

ICS 33.040.40

L 79

YD

中华人民共和国通信行业标准

YD/T 2706-2014

园区网间用户标识与属性互通技术要求

User identifier and attributes interoperation specification
between campus networks

2014-10-14 发布

2014-10-14 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
4 园区网间用户标识与属性互通技术框架	1
5 园区网间身份联盟中用户标识与属性	3
附录 A (资料性附录) 用户标识与属性举例	7

前 言

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：北京大学、清华大学、北京邮电大学、工业和信息化部电信研究院、中兴通信股份有限公司、北京聚宝网络科技有限公司、公安部第三研究所。

本标准主要起草人：陈 萍、吕 洁、王继龙、黄小红、武 静、刘尚焱、高 峰、朱红儒、杨明慧、石 丰、裘 羽。

园区网间用户标识与属性互通技术要求

1 范围

本标准规定了园区网间用户标识与属性互通技术框架和用户标识与属性描述方法。
本标准适用于组成身份认证联盟的园区网。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 2094—2010 安全断言标记语言（所有部分）

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文件。

3.1.1

园区网 Campus Network

在某地理区域内、由多个相互连接的局域网组成的计算机网络。园区网内的网络设备（如交换机、路由器等）、传输媒介（光纤、铜线等）及应用系统由园区所属机构（如公司、大学）拥有并管理。

3.1.2

园区网间身份联盟 Identity Federation over Campus Networks

使用公共软件框架用来交换和使用身份标识和属性，支持园区网间互通互访的一个协作组织。

3.2 缩略语

下列缩略语适用于本文件。

HTTP	HyperText Transfer Protocol	超文本传输协议
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer	基于安全套接层的超文本传输协议
HTML	HyperText Markup Language	超文本标记语言
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
SAML	Security Assertion Markup Language	安全断言标记语言
URL	Uniform Resource Locator	统一资源定位符

4 园区网间用户标识与属性互通技术框架

4.1 园区网间身份联盟

本标准指定的用户标识与属性互通技术要求主要应用于园区网间身份联盟。

园区网间身份联盟为一种指定结构的身份联盟，它在各个园区之间共享用户园区内身份信息。联盟的基本组成要素是园区网。园区网内部参与网间身份联盟的主要组件有：园区网身份提供者IdP和园区网

服务提供者SP。从身份联盟的角度看，一个园区网可以配置0或1个身份提供者，身份提供者具备两项功能：一是该园区网用户的身份认证功能；二是该园区网用户的身份信息发布功能。一个园区网可配置多个服务提供者，每个服务提供者可支持一个或多个应用系统被身份联盟中来自本园区网或者是其他园区网的用户访问。园区网间身份联盟同时支持应用系统以独立的服务提供者身份加入联盟，支持联盟中各个园区用户的访问。园区网间身份联盟基于安全断言标记语言（SAML, Security Assertion Markup Language）而建立。身份提供者、服务提供者和用户浏览器之间采用SAML协议传输身份相关信息。安全断言标记语言相关标准见YD/T 2094-2010。

园区网间身份联盟的基本组成结构如图1所示。

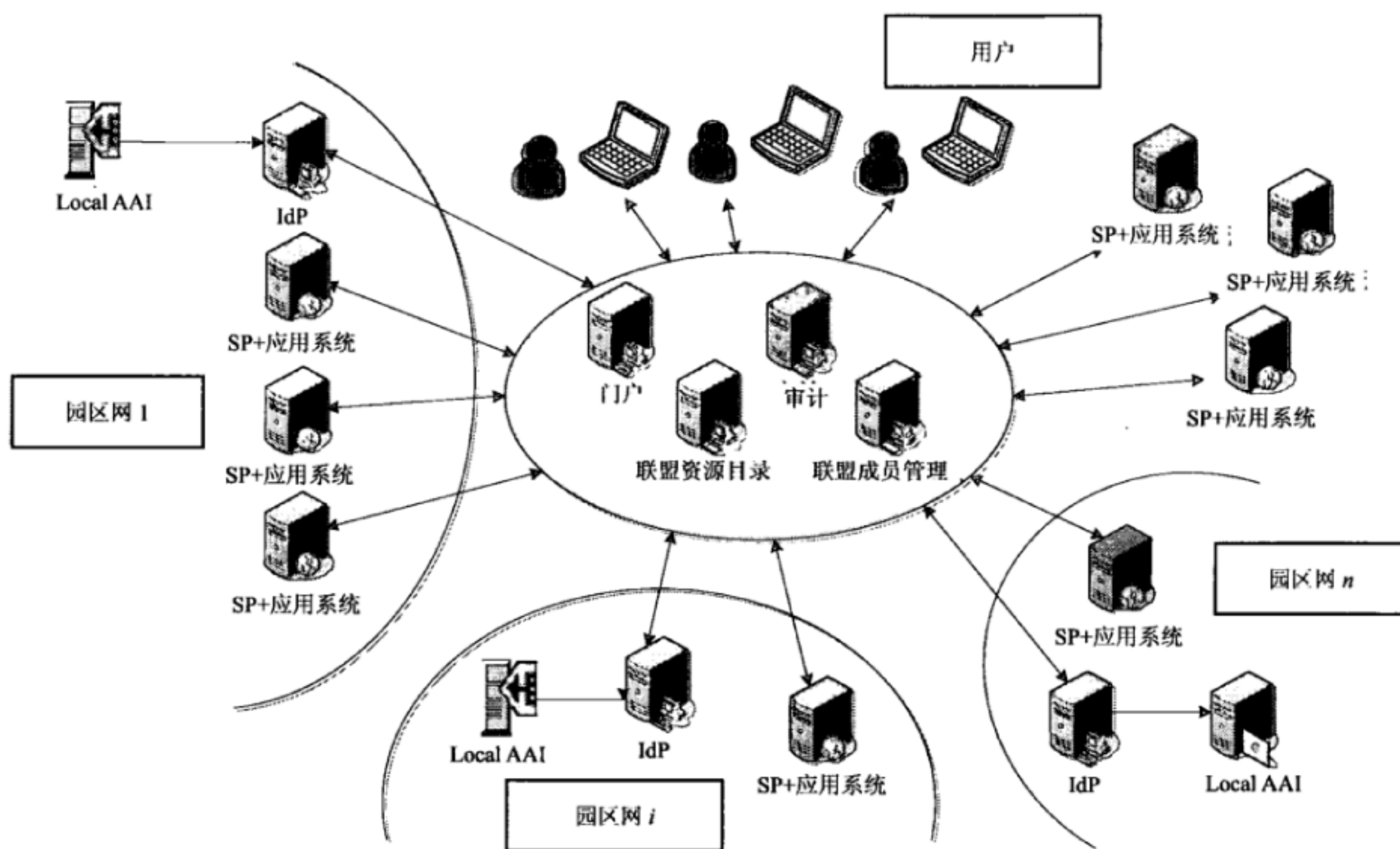


图1 园区网间身份联盟组成结构

园区网间身份联盟包括客户端（用户浏览器）、身份提供者IdP和服务提供者SP三种逻辑组件：。这三种组件分别为运行于不同的操作系统和主机之上，按照OSI七层网络协议划分，这些组件均运行于应用层，正常运行的基础是上述组件软件所在主机已经通过网络层认证，获取网络访问权限。

4.2 用户跨园区访问

典型的园区间访问场景是A园区中的一位用户通过浏览器试图访问B园区中的应用系统，从而触发联盟系统的认证和授权机制。服务提供者首先确定该用户所属的身份提供者，然后将用户重定向到其所属A园区的身份提供者。A园区身份提供者对用户进行身份鉴别，之后用户携带身份提供者签发的断言，再次访问服务提供者。如果需要作进一步的访问控制检查，服务提供者会向身份提供者发出用户属性请求，检查通过后，允许用户访问受限资源。

园区网间身份联盟体系中用户跨园区访问示意如图2所示。

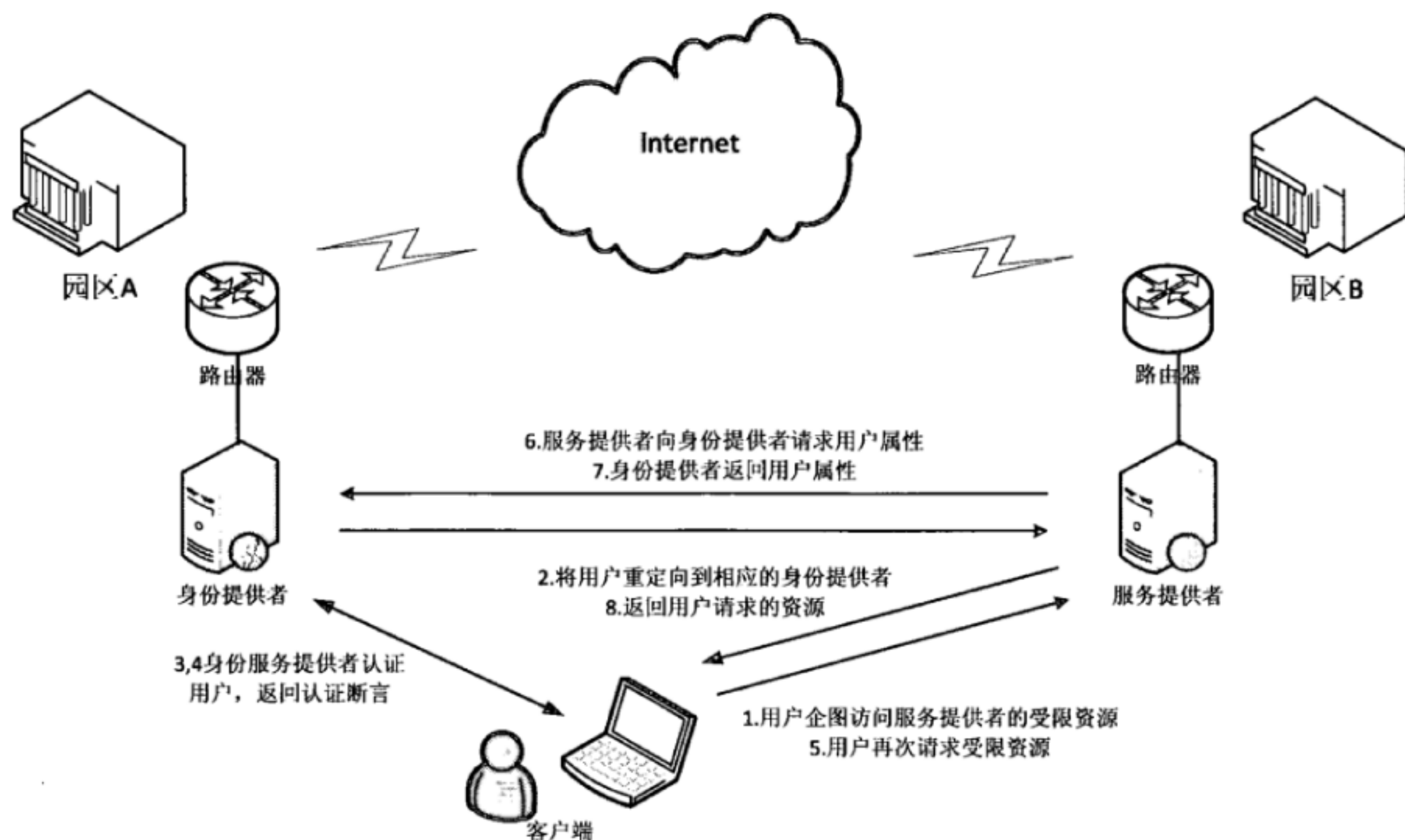


图2 园区网间身份联盟用户跨园区访问示意

用户跨园区网访问的基本流程如下：

- 1) 用户向服务提供者保护的应用系统发送HTTP请求。
- 2) 服务提供者收到请求后，判断是否为已认证用户。若非已认证用户，则确定用户所属的身份提供者，将用户重定向到身份提供者以启动身份认证。
- 3) 用户向身份提供者提供本人身份。
- 4) 身份提供者通过某种方式认证用户身份（例如返回一张HTML表单，让用户提供用户名、密码），根据认证结果，构造认证断言消息，并将用户重定向到服务提供者。
- 5) 用户向服务提供者再次提出访问请求，提供认证结果。
- 6) 服务提供者根据身份提供者签发的断言检查用户，如通过验证，则将用户重定向到资源。如果需要用户属性作进一步授权决定，服务提供者继续向身份提供者的属性中心请求属性服务。
- 7) 身份提供者根据请求，返回相应用户属性，服务提供者作授权决定。
- 8) 本标准中规定的用户标识和属性互通技术要求主要应用在以上用户跨园区访问流程中的步骤3)、4)和6)、7)中。

5 园区网间身份联盟中用户标识与属性

5.1 概述

在园区网间身份联盟中，一种常见的场景是用户跨越园区访问应用系统，也就是说，用户身份所在园区和用户要访问的应用系统所在园区可以不是一个园区。在这种模式下，无论是维护用户身份的身份管理者，还是接受用户访问的服务提供者，它们需要通过交换用户标识和属性实现互通和合作。本标准的作用就是定义一套用户标识和属性规范，无论是哪个园区的身份提供者，无论它是采用何种技术实现，无论它内部的用户标识和属性描述方式如何，在将用户信息传递给服务提供者之前，首先将园区内用户

信息定义方式转换成本标准定义的用户描述方式。同样，服务提供者在使用用户信息之前，将它们从本标准定义的方式转换为应用系统能够识别和使用的描述方式。本标准定义的用户标识和属性起到了桥梁的作用，实现了异构的多个园区之间的用户信息互通，进一步，实现了园区网间的用户信息共享和跨园区应用系统访问。

5.2 园区网间身份联盟中的用户标识

标识是人员属性中最常用的一个，是园区网间身份联盟中用户的唯一网络标识，是属性对象定义中必须指定的一种属性。表示成“localID@org”形式。其中，localID为人员在园区网内部的身份标识，它的长度、格式、命名规则由园区网管理人员指定，园区网间身份联盟直接使用；org唯一标识用户所属园区，通常采用园区网域名，如北京大学的org是“pku.edu.cn”，电信传输研究所的org是“ritt.cn”。建议不要在标识中使用多个@符号。左起第一个@符号将被看作分隔符，左边是用户标识符，右边是园区标识符。如果该园区已经注册域名，园区标识符通常为注册域名。比如“10548880@pku.edu.cn”隐含指出该用户身份所在园区的域名是“pku.edu.cn”，园区网内帐号为“10548880”，园区网间身份联盟的用户标识为“10548880@pku.edu.cn”。每个org都定义了一个名字空间，在该名字空间中用户名字是唯一的。基于该规则，任何两个用户标识的值都不会冲突，相同的用户标识对应相同管理域的同一个用户。用户一旦被赋予该标识符，园区网用户管理系统应该能够充分肯定被认证的用户就是被赋予该标识符的那个人。

人员标识具有持久性（Persistence）、私密性（privacy）、唯一性（Uniqueness）的特点。

5.3 园区网间身份联盟中的互通属性对象定义

所有园区网间身份联盟中的人员属性都是由campFedPerson开头，属于campFedPerson对象类，campFedPerson的数据结构使用ASN.1语言描述如下，人员对象可以有选择性地包含以下属性。

```
AttrValueType ::= SEQUENCE {
    attrName  UTF8String,
    attrValue UTF8String
}
campFedPerson ::= SEQUENCE { --人员对象属性
    campFedPersonPrincipalName  UTF8String,
    campFedPersonAffiliation     ENUMERATED{
        student (0),
        faculty (1),
        alum (2),
        staff (3),
        manager (4),
        member (5),
        other (6)
    },
    campFedPersonEntitlement      UTF8String,
    campFedPersonOrg             UTF8String,
    campFedPersonLocalID         UTF8String,
```

campFedPersonSurName	UTF8String,
campFedPersonGivenName	UTF8String,
campFedPersonFullName	UTF8String,
campFedPersonDepartment	UTF8String,
campFedPersonMailAddress	UTF8String,
campFedPersonTelephone	UTF8String,
campFedPersonMobile	UTF8String,
campFedPersonEmail	UTF8String,
campFedPersonDescription	UTF8String,
campFedPersonOtherAttrs	SEQUENCE OF AttrValueType

}

5.3.1 campFedPersonPrincipalName

campFedPersonPrincipalName定义为UTF8String。

指园区网身份联盟中的用户网络标识。详细介绍见5.2。

5.3.2 campFedPersonAffiliation

campFedPersonAffiliation定义为ENUMERATED{ student, faculty, alum, staff, manager, member, other}, 指定用户在园区中的主要身份, 如学生、教师、校友、员工、部门经理、普通成员等。member指除以上列出的几类外, 园区中拥有身份的人员, 他们共同拥有园区成员身份的一些基本权限, 例如内部的电子邮件账户, member不包括student、faculty、alum、staff、manager、other。other为一个可扩展属性, 身份管理员和应用管理员可以根据实际应用协商定义。

5.3.3 campFedPersonEntitlement

campFedPersonAffiliation定义为UTF8String。

指对特定资源的URL拥有权限。

campFedPersonEntitlement使用户有权限访问该URL指定的服务提供者。如果用户所属园区的目录允许声明这样的访问资格, 则关于属性是否具有访问资格的决定在用户身份所在的园区进行。除了用户所具有的访问权利之外, 服务提供者并不了解用户其他特征。两者之间的信任关系通过其他方式建立。例如服务提供者维护一张已订制该服务的机构列表, 对不在列表中的机构所声明的访问权利则不予考虑。

5.3.4 campFedPersonOrg

campFedPersonOrg定义为UTF8String。

指用户所属园区。campFedPersonPrincipalName中的园区网标识, “@”之后的部分, 通常为园区域名。

5.5.5 campFedPersonLocalID

campFedPersonLocalID定义为UTF8String。

指用户在园区内的标识。campFedPersonPrincipalName中“@”之前的部分, 通常为用户在园区网身份管理系统中的本地标识。

5.3.6 campFedPersonSurName

campFedPersonSurName定义为UTF8String。

指用户姓氏。

5.3.7 campFedPersonGivenName

campFedPersonGivenName定义为UTF8String。

指用户名字。

5.3.8 campFedPersonFullName

campFedPersonFullName定义为UTF8String。

指用户全名。由campFedPersonGivenName和campFedPersonSurName组成。campFedPersonGivenName在前。

5.3.9 campFedPersonDepartment

campFedPersonDepartment定义为UTF8String。

指用户在园区内所属部门。

5.3.10 campFedPersonMailAddress

campFedPersonMailAddress定义为UTF8String。

指用户邮寄通讯地址。

5.3.11 campFedPersonTelephone

campFedPersonTelephone定义为UTF8String。

指用户办公电话号码。

5.3.11 campFedPersonMobile

campFedPersonMobile定义为UTF8String。

指用户移动电话号码。

5.3.12 campFedPersonEmail

campFedPersonEmail定义为UTF8String

指用户电子邮件地址。

5.3.13 campFedPersonDescription

campFedPersonDescription定义为UTF8String。

指关于用户的附加描述。

5.3.14 campFedPersonOtherAttrs

AttrValueType定义为SEQUENCE {

attrName UTF8String,

attrValue UTF8String

}

指用户的属性名和属性值。其中，attrName是属性名，attrValue是属性值。

campFedPersonOtherAttrs定义为SEQUENCE OF AttrValueType。

指关于用户其他属性定义。

5.4 用户属性发布控制和隐私保护

身份提供者在向服务提供者分发属性断言之前，需要提供某种方式，使得用户可以选择是否将自己的属性信息发送给目标应用。

附 录 A
(资料性附录)
用户标识与属性举例

以下是SAML认证请求的例子，增加了断行以增强可读性。

```
<urn:AuthnRequest xmlns:urn="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceIndex="4" ID="_-4511628885607801801"
  IssueInstant="2013-02-19T14:08:27.974Z" Version="2.0">
  <urn1:Issuer xmlns:urn1="urn:oasis:names:tc:SAML:2.0:assertion">
    https://sp.tshhosting.com/shibboleth</urn1:Issuer>
  <urn:NameIDPolicy Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
</urn:AuthnRequest>
```

以下是SAML认证断言和属性断言的例子。增加了断行以增强可读性。

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_aaa4dcca3c3b4b872895673e957a49a" IssueInstant="2013-02-19T14:08:27.084Z"
  Version="2.0">
  <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
    https://idp2.pku6.edu.cn/idp/shibboleth/carsifed
  </saml:Issuer>
  <saml:Subject>
    <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
      _49da4f3105de56ee3db0d732630b4555
    </saml:NameID>
    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml:SubjectConfirmationData
        Address="2001:da8:201:1042:e188:a2f5:f73c:17fd"
        InResponseTo="_-4511628885607801801"
        NotOnOrAfter="2013-02-19T14:13:27.084Z"
        Recipient="https://www.webofknowledge.com/?auth=Shibboleth">
      </saml:SubjectConfirmationData>
    </saml:SubjectConfirmation>
  </saml:Subject>
  <saml:Conditions NotBefore="2013-02-19T14:08:27.084Z"
    NotOnOrAfter="2013-02-19T14:13:27.084Z">
    <saml:AudienceRestriction>
      <saml:Audience>https://sp.tshhosting.com/shibboleth</saml:Audience>
```

```

    </saml:AudienceRestriction>
  </saml:Conditions>
  <saml:AuthnStatement AuthnInstant="2013-02-19T14:08:27.056Z"
    SessionIndex="b65e3e16599b9597b8a79ed5cb9326d70f8f3fa54286385f239b5f55efd94749">
    <saml:SubjectLocality Address="2001:da8:201:1042:e188:a2f5:f73c:17fd">
    </saml:SubjectLocality>
    <saml:AuthnContext>
      <saml:AuthnContextDeclRef>
        urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
      </saml:AuthnContextDeclRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
  <saml:AttributeStatement>
    <saml:Attribute FriendlyName="uid" Name="uid"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="xs:string">0093000</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute FriendlyName="affiliation" Name="affiliation"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="xs:string">
        student
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>

```

其中，<saml:AttributeStatement>是用户属性断言，1个用户属性断言中可以包含1个或者多个用户属性元素<saml:Attribute>。<saml:Attribute>元素的Name属性是用户属性名，该属性名应符合本标准的规定。<saml:Attribute>元素的子元素<saml:AttributeValue>的值是用户属性的值。

中 华 人 民 共 和 国
通 信 行 业 标 准
园区网间用户标识与属性互通技术要求
YD/T 2706-2014

*

人民邮电出版社出版发行
北京市丰台区成寿寺路1号邮电出版大厦
邮政编码：100164
北京康利胶印厂印刷
版权所有 不得翻印

*

开本：880×1230 1/16 2015年9月第1版
印张：1 2015年9月北京第1次印刷
字数：52千字

15115·494

定价：10元

本书如有印装质量问题，请与本社联系 电话：(010)81055492