ICS 33.030
M 21

YD

中华人民共和国通信行业标准

YD/T 2127.2-2010

移动 Web 服务网络身份认证技术要求 第 2 部分：网络身份 Web 服务框架

Technical requirements for mobile Web services network identity authentication
Part 2：Network identity Web service 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
4.1　无 OWSER 网络身份的 OWSER 核心 Web 服务……2
4.2　使用网络身份的 Web 服务……3
5　功能元素的描述……6
5.1　服务提供商……6
5.2　身份提供商……6
5.3　发现服务……6
5.4　属性提供商……7
6　流程描述……7
6.1　属性查询……7
6.2　属性修改……9
6.3　使用指导……10
6.4　交互服务……11
6.5　基于Web服务框架的引导身份……12
6.6　发现服务……12
6.7　用户代理和设备(LUAD)……15
6.8　安全……16
参考文献……18

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2部分。

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 2 部分：网络身份 Web 服务框架

1 范围

本部分规定了基于移动Web服务网络身份的Web服务框架，规定了在不同环境下，多种可移动设备（如移动电话、PDA、掌上电脑等）与Web服务提供商、属性提供商之间进行数据和信息交换的功能体和交互流程。

本部分适用于网络身份Web服务框架的要求，包括为了实现该框架的终端与服务提供商、属性提供商间的数据交流的方法和流程。

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标部分。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。

ID-FF(2003)	自由ID-FF架构概述Liberty ID-FF Architecture Overview
ID-WSF（2004）	自由ID-WSF网络服务框架概述Liberty ID-WSF Web Service Framework Overview, Version 1.0
Liberty-ID-WSF-DST (2005)	自由ID-WSF数据服务模板规范Liberty ID-WSF Data Services Template Specification
OMA OWSER NI AD (2006)	OMA Web服务网络身份引擎：架构OMA Web Services Network Identity Enabler (OWSER NI): Architecture

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

数据服务模板 Data Service Template

见ID-WSF数据服务模板。

3.1.2

自由激活的用户代理和设备 Liberty Enabled User and Devices

指发送或使用ID-WSF（或ID-FF）规范声明的协议消息的用户代理和设备。LUAD的定义特性在于，它与某个用户（或一些用户，比如一个家庭）“紧密相连”。

3.1.3

资源参考 Resource Offering

资源与服务实例的结合。这种结合是必需的，因为资源与服务实例之间存在“多对多”的关系。一个单独的服务实例可能为多个资源服务。比如，概要都有一个个单独的协议终止点，服务提供商可能在一个单一的服务实例背后提供许多概要。

3.1.4

服务实例　Service Instance

在协议终止点运行的Web服务。

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。

3.2　缩略语

AP	Attribute Provider	属性提供商
IdP	Identity Provider	身份提供商
ID-FF	Identity Federation Framework	身份联合框架
ID-WSF	Identity Web Services Framework	身份Web服务框架
IS	Interaction Service	交互服务
NI	Network Identity	网络身份
OMA	Open Mobile Alliance	开放移动联盟
OSE	OMA Service Environment	OMA服务环境
OWSER	OMA Web Services Enabler Release	OMA Web服务Enabler
SASL	Simple Authentication and Security Layer	简单认证和安全层
SP	Service Provider	服务提供商
WSC	Web Service Consumer	Web服务消费者
WSP	Web Service Provider	Web服务提供商
WSR	Web Service Requester	Web服务请求者

4　概述

4.1　无 OWSER 网络身份的 OWSER 核心 Web 服务

本部分定义了在Web服务请求者和Web服务提供商之间的交互过程中所使用的标准协议，该协议包括一个XML消息信封（SOAP）、一个Web服务注册访问协议（UDDI），以及将安全令牌封装为SOAP消息信封中的头元素的机制（参见OASIS Web Services. Security）。

图1说明了没有网络身份协议和服务时，由此部分规范支持的Web服务交互过程。

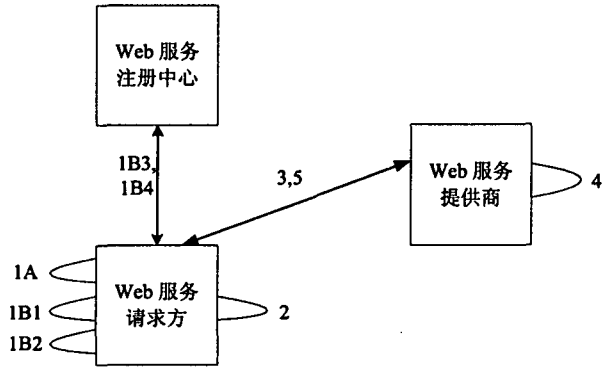

图 1　无网络身份协议和服务时，Web 服务交互流程

执行流程如下：

a）Web 服务请求者决定如何确定 Web 服务提供商的位置，以及如何与其交互。

1）Web 服务请求者使用带外（out-of-band）信息，比如本地配置信息，来识别某个特定的 Web 服务提供商。

2）Web 服务请求者使用 Web 服务注册中心（Web Service Registry）来定位提供所需服务的 Web 服务提供商。

——Web 服务请求者使用带外信息，比如本地配置信息，来识别某个特定的 Web 服务注册中心；

——Web 服务请求者生成一个 UDDI 查询消息；

——Web 服务请求者把这个查询消息发给注册中心；

——Web 服务注册中心返回一个响应消息，该消息所包含的信息使得 Web 服务请求者得以对提供所需服务的 Web 服务提供商进行定位，并与之通信。

b）Web 服务请求者生成一个用 WSDL 描述的符合 SOAP/HTTP 内容描述的消息，根据此核心规范在 SOAP 头中嵌入一个安全令牌以生成请求者的身份和证书。

c）Web 服务请求者把消息发送给 Web 服务提供商。

d）Web 服务提供商接收消息，分析后处理安全头中的安全令牌以对用户进行认证，执行其功能并生成包含属性信息的响应消息。

e）发送响应消息给 Web 服务请求者。

为了描述方便，上文的例子经过了简化，并未包含加密、签名、代理和此核心规范包含的其他元素或功能。

4.2 使用网络身份的 Web 服务

4.2.1 概述

本部分基于自由联盟身份联合框架（ID-FF）提出的网络身份（Network Identity）的概念。自由联盟身份联合框架定义了一个明确的服务提供商即身份提供商（Identity Provider）以及相关协议（身份联合、名字注册等），它们共同实现在一个信任圈内跨越多个服务提供商的对联合用户身份的管理，同时允许用户管理和控制身份。这些身份可以让它们在任一个服务提供商处都能被识别，从而在跨越多个服务提供商之间的多个独立的交互中保护用户的隐私数据，属性提供商可以对服务提供商的属性查询请求进行安全认证，用于对用户或对其他用户的属性查询进行隐私保护。本网络身份规范还定义了单点登录服务，它融合了身份联合，允许基于web的应用服务提供商和用户在一个信任圈内的多个这种服务提供商处，通过在一个信任团体（身份提供商）共享一个认证事件来进行身份认证。

本部分以下所述为基础并增加额外的机制，基于自由联盟身份Web服务框架，符合OMA OWSER Core规范，后者在WSR和WSP的Web服务交互中使用联合身份和单点登录，并提供自由联盟激活的Web服务环境中以隐私受保护的方式对用户身份属性进行无缝接入和切换。本规范定义了一类Web服务提供商、一个属性提供商，以及相关的用来管理访问用户身份属性（在用户允许的前提下）的协议。另有一个单独的属性提供商，即ID-WSF发现服务，它使属性提供商们的一个Web服务请求者能够运行发现进程，这些属性提供商能够在用户允许的前提下提供与某个特定用户相关的身份属性，并可以提供断言，Web服务提供商在与这些属性提供商的后续Web服务交互中可使用这些断言。

4.2.2 访问用户的身份属性

图2说明了在一个AP处访问用户的身份属性所需的交互过程。

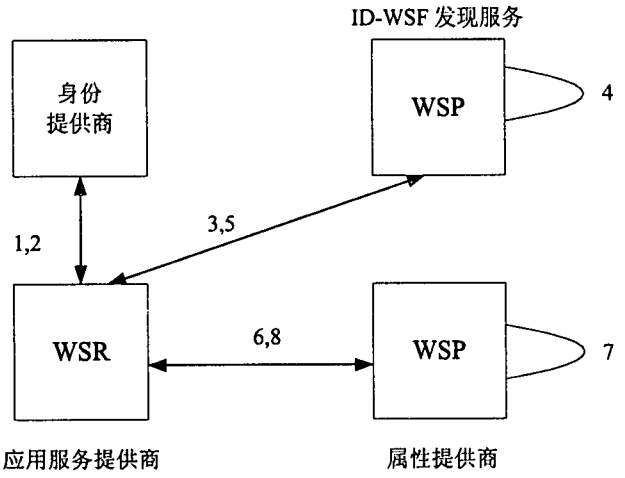

图 2　属性运营商处访问用户身份属性所需的交互

执行流程如下：

a）WSR 向 IdP 发起一个 ID-FF 认证请求，请求对用户的 SAML 断言进行认证。ID-FF 认证请求使用对应用客户端的重定向，具体细节见 OMA OWSER NI AD (2006)，本部分不再赘述。

b）IdP 对用户的 SAML 断言进行认证，当认证通过时，向 WSR 返回用户的 SAML 断言认证通过结果和用户的 ID-WSF 发现服务的资源参考，当认证不通过时，向 WSR 返回用户的 SAML 断言认证不通过的结果。

c）WSR 根据 IdP 提供的资源参考请求对应的 ID-WSF 发现服务提供属性提供商的资源参考，同时将用户的 SAML 断言发送到 ID-WSF 发现服务。

d）ID-WSF 发现服务将收到的用户的 SAML 断言发送到 IdP 进行认证，根据 IdP 所返回的认证结果生成一个响应消息，当认证结果为通过时，响应消息包含用户的 SAML 断言认证结果和 WSR 所需属性提供商的资源参考；当认证结果为不通过时，响应消息包含用户的 SAML 断言认证结果。

e）ID-WSF 发现服务把上述响应消息发给 WSR。

f）WSR 使用 ID-WSF 提供的资源参考，将用户的 SAML 断言发往对应的属性提供商，并向其请求所需的属性信息。

g）属性提供商将收到的用户的 SAML 断言发送到 IdP 进行认证，根据 IdP 所返回的认证结果生成一个响应消息，当认证结果为通过时，响应消息包含用户的 SAML 断言认证结果和 WSR 所需属性；当认证结果为不通过时，响应消息包含用户的 SAML 断言认证结果。

h）属性提供商把上述响应消息发给 WSR。

为了描述方便，本例进行了简化，并未反映加密、签名、代理以及其他Liberty规范所包含的其他元素。

4.2.3　基于 Web 服务环境中的单点登录

IdP可以通过支持ID-WSF认证服务和ID-WSF单点登录服务（ID-WSF Single Sign-on Service），来给WSR提供单点登录服务。注意WSR不能直接使用本规范单点登录服务，因为那是给基于浏览器的环境的。在基于浏览器的环境中，对服务提供商（Service Provider，SP）的单点登录是通过认证请求的浏览器重定向来实现的。

如果没有浏览器重定向，WSR直接在IdP处认证，并把这次认证事件的结果，传达给信任圈中与它交互的任一SP（WSP）。IdP接收用户携带终端标识的的认证请求，根据标识对终端进行认证，并向用户返回终端认证响应。IdP必须支持Liberty ID-WSF认证服务，这种服务使用标准的SASL协议来完成认证交互。

认证结果包括一个给ID-WSF单点登录服务（SSOS）的资源参考。然后WSR与SSOS进行交互，来获取与信任圈中任一WSP相交互时可使用的证书。与SSOS交互中的认证请求/响应消息，与基于浏览器的SSO中的信息完全相同，不同的只是封装协议和传送机制。

对于自由联盟激活的WSR，一个可选项是主体属性的发现服务（Discovery Serivce，DS），也就是SSOS把指定WSP的资源参考返回给那里。这个DS反过来也应能够为某特定属性资源的WSP提供资源参考。

在与访问用户身份属性无关的交互中，ID-WSF认证服务和SSOS对任意WSR都可用。

这一方案通过使用特定WSP处有效的匿名或者假名等标识符来继续保护用户的隐私信息。这些识别符是在身份联合的时候设定的。

认证服务和SSOS的使用见图3。

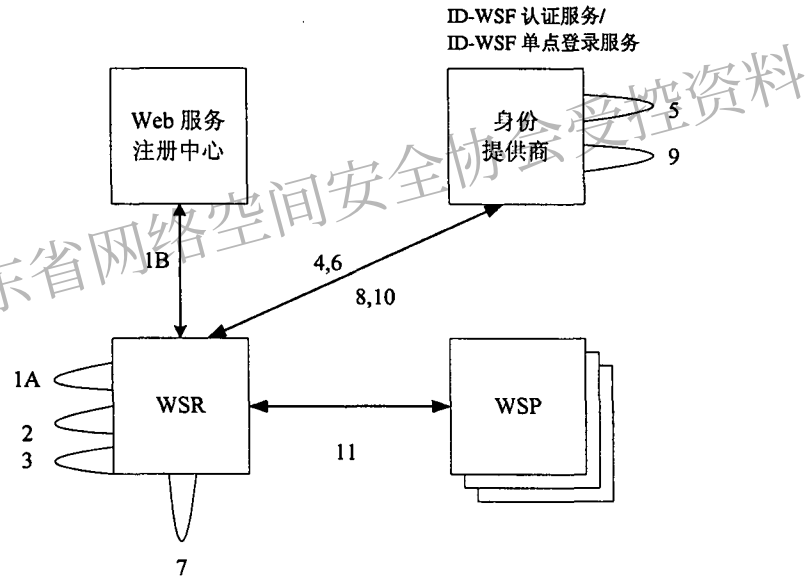

图 3　SSOS 与认证服务

执行流程如下：

a）WSR 决定如何定位一个 WSP 以及如何与其交互。

1）1A Web 服务请求者使用带外信息（out-of-band information），如本地配置信息，来识别特定的 WSP；

2）1B WSR 使用 Web 服务注册中心来对提供所需服务的 WSP 进行定位；

3）1B 中的交互细节与 4.2 中 1B 的交互细节相同，此处不再赘述。

b）WSR 使用带外信息，如本地配置信息，来识别 ID-WSF 认证服务。

c）WSR 根据需要生成一个 ID-WSF 认证服务请求（Authentication Service Request）来请求一个安全令牌（security token），使其能够在 ID-WSF SSOS 服务处通过认证。

d） WSR 把这个认证请求发送给 ID-WSF 认证服务。

e）ID-WSF 认证服务验证这个认证请求的合法性，并生成一个认证响应消息（Authentication Response），内容包括一个能使 WSR 在 ID-WSF SSOS 处通过认证的安全令牌。

f）ID-WSF 认证服务把这个认证响应发给 WSR。

g）WSR 生成 ID-WSF SSOS 请求，包含一个 SOAP 头和 SOAP 主体。前者含有从 ID-WSF 认证服务处获得的安全令牌，后者包含一个 ID-FF 认证请求。

h）WSR 向 ID-WSF SSOS 发送请求，获取允许其与 WSP 交互的断言。

i）ID-WSF SSOS 验证收到请求的合法性，生成一个含有 ID-FF 认证响应的 SOAP 响应消息。

j）ID-WSF SSOS 把响应消息发送给 WSR。

k）WSR 向 WSP 发送请求并接收响应。

这一步交互的细节与 4.1 节中的 b—e 步相同，此处不作赘述。

为了描述方便，本例进行了简化，并未反映如加密、签名、代理等 Liberty 规范包含的元素。

5 功能元素的描述

5.1 服务提供商

服务提供商是提供服务和（或）商品的实体。

服务提供商可以是Web服务请求者（Web Service Requestor，WSR），此时与其交互的属性提供商相当于Web服务提供商（Web Service Provider，WSP）。这种情况下，当服务提供商接收到用户发送的属性查询请求后，服务提供商可以使用属性查询（Attribute Query）机制来向属性提供商请求属性。当属性提供商收到用户使用<Query>元素进行属性查询的请求时，消息中包含一个<UsageDirective>头来携带终端标识和指示处理属性的策略，属性提供商根据其标识信息向用户查询请求进行响应。服务提供商也可以使用属性修改机制在属性提供商处对某个主体的属性进行修改。

如果服务提供商位于自由用户代理和设备（Liberty User Agent and Device,LUAD）内，那么它也可以充当LUAD Web服务消费者（Web Service Consumer，WSC）的角色。

服务提供商也是一个从属服务商（affiliation）。

5.2 身份提供商

身份提供商是“一种特殊的服务提供商，它生成、维护和管理主体的身份信息，并且能够为某认证域（甚至信任圈）中的其他服务提供商或主体提供认证断言以及访问主体发现服务所需的引导信息”。

只有当在服务提供商和身份提供商之间发生了某个确定主体的身份联合后，这个主体才可能使用单点登录。

5.3 发现服务

发现服务允许请求者发现资源参考。

当服务提供商想要确定究竟是哪个（或者哪些）属性提供商主管着所需资源时，它根据所获取的引导信息当中所包含的访问权限和信息与发现服务（Discovery Service ，DS）联系，以获得所需资源的信息。发现服务给进行查询的服务提供商提供访问这个（或这些）属性提供商时所必需的证书，以确保服务提供商对这些属性的访问权限。

为了获得适当的资源参考，请求者需要在发现服务那里初始化一个发现查找（discovery lookup）进程。为了实现资源参考的插入、删除和修改，则需要在发现服务那里初始化发现更新（Discovery Update）进程。

5.4 属性提供商

属性提供商是一种特殊的服务提供商，其服务就是提供某个用户的属性。

属性提供商也可以作为Web服务提供商（Web Service Provider，WSP），此时与它交互的服务提供商作为Web服务请求者（Web Service Requester，WSR）。这种情况下，当服务提供商使用属性查询机制向属性提供商请求用户或其他用户属性时，属性提供商在用户有查询权限的情况下向用户返回属性信息。判断用户是否有权限查询依据查询方的身份标识与被查询方的相关属性访问权限列表比较的结果，属于该列表则为有权限查询。查询方可与被查询方协商认证来获得权限，被查询方可为查询方配置相关属性访问列表，保存在属性提供商设备中。当属性提供商使用<QueryResponse>元素对服务提供商进行响应时，它包含一个<UsageDirective>头来指示这些被发布的属性的后续使用策略。

属性提供商接收用户发送的携带用户当前使用的终端的标识的用户属性查询请求，该属性提供商根据终端标识获取终端属性，并将终端属性携带在属性查询响应消息中返回给终端。当服务提供商使用属性修改机制在属性提供商处修改某个主体的属性时，该属性提供商用一个修改响应消息进行反馈。

属性提供商所处的设备可能不支持HTTP服务器，可能无法与互联网连接或者在网络上无法寻址，在这种情况下，可以用PAOS机制来从属性提供商那里找回属性。

6 流程描述

6.1 属性查询

6.1.1 属性查询流程

服务提供商可使用自由数据服务模板（Data Service Template，DST）[Liberty-ID-WSF-DST]定义的机制来向属性提供商发起查询。在这种情况下，一个服务提供商应使用<Query>元素，且属性提供商在对服务提供者的响应中应使用<QueryResponse>元素。

[Liberty-ID-WSF-DST]中定义的DST元素并非仅仅用作消息。更重要的是DST提供了可在WSDL中实际使用的XML模板来实现查询/修改语法。

图4说明了消息的交互过程。

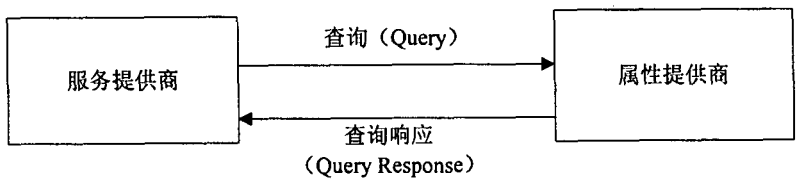

图 4 属性查询

<Query>元素的使用应遵循[Liberty-ID-WSF-DST]的3.2.1小节。<QueryResponse>元素的使用应遵循[Liberty-ID-WSF-DST]3.2.2小节。<Query>元素和<QueryResponse>元素的处理规则应遵循[Liberty-ID-WSF-DST]3.2.3小节。

下面，我们举一个<Query>元素的例子。其资源由资源ID http://OWSER-attributeprovider.com/u6gh8jlx90bt8h1o作为标识。这是对名字和家庭地址的查询：

```
<Query>
    <ResourceID>http://OWSER-attribute-provider.com/u6gh8jlx90bt8h1o</ResourceID>
    <QueryItem itemID="name">
        <Select>/pp:PP/pp:CommonName</Select>
    </QueryItem>
    <QueryItem itemID="home">
        <Select>/pp:PP/pp:AddressCard[pp:AddressType="urn:liberty: id-sis-pp:addrType:home"]</Select>
    </QueryItem>
</Query>
```

下面是一个用于响应上面<Query>请求的<QueryResponse>的例子。资源的公共名字返回值为Dr.Genie Wunderkid，另一个可选的公共名字为Dr.Genie Wunder。资源地址也已给出。

```
<QueryResponse>
    <Status code="OK"/>
    <Data itemIDRef="name">
        <CommonName>
            <CN>Genie Wunderkid</CN>
            <AnalyzedName nameScheme="firstlast">
                <FN>Genie</FN>
                <SN>Wunderkid</SN>
                <PersonalTitle>Dr.</PersonalTitle>
            </AnalyzedName>
            <AltCN>Genie Wunder</AltCN>
        </CommonName>
    </Data>
    <Data itemIDRef="home">
        <AddressCard id="9812">
            <AddressType>urn:liberty:id-sis-pp:addrType:home</AddressType>
            <Address>
                <PostalAddress>c/o Senthil Sengodan$12278 Scripps Summit Drive</PostalAddress>
                <PostalCode>92131-2341</PostalCode>
                <L>San Diego</L>
                <ST>ca</ST>
                <C>us</C>
            </Address>
        </AddressCard>
    </Data>
</QueryResponse>
```

服务提供商接收用户发送的携带用户当前使用终端的标识的用户属性查询请求后，可以首先向身份提供商发送携带该终端标识的身份认证请求，身份提供商对该标识对应的终端进行认证，并返回携带认证状态的认证响应。服务提供商根据终端的认证状态确定终端合法后，才根据该终端标识向属性提供商查询终端属性，属性提供商根据终端标识获取终端属性，并将终端属性携带在属性查询响应消息中返回给终端。如果认证响应中携带该终端对应用户的其他终端已登录的信息，则服务提供商可以通知其他终端退出，或自动断开其他终端的登录。

6.1.2 使用 PAOS 的属性查询

按照[Liberty-Paos]定义，属性查询可使用反向HTTP绑定SOAP。在这种情况下的处理程序应遵循[Liberty-Paos]中的定义。

反向HTTP绑定SOAP的应用场景举例如下：

— 由一个支持 HTTP 客户端，而不是 HTTP 服务器的设备提供属性提供商的功能。这可能是设备的资源受限时的应用场景。

— 由未接入到 Internet 或无法进行网络寻址的设备提供属性提供商功能。按照[Liberty-Paos]第 7 章中的定义，支持两种消息交互模式。

— 在请求－响应消息交互模式中，支持 PAOS 的用户代理发送一个 HTTP 请求到 HTTP 服务器，然后 HTTP 服务器在 HTTP 响应消息中发送 SOAP 请求。用户代理在第二个 HTTP 请求中发送 SOAP 响应。应遵循[Liberty-Paos]第 5 章中定义的处理程序来使用请求－响应消息交互模式。

— 在响应消息交互模式中，支持 PAOS 的用户代理发送一个 HTTP 请求到 HTTP 服务器，然后 HTTP 服务器在 HTTP 响应消息中发送 SOAP 响应。应遵循[Liberty-Paos]第 9 章中定义的处理程序来使用响应消息交互模式。请求—响应模式对于查询用户属性具有同样应用场景。例如在查询时需要携带查询方身份信息，响应中携带被查询方属性信息。

请求－响应消息交互模式举例如下：

一个移动设备中的用户代理发送一个HTTP请求到HTTP服务器去买某件商品。HTTP服务器在HTTP响应消息中，包括一个用来请求用户的信用卡号的SOAP请求。用户代理作为该信用卡号属性的属性提供商，发起一个新的HTTP请求给该HTTP服务器，此请求中含有包含信用卡号的SOAP响应消息，查询方身份信息。该HTTP将回复一个200OK消息。

响应消息交互模式举例如下：

一个用户希望选取消息通知服务来确认消息的成功传输。为了实现这一目的，用户代理发送一个HTTP请求到提供消息通知服务的HTTP服务器，查询消息传输确认。HTTP服务器发送HTTP响应，它包含SOAP响应消息，其中包含了消息传输确认的信息，查询到的属性信息。

6.2 属性修改

为了更改储存在属性提供商处的属性，服务提供商可使用由自由数据服务模板[Liberty-ID-WSF-DST]定义的机制。在这种情况下，服务提供商应使用<Modify>元素，且属性提供商在对服务提供者的响应中应使用<ModifyResponse>元素。

[Liberty-ID-WSF-DST]中定义的DST元素并非仅仅用作消息。更重要的是DST提供了可在WSDL中实际使用的XML模板来实现查询/修改语法。

图5说明了消息的交互。

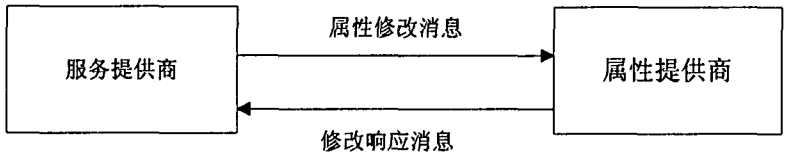

图5 属性修改

<Modify>元素的schema定义和使用方法应遵循[Liberty-ID-WSF-DST]3.3.1小节中定义。<ModifyResponse>的使用应遵循[Liberty-ID-WSF-DST]3.3.2小节中的定义。<Modify>和<ModifyResponse>元素的处理规则应遵照[Liberty-ID-WSF-DST]3.3.3小节中的描述。

下面的例子描述了如何对存储在profile.MobileOperator.com中的个人概要进行插入或更改。

```
<Modify>
    <ResourceID>http://profile.MobileOperator.com/8fhelk9savbq4p0j</ResourceID>
    <Modification overrideAllowed="True">

<Select>/pp:PP/pp:AddressCard[pp:AddressType= 'urn:liberty:id-sis-pp:addrType:home']</Select>
        <NewData>
            <AddressCard id="45387">
                <AddressType>urn:liberty:id-sis-pp:addrType:home</AddressType>
                <Address>
                    <PostalAddress>Sophie Wunderkid$1234 Wonderland Drive</PostalAddress>
                    <PostalCode>12345-1234</PostalCode>
                    <L>Olympia</L>
                    <ST>CA</ST>
                    <C>us</C>
                </Address>
            </AddressCard>
        </NewData>
    </Modification>
</Modify>
```


6.3 使用指导

当一个服务提供商使用<Query>元素向属性提供商进行属性查询时，服务提供商可以包括一个<UsageDirective>头，用于指示这些属性的处理策略，用户和其他用户身份信息。属性提供商可以根据这些属性的处理策略及用户的查询权限列表，将查询的属性结果返回给服务提供商。这些属性的处理策略可以包括用户或其他用户的属性访问权限，以便属性提供商根据该策略进行相应的处理。当属性提供商使用<QueryResponse>来响应服务提供商时，属性提供商包含一个<UsageDirective>头说明这些被发布的属性的后续使用策略。因此，<Query>元素中的<UsageDirective>头描述了对这些属性预想的用法，而<QueryResponse>元素中的<UsageDirective>头则描述了对这些属性要求的用法。

流程应用<UsageDirective>头时应遵循[Liberty-IDWSF-Soap-Binding]6.6描述的处理程序。使用指导举例请见[Liberty-IDWSF-Soap-Binding]6.6.3小节。

图6描述了可选的从服务提供商发送到属性提供商的查询消息中包括的UsageDirective头。它也描述了可选的从属性提供商发送到服务提供商的查询响应消息中包括的UsageDirective头。

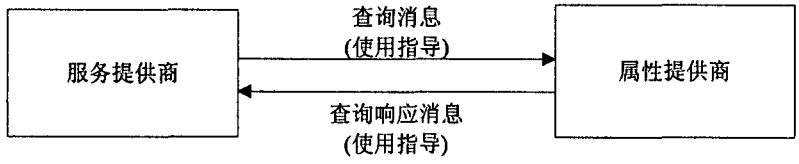

图 6 使用指导

节选自[Liberty-IDWSF-Soap-Binding]中的如下schema定义提供了一个UsageDirective头的例子。从该例子中可见：使用指导指出了属性的使用方法须与EU使用指导规则一致。

<UsageDirective id="directive1000" ref="#datarequest001" S:MUSTUnderstand="1">

<cot:PrivacyPolicyReference xmlns:cot="http://circle-of-trust.com/isf">

http://circle-of-trust.com/policies/eu-compliant

</cot:PrivacyPolicyReference>

</UsageDirective>

6.4 交互服务

6.4.1 交互服务流程

属性提供商可能使用交互服务来询问主体，通过发送<InteractionRequest>元素到交互服务，该服务与主体交互后发送含有<InteractionResponse>元素的响应消息。图7描述了此情况下，当服务提供商向属性提供商提交查询时的消息交互。

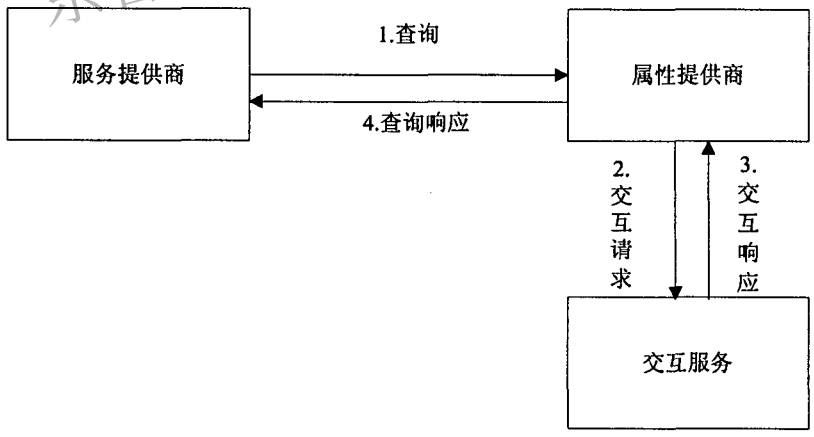

图 7 交互服务

交互请求应遵照[Liberty-ID-WSF-Interaction-Svc]5.1节中的描述，且交互响应应遵照[Liberty-ID-WSF-Interaction-Svc]5.2节中的描述。

6.4.2 交互重定向

当一个属性提供商（作为Web服务提供商）要请求服务提供商（Web服务请求方）来把主体重定向到属性提供商的URL时，应遵照[Liberty-ID-WSF-Interaction-Svc]第4章中的机制。如图8所示，为了达到

此目的而使用了<RedirectRequest>元素，并且就重定向主体向服务提供商作了指示。在属性提供商获得必需的信息后，它将主体重定向回服务提供商。

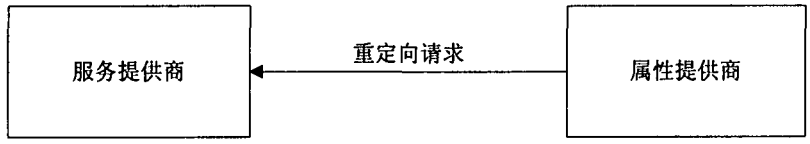

图 8　交互重定向

6.5　基于 Web 服务框架的引导身份

6.5.1　两种认证机制

为了接入基于Web服务框架的身份认证，提供两种机制：

— 发现服务引导；

— 认证服务和单点登录服务。

6.5.2　发现服务引导

身份提供商可以应用发现服务引导这种机制提供给服务提供商接入一个发现服务所需的资源参考。身份提供商可以通过访问权限列表和身份联合框架来对这个过程进行控制。应遵照[Liberty-ID-WSF-Disco]第 6 章中的定义来支持发现服务引导。

6.5.3　认证服务

通过认证服务这种机制，一个身份提供商可以提供给服务提供商接入其他提供商（包括发现服务）所需的资源参考。应遵照[Liberty-ID-WSF-Disco]第5章中的定义来支持认证服务。

6.5.4　单点登录服务

应遵照[Liberty-ID-WSF-Disco]第5章中的定义来支持单点登录服务。

6.6　发现服务

6.6.1　发现服务的功能要求

当服务提供商想要确定究竟是哪个（或者哪些）属性提供商主管着所需资源时，它可与发现服务联系，以获得这些信息。发现服务也可给进行询求的服务提供商提供访问这个（或这些）属性提供商时所必需的证书，以确保服务提供商对这些属性的访问权限。

发现服务根据服务提供商的访问权限许可请求方发现资源参考。一个资源参考是资源和服务实例的关联体。服务实例是一个在确定的协议端点处运行的Web服务。这种关联是必需的，因为在资源和服务实例间有多种对应关系。某单一服务实例可服务于若干个资源。例如，一个用户概要服务提供商将在一个单一服务实例背后服务于许多概要资源。

图9描述了一个持有多个主体的日历资源的日历服务实例（P1、P2、P3、P4、P5、P6）。各种资源参考也在图9中进行了描述，这些资源参考为每一个带有日历服务实例的主体指示了与日历资源的关联。图9有6个资源参考。

图10描述了P1这个主体持有3种不同资源的单一服务实例，包括日历、电话簿、个人概况。图中的资源参考表示服务实例与各种资源的关联关系。在这个例子中，有3个资源参考。

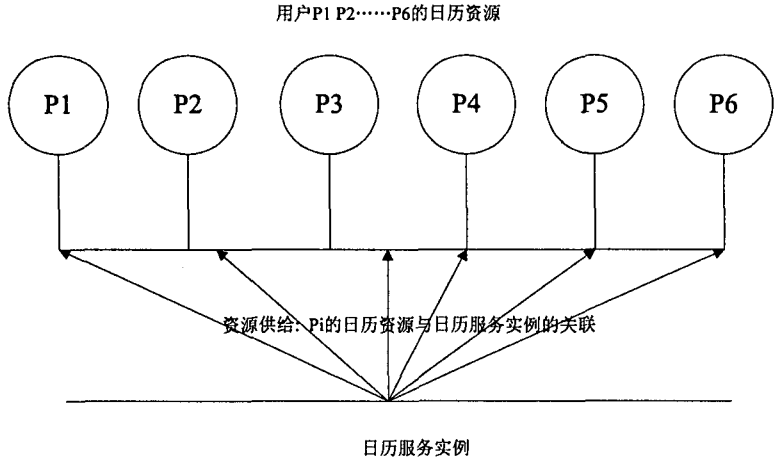

图 9　持有不同用户日历资源的日历服务例子的说明

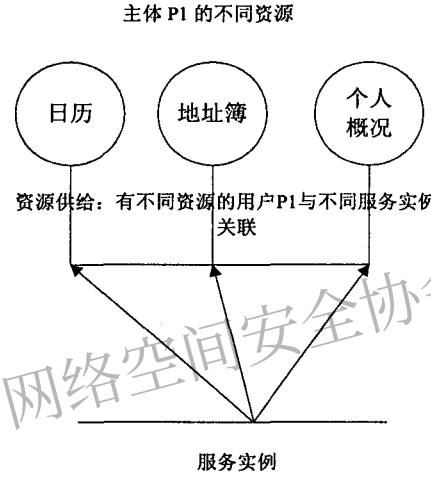

图 10　某一主体的不同资源的说明

下面的schema定义提供了一个表示资源（由资源ID描述）和服务实例间关联的资源参考的描述。下面的例子中，资源参考元素有两个子元素：<ResourceID>和< ServiceInstance>元素。<ResourceID>元素中的URI:http://CalendarServiceProvider.com/profiles/l4m0B82k15csaUxs标识了一个特定主体的日历资源。< ServiceInstance>元素对服务类型，服务提供商ID和服务本身进行了描述。

```
<ResourceOffering xmlns="urn:liberty:disco:2003-08">
    <ResourceID>http://CalendarServiceProvider.com/profiles/l4m0B82k15csaUxs</ResourceID>
    <ServiceInstance xmlns="urn:liberty:disco:2003-08">
        <ServiceType>urn:CalendarService:2003-08</ServiceType>
        <ProviderID>http://CalendarServiceProvider.com/</ProviderID>
        <Description>
            <SecurityMechID>urn:liberty:security:2003-08:TLS:SAML</SecurityMechID>
            <Endpoint>https://soap.CalendarServiceProvider.com/soap/</Endpoint>
        </Description>
    </ServiceInstance>
</ResourceOffering>
```

6.6.2 发现查找

为了获得适当的资源参考，请求者需要在发现服务那里初始化一个发现查找（discovery lookup）进程。该进程应遵照[Liberty-ID-WSF-Disco]第5.1节中的描述。如图11所示，请求方发送<Query>消息到发现服务，发现服务以<QueryResponse>消息作为响应。

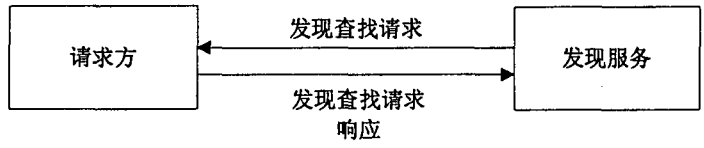

图 11 发现查找

从请求方发送到发现服务的<Discovery Lookup Query>消息应与[Liberty-ID-WSF-Disco]第5.1.1小节中的定义的一致。<Discovery Lookup Query>包含<ResourceID>元素，它为发现服务指出被请求的具体资源。

以下是<Discovery Lookup Query>schema.定义的一个示例：

```
<Query xmlns="urn:liberty:disco:2003-08">
    <ResourceID> http://CalendarServiceProvider.com/profiles/l4m0B82k15csaUxs< disco:/ResourceID>
    <RequestedServiceType>
        <ServiceType> urn:CalendarService:2003-08</ disco:ServiceType>
    </RequestedServiceType>
</Query>
```

从发现服务发送到请求方的<Discovery Lookup QueryResponse>消息应与[Liberty-ID-WSF-Disco]第5.1.2小节中的定义一致。<Discovery Lookup QueryResponse>消息中包含有能够满足该请求的<ResourceOffering>字段。

以下是<Discovery Lookup QueryResponse>消息的schema.定义的一个示例：

```
<QueryResponse xmlns="urn:liberty:disco:2003-08">
    <ResourceOffering xmlns="urn:liberty:disco:2003-08">
        <ResourceID>http://CalendarServiceProvider.com/profiles/l4m0B82k15csaUxs</ResourceID>
        <ServiceInstance xmlns="urn:liberty:disco:2003-08">
            <ServiceType>urn:CalendarService:2003-08</ServiceType>
            <ProviderID>http://CalendarServiceProvider.com/</ProviderID>
            <Description>
                <SecurityMechID>urn:liberty:security:2003-08:TLS:SAML</SecurityMechID>
                <Endpoint>https://soap.CalendarServiceProvider.com/soap/</Endpoint>
            </Description>
        </ServiceInstance>
    </ResourceOffering>
</QueryResponse>
```

6.6.3 发现更新

为了在发现服务处插入、删除或更新资源参考，需要初始化发现更新进程。进程应遵循[Liberty-ID-WSF-Disco]第5.2节中的定义。如图12所示，发送方发送<Discovery Update Modify>消息到发现服务，然后发现服务返回<Discovery Update ModifyResponse>消息。

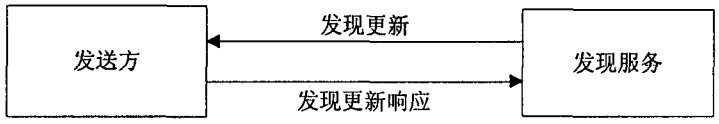

图 12　发现更新

发送方所发送的发现服务的<Discovery Update Modify>消息应遵循[Liberty-ID-WSF-Disco]第5.2.1小节中的定义。<Discovery Update ModifyResponse>消息应遵循[Liberty-ID-WSF-Disco]第5.2.2小节中的定义。

```
<Modify xmlns="urn:liberty:disco:2003-08">
    <ResourceID>http://example.com/disco/d0CQF8elJTDLmzEo</disco:ResourceID>
    <InsertEntry>
        <ResourceOffering xmlns="urn:liberty:disco:2003-08">

<ResourceID>http://CalendarServiceProvider.com/profiles/l4m0B82k15csaUxs</ResourceID>
            <ServiceInstance xmlns="urn:liberty:disco:2003-08">
                <ServiceType>urn:CalendarService:2003-08</ServiceType>
                <ProviderID>http://CalendarServiceProvider.com/</ProviderID>
                <Description>
                    <SecurityMechID>urn:liberty:security:2003-08:TLS:SAML</SecurityMechID>
                    <Endpoint>https://soap.CalendarServiceProvider.com/soap/</Endpoint>
                </Description>
            </ServiceInstance>
        </ResourceOffering>
        <AuthenticateRequester descriptionIDRefs="saml"/>
        <AuthorizeRequester descriptionIDRefs="samlclientTLS"/>
    </InsertEntry>
    <RemoveEntryentry ID="1"/>
</Modify>

<ModifyResponse xmlns="urn:liberty:disco:2003-08" newEntryIDs="2">
    <Status code="OK"/>
</ModifyResponse>
```


6.7　用户代理和设备(LUAD)

6.7.1　作为 WSC 的 LUAD

Web服务消费者（WSC）或一个Web服务提供者与一个或几个用户相关联，而不是与很多用户相关联。持有这些WSC或WSP的用户代理和设备就称为自由联盟用户代理和设备（Liberty enabled User Agents and Devices，LUAD）。在这种情况下，应遵循[Liberty-ID-WSF-Client-Profiles]所定义的机制。

当LUAD作为WSC时，应遵循[Liberty-ID-WSF-Client-Profiles]第3章中所定义的机制，LUAD WSC可不与浏览进程中保持的会话相关联。

6.7.2 作为 WSP 的 LUAD

当LUAD作为WSP时，应遵循[Liberty-ID-WSF-Client-Profiles]第4章中所定义的机制。

6.8 安全

6.8.1 认证

定义了两种认证机制来支持不同的配置场景——对等实体认证和消息认证。

a）对等实体认证：当 Web 服务请求方（WSR）直接与某 Web 服务提供商（WSP）相交互时，提供商需要实现双向的认证，并可能使用通信信道认证来传输它的身份。一个候选机制是基于 SSL3.0/TLS1.0 客户端 X.509v3 的认证。当通信提供商使用对等实体认证，处理程序应遵循[Liberty-ID-WSF-Security-Mechanisms]6.2 小节中的定义。空实体和对等实体的认证机制应支持[Liberty-ID-WSF-Security-Mechanisms]6.2 小节中的定义。

b）信息认证：当 WSR 通过一个或多个活动中的中介（如：代理）与某 WSP 相交互时，该提供商可明确地将它的身份传送到接收者。可以支持如下两种形式的消息认证：

1）X.509 v3 认证消息认证；

2）SAML 断言消息认证。

当通信提供商使用消息认证时，应遵循[Liberty-IDWSF-Security-Mechanisms]6.3节中的定义。空消息和发送方消息认证机制，应支持[Liberty-IDWSF-Security-Mechanisms]第6.3节中定义。

6.8.2 机密和隐私

应采用保密机制来保证传输的信息只有授权方能够看懂。提供了多级保密机制，即：传输级，消息级，资源标识符级保密机制。这些机制应遵循[Liberty-IDWSF-Security-Mechanisms]第5章中的定义。

a）传输层信道保护：当通信提供商之间直接进行交互，而不是通过中介（如：代理）交互时，那么传输层保密机制可以保证信息交互的完整性和机密性。应使用合适的 SSL/TLS 密码组来实现传输层信道保护。按照[Liberty-IDWSF-Security-Mechanisms]第 5.1 节中的定义，宜使用如下 SSL/TLS 密码组：

1）TLS_RSA_WITH_RC4_128_SHA

2）TLS_RSA_WITH_3DES-EDE-CBC-SHA

3）TLS_DHE_DSS-WITH_3DES_EDE-CBC_SHA

4）TLS-RSA_WITH_AES_CBC_SHA

5）TLS_DHE-DSS_WITH-AES_CBC-SHA

其他协议例如 Kerberos 和 IPSEC 只要能提供同等级的保护，也可采用。

b）消息机密保护：在活动中的中介（代理，网关）存在的情况下，通信中的提供商之间消息交互的完整性和机密性应得到消息级的保证。在这种情况下，通信端应保护敏感信息不被未授权方截获。按照[Liberty-IDWSF-Security-Mechanisms]第 5.2 节中的定义，为了满足这一要求，通信端应使用[wss-sms]定义的保密机制来加密 SOAP 体的子元素。

c）标识符机密保护：当可信权威因被激活的服务消费而发送的信息中包含有敏感数据（如：联合名字空间标识符）时，这些消息应不能让不可信的中介实体截获。应有对命名标识符和(或)URI 机制的加密，应遵循[Liberty-IDWSF-Security-Mechanisms]第 5.3 节中的定义。

6.8.3 认证

为了生成、传输和使用认证信息，应遵循[Liberty-IDWSF-Security-Mechanisms]第8章中的定义。为了执行在给定消息交互过程中认证请求消息的传输，认证机制需依赖于XML schema。这些主体向身份提供商的认证请求消息包括用于传送代理身份的代理schema，用于控制服务提供商属性查询权限的访问列表，用于将会话状态从一个实体传送到另一个实体的会话环境，和用于传送与接入实体和试图接入资源相关的信息的资源入口。

6.8.4 消息相关性

协议参与方之间所交互的消息可需要确保响应与请求之间的相关性，为了达到这个目的，请求方可以在消息头部嵌入相关性元素。应遵循[Liberty－IDWSF-Soap－Binding]中定义的机制。

参 考 文 献

[1] OMA IOPPROC	OMA Interoperability Policy and Process
[2] IETF RFC2119（1997）	Key words for use in RFCs to Indicate Requirement Levels
[3] IETF RFC2234（1997）	Augmented BNF for Syntax Specifications: ABNF
[4] IETF RFC2828(2000)	Internet Security Glossary
[5] Liberty-ID-FF-Protocols-Schema(2003)	Liberty ID-FF Protocols and Schema Specification
[6] Liberty-ID-WSF-Interaction-Svc(2005)	Liberty ID-WSF Interaction Service Specification
[7] Liberty-ID-WSF-Soap-Binding(2005)	Liberty ID-WSF SOAP Binding Specification
[8] Liberty-Paos (2005)	Liberty Reverse HTTP Binding for SOAP Specification
[9]Liberty-ID-WSF-Disco (2005)	Liberty ID-WSF Discovery Service Specification
[10]Liberty-ID-WSF-Client-Profiles(2004)	Liberty ID-WSF Profiles for Liberty Enabled User Agents and Devices
[11]Liberty-ID-WSF-Security-Mechanisms(2005)	Liberty ID-WSF Security Mechanisms
[12]Liberty-ID-WSF-AuthnSSO(2005)	Liberty ID-WSF Authentication Service and Single Sign-On Service Specification
[13]OMA NI-RD（2006）	MWS Identity Management Requirements
[14]OMA OWSER1.0（2006）	OMA Web Services Enabler Release
[15] OMA OWSER1.0-NI（2006）	OMA Web Services Enabler (OWSER) Network Identity Specifications
[16] OMA OWSER Core（2006）	OMA Web Services Enabler (OWSER): Core Specifications
[17] OMA OWSER NI FF（2006）	OMA Web Services Network Identity Enabler (OWSER NI): Federation Framework
[18] OMA OWSER NI WSF（2006）	OMA Web Services Network Identity Enabler (OWSER NI): Identity Web Services Framework

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 2 部分：网络身份 Web 服务框架
YD/T 2127.2-2010
*
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
*