ICS 33.030
M 21

YD

中华人民共和国通信行业标准

YD/T 2127.3-2010

移动 Web 服务网络身份认证技术要求 第 3 部分：网络身份联合框架

Technical requirements for mobile Web services network identity authentication Part 3：Network identity federation framework

2010-12-29 发布　　2011-01-01 实施

中华人民共和国工业和信息化部　发布

目　次

前　言……II
1　范围……1
2　规范性引用文件……1
3　术语、定义和缩略语……1
3.1　术语和定义……1
3.2　缩略语……2
4　概述……2
5　网络身份支持的功能……3
5.1　身份提供商定义……3
5.2　身份联合和单点登录……3
5.3　名字注册……7
5.4　认证上下文……9
5.5　单点退出……9
5.6　联合终止通告……11
5.7　安全考虑……12
附录A（规范性附录）静态的一致性需求……13
附录B（资料性附录）服务提供商和身份提供商的消息交换……15
附录C（资料性附录）规范图解……17
参考文献……23

前　言

YD/T 2127《移动Web服务网络身份认证技术要求》分为3个部分：

——第1部分：总体技术要求；

——第2部分：网络身份Web服务框架；

——第3部分：网络身份联合框架。

本部分为YD/T 2127的第3部分。第4章、第5章及附录部分分别对应于开放移动联盟MWS工作组制定的移动Web服务网络身份联合框架协议第4章、第5章及附录部分，在技术内容上保持一致。

本部分附录A为规范性附录，附录B和附录C为资料性附录。

本部分由中国通信标准化协会提出并归口。

本部分起草单位：北京邮电大学、中国普天信息产业股份有限公司、中国联合网络通信集团有限公司、华为技术有限公司。

本部分主要起草人：张　勇、宋俊德、宋　梅、宋美娜、由　磊、鄂海红、蔡　杰、邱　琳、唐显莉、刘　博、郭　达、陈国乔、杨　健、王　雷。

移动Web服务网络身份认证技术要求
第3部分：网络身份联合框架

1 范围

本部分规定了移动Web服务网络身份联合框架，包括Web服务中网络身份联合所以支持的功能和要求，以及实现网络身份联合的框架要求。同时为了实现该框架，还规定了终端与服务提供商、属性提供商间的交互方法、流程、接口和协议。

本部分适用于Web服务网络身份认证联合要求，包括实现网络联合身份的基础框架、设备和消息流程的要求。

2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分。然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

Liberty-BindProf (2003) 自由绑定和概要规范Liberty Bindings and Profiles Specification

Liberty-ProtSchema (2003) 自由协议和Schema 规范Liberty Protocols and Schema Specification

OMA OWSER Core（2006） OMA Web 服务引擎:核心规范OMA Web Services Enabler (OWSER): Core Specifications

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本部分。

3.1.1

网络身份 Network Identity

从主体所有的帐户中提取的一组全局属性。

3.1.2

代理 Proxy

在客户端与服务器端之间的计算机系统中传递协议的计算机处理程序。它对客户端来说看起来像服务器，而对服务器来说看起来像客户端。

3.1.3

订阅者 Subscriber

与服务提供商建立了订阅关系的实体（与一个或多个用户相关联）。订阅者可以对服务进行订阅和取消，可以得到服务使用授权的一个用户或多个用户进行注册，还可以对用户使用这些服务设置限制条件。([3GPP-TR21.905])

3.1.4

订阅 Subscription

订阅者和服务提供商之间的商业关系的描述。([3GPP-TR21.905])

3.1.5

Web服务安全 WS-Security

在SOAP消息包中添加安全机制，以保证消息的完整性、机密性和单个消息的认证。 这些机制支持多种安全模式和加密技术。

3.1.6

用户代理 User Agent

任何一种能够代表用户与其他实体进行交互和对资源进行处理的软件或设备。

3.2 缩略语

下列缩略语适用于本部分。

HTTP	Hyper Text Transfer Protocol	超文本传输协议
HTTPS	HTTP Secure (aka HTTP over SSL)	安全超文本传输协议；HTTP的安全版
MIME	Multipurpose Internet Mail Extensions	多用途Internet邮件扩允协议
LECP	Liberty-enabled Client/Proxy	多用途Internet邮件扩允协议
OASIS	Organization for the Advancement of Structured Information	结构化信息标准促进组织
PKCS	Public Key Cryptography Standards	公钥加密标准
PKI	Public Key Infrastructure	公钥基础设施
SAML	Security Assertion Markup Language	安全声明标记语言
SSL	Secure Socket Layer	安全套接层
SOAP	Simple Object Access Protocol	简单对象访问协议
TCP	Transmission Control Protocol	传输控制协议
TLS	Transport Layer Security	传输层安全
URI	Uniform Resource Identifier	统一资源标识符
WS	Web Services	Web服务
WSDL	Web Service Description Language	Web服务描述语言
WSF	Web Services Framework	Web服务框架
WSR	Web Service Requester	Web服务请求者

4 概述

移动终端用户可使用多种服务，但并不是所有服务都位于其网络运营商的信任域内。为了提高终端用户体验，身份联合的概念应运而生。网络身份这个术语用来描述在多种网络服务中，提供终端用户的状态或数据一致性的基本功能。这种服务的一个例子就是单点登录。在本部分所定义的网络身份消息交换中，确定了三种角色：主体、身份提供商、服务提供商。

《移动Web服务网络身份认证技术要求》，在Web服务网络身份规范所支持的网络身份中，针对必需的几个部分进行了标准化。包括身份服务定义、身份联合和单点登录、名字注册、认证上下文、单点退出、联合终止、服务提供商联盟、身份提供商的动态代理。附录A对这些功能进行了描述。

《移动Web服务网络身份认证技术要求》是为了满足移动网络运营商（本部分作为身份提供商的典型代表）、运营商的订阅者和第三方服务提供商，日益增长的业务需求。因此，“Web服务网络身份认证技术要求》的系列标准，专注于作为终端用户或者订阅者角色的主体（使终端用户设备支持诸如单点登录等功能），而不是代表软件系统中的所有元素。

为了支持各种网络身份鉴权的功能，本部分对协议作了定义，并且在附录B中对消息流程作了规定。

5 网络身份支持的功能

本部分为OWSER NI中网络身份所支持的功能提供了标准化文本，这些标准化文本参考自由联盟OMA规范。这些规范包括：

—— 自由联盟协议族和 Schema 规范，[Liberty-ProtSchema]版本，其中自由联盟协议和消息，以及相关的 XML schema，都是为身份联合、单点登录、名字注册、联合终止和单点退出而定义的；

—— 自由联盟绑定和规范，[Libert-BindProf]版本，其中对[Liberty-ProtSchema]里定义的自由联盟协议和消息的自由联盟绑定和规范均进行了详细说明；

—— 自由联盟认证上下文规范， [Liberty-AuthnContext]1.1 版本，其中对认证上下文声明和自由联盟认证上下文分类的初始列表的语法进行了定义。

本部分为身份联合、单点登录、名字注册、联合终止和单点退出而定义的协议和消息，应与[Liberty-ProtSchema]中所定义的协议和消息具备一致。本部分所定义的与身份联合相关的协议族应与[Liberty-BindProf]中定义的协议族一致。本部分定义了与[Liberty-BindProf]中的定义相同的规范，如：相同的消息内容规范的联合和单一客户端类型的消息传输机制。与之不同的规范根据各自的特征在相应章节进行定义。特别地，所有规范实现应遵从的规则在[Liberty-BindProf]3.1节中有定义。

5.1 身份提供商定义

可以提供网络身份认证的服务提供商，需要知道与某一主体相关联的身份的提供商。在[Liberty-BindProf]中基于公共域cookie定义了介绍性的规范。

主体的用户代理已经得到，或者知道如何得到有关主体与服务提供商使用的身份提供商的信息，用户代理向身份提供商请求认证时，在请求消息中携带终端标识，身份提供商根据标识进行认证，向用户代理发送终端的认证响应。在[Liberty-BindProf]中这种用户代理被称为支持自由联盟的客户端/代理。

客户端或者用户代理需要向服务提供商提供如下信息：

—— 负责为服务提供商选定身份提供商，并选择认证的方式。

—— 在主体应向服务提供商发送的消息中，添加适当的头域来携带主体身份信息、认证方式等信息。

该头域信息应按照[Liberty-BindProf]3.2.5.1小节中的规定来进行定义。

5.2 身份联合和单点登录

5.2.1 身份联合和单点登录的功能要求

本部分中描述的身份联合和单点登录，是利用身份联合和单点登录时的请求/响应消息的相关协议。主体通过向服务提供商发送HTTP请求，发起单点登录。其协议的工作流程如下：

a）服务提供商向身份提供商发送<lib:AuthnRequest>消息，指示身份提供商为服务提供商，终端用户和主体提供认证断言。作为可选项，服务提供商可请求将终端用户和主体在各个服务提供商处的本地身份联合起来，也可以是不同用户的联合。该联合具有信任关系。

b）作为该请求的响应，身份提供商要么给服务提供商，终端用户和主体回送包含认证断言的<lib:AuthnResponse>消息，要么回送能够通过解析来获取认证断言的结果。此外，如果服务提供商已发出请求，需要将终端用户主体及与其它主体的各个本地身份联合起来，那么身份提供商宜执行这一请求。

身份联合和单点登录协议应遵照[Liberty-ProtSchema]3.2节中的规定，联合的身份信息可保存在身份提供商中。

身份提供商通过对收到的请求进行恰当的处理以及和生成响应，使单点登录和身份联合变得容易实现起来。当身份提供商接收到用户的身份认证请求中携带终端标识信息时，根据标识对终端进行认证，并向用户返回身份认证响应。[Liberty-BindProf]3.2.1小节中的交互图描述了单点登录的大体架构，简要步骤请参考此图。安全性方面，身份提供商在用户包含联合信息时，判定具有访问权限。如果主体已经通过了身份提供商的认证，并且在身份提供商处，已经存在一个已认证的主体的会话，那么这种初始认证的建立是与单点登录所提供的功能，是相独立的。

身份提供商需要采取两项行动：

—— 身份提供商应按照[Liberty-ProtSchema]中指定的规则对<lib:AuthnRequest>消息进行处理。作为<lib:AuthnRequest>消息中的一部分，服务提供商可在消息中包含一个标识，要求对终端用户，主体和服务提供商进行认证断言，并请求将终端用户和主体在各个身份提供商和服务提供商处的本地身份联合起来。

—— 身份提供商应回送一个<lib:AuthnResponse>、一个 SAML 结果或一个 error 作为响应，用来说明认证断言的结果，同时，响应的格式应依照该服务提供商所采用的绑定协议。

为了满足主体用户代理的不同性能以及诸如支持Liberty的代理之类的网络性能的有效性，本部分描述了身份联合和单点登录协议涉及到的3个规范。

—— 浏览器结果规范；

—— 浏览器 POST 规范；

—— 支持自由联盟的客户端/代理规范。

每个规范都应遵循[Liberty-BindProf]3.2.1小节中指定的通用交互和处理规则。附录B对这些规范中的每一个消息交互均做了图解说明。

5.2.2 浏览器结果规范

浏览器结果规范以认证结果（SAML 结果）的使用为基础，服务提供商通过对这种认证结果进行解析，从而得到由身份提供商发出的认证断言来确定主体是否已通过认证。本部分作为对[SAMLBind][SAMLCore]中SAML的“浏览器/结果规范”的改写，应依照[Liberty-BindProf]3.2.2小节中的说明来实现。

本部分立足于服务提供商和身份提供商均实现了应实现的网络身份特征。本节所列的必要条件应依照后面将要介绍的[Liberty-BindProf]中的相关章节来实现。

[Liberty-BindProf]中的图2描述了单点登录中的浏览器结果规范。如[Liberty-BindProf]3.2.1小节所述，主体通过向服务提供商发送HTTP请求发起单点登录。接着，服务提供商作出如下处理：

—— 服务提供商得到相应的身份提供商的地址（参见 5.1 节）；

—— 如[Liberty-BindProf]3.2.2.1 小节中的第 3 步所述，服务提供商应向主体的用户代理发送包含身份提供商地址信息的<lib:AuthnRequest>消息的 HTTP 重定向作为响应；

—— 在得到源于身份提供商的 SAML 结果后，服务提供商应如[Liberty-BindProf]3.2.2 小节中的第 8 步所述那样，向身份提供商的 SOAP 端点发送<samlp:Request>SOAP 消息；

—— 服务提供商应如[Liberty-BindProf]3.2.1 小节中的第 10 步所述那样，对身份提供商返回的<samlp:Assertion>进行处理。

为了实现此功能，身份提供商应完成处理认证请求，处理SAML请求这两个步骤。请求认证断言的交互过程如下：

—— 身份提供商应如[Liberty-BindProf]3.2.1 小节中的第 5 步所述那样，对<lib:AuthnRequest>消息进行处理；

—— 如[Liberty-BindProf]3.2.2.1 小节中的第 6 步所述，作为对<lib:AuthnRequest>的响应，身份提供商应执行包含 SAML 结果 的 HTTP 重定向；

—— 身份提供商应处理由服务提供商在单点登录交互的第 8 步中所生成的<samlp:Request>，且应按照[Liberty-BindProf]3.2.1 小节中的第 9 步所述生成<samlp:Response>；

—— 由身份提供商生成的结果应符合[Liberty-BindProf]3.2.2.2 小节中定义的格式。

5.2.3 浏览器 POST 规范

浏览器POST规范允许向身份提供商传达认证断言而不使用结果。本部分作为对 [SAMLBind]中SAML的“Browser/post规范”的改写，应依照[Liberty-BindProf]3.2.3小节中的说明来实现。

服务提供商和身份提供商可选择是否支持本部分。尽管身份提供商并不强行要求应支持本部分，但是为了与使用本部分的服务提供商之间有效交互的顺利进行，身份提供商宜支持本部分。本节所列的必要条件应依照后面将要介绍的[Liberty-BindProf]中的相关章节来实现。

[Liberty-BindProf]中的图3描述了单点登录中的浏览器POST规范。如[Liberty-BindProf]3.2.1小节所述，主体通过向服务提供商发送HTTP请求发起单点登录。接着，服务提供商作出如下处理：

—— 服务提供商得到相应的身份提供商的地址；

—— 如[Liberty-BindProf]3.2.3 小节中的第 3 步所述，服务提供商应向主体的用户代理发送包含身份提供商地址信息的<lib:AuthnRequest>消息的 HTTP 重定向作为响应；

—— 在得到认证断言后，主体的用户代理应重新向服务提供商发送包含<lib:AuthnResponse>的 HPPT POST 请求，服务提供商应如[Liberty-BindProf]3.2.1 小节中的第 10 步所述那样对该请求进行处理。

在身份提供商处，请求认证断言的交互过程如下：

—— 身份提供商应如[Liberty-BindProf]3.2.1 小节中的第 5 步所述那样对<lib:AuthnRequest>消息进行处理；

—— 身份提供商生成包含认证响应<lib:AuthnResponse>的 HTTP 200 响应。该响应应符合[Liberty-BindProf]3.2.3 小节步骤 6 中所定义的格式。

5.2.4 支持 Liberty 的客户端/代理（LECP）规范

客户端或代理（LECP）规定了客户端/代理、服务提供商和身份提供商之间的交互。客户端是一个主体用户代理，即为了实现基于如单点登录等服务的网络身份，并已经得到或者知道，如何得到有关E主体，希望与服务提供商，来使用身份提供商提供的信息。此外，支持自由联盟的客户端通过在HTTP请求和响应消息体中发送和接受消息，实现了网络身份协议。与基于浏览器的用户代理相比，在支持Liberty的客户端在协议消息的大小方面没有限制。

客户端，除了需符合[Liberty-BindProf]3.1节的通用要求外，还应在发起的每一个HTTP请求中的HTTP User-Agent头内添加'Liberty-Enabled' HTTP头或入口。首选的方法是添加'Liberty-Enabled' 头。因此，支持自由联盟的客户端宜通过添加'Liberty-Enabled'HTTP头来对此性能进行指示。[Liberty-BindProf]3.2.2.2小节介绍了Liberty-Enabled HTTP头和HTTP User-Agent头入口的格式。

本部分中的Liberty-enabled Client/Proxy (LECP)规范应按照[Liberty-BindProf]3.2.5小节来实现。[Liberty-BindProf]图5描述了单点登录的LECP规范。在实现基于网络身份性能的服务提供商和身份提供商处，支持LECP规范是一项强制要求。本节所列的必要条件应依照后面将要介绍的[Liberty-BindProf]中的相关章节来实现。

如[Liberty-BindProf]3.2.5.2小节中的第1步所述，主体通过向服务提供商发送HTTP请求发起单点登录。主体的用户代理向服务提供商提交包含上面介绍的必需的支持自由联盟指示的请求。在服务提供商方：

—— 服务提供商若接收到主体用户代理是支持自由联盟的指示，那么它严禁获取身份提供商的地址或执行身份提供商的介绍；

—— 服务提供商应向主体的用户代理发送一个 HTTP 200 OK 响应。该响应应遵循[Liberty-BindProf]3.2.5.2 小节中第 3 步的规范。服务提供商宜如[Liberty-BindProf]3.2.5.2 小节中的第 3 步所述那样在响应中放置合适的头，以确保响应不会被缓存起来。

在身份提供商处：

—— 身份提供商应如[Liberty-BindProf]3.2.1 小节的第 5 步中所述那样对来自支持 Liberty 的客户端/代理的 SOAP POST 消息体中的<lib:AuthnRequest>进行处理；

—— 身份提供商应如[Liberty-BindProf]3.2.5.2 小节的第 6 步所述的那样，以一个 HTTP 200 OK 响应作为对<lib:AuthnRequest>的响应，该响应带有正确的 MIME 类型（application/vnd.liberty-response+xml）和支持自由联盟的 HTTP 头（见[Liberty-BindProf]3.2.5.1 小节）。该响应应遵照[Liberty-ProtSchema]在 SOAP 消息体中添加<lib:AuthnResponseEnvelope>；

—— 在获得认证断言后，如[Liberty-BindProf]3.2.5.2 小节的第 7 步所述那样，主体的用户代理将向服务提供商发起包含<lib:AuthnResponse>消息的 HTTP POST 请求；

—— 服务提供商应如[Liberty-BindProf]3.2.1 小节的第 10 步所述的那样对接收到的来自于主体用户代理的 HTTP POST 请求中的<lib:AuthnResponse>消息进行处理。

5.2.5 从属关系

依照[Liberty-ProtSchema]3.1.3小节所述，从属关系应该用基于URI的标识符来加以标识。

当身份提供商和服务提供商所在的联盟之间发生了单点登录和身份联合时，应遵照[Liberty-ProtSchema]3.2节中的单点登录和联合协议，将用户的身份信息以及访问权限提交给身份提供商。在认证请求中，服务提供商若想要说明自己联盟成员的身份，则应如[Liberty-ProtSchema]3.2.2.6小节中所述那样，在 <AuthnRequest> 中添加 <AffiliationID> 元素。处理规则应遵照[Liberty-ProtSchema]3.2.2.6小节所定的规则。

主体终止身份提供商和服务提供商所在联盟之间的身份联合时，应遵照 [Liberty-ProtSchema]3.4小节所介绍的联合终止通告协议。

当主体通过在服务提供商处退出而发起单点退出请求后，它将从由该身份提供商认证的，包括与联盟的会话在内的所有会话中退出。应遵照 [Liberty-ProtSchema]3.5小节所介绍的单点登录出协议。

当服务提供商为和它有身份联合关系的主体申请名字标识符，但该名字标识符所涉及的是身份提供商和另一个服务提供商之间的身份联合时，它能通过使用名字标识符映射协议来得到这个标识符。这两个服务提供商中的任何一个都可属于某affilication。若使用了名字标识符映射协议，则应遵照[Liberty-ProtSchema]3.6节中的处理程序。

下面将给出一个<AuthnRequest>的例子，其中，联盟的affiliationID为http://OWSERCompatible Affiliation.com，联盟一个成员的ProviderID 为http://OWSERCompatibleSP.com。可选的AffiliationID元素出现，表示此SP是该联盟的成员。

<lib:AuthnRequest RequestID="1pY6tWugT8Vz+L8+rURp51oFX6rt" MajorVersion="1" MinorVersion="2" consent="urn:liberty:consent:obtained" IssueInstant="2005-03-24T21:42:4Z"

xmlns:lib="urn:liberty:iff:2003-08">

<ds:Signature> . .. </ds:Signature>

<lib:ProviderID>http://OWSERCompatibleSP.com</lib:ProviderID>

<lib:AffiliationID>http://OWSERCompatibleAffiliation.com</lib:AffiliationID>

<lib:NameIDPolicy>federate</lib:NameIDPolicy>

<lib:ForceAuthn>false</lib:ForceAuthn>

<lib:IsPassive>false</lib:IsPassive>

<lib:ProtocolProfile>http://projectliberty.org/profiles/brws-post</lib:ProtocolProfile>

<lib:RequestAuthnContext>

<lib:AuthnContextClassRef>http://projectliberty.org/schemas/authctx/classes/Password-ProtectedTransport</lib:AuthnContextClassRef>

<lib:AuthnContextComparison>exact</lib:AuthnContextComparison>

</lib:RequestAuthnContext>

<lib:RelayState>Yu8IODlhcgGSUitRAA8UhbMmCZtuYalPA2gh</lib:RelayState>

<lib:Scoping>

<lib:ProxyCount>1</lib:ProxyCount>

</lib:Scoping>

</lib:AuthnRequest>

5.2.6 身份提供商的动态代理

身份提供商的动态代理，使身份提供商可接收主体的认证请求，并将该认证请求转发给另一个可能已经对该主体进行过认证的身份提供商。身份提供商的动态代理应遵循[Liberty-ProtSchema]3.2.2.7小节所介绍的机制。

5.3 名字注册

5.3.1 名字注册的功能要求

在身份联合时，身份提供商生成一个不透明句柄，当服务提供商和身份提供商之间，为实现诸如单点登录等基于联合网络身份的性能，而进行交互时，它们将把此句柄作为主体的初始名字标识。此名字标识符的标签元素为<lib:IdPProvidedNameIdentifier>。

在身份联合之后，服务提供商或者身份提供商均可发起名字注册协议，并为主体注册一个新的名字标识符。联合后，身份提供商可注册一个新的<lib:IdPProvidedNameIdentifier>。此外，服务提供商可注册一个标签元素为<lib:IdPProvidedNameIdentifier>的不同，的不透明句柄与服务提供商对应。在服务提供商进行名字注册后，当与服务提供商相交互时，身份提供商应使用<lib:SPProvidedNameIdentifier>来标识主体。注意：SP和IdP可发起名字注册意味着在每一个部署场景中，IdP和SP能够互相协同，且应支持对方消息的接收。

在进行名字注册时，SP和IdP应遵照[Liberty-ProtSchema]3.3节所介绍的处理程序。为实现名字注册，应使用[Liberty-ProtSchema]中定义的<lib:RegisterNameIdentifierRequest> 和<lib:RegisterNameIdentifierResponse>消息，且应符合下面的强制性声明。

身份提供商和服务提供商均可发起名字注册。本部分描述了名字注册的两个规范：

—— 基于 HTTP 重定向的名字注册；

—— 基于 SOAP/HTTP 重定向的名字注册。

本部分中所描述的规范的实现应遵照[Liberty-BindProf]3.3节的规范。服务提供商和身份提供商应支持基于SOAP/HTTP重定向的名字注册规范，同时可选择支持基于HTTP重定向的名字注册规范。虽然支持基于HTTP重定向的名字注册规范是可选的，但是为了实现与使用此规范的服务提供商之间的互操作，身份提供商宜支持此规范。当由身份提供商发起名字注册时，应遵照[Liberty-BindProf]3.3.1小节介绍的机制。当由服务提供商发起名字注册时，应遵照[Liberty-BindProf]3.3.2小节介绍的机制。

不管名字注册是由身份提供商发起的还是服务提供商发起的，下面所介绍的反应和处理步骤都是对称的。下面仅描述名字注册是由身份提供商所发起的情况。相应的名字注册是由服务提供商所发起的情况，可通过将“身份提供商”替换为“服务提供商”、将IdPProvidedNameIdentifier替换为SPProvidedNameIdentifier，以及将参考3.3.1.x小节替换为参考3.3.2.x小节而得到相应的响应和处理过程。

附录B对这些规范均作了消息交换的图解说明。

5.3.2 由身份提供商发起的名字注册

5.3.2.1 概述

当身份提供商发起名字注册时，应遵照[Liberty-BindProf]3.3.1小节所介绍的机制。

5.3.2.2 身份提供商的处理过程

5.3.2.2.1 基于 HTTP 重定向规范

本节定义了身份提供商根据[Liberty-BindProf]3.3.1.1小节所定义的交互而发起基于HTTP重定向的名字注册时，应采取的行动/处理过程。注意：虽然[Liberty-BindProf]给了一些例子，但是此交互的定时和发起机制并没有明确的标准。仅当服务提供商元数据指定了[Liberty-BindProf]3.3.1.1小节所指定的URI标识符时，身份提供商才应发起基于HTTP重定向的名字注册。

如[Liberty-BindProf]3.3.1.1小节中的第2步所述，身份提供商应将主体的用户代理重定向至服务提供商的身份注册服务。

5.3.2.2.2 基于 SOAP/HTTP 规范

仅当服务提供商元数据按照[Liberty-BindProf]3.3.1.2小节所规定的那样指定了URI标识符时，身份提供商才应发起基于SOAP/HTTP重定向的名字注册。

基于SOAP/HTTP的名字注册处理应使用[Liberty-BindProf]2.1中定义的Liberty SOAP绑定协议。

如 [Liberty-BindProf]3.3.1.2小节所述，身份提供商应通过向服务提供商的SOAP终端发送<lib:RegisterNameIdentifierRequest>消息来发起名字注册。

身份提供商应按照[Liberty-ProtSchema]3.3.3小节所定义的协议，处理来自服务提供商的<lib:RegisterNameIdentifierResponse>消息。

5.3.2.3 服务提供商的处理过程

5.3.2.3.1 基于 HTTP 重定向规范

服务提供商应按照[Liberty-ProtSchema]3.3.3小节和[Liberty-BindProf]3.3.1.1小节中第4步的定义来处理来自身份提供商的<lib:RegisterNameIdentifierRequest>消息。

服务提供商应用一个重定向URL来作为对身份提供商的响应，此重定向URL在[Liberty-ProtSchema]第4章中的RegisterNameIdentifierServiceReturnURL metadata元素中有定义。此重定向应遵照[Liberty-BindProf]3.3.1.1小节中的第5步所指定的规则。

5.3.2.3.2 基于 SOAP/HTTP 规范

基于SOAP/HTTP的名字注册交互应使用[Liberty-BindProf]2.1中定义的Liberty SOAP绑定协议。

在使用该协议时，身份提供商应给服务提供商发送<lib:RegisterNameIdentifierRequest>消息。该服务提供商应记录这个新的<lib:IDPProvidedNameIdentifier>。

在<lib:IDPProvidedNameIdentifier>注册成功后，服务提供商应按照[Liberty-ProtSchema]3.3.3小节所介绍的处理规则，用一个<lib:RegisterNameIdentifierResponse>作为响应。

5.4 认证上下文

认证上下文是作为认证断言的附加信息来定义的。服务提供商在决定为收到的断言授予哪些服务的访问权限前，可能需要此认证上下文。此信息宜包括认证机制，证书储存和保护机制、初始的用户验证机制等。

为简化服务提供商对认证断言的评定和比较，[Liberty-AuthnContext]定义了代表现有技术和实践的认证上下文分类。例如，典型的认证上下文就是主体在服务器认证的SSL会话中使用自选密码来向身份提供商提供认证信息。

身份提供商和服务提供商应认可<lib:AuthnContext>所包含的内容，也就是<lib:AuthnRequest> 和<lib:AuthnResponse>消息。当服务提供商想要向身份提供商请求特定认证上下文时，它应在向身份提供商发送的<lib:AuthnRequest>消息中包含<lib:AuthnContext>元素。当身份提供商想要传送给服务提供商一个特定的认证上下文时，它应在向身份提供商发送的<lib:AuthnResponse>消息中包含<lib:AuthnContext>元素。

[Liberty-AuthnContext]为认证上下文声明和认证上下文分类的初始列表的定义作了语法限定。

5.5 单点退出

当主体在服务提供商处调用单点退出进程时，服务提供商应向为该会话提供了认证服务的身份提供商发送<lib:LogoutRequest>消息。

不管是主体在身份提供商处请求单点退出还是服务提供商发送一个单点退出请求到该主体的身份提供商，身份提供商都应向每一个当前会话中获得过该主体认证断言的服务提供商发送<lib:LogoutRequest>消息，但是向身份提供商发送<lib:LogoutRequest>消息的服务提供商除外。在收到<lib:LogoutRequest>消息后，响应方应返回<lib:LogoutResponse>消息。

单点退出机制应遵照[Liberty-ProtSchema]3.5小节所指定的程序。[Liberty-ProtSchema]3.5.1.1小节列出了<lib:LogoutRequest>的schema片段。[Liberty-ProtSchema]3.5.2.1小节列出了<lib:LogoutResponse>的schema片段。

单点退出可能发起于身份提供商，也可能发起于服务提供商。针对单点退出由身份提供商发起的情况，指定了三个要求：

—— 基于 HTTP 重定向要求；

—— 基于 HTTP GET 要求；

—— 基于 SOAP/HTTP 要求。

针对单点退出由服务提供商发起的情况，指定了两个要求：

—— 基于 HTTP 重定向要求；

—— 基于 SOAP/HTTP 要求。

本部分中描述的该部分要求由[Liberty-BindProf]3.5节详细说明。服务提供商和身份提供商应支持基于SOAP/HTTP重定向的规范，同时可选择性地支持其它规范。虽然支持基于HTTP重定向要求和基于HTTP GET要求是可选的，但是为了实现与使用此规范的服务提供商之间的互操作，身份提供商宜支持它们。附录B对每一个规范的消息交换均作了图解说明。

单点退出发起后，身份提供商应终止该主体的当前会话，并且不允许再给服务提供商发送任何一个有关该主体的认证断言。

5.5.1 由身份提供商发起的单点退出

5.5.1.1 基于 HTTP 重定向要求

此交互只有在服务提供商 SingleLogOutProtocolProfile metadata 元素中指定了 URI http://projectliberty.org/profiles/slo-idp-http时才允许使用。

在对主体退出请求的响应中，身份提供商应将主体用户代理重定向至向当前会话中获得过该主体认证断言的每一个服务提供商的单点退出URL。每一个重定向都应遵照[Liberty-BindProf]3.5.1.1.1小节第1步中所指定的规则。

如身份提供商metadata中所定义，在接收到来自主体用户代理的发送给SingleLogoutService ReturnURL的请求后（在[Liberty-ProtSchema]第4章中有所描述），该身份提供商应对此请求作出处理并且向该主体的用户代理发送HTTP响应，以确认单点退出的请求已完成。

5.5.1.2 基于 HTTP GET 要求

此交互只有在服务提供商的元数据元素 SingleLogOutProtocolProfile 指定了 URI http://projectliberty.org/profiles/slo-idp-http时，才允许使用。

在对主体退出请求的响应中，身份提供商应向当前会话中从身份提供商处获得过该主体认证断言的每一个服务提供商发送一个代表退出服务URL的包含有图像标签的HTTP 200 response作为响应。每一个图像标签都应遵照[Liberty-BindProf]3.5.1.1.2小节第2步中所指定的规则。

如身份提供商元数据中所定义，在接收到来自SingleLogoutServiceReturnURL（在[Liberty-ProtSchema]第4章中有所描述）处的主体用户代理的发送给的请求后，该身份提供商应对此请求作出处理并且向该主体的用户代理发送HTTP响应，以确认单点退出的请求已完成。

5.5.1.3 基于 SOAP/HTTP 要求

此交互只允许在服务提供商SingleLogOutProtocolProfile元数据元素中指定了URI http://projectliberty.org/profiles/slo-idp-http时，才允许使用。

为了响应来自服务提供商的带有SOAP <lib:LogoutRequest>消息的HTTP 200 OK消息，服务提供商应发送一个HTTP响应，以确认单点退出的请求已完成。

5.5.2 由服务提供者发起的单点退出

5.5.2.1 基于 HTTP 重定向要求

使用基于HTTP重定向要求时，主体的用户代理应得到该服务提供商的单点退出服务URL。服务提供商的单点退出服务URL将用户代理重定向至身份提供商的单点退出服务URL。身份提供商应根据[Liberty-ProtSchema]3.5.1小节所定义的规则对<lib:LogoutRequest>进行处理。

身份提供商应如 [Liberty-BindProf]3.5.2.1小节中第4步所述，采用服务提供商倾向使用的规范向那些从身份提供商处获得过认证断言的服务提供商通报主体的退出请求。

身份提供商应遵循[Liberty-BindProf]3.5.2.1小节的说明，对主体的用户代理作出响应，并且通过使用从SingleLogoutServiceReturnURL 元数据元素中得到的返回URL地址（[Liberty-ProtSchema]第4章中有所描述），将用户代理重定向至服务提供商。

5.5.2.2 基于 SOAP/HTTP 要求

在接收到来自服务提供商的< lib:LogoutRequest>后，身份提供商应按照[Liberty-ProtSchema]3.5.1小节所定义的规则来进行处理。

身份提供商应向主体当前会话中每一个获得过认证断言的服务提供商发送一个主体退出请求，如[Liberty-BindProf]3.5.2.2小节的第3步的详细说明。

身份提供商应用带有SOAP <lib:LogoutRequest>消息的HTTP 200 OK作为对<lib:LogoutRequest>的响应。按[Liberty-BindProf]3.5.2.2小节的详细说明。

5.6 联合终止通告

5.6.1 联合终止通告的功能要求

按[Liberty-ProtSchema]3.4小节的详细说明，当主体终止服务提供商和身份提供商之间的身份联合时 ，应使用联合终止通告协议。有四种联合终止通告交互形式：联合终止通告可由身份提供商发起或者由服务提供商发起，且协议绑定基于HTTP重定向或基于SOAP/HTTP消息交换。服务提供商和身份提供商应支持基于SOAP/HTTP的要求，同时选择支持基于HTTP重定向的要求。虽然支持基于HTTP重定向的要求是可选的，但是为了实现与使用此规范的服务提供商之间的互操作，身份提供商宜支持此规范。在[Liberty-BindProf]3.4小节对这四种交互进行定义。附录B对每一个规范的消息交换均作了图解说明。

不管联合终止通告是由身份提供商发起的还是服务提供商发起的，以下定义的行为和处理步骤都是对称的。下面仅描述联合终止通告是由身份提供商所发起的情况。相应的联合终止通告是由服务提供商所发起的情况，可通过将“身份提供商”替换为“服务提供商”、将IdPProvidedNameIdentifier替换为SPProvidedNameIdentifier，以及将参考3.4.1.x小节替换为参考3.4.2.x小节而得到相应的行为和处理过程。

5.6.2 由身份提供商发起的联合终止通告

5.6.2.1 身份提供商的处理

5.6.2.1.1 HTTP 重定向

本部分只允许在服务提供商FederationTerminationNotificationProtocolProfile metadata元素中指定了URI http://projectliberty.org/profiles/fedterm-idp-http时，才允许使用。

本部分要求满足[Liberty-BindProf]3.4.1.1小节中指定的某些前提条件。

身份提供商在对联合终止服务URL请求响应时，应将主体用户代理重定向至服务提供商处的联合终止服务。此重定向应遵循[Liberty-BindProf]3.4.1.1小节中第2步所指定的规则。

5.6.2.1.2 SOAP/HTTP

本部分只允许在服务提供商FederationTerminationNotificationProtocolProfile metadata元素中指定了URI

本部分要求满足[Liberty-BindProf]3.4.1.2小节中指定的某些前提条件。

身份提供商响应来自主体用户代理的联合终止服务URL请求时，应向服务提供商的SOAP终端发送一SOAP/ HTTP通告消息。此SOAP消息应遵照[Liberty-BindProf]3.4.1.2小节中第2步所指定的规则。

服务提供商将回复一个HTTP 204 OK 响应。

身份提供商应对来自服务提供商的HTTP 204 响应作处理，并发送一个HTTP响应，以确认满足对指定服务提供商联合终止的请求。

5.6.2.2 服务提供者的处理

5.6.2.2.1 HTTP 重定向

基于HTTP重定向的联合终止通告（由身份提供商发起的）必须有服务提供商的支持。

服务提供商应按照[Liberty-ProtSchema]3.4.2小节和[Liberty-BindProf]3.4.1.1小节第4步中所定义的规则，来处理从主体用户代理得到的<lib:FederationTerminationNotification>。

服务提供商的联合终止服务应按照 [Liberty-BindProf]3.4.1.1小节中第5步的说明，通过将主体的用户代理重定向来响应。

5.6.2.2.2 SOAP/HTTP

服务提供商应按照[Liberty-ProtSchema]3.4.2小节和[Liberty-BindProf]3.4.1.2小节第3步中定义的规则，对来自身份提供商的SOAP消息中的<lib:FederationTerminationNotification>作出处理。

服务提供商按照[Liberty-BindProf]3.4.1.2中所述，回送一个HTTP 204 OK作为 对<lib:Federation TerminationNotification>的响应。

5.7 安全考虑

在[Liberty-BindProf]第4章中能找到应用于本部分的相同的安全考虑事项。若需要SSL/TLS，则应遵照[OWSRSpec]7.1.2.1小节。此版本的网络身份规范所基于的规范：[Liberty-ProtSchema]和[Liberty-BindProf]并没有定义对SOAP消息级安全的使用。但是当需要SOAP消息级安全时，宜遵循[OWSRSpec7.1.2.2。当使用XML签名时，应遵循[OWSRSpec]7.1.2.3.1小节和[Liberty-ProtSchema]3.1节。当使用XML加密时，应遵循[OWSRSpec]7.1.2.3.2小节。

附 录 A
（规范性附录）
静态的一致性需求

本附录中使用的符号在[CREQ]中有详细说明。

A.1 IdP

表 A.1 1 IdP 的 SCR

条 目	功 能	参考标准	状 态	要 求
NI-IDP-001	公共域 Cookie 介绍协议	5.1	O	
NI-IDP-002	单点登录和联合	5.2	M	NI-IDP-003 AND NI-IDP-005 AND NI-IDP-023
NI-IDP-003	浏览器要求	5.2.1	O	OWSER-All-002
NI-IDP-004	浏览器 POST 要求	5.2.2	O	
NI-IDP-005	LECP 要求	5.2.3	O	OWSER-All-002
NI-IDP-007	IdP 发起的名字注册	5.3.1	O	
NI-IDP-008	SP 发起的名字注册	5.3.1	M	NI-IDP-010
NI-IDP-009	基于 HTTP 重定向的名字注册	5.3.1.1.1	O	
NI-IDP-010	基于 SOAP 的名字注册	5.3.1.1.2	M	OWSER-All-002
NI-IDP-011	认证上下文分类	5.4	O	
NI-IDP-012	单点退出	5.5	M	NI-IDP-013 AND NI-IDP-014
NI-IDP-013	IdP 发起的单点退出	5.5.1	O	NI-IDP-017
NI-IDP-014	SP 发起的单点退出	5.5.2	O	NI-IDP-017
NI-IDP-015	基于 HTTP 重定向的单点退出	5.5.1.1 5.5.2.1	O	
NI-IDP-016	基于 HTTP GET 的单点退出	5.5.1.2	O	
NI-IDP-017	基于 SOAP 的单点退出	5.5.1.3 5.5.2.2	O	OWSER-All-002
NI-IDP-018	联合终止通告	5.6	M	NI-IDP-019 AND NI-IDP-020
NI-IDP-019	IdP 发起的联合终止通告	5.6.1	O	NI-IDP-022
NI-IDP-020	SP 发起的联合终止通告	5.6.1	O	NI-IDP-022
NI-IDP-021	基于 HTTP 重定向的联合终止通告	5.6.1.1.1 5.6.1.2.1	O	
NI-IDP-022	基于 SOAP 的联合终止通告	5.6.1.1.2 5.6.1.2.2	O	OWSER-All-002
NI-IDP-023	从属	5.2.4	M	
NI-IDP-024	IdP 的动态代理	5.2.5	M	

A.2 SP

表 A.2 SP 的 SCR

条 目	功 能	参考标准	状 态	要 求
NI-SP-001	公共域 Cookie 介绍协议	5.1	O	
NI-SP-002	单点登录和联合	5.2	M	NI-SP-003 AND NI-SP-005 AND NI-SP-023
NI-SP-003	浏览器要求	5.2.1	O	OWSER-All-002
NI-SP-004	浏览器 POST 要求	5.2.2	O	
NI-SP-005	LECP 要求	5.2.3	O	OWSER-All-002
NI-SP-007	IdP 发起的名字注册	5.3.1	M	NI-SP-010
NI-SP-008	SP 发起的名字注册	5.3.1	O	
NI-SP-009	基于 HTTP 重定向的名字注册	5.3.1.1.1	O	
NI-SP-010	基于 SOAP 的名字注册	5.3.1.1.2	M	OWSER-All-002
NI-SP-011	认证上下文分类	5.4	O	
NI-SP-012	单点退出	5.5	M	NI-SP-013 AND NI-SP-014
NI-SP-013	IdP 发起的单点退出	5.5.1	O	NI-SP-017
NI-SP-014	SP 发起的单点退出	5.5.2	O	NI-SP-017
NI-SP-015	基于 HTTP 重定向的单点退出	5.5.1.1 5.5.2.1	O	
NI-SP-016	基于 HTTP GET 的单点退出	5.5.1.2	O	
NI-SP-017	基于 SOAP 的单点退出	5.5.1.3 5.5.2.2	O	OWSER-All-002
NI-SP-018	联合终止通告	5.6	M	NI-SP-019 AND NI-SP-020
NI-SP-019	IdP 发起的联合终止通告	5.6.1	O	NI-SP-022
NI-SP-020	SP 发起的联合终止通告	5.6.1	O	NI-SP-022
NI-SP-021	基于 HTTP 重定向的联合终止通告	5.6.1.1.1 5.6.1.2.1	O	
NI-SP-022	基于 SOAP 的联合终止通告	5.6.1.1.2 5.6.1.2.2	O	OWSER-All-002
NI-SP-023	从属	5.2.4	M	
NI-SP-024	IdP 的动态代理	5.2.5	O	

A.3 LECP

表 A.3 LECP 的 SCR

条 目	功 能	功 能	参 考	状 态
NI-LECP-001	单点登录和联合	5.2	M	NI-LECP-002
NI-LECP-002	LECP 要求	5.2.3	O	OWSER-All-002

附 录 B
（资料性附录）
服务提供商和身份提供商的消息交换

本部分所描述的网络身份协议和规范，包括服务提供商（SP）和身份提供商(IdP)之间的交换。本附录将对其中的一些交换作图解说明。本部分是非标准化的且仅以说明为目的。

图B.1对服务提供商（SP）和身份提供商(IdP)之间普通的消息交换作了简要说明。SP给IdP发送一个请求消息（图1中的消息1），IdP给SP回送一个响应消息（图1中的消息2）。

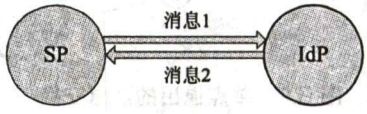


图 B.1 SP 与 IdP 之间普通的消息交换

本附录的其余部分，将把本部分中的部分协议和规范与消息1和消息2作匹配。

B.1 身份联合

如5.2节所述，身份联合是将终端用户的某一明确的服务提供商与身份提供商处的帐号连接起来的方法。服务提供商给身份提供商发送一个<lib:AuthnRequest>消息，身份提供商将响应给服务提供商一个<lib:AuthnResponse>消息。在5.2.3小节所述的支持Liberty的客户端/代理规范中，支持Liberty的客户端/代理给身份提供商发送<lib:AuthnRequest>消息，身份提供商回送<lib:AuthnResponse>消息作为响应。这些消息正确的实例化促成了身份联合。

B.2 单点登录

如5.2节所述，单点登录是指用户在某身份提供商处一次登录后，能够继续访问服务提供商（与该身份提供商有信任关系）处资源。单点登录建立在身份联合基础上。

在5.2.1所述的浏览器结果规范中，为了解析结果得到认证断言，服务提供商给身份提供商发送<samlp:Request>消息，身份提供商相应地回送给服务提供商<samlp:Response>消息。

在5.2.3小节所述的支持Liberty的客户端/代理规范中，支持Liberty的客户端/代理给身份提供商发送<lib:AuthnRequest>消息，然后身份提供商回复给服务提供商<lib:AuthnResponse>消息。

B.3 名字注册

5.3小节描述了名字注册。在身份联合时，身份服务者产生一个充当名字标识符的不透明句柄，服务提供商和身份提供商在相互交流时，使用涉及到的主体均使用名字标识符来标识。此名字标识符的术语是IdP提供者名字标识符。在联合后的任何时候，服务提供商或身份提供商都可为一个主体注册一个新的名字标识符。为此目的使用的协议是名字注册协议。

当服务提供商想要为主体注册一个新的名字标识符时，服务提供商将发起与身份提供商的交互。类似地，当身份提供商想要为主体注册一个新的名字标识符时，身份提供商将发起与服务提供商的交互。

B.4 单点退出

如图B.2中所示，身份提供商(IdP)给用户需要退出的每一个服务提供商发送<lib:LogoutRequest>消息，然后，服务提供商(SP1, SP2) 给该身份提供商回送<lib:LogoutResponse>消息。

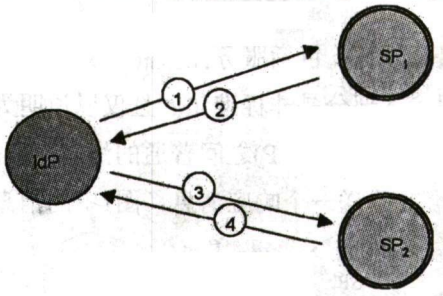


图 B.2 单点退出的消息交换

B.5 联合终止

图B.3说明了对由身份提供商发起的联盟合终止的消息交换。如5.6所述，主体终止服务提供商和身份提供商之间的身份联盟时，将使用联盟终止协议。

图 B.3 联合终止消息交换

附 录 C
（资料性附录）
规范图解

本附录的目的是阐明本部分的第5章所详细说明的各种规范的使用。

C.1 身份联合和单点登录规范

本节将图解说明5.2节中所详细说明的身份联合和单点登录的三个规范：

—— 浏览器要求；

—— 浏览器 POST；

—— 支持 Liberty 的客户端/代理。

C.1.1 浏览器规范

图C.1是[Liberty-BindProf]中的图2，它用来图解说明浏览器规范。服务提供商和身份提供商之间的<samlp:Request>和<samlp:Response>消息流（消息8和消息9中）使用SOAP over HTTP。

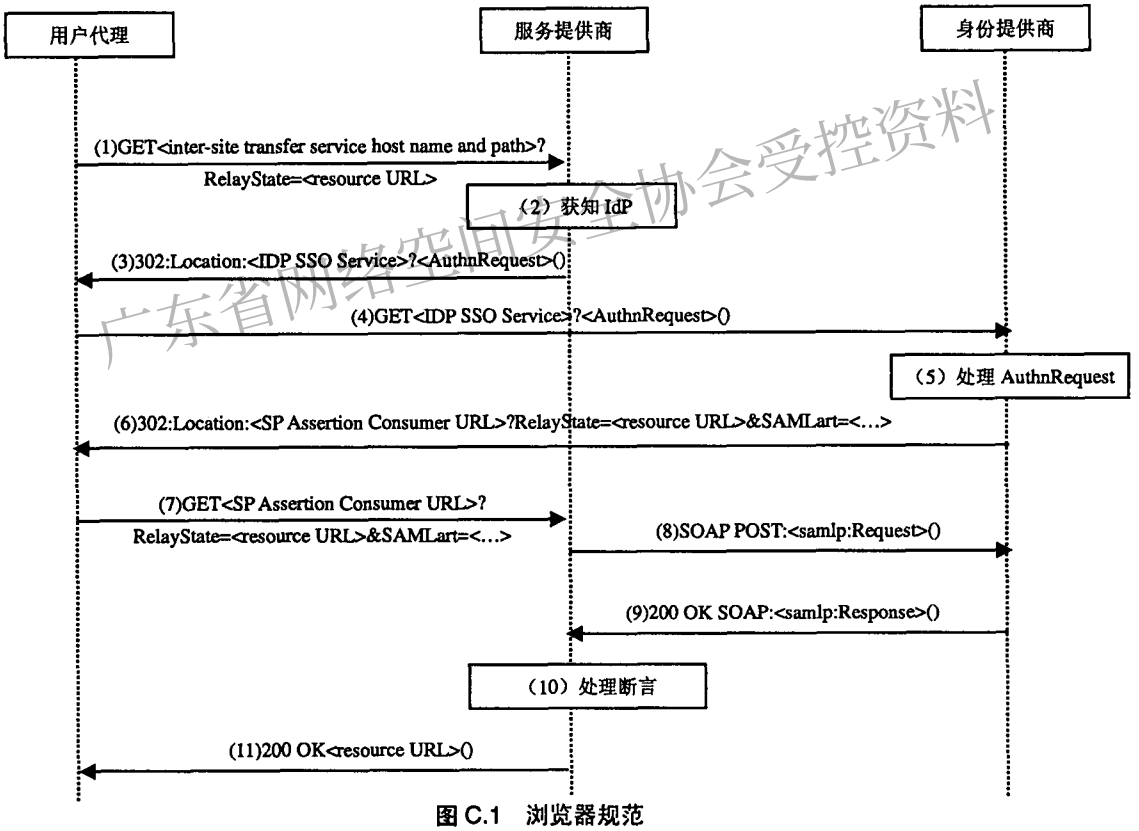


图 C.1 浏览器规范

C.1.2 浏览器POST要求

图C.2是[Liberty-BindProf]中的图3，它图解说明了浏览器POST要求。

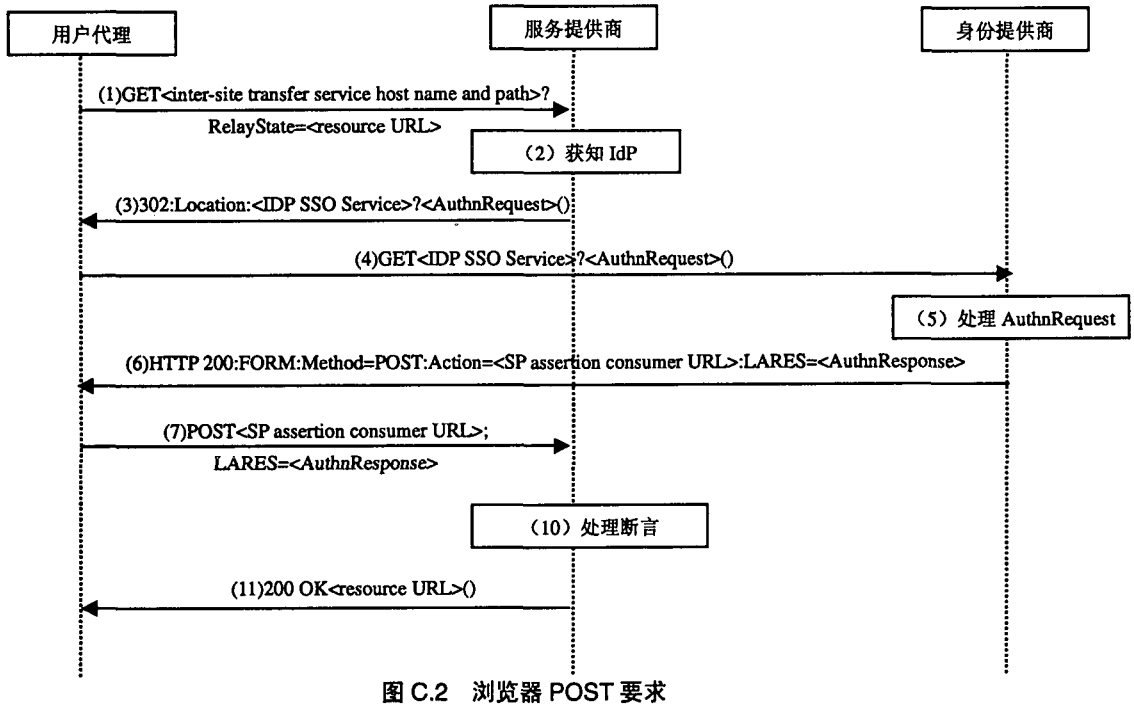


图 C.2　浏览器 POST 要求

C.1.3　支持Liberty的客户端/代理要求

支持Liberty的客户端和代理已经具有或知道如何得到身份提供商(IdP)的信息，主体欲使用该信息与服务提供商(SP)交互。SP需要知道它所交互的客户端是一个LECP，以便于将确定IdP的工作交给客户端。因为客户端使用HTTP协议与SP相交互，所以包含了适当的HTTP头。此HTTP头将该客户端是LECP的信息传达给SP，这样确定IdP的任务留给了LECP。或者用备选方法：LECP可使用User-Agent头来将该客户端是LECP的信息传达给SP。[Liberty-BindProf]3.2.5.1小节详细说明了User-Agent头的使用方法。图6中的消息1包含了这个User-Agent头。下图基于[Liberty-BindProf]中的图C.3绘制。

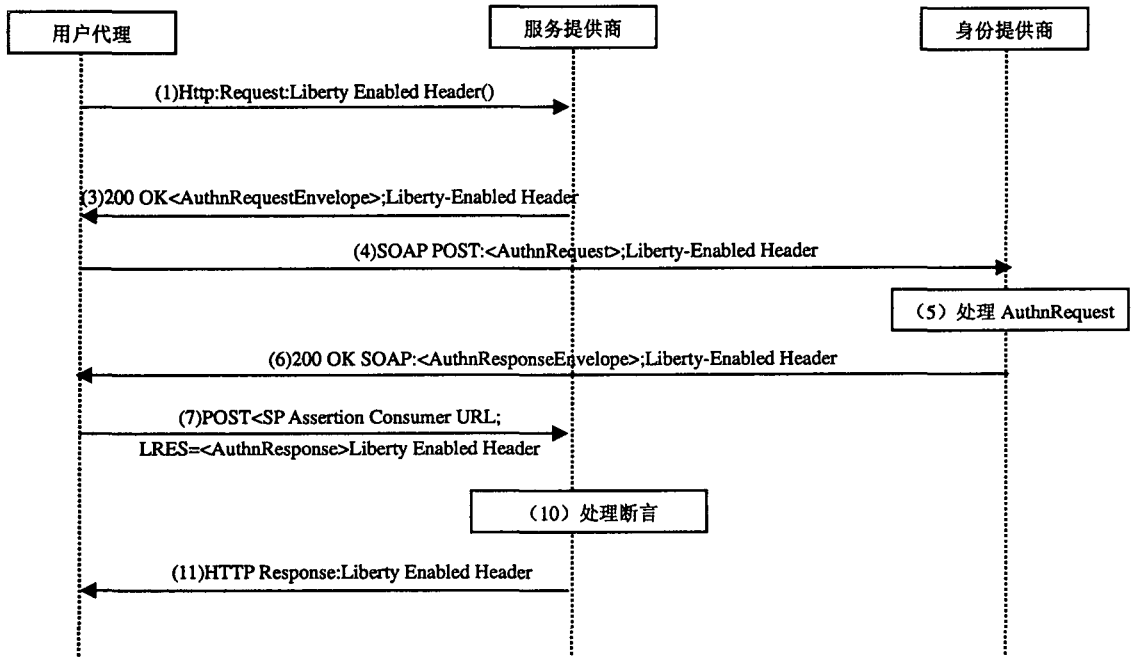


图 C.3　支持 Liberty 的客户端/代理要求

[Liberty-BindProf]的3.2.5.2小节描述了图6的消息流。LECP和IdP之间<lib:AuthnRequest>和<lib:AuthnResponse>消息流（消息4和消息5中）使用SOAP over HTTP。

C.2 名字注册要求

本节将图解说明5.3节中所述的名字注册的两个要求：

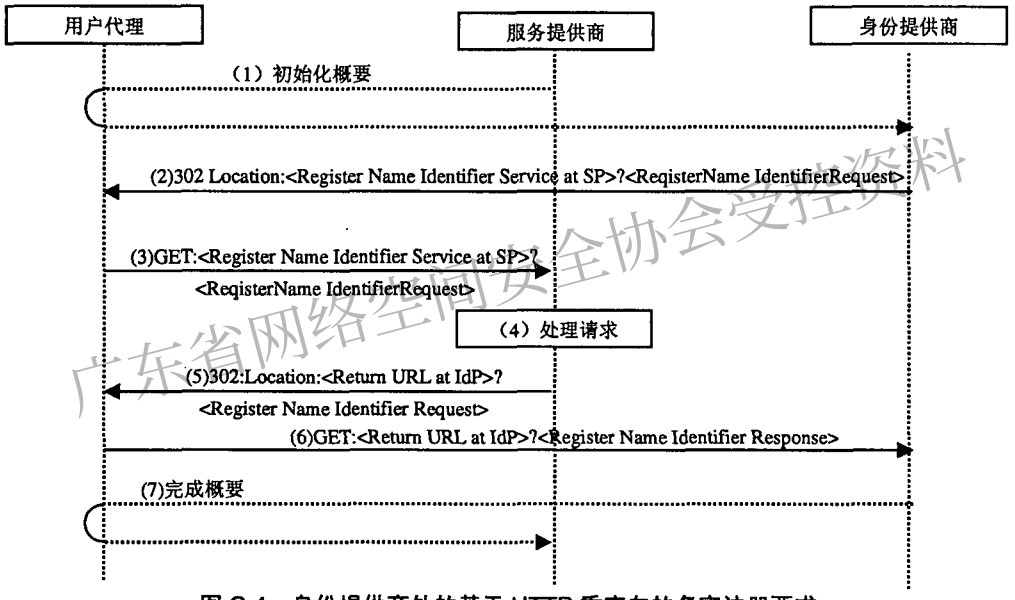
—— 基于HTTP重定向；

—— 基于SOAP/HTTP。

名字注册可在服务提供商处发起，也可在身份提供商处发起。

C.2.1 基于HTTP重定向要求

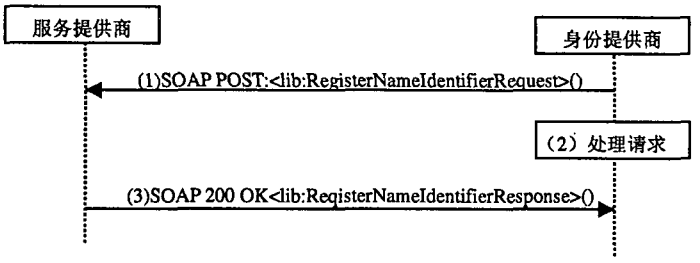
图C.4是[Liberty-BindProf]中的图6，在这里是用来图解说明由身份提供商发起的基于HTTP重定向的名字注册的要求。如图C.4所示，<lib:RegisterNameIdentifierRequest>由身份提供商发起并且发送给服务提供商（消息2和消息3），然后服务提供商给身份提供商回送<lib:RegisterNameIdentifierResponse>消息作为响应（消息5和消息6）。



图C.4 身份提供商处的基于HTTP重定向的名字注册要求

C.2.2 基于SOAP/HTTP要求

图C.5是[Liberty-BindProf]中的图7，用于图解说明由身份提供商发起的基于SOAP的名字注册的要求。如图C.5所示，<lib:RegisterNameIdentifierRequest>由身份提供商发起并且发送给服务提供商（消息1），然后服务提供商给身份提供商回送<lib:RegisterNameIdentifierResponse>消息作为响应（消息3）。消息1和消息3使用 SOAP over HTTP。



图C.5 身份提供商处的基于SOAP的名字注册要求

C.3 单点退出要求

本节将图解说明5.5节中所述的单点退出的两个要求：

—— 基于 HTTP 重定向；

—— 基于 SOAP/HTTP。

单点退出可在服务提供商处发起，也可在身份提供商处发起。

C.3.1 基于HTTP重定向要求

图C.6是[Liberty-BindProf]中的图10，它图解说明了由身份提供商发起的基于HTTP重定向的单点退出要求。

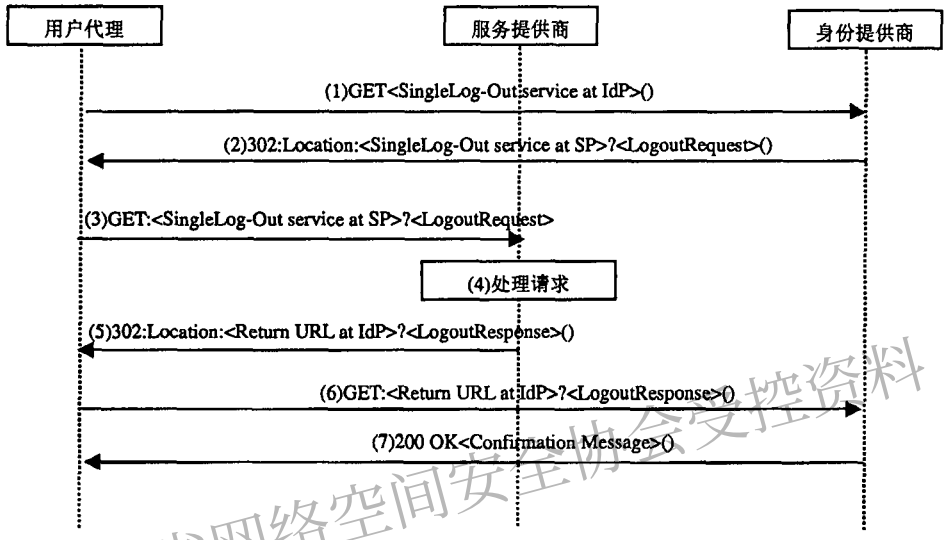


图 C.6 身份提供商发起的基于 HTTP 重定向的单点退出要求

图C.7是[Liberty-BindProf]中的图13，说明了由服务提供商发起的基于HTTP重定向的单点退出要求。

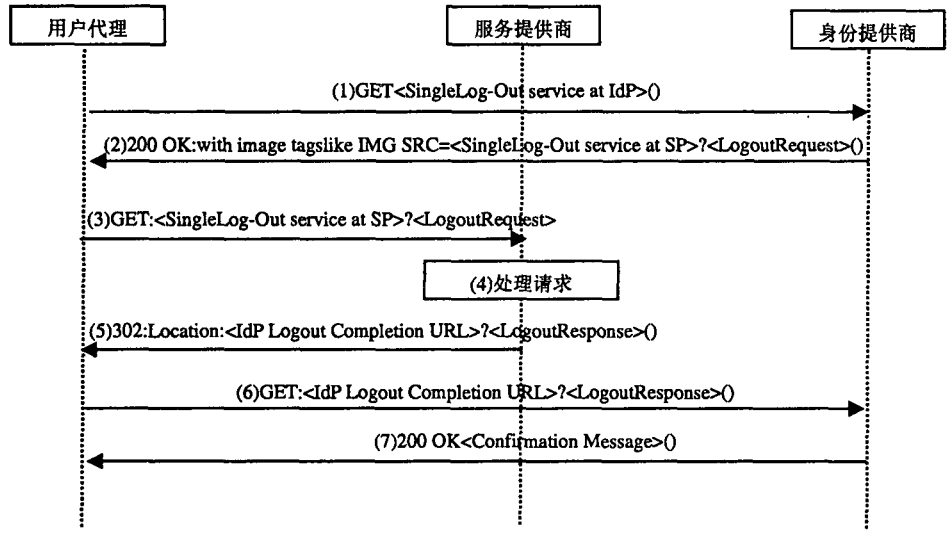


图 C.7 服务提供商发起的基于 HTTP 重定向的单点退出要求

C.3.2 HTTP GET要求

图C.8是[Liberty-BindProf]中的图11，说明由身份提供商发起的基于HTTP-GET的单点退出要求。

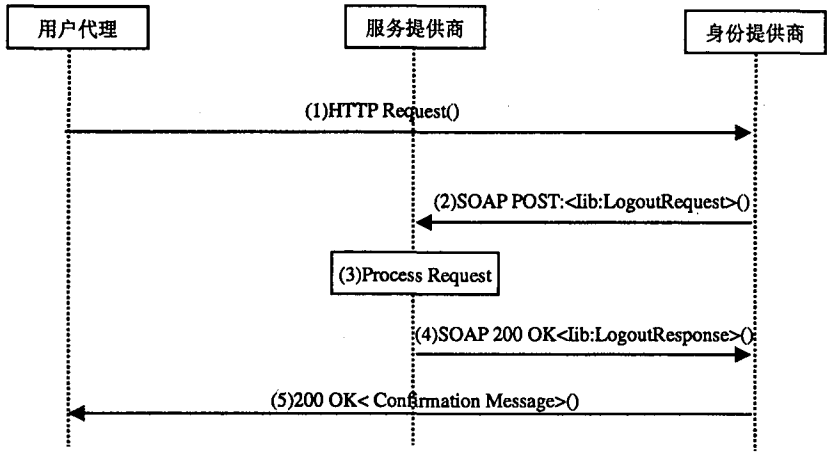


图 C.8　身份提供商发起的基于 HTTP-GET 的单点退出要求

C.3.3　基于SOAP/HTTP要求

图C.9是[Liberty-BindProf]中的图12，说明由身份提供商发起的基于SOAP/HTTP的单点退出要求。

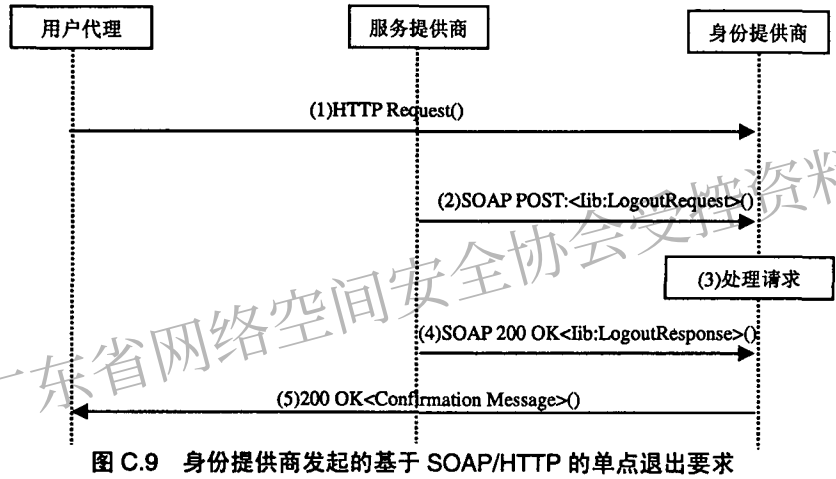


图 C.9　身份提供商发起的基于 SOAP/HTTP 的单点退出要求

图C.10是[Liberty-BindProf]中的图14，说明由服务提供商发起的基于SOAP/HTTP的单点退出要求。

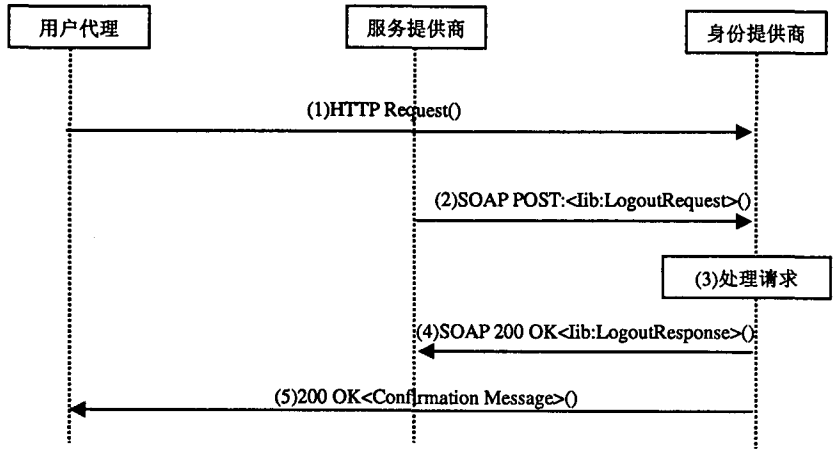


图 C.10　服务提供商发起的基于 SOAP/HTTP 的单点退出要求

C.4　联合终止要求

本节将图解说明5.6节中所述的联合终止的两个要求：

—— 基于 HTTP 重定向；

—— 基于 SOAP/HTTP。

联合终止可在服务提供商处发起，也可在身份提供商处发起。

C.4.1 基于HTTP重定向要求

图C.11是[Liberty-BindProf]中的图8，说明由身份提供商发起的基于HTTP重定向的联合终止要求。

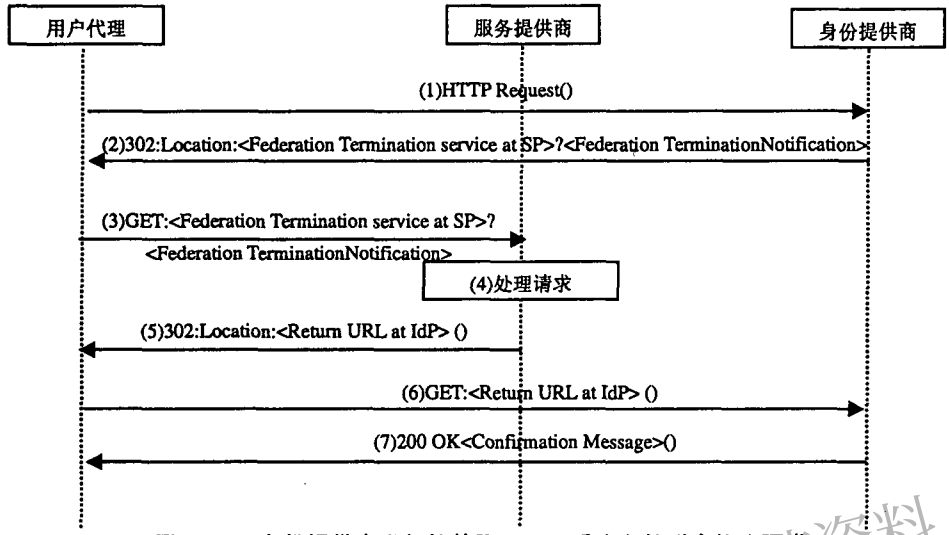


图 C.11 身份提供商发起的基于 HTTP 重定向的联合终止要求

C.4.2 基于SOAP/HTTP要求

图C.12是[Liberty-BindProf]中的图9，说明由身份提供商发起的基于SOAP/HTTP的联合终止要求。

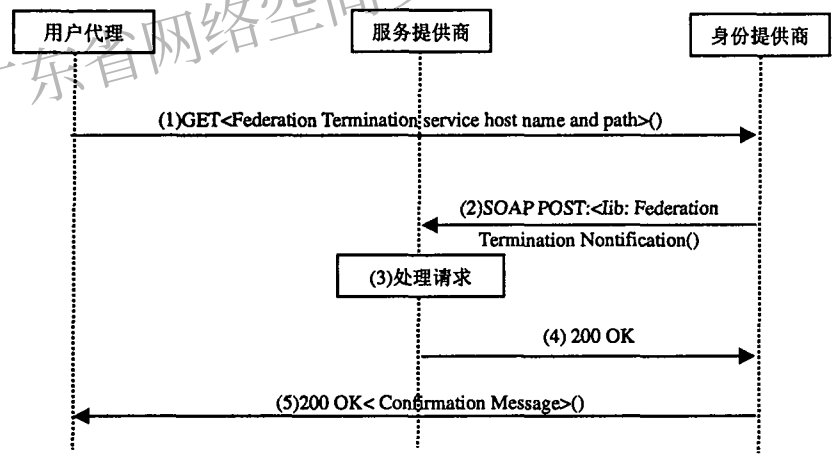


图 C.12 身份提供商发起的基于 SOAP/HTTP 的联合终止要求

参 考 文 献

[1]Liberty-Glossary (2003)	Liberty Architecture Glossary
[2]Liberty-Overview(2003)	Liberty Architecture Overview
[3]OMA SESWP	OMA Service Enabler Strategy White Pap
[4]OMA OWSER NI FF（2006）	OMA Web Services Network Identity Enabler (OWSER NI): Identity Federation Framework
[5]OMA OWSER NI WSF (2006)	OMA Web Services Network Identity Enabler(OWSER NI): Identity Web Services Framework:
[6]OMA OWSER NI AD(2006)	OMA Web Services Network Identity Enabler(OWSER NI): Architect
[7]OMA Dictionary（2004）	Dictionary for OMA Specifications
[8]IETF RFC2828(2000)	Internet Security Glossary
[9]3GPP-TR21.905	3G Vocabulary
[10]OMA IOPPROC	OMA Interoperability Policy and Process
[11]Liberty-ProtSchema（2003）	Liberty Protocols and Schema Specification
[12]Liberty-AuthnContext（2003）	Liberty Authentication Context Specification
[13]OMA OWSRSpec	OMA Web Services Enabler (OWSER): Core Specifications
[14]IETF RFC2119 (1997)	Key words for use in RFCs to Indicate Requirement Levels
[15]Oasis SAMLCore（2002）	Assertions and Protocol for the Oasis Security and Assertions Markup Language (SAML)
[16]Oasis SAMLBind（2002）	Bindings and Profiles for the Oasis Security and Assertions Markup Language (SAML)

中华人民共和国
通信行业标准
移动Web服务网络身份认证技术要求
第3部分：网络身份联合框架
YD/T 2127.3-2010
*
人民邮电出版社出版发行
北京市崇文区夕照寺街14号A座
邮政编码：100061
*