preference to receive logout request via the SOAP/HTTP-based profile. See Figure 12.

The following URI-based identifier MUST be used when referencing this specific profile:

URI: `http://projectliberty.org/profiles/slo-idp-soap`

This URI identifier MUST be specified in the service provider metadata element `SingleLogOutProtocolProfile` when the service provider intends to indicate to the identity provider a preference for receiving logout requests via SOAP over HTTP.

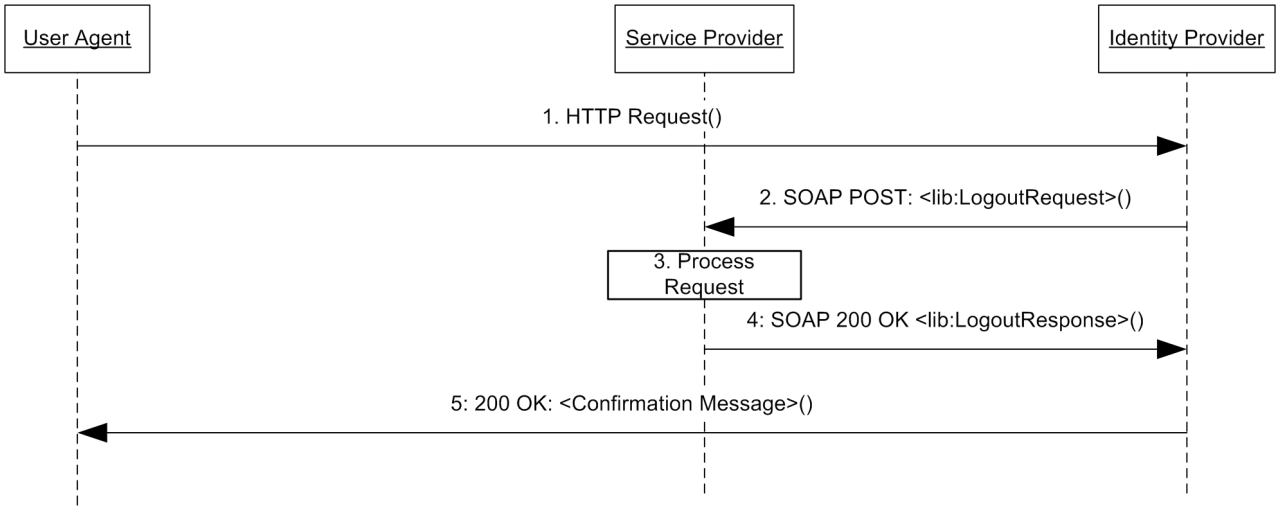


Figure 12: SOAP/HTTP-based profile for single logout initiated at identity provider

Note: Steps 2 through 4 may be an iterative process for each service provider that has been issued authentication assertions during the Principal's current session and has indicated a preference to receive logout requests via the SOAP/HTTP message profile.

Step 1: Accessing the Single Logout Service

In step 1, the user agent accesses the single logout service URL at the identity provider via an HTTP request.

Step 2: Logout Request

In step 2, the identity provider sends a SOAP over HTTP request to the SOAP endpoint of each service provider for which it provided authentication assertions during the Principal's current session. The SOAP message MUST contain exactly one `<lib:LogoutRequest>` element in the SOAP body and adhere to the construction rules defined in [LibertyProtSchema].

If a SOAP fault occurs, the identity provider SHOULD employ best efforts to resolve the fault condition and resend the single logout request to the service provider.

Step 3: Processing the Logout Request

In step 3, the service provider MUST process the `<lib:LogoutRequest>` according to the rules defined in [LibertyProtSchema].

The service provider MUST invalidate the session for the Principal specified by the name identifier provided by the identity provider in the `<lib:LogoutRequest>.`

Step 4: Responding to the Request

In step 4, the service provider MUST respond to the `<lib:LogoutRequest>` with a `SOAP 200 OK <lib:LogoutResponse>` message.

1850 **Step 5: Confirmation**

1851 In step 5, the user agent is sent an HTTP response that confirms the requested action of single
1852 logout has completed.

1853 ### 3.5.2 Single Logout Initiated at Service Provider

1854 The profiles in 3.5.2.1 and 3.5.2.2 are specific to the Principal's initiation of the single logout
1855 request process at the service provider.

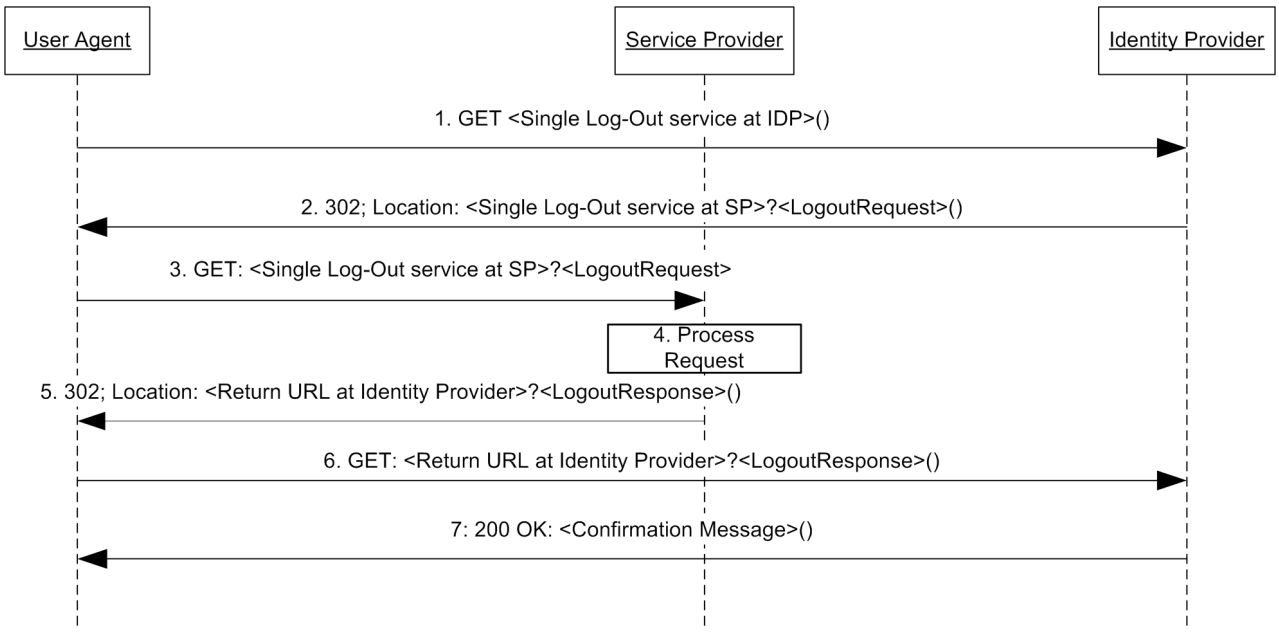
1856 #### 3.5.2.1 HTTP-Redirect-Based Profile

1857 The HTTP-redirect-based profile relies on using a HTTP 302 redirect to communicate a logout
1858 request with the identity provider. The identity provider will then communicate a logout request to
1859 each service provider with which it has established a session for the Principal using the service
1860 provider's preferred profile for logout request from the identity provider (see 3.5.1). See Figure 13.

1861 The following URI-based identifier MUST be used when referencing this specific profile:

1862 URI: `http://projectliberty.org/profiles/slo-sp-http`

1863 This URI identifier is intended for service provider consumption and is not needed in provider
1864 metadata.



1865

1866 **Figure 13: HTTP-redirect-based profile for single logout initiated at service provider**

1867 Note: Step 4 may involve an iterative process by the identity provider to
1868 implement the preferred profile for logout requests for each service provider that
1869 has been issued authentication assertions during the Principal's current session.

Step 1: Accessing the Single Logout Service at the Service Provider

In step 1, the user agent accesses the single logout service URL at the service provider indicating that session logout is desired at the associated identity provider and all service providers for which this identity provider has provided authentication assertions during the Principal's current session. If a current session exists for the Principal at the service provider, it is RECOMMENDED that the service provider terminate that session prior to step 2.

Step 2: Redirecting to the Single Logout Service at the Identity Provider

In step 2, the service provider's single logout service responds and redirects the user agent to the single logout service URL at the identity provider.

The redirection MUST adhere to the following rules:

- The Location HTTP header MUST be set to the identity provider's single logout service URL.
- The identity provider's single logout service URL MUST specify `https` as the URL scheme; if another scheme is specified, the service provider MUST NOT redirect to the identity provider.
- The Location HTTP header MUST include a `<query>` component containing the `<lib:LogoutRequest>` protocol message as defined in [LibertyProtSchema] with formatting as specified in 3.1.2.

The HTTP response MUST take the following form:

```
<HTTP-Version> 302 <Reason Phrase>
<other headers>
Location : https://<Identity Provider single log-out service URL>?<query>
<other HTTP 1.0 or 1.1 components>
```

where

`<Identity Provider single log-out service URL>`
: This element provides the host name, port number, and path components of the single logout service URL at the identity provider.

`<query>= …<URL-encoded LogoutRequest>…`
: The `<query>` MUST contain a single logout request.

Step 3: Accessing the Identity Provider Single Logout Service

In step 3, the user agent accesses the identity provider's single logout service URL with the `<lib:LogoutRequest>` information attached to the URL fulfilling the redirect request.

Step 4: Processing the Request

In step 4, the identity provider MUST process the `<lib:LogoutRequest>` according to the rules defined in [LibertyProtSchema].

Each service provider for which the identity provider has provided authentication assertions during the Principal's current session MUST be notified via the service provider's preferred profile for logout request from the identity provider (see 3.5.1).

The identity provider's current session with the Principal MUST be terminated, and no more authentication assertions for the Principal are to be given to service providers.

Step 5: Redirecting to the Service Provider Return URL

In step 5, the identity provider's single logout service responds and redirects the user agent back to service provider using the return URL location obtained from the `SingleLogoutServiceReturnURL` metadata element. If the URL-encoded `<lib:LogoutRequest>` message received in step 3 contains a parameter named `RelayState`, then the identity provider MUST include a `<query>` component containing the same `RelayState` parameter and its value in its response to the service provider.

The purpose of this redirect is to return the user agent to the service provider.

The HTTP response MUST take the following form:

```
<HTTP-Version> 302 <Reason Phrase>
<other headers>
Location : https://<Service Provider Return Service URL>?<query>
<other HTTP 1.0 or 1.1 components>
```

where

`<Service Provider Service Return URL>`
: This element provides the host name, port number, and path components of the return URL location at the service provider.

`<query>= …<URL-encoded LogoutResponse>`
: The `<query>` component MUST contain a single logout response. The `<URL-encoded LogoutResponse>` component MUST contain the identical `RelayState` parameter and its value that was received in the URL-encoded logout request message obtained in step 3. If no `RelayState` parameter was provided in the step 3 message, then a `RelayState` parameter MUST NOT be specified in the `<URL-encoded LogoutResponse>`.

Step 6: Accessing the Service Provider Return URL

In step 6, the user agent accesses the service provider's return URL location fulfilling the redirect request.

Step 7: Confirmation

In step 7, the user agent is sent an HTTP response that confirms the requested action of a single logout has been completed.

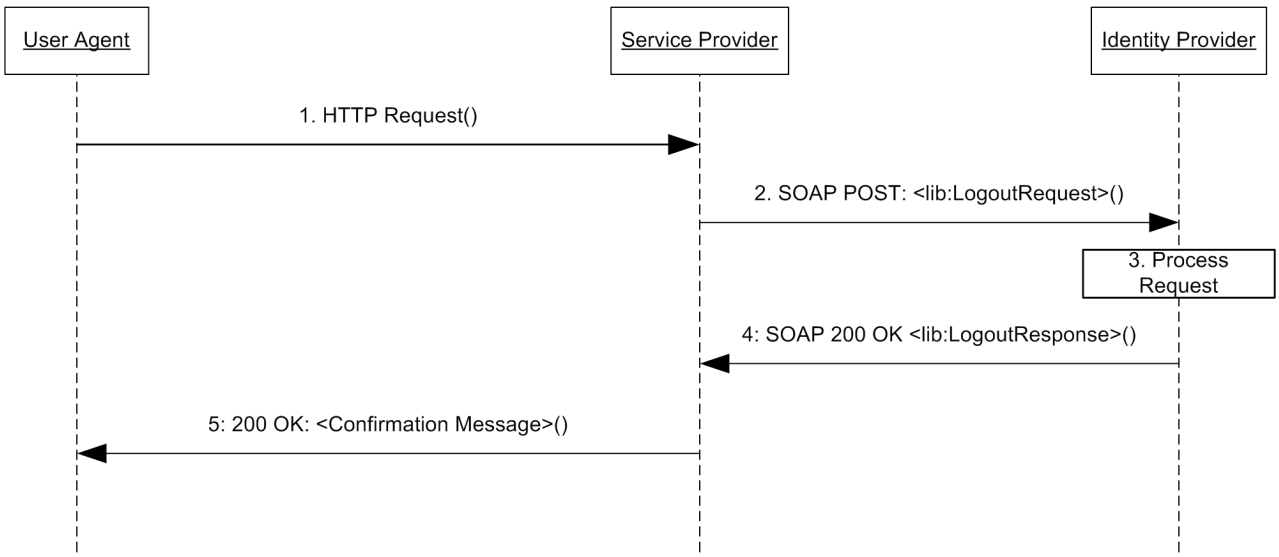
3.5.2.2 SOAP/HTTP-Based Profile

The SOAP/HTTP-based profile relies on using SOAP over HTTP messages to communicate a logout request to the identity provider. The identity provider will then communicate a logout request to each service provider it has established a session with for the Principal via the service provider's preferred profile for logout requests from the identity provider (see 3.5.1). See Figure 14.

The following URI-based identifier MUST be used when referencing this specific profile:

URI: `http://projectliberty.org/profiles/slo-sp-soap`

1947 This URI identifier is intended for service provider consumption and is not needed in provider
1948 metadata.



1949

1950 **Figure 14: SOAP/HTTP-based profile for single logout initiated at service provider**

1951 Note: Step 3 may involve an iterative process by the identity provider to
1952 implement the preferred profile for logout requests for each service provider that
1953 has been issued authentication assertions during the Principal's current session.

1954 ### Step 1: Accessing Single Logout Service

1955 In step 1, the user agent accesses the single logout service URL at the service provider via an
1956 HTTP request.

1957 ### Step 2: Logout Request

1958 In step 2, the service provider sends a SOAP over HTTP request to the identity provider's SOAP
1959 endpoint. The SOAP message MUST contain exactly one `<lib:LogoutRequest>` element in the
1960 SOAP body and adhere to the construction rules as defined in [LibertyProtSchema].

1961 If a SOAP fault occurs, the service provider SHOULD employ best efforts to resolve the fault
1962 condition and resend the single logout request to the identity provider.

1963 ### Step 3: Processing the Logout Request

1964 In step 3, the identity provider MUST process the `<lib:LogoutRequest>` according to the rules
1965 defined in [LibertyProtSchema].

1966 Each service provider for which the identity provider has provided authentication assertions during
1967 the Principal's current session MUST be requested to logout the Principal via the service
1968 provider's preferred profile for logout requests from the identity provider. If the identity provider
1969 determines that one or more of service providers to which it has provided assertions regarding this
1970 Principal do not support the SOAP profiles for the single logout, the identity provider MUST
1971 return a `<lib:LogoutResponse>` containing a status code of `<lib:UnsupportedProfile>`.

The service provider MUST then re-submit its LogoutRequest via the HTTP profile described above.

The identity provider's current session with the Principal MUST be terminated, and no more authentication assertions for the Principal are to be given to service providers.

Step 4: Responding to the Logout Request

In step 4, the identity provider MUST respond to the `<lib:LogoutRequest>` with a `SOAP 200 OK <lib:LogoutResponse>` message.

Step 5: Confirmation

In step 5, the user agent is sent an HTTP response that confirms the requested action of single logout was completed.

3.6 Identity Provider Introduction

This section defines the profiles by which a service provider discovers which identity providers a Principal is using. In identity federation networks having more than one identity provider, service providers need a means to discover which identity providers a Principal uses. The introduction profile relies on a cookie that is written in a domain that is common between identity providers and service providers in an identity federation network. The domain that the identity federation network predetermines for a deployment is known as the *common domain* in this specification, and the cookie containing the list of identity providers is known as the *common domain cookie*.

Implementation of this profile is OPTIONAL. Whether identity providers and service providers implement this profile is a policy and deployment issue outside the scope of this specification. Also, which entities host web servers in the common domain is a deployment issue and is outside the scope of this specification.

3.6.1 Common Domain Cookie

The name of the cookie MUST be `_liberty_idp`. The format of the cookie content MUST be a list of base64-encoded (see [RFC2045]) identity provider succinct IDs separated by a single white space character. The identity provider IDs MUST adhere to the creation rules as defined in 3.2.2.2. The identity provider ID is a metadata element, as described in 0 and defined in [LibertyProtSchema].

The common domain cookie writing service SHOULD append the identity provider ID to the list. If the identity provider ID is already present in the list, it MAY remove and append it when authentication of the Principal occurs. The intent is that the most recently established identity provider session is the last one in the list.

The cookie MUST be set with no `Path` prefix or a `Path` prefix of "`/`". The `Domain` MUST be set to "`.[common-domain]`" where `[common-domain]` is the *common domain* established within the identity federation network for use with the introduction protocol. The cookie MUST be marked as `Secure`.

The cookies MAY be either session or persistent (see [RFC2109]), the implementation of which is a policy and deployment issue of the identity federation network.

3.6.2 Setting the Common Domain Cookie

After the identity provider authenticates a Principal, it MAY set the common domain cookie. The means by which the identity provider sets the cookie are implementation-specific so long as the cookie is successfully set with the parameters given above. One possible implementation strategy follows and should be considered non-normative. The identity provider may:

- Have previously established a DNS and IP alias for itself in the common domain
- Redirect the user agent to itself using the DNS alias using a URL specifying "https" as the URL scheme. The structure of the URL is private to the implementation and may include session information needed to identify the user-agent.
- Set the cookie on the redirected user agent using the parameters specified above
- Redirect the user agent back to itself, or, if appropriate, to the service provider.

3.6.3 Obtaining the Common Domain Cookie

When a service provider needs to discover which identity providers the Principal uses, it invokes a protocol exchange designed to present the common domain cookie to the service provider after it is read by an HTTP server in the common domain.

If the HTTP server in the common domain is operated by the service provider, the service provider MAY redirect the user agent to an identity provider's intersite transfer service for an optimized single sign-on process.

The specific means by which the service provider reads the cookie are implementation-specific so long as it is able to cause the user agent to present cookies that have been set with the parameters given in section 3.6.1. One possible implementation strategy is described as follows and should be considered non-normative. Additionally, it may be sub-optimal for some applications.

- Have previously established a DNS and IP alias for itself in the common domain
- Redirect the user agent to itself using the DNS alias using a URL specifying "`https`" as the URL scheme. The structure of the URL is private to the implementation and should encode session state information needed to identify the user-agent, since it will not present any session cookies that were set using the service provider's original DNS name. This redirection could be performed via an HTTP 302 response or via an image tag in an HTML page sent to the user agent.
- Read the cookie sent by the user agent, if any. Using the session state information encoded in the request URL, store the information retrieved from the cookie.
- Use the session state information to determine what resource the user agent was attempting to access when it was redirected, if necessary. Send the user agent an HTTP 302 response redirecting it to the original resource.

4 Security Considerations

4.1 Introduction

This section describes security considerations associated with Liberty protocols for identity federation, single sign-on, federation termination, and single logout.

Liberty protocols, schemas, bindings, and profiles inherit and use extensivelythe SAML protocols. Therefore, the security considerations published along with the SAML specification have direct relevance (see [SAMLCore], [SAMLBind], and [SAMLSec]). Throughout this section if, for any reason, a specific consideration or countermeasure does not apply or differs, notice of this fact is made; and a description of alternatives is supplied, where possible.

4.2 General Requirements

4.2.1 Security of SSL and TLS

SSL and TLS utilize a suite of possible cipher suites. The security of the SSL or TLS session depends on the chosen cipher suite. An entity (that is, a user agent, service provider, or identity provider) that terminates an SSL or TLS connection needs to offer (or accept) suitable cipher suites during the handshake. The following list of TLS 1.0 cipher suites (or their SSL 3.0 equivalent) is recommended.

- `TLS_RSA_WITH_RC4_128_SHA`
- `TLS_RSA_WITH_3DES_EDE_CBC_SHA`
- `TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA`

The above list is not exhaustive. The recommended cipher suites are among the most commonly used. Note: New cipher suites are added as they are standardized and should be considered for inclusion if they have sufficiently strong security properties. For example, it is anticipated that the AES-based cipher suites being standardized in the IETF will be widely adopted and deployed.

4.2.2 Security Implementation

The suitable implementation of security protocols is necessary to maintain the security of a system, including

- Secure random or pseudo-random number generation
- Secure storage

4.3 Classification of Threats

4.3.1 Threat Model

For an analysis of threat classifications, an Internet threat model has been used. In other words, the threat model assumes that intermediary and end-systems participating in Liberty protocol exchanges have not been compromised. However, where possible, the consequences and containment properties of a compromised system entity are described and countermeasures are suggested to bolster the security posture so that the exposure from a security breach is minimized.

Given the nature of the Internet, the assumption is made that deployment is across the global Internet and, therefore, crosses multiple administrative boundaries. Thus, an assumption is also made that the adversary has the capacity to engage in both passive and active attacks (see 4.3.3).

4.3.2 Rogue and Spurious Entities

Attackers may be classified based on their capabilities and the roles that they play in launching attacks on a Liberty system as follows:

- **Rogue Entities:** Entities that misuse their privileges. The rogue actors may be Principals, user agents, service providers, or identity providers. A rogue Principal is a legitimate participant who attempts to escalate its privileges or masquerade as another system Principal. A rogue user agent may, for instance, misuse the relationships between its associated Principals and an identity provider to launch certain attacks. Similarly, a rogue service provider may be able to exploit the relationship that it has either with a Principal or with an identity provider to launch certain attacks.
- **Spurious Entities:** Entities that masquerade as a legitimate entity or are completely unknown to the system. The spurious actors include Principals, user agents (i.e., user agents without associated legitimate Liberty Principals), service providers, or identity providers. A spurious service provider may, for instance, pretend to be a service provider that has a legitimate relationship with an identity provider. Similarly, a spurious Principal may be one that pretends to be a legitimate Principal that has a relationship with either a service provider or an identity provider.

4.3.3 Active and Passive Attackers

Both rogue and spurious entities may launch active or passive attacks on the system. In a passive attack the attacker does not inject traffic or modify traffic in any way. Such an attacker usually passively monitors the traffic flow, and the information that is obtained in that flow may be used at a later time. An active attacker, on the other hand, is capable of modifying existing traffic as well as injecting new traffic into the system.

4.3.4 Scenarios

The following scenarios describe possible attacks:

- **Collusion: The secret cooperation between two or more Liberty entities to launch an attack, for example,**
  - Collusion between Principal and service provider
  - Collusion between Principal and identity provider
  - Collusion between identity provider and service provider
  - Collusion among two or more Principals
  - Collusion between two or more service providers
  - Collusion between two or more identity providers
- **Denial-of-Service Attacks:** The prevention of authorized access to a system resource or the delaying of system operations and functions.
- **Man-in-the-Middle Attacks:** A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association.

- **Replay Attacks:** An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack.
- **Session Hijacking:** A form of active wiretapping in which the attacker seizes control of a previously established communication association.

4.4 Threat Scenarios and Countermeasures

In this section, threats that may apply to all the Liberty profiles are considered first. Threats that are specific to individual profiles are then considered. In each discussion the threat is described as well as the countermeasures that exist in the profile or the additional countermeasures that may be implemented to mitigate the threat.

4.4.1 Common Threats for All Profiles

Threat: Request messages sent in cleartext

Description: Most profile protocol exchanges do not mandate that all exchanges commence over a secure communication channel. This lack of transport security potentially exposes requests and responses to both passive and active attacks.

One obvious manifestation is when the initial contact is not over a secure transport and the Liberty profile begins to exchange messages by carrying the request message back to the user agent in the location header of a redirect.

Another such manifestation could be a request or response message which carries a URI that may be resolved on a subsequent exchange, for instance `lib:AuthnContextClassRef`. If this URI were to specify a less or insecure transport, then the exchange may be vulnerable to the types of attacks described above.

Countermeasure: Ensure that points of entry to Liberty protocol exchanges utilize the `https` URL `<scheme>` and that all interactions for that profile consistently exchange messages over `https`.

Threat: Malicious redirects into identity or service provider targets

Description: A spurious entity could issue a redirect to a user agent so that the user agent would access a resource that disrupts single sign-on. For example, an attacker could redirect the user agent to a logout resource of a service provider causing the Principal to be logged out of all existing authentication sessions.

Countermeasure: Access to resources that produce side effects could be specified with a transient qualifier that must correspond to the current authentication session. Alternatively, a confirmation dialog could be interposed that relies on a transient qualifier with similar semantics.

Threat: Relay state tampering or fabrication

Description: Some of the messages may carry a `<lib:RelayState>` element, which is recommended to be integrity-protected by the producer and optionally confidentiality-protected. If these practices are not followed, an adversary could trigger unwanted side effects. In addition, by not confidentiality-protecting the value of this element, a legitimate

system entity could inadvertently expose information to the identity provider or a passive attacker.

Countermeasure: Follow the recommended practice of confidentiality- and integrity-protecting the `<lib:RelayState>` data. Note: Because the value of this element is both produced and consumed by the same system entity, symmetric cryptographic primitives could be utilized.

4.4.2 Single Sign-On and Federation

4.4.2.1 Common Interactions for All Single Sign-On and Federation Profiles

Threat: `<lib:AuthnRequest>` sent over insecure channel

Description: It is recommended that the initial exchange to access the intersite transfer service be conducted over a TLS-secured transport. Not following this recommendation can expose the exchange to both passive and active attacks.

Countermeasure: Deploy the intersite transfer service under an `https` scheme.

Threat: Unsigned `<lib:AuthnRequest>` message

Description: The signature element of an `<lib:AuthnRequest>` is optional and thus the absence of the signature could pose a threat to the identity provider or even the targeted service provider. For example, a spurious system entity could generate an unsigned `<lib:AuthnRequest>` and redirect the user agent to the identity provider. The identity provider must then consume resources.

Countermeasure: Sign the `<lib:AuthnRequest>`. The IDP can also verify the identity of the Principal in the absence of a signed request.

Threat: Replay of an authentication assertion

Description: After obtaining a valid assertion from an identity provider, either legitimately or surreptitiously, the entity replays the assertion to the Service at a later time. A digital signature must cover the entire assertion, thus elements within the assertion cannot be corrupted without detection during the mandatory verification step. However, it is possible to fabricate an `<lib:AuthnResponse>` with the valid assertion.

Countermeasure: The issuer should sign `<lib:AuthnResponse>` messages. Signing binds the `<samlp:IssueInstant>` of the response message to the assertion it contains. This binding accords the relying party the opportunity to temporally judge the response. Additionally, a valid signature over the response binds the `<samlp:InResponseTo>` element to the corresponding `<lib:AuthnRequest>`. (Specifying a short period that the authentication assertion can be relied upon will minimize, but not mitigate this threat. Binding the `<lib:AssertionId>` to the request/`<samlp:InResponseTo>` element may also be handy.)

Threat: Fabricated `<lib:AuthnResponse>` denial of service

Description: An attacker captures the `<samlp:RequestID>` sent in an `<lib:AuthnRequest>` message by a service provider to an identity provider, and sends several spurious `<lib:AuthnResponse>` messages to the service provider with the same `<samlp:InResponseTo>`. Because the `<samlp:InResponseTo>` matches a

<samlp:RequestID> that the service provider had used, the service provider goes through the process of validating the signature in the message. Thus, it is subject to a denial of service attack.

Countermeasure: A secure communication channel should be established before transferring requests and responses.

Threat: Collusion between two Principals

Description: After getting an artifact or <lib:AuthnResponse> in step 6 (see 3.2.1), a legitimate Principal A could pass this artifact or <lib:AuthnResponse> on to another Principal, B. Principal B is now able to use the artifact or <lib:AuthnResponse>, while the actual authentication happened via Principal A.

Countermeasure: Implementations where this threat is a concern MUST use the <saml:AuthenticationLocality> in the authentication statement. The IP address that Principal B uses would be different from the IP address within the <saml:AuthenticationLocality>. This countermeasure may not suffice when the user agent is behind a firewall or proxy server. IP spoofing may also circumvent this countermeasure.

Threat: Stolen artifact and subsequent Principal impersonation

Description: See Section 4.1.1.9.1 in [SAMLBind]

Countermeasure: Identity providers MUST enforce a policy of one-time retrieval of the assertion corresponding to an artifact so that a stolen artifact can be used only once. Implementations where this threat is a concern MUST use the <saml:AuthenticationLocality> in the authentication statement. The IP address of a spurious user agent that attempts to use the stolen artifact would be different from IP address within the <saml:AuthenticationLocality>. The service provider may then be able to detect that the IP addresses differ. This countermeasure may not suffice when the user agent is behind a firewall or proxy server. IP address spoofing may also circumvent this countermeasure.

Threat: Stolen assertion and subsequent Principal impersonation

Description: See Section 4.1.1.9.1 in [SAMLBind]

Countermeasure: Refer to the previous threat for requirements.

Threat: Rogue service provider uses artifact or assertion to impersonate Principal at a different service provider

Description: Because the <lib:AuthnResponse> contains the <lib:ProviderID>, this threat is not possible.

Countermeasure: None

Threat: Rogue identity provider impersonates Principal at a service provider

Description: Because the Principal trusts the identity provider, it is assumed that the identity provider does not misuse the Principal's trust.

Countermeasure: None

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 <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 <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 <AuthnRequest> and an active session before issuing an <AuthnResponse> without first authenticating the Principal. Cookies posted by identity providers MAY be used to support this validation process, though Liberty does not mandate a cookie-based approach.

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 that identity and service providers must exchange in the process of establishing their operational relationship (see sections 3.1 and 3.1.3).

4.4.2.3 Federation

Threat: Collusion among service providers can violate privacy of the Principal

Description: When a group of service providers collude to share the <lib:IDPProvidedNameIdentifier> of a Principal, they can track and in general compromise the privacy of the principal. More generally, this threat exists for any common data (e.g. phone number) shared by rogue system entities.

Countermeasure: The <lib:IDPProvidedNameIdentifier> is required to be unique for each identity provider to service provider relationship. However, this requirement does

not eliminate the threat when there are rogue participants under the Principal's identity federation. The only protection is for Principals to be cautious when they choose service providers and understand their privacy policies.

Threat: Poorly generated name identifiers may compromise privacy

Description: The federation protocol mandates that the `<lib:NameIdentifier>` elements be unique within a Principal's federated identities. The name identifiers exchanged are pseudonyms and, to maintain the privacy of the Principal, should be resistant to guessing or derivation attacks.

Countermeasure: Name identifiers should be constructed using pseudo-random values that have no discernable correspondence with the Principal's identifier (or name) used by the entity that generates the name identifier.

4.4.3 Name Registration

No known threats.

4.4.4 Federation Termination: HTTP-Redirect-Based Profile

Threat: Attacker can monitor and disrupt termination

Description: During the initial steps, a passive attacker can collect the `<lib:FederationTerminationNotification>` information when it is issued in the redirect. This threat is possible because the first and second steps are not required to use `https` as the URL scheme. An active attacker may be able to intercept and modify the message conveyed in step 2 because the digital signature only covers a portion of the message. This initial exchange also exposes the name identifier. Exposing these data poses a privacy threat.

Countermeasure: All exchanges should be conducted over a secure transport such as SSL or TLS.

4.4.5 Single Logout: HTTP-Redirect-Based Profile

Threat: Passive attacker can collect a Principal's name identifier

Description: During the initial steps, a passive attacker can collect the `<lib:LogoutRequest>` information when it is issued in the redirect. Exposing these data poses a privacy threat.

Countermeasure: All exchanges should be conducted over a secure transport such as SSL or TLS.

Threat: Unsigned `<lib:LogoutRequest>` message

Description: An Unsigned `<lib:LogoutRequest>` could be injected by a spurious system entity thus denying service to the Principal. Assuming that the `NameIdentifier` can be deduced or derived then it is conceivable that the user agent could be directed to deliver a fabricated `<lib:LogoutRequest>` message.

Countermeasure: Sign the `<lib:LogoutRequest>` message. The identity provider can also verify the identity of a Principal in the absence of a signed request.

4.4.6 Identity Provider Introduction

No known threats.

5 References

5.1 Normative

[HTML4] Raggett, D., Le Hors, A., & Jacobs, I., eds (December 1999). "HTML 4.01 Specification," W3C Recommendation. World Wide Web Consortium. <http://www.w3.org/TR/html401> [18 December 2002].

[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/>.

[RFC1750] Eastlake 3rd, D., Croker, S., & Schiller, J. (December 1994). "Randomness Recommendations for Security," RFC 1750. The Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc1750.txt> [18 December 2002].

[RFC1945] Berners-Lee, T., Fielding, R., Frystyk, H. (May 1996). "Hypertext Transfer Protocol -- HTTP/1.0," RFC 1945. The Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc1945.txt> [18 December 2002].

[RFC2045] Freed, N., Borenstein, N. (November 1996). "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies," RFC 2045. The Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc2045.txt> [18 December 2002].

[RFC2109] Kristol, D., & Montulli, L. (February 1997). "HTTP State Management Mechanism," RFC 2109. The Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc2109.txt> [18 December 2002].

[RFC2119] Bradner, S. (March 1997). "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119. The Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc2119.txt> [18 December 2002].

[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]

[RFC2396] Berners-Lee, T., Fielding, R., & Masinter, L. (August 1998). "Uniform Resource Identifiers (URI): Generic Syntax," RFC 2396. The Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc2396.txt> [18 December 2002].

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., & Berners-Lee, T. (June 1999). "Hypertext Transfer Protocol -- HTTP/1.1,"

RFC 2616. The Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc2616.txt> [18 December 2002].

[RFC2617] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., & Stewart, L. (June 1999). "HTTP Authentication: Basic and Digest Access Authentication," RFC 2617. The Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc2617.txt> [18 December 2002]

[RFC2774] Nielsen, H., Leach P., & Lawrence, S. (February 2000). "An HTTP Extension Framework," RFC 2774. The Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc2774.txt> [18 December 2002].

[RFC3106] Eastlake, D., & Goldstein, T. (April 2001). "ECML v1.1: Field Specifications for E-Commerce," RFC 3106. The Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc3106.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].

[SAMLGloss] Hodges, J., Maler, E, eds. (05 Nov. 2002). "Glossary 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].

[SAMLReqs] Platt, D., Prodromou, E., eds. (05 Nov. 2002). "SAML Requirements and Use Cases," Version 1.0, OASIS Standard. Organization for the Advancement of Structured Information Standards, <http://www.oasis-open.org/committees/security/#documents> [18 December 2002].

[SAMLSec] McLaren, C., ed. (05 Nov. 2002). "Security Considerations 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].

[Schema1] Thompson, H. S., Beech, D., Maloney, M., & Mendleshon, N., eds. (May 2002). "XML Schema Part 1: Structures," Recommendation. World Wide Web Consortium, <http://www.w3.org/TR/xmlschema-1/> [18 December 2002].

[Schema2] Biron, P. V., & Malhotra, A., eds. (May 2002). "XML Schema Part 2: Datatypes," Recommendation. World Wide Web Consortium, <http://www.w3.org/TR/xmlschema-2/> [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].

[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].

5.2 Informative

[Anders] Rundgren, A. (August 2001). "A suggestion on how to implement SAML browser bindings without using Artifacts." <http://www.x-obi.com/OBI400/andersr-browser-artifact.ppt> [18 December 2002].

[Rescorla-Sec] Rescorla, E., & Korver, B., eds. (October 2002). "Guidelines for Writing RFC Text on Security Considerations," Draft 01. The Internet Engineering Task Force. <http://www.ietf.org/internet-drafts/draft-iab-sec-cons-01.txt> [18 December 2002].

[ShibMarlena] Erdos, M. (June 2001). "Shibboleth Architecture" Draft V1.1. Internet2, <http://shibboleth.internet2.edu/docs/draft-erdos-shibboleth-architecture-01.pdf> [18 December 2002].