# 基于 Shibboleth 和 SAML 的跨校统一身份认证系统

孙思纬,夏洪山

(南京航空航天大学 民航学院,江苏 南京 210016)

**摘 要**:结合跨域统一身份认证的基础技术平台 Shibboleth 和跨域统一身份认证的技术标准 SAML,设计出跨校统一身份认证系统。该系统可实现用户"异地访问—本地认证"功能,避免了异地认证的繁琐,简化了业务流程;身份联盟各子系统交互采用 SAML 标准,有效地保证了系统通信的安全,保障了用户的隐私,满足了应用管理的需求。

**关键词**:身份认证;单点登录;统一身份认证;身份联盟

**中图分类号**:TP393 **文献标识码**:A

## The unified identity authentication system across schools on based Shibboleth and SAML

SUN Si-Wei, XIA Hong-Shan

(College of Civil Aviation, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

**Abstract**: In this paper, a combination of cross-border basis of unified authentication Shibboleth technology platform and cross-domain authentication unified technical standards SAML, design schools across the uniform identity authentication system. The system user "in different places to visit-local certification" function, to avoid cumbersome remote authentication and simplifies the business processes; identity federation using SAML interaction of various subsystems standards, effective communication to ensure the safety of the system to protect the privacy of users, very good to meet the needs of the application management.

**Key words**: identity authentication; single sign on; uniform identity authentication; identity federation

随着技术的发展,越来越多的大学、公司以及政府机构都通过网络对外提供资源、服务,并且彼此协作日益紧密、信息共享日益频繁。例如,大学之间的"跨校选课"、"共享图书资源"等。因此简化这些业务中身份认证的流程,同时做到安全高效成为迫切需要解决的问题。

## 1 Shibboleth 简介

Shibboleth 是 Internet2/MACE 项目之一,得到了 IBM 的技术和资金支持。Shibboleth 是一个使用标准语言描述的体系结构和策略框架,支持安全 Web 资源和服务共享[1]。

Shibboleth 主要针对分布式资源如何有效访问的问题。与其他系统的区别在于 Shibboleth 将认证模块放在客户端,资源提供者只需进行少量的验证工作,极大地减轻了资源提供者的负担,简化了访问程序、提高了访问资源的效率、安全性得到了保证。在系统扩展方面,Shibboleth 采用了 SAML 规范,同时也在 SAML 上作了改进,保证了系统的可扩展性。

Shibboleth 主要由 3 个部分组成:

(1)Origin

对应 Identity Provider(IdP),身份提供端。主要作用是向资源提供者提供用户的属性,以便使资源服务器根据其属性对操作进行判决响应。

(2)Target

对应 Resource/Service Provider,资源/服务提供端。主要作用是响应用户的资源请求,并向该用户所在的 Origin 查询用户的属性,然后根据属性做出允许或拒绝访问资源的决策。

(3)WAYF

WAYF 是 Where Are You From 的首字母简称。SHIRE 使用 WAYF 来进行大部分初始化工作。WAYF 组件知道每一个 Origin 端句柄服务器的名称和位置。其主要功能

是将Origin端站点名称映射到HS信息上。WAYF的另一个作用是为用户查询HS并将句柄发送给SHIRE。WAYF通过与用户打交道,询问“你从哪来”,用户输入组织名称,WAYF便在用户组织的名称与HS的URL之间进行映射。

## 2 SAML简介

安全断言标记语言SAML(Security Assertion Markup Language)提供了一个健壮的、可扩展的数据格式集,在各种环境下交换数据和身份识别信息。SAML将所有与检索、传输和共享安全信息相关的功能标准转化为以下形式[2]:

(1)为用户提供XML安全信息格式,请求、传输信息的格式。

(2)定义这些消息与SOAP(Simple Object Access Protocol)等协议协作的方式。

(3)为像Web SSO(Single Sign-On)类似的常见用例定义精确的消息交换。

(4)支持多种隐私保护机制,包括在不披露用户身份的情况下确定用户属性的功能。

(5)详述在Unix、Microsoft Windows、X509、LDAP、DCE和XCML技术所提供的格式中处理身份信息的方法。

(6)提供系统的元数据机制,使得所有参与的系统能就所支持的SAML选项进行通信。

SAML的设计特别关注了灵活性,当遇到标准尚未涵盖的需求时,可以扩展。其所描述的环境包括3个角色,如图1所示,即信任方(Service Provider)、断言方(Identity Provider)和主题(与身份信息相关的用户)。


图1 SAML中的角色

IdP与SP通过SAML消息传送用户的身份认证和属性等信息。SAML消息定义了2种重要的语句:(1)身份验证语句,关于该主题在何时何地、使用何种身份进行过验证的报告。SAML提供了超过20种不同身份验证方法的详细定义。身份验证语句支持SSO,其中IdP代表SP进行登录。(2)属性语句,包含了与主题有关的属性。属性语句中典型的属性是组和角色。

SAML定义了一组XML格式的请求和应答消息,SP可使用这些消息直接获取断言[3]。请求会指定SP需要的信息,例如“所有张晓明的属性”,应答消息返回1个或多个匹配请求的断言。为使不同的产品能够交互操作,SAML的SOAP绑定详细说明了怎样在SOAP消息体中传送信息。SAML还为支持联盟身份环境提供了其他许多有用的机制:(1)协议允许SP确定通过将来自几个可能IdP的特定用户请求指示到何处;(2)协议允许2个IdP将他们各自拥有的同一个用户账户关联在一起(需用户许可)。另外,SAML还支持加密全部断言(也可选择加密其敏感部分)、指定一个断言的目标用户等功能。

## 3 Shibboleth在本系统中的作用

(1)系统将基于Shibboleth的框架进行开发,但不完全使用Shibboleth,需要根据用户的实际需求对其进行改造。

(2)Shibboleth构成跨域统一身份认证系统的核心部分,包括IdP、SP和WAYF组成的整个跨域统一身份认证系统的架构。

(3)通过将Shibboleth的IdP组件与各个学校的统一身份认证系统集成,将身份数据的管理和身份凭据的认证交给各个学校自身的统一身份认证系统。跨域认证中心只是作为跨域认证的索引,并不维护任何身份数据。

## 4 跨校统一身份认证系统的实现

### 4.1 跨校统一身份认证系统设计

该身份认证系统可分为3个子系统,身份提供方IdP(Identity Provider)、服务提供方SP(Service Provider)和身份联盟中心FC(Federation Centre)。这3个子系统在实现联盟认证时,工作原理与Shibboleth基本相同。下面从实现用户身份联盟认证的角度介绍这3个子系统的结构、工作机制以及交互方式。

#### 4.1.1 身份提供方(IdP)

IdP是负责认证用户身份和提供用户认证、属性信息的实体,它需要维护3个模块,即单点登录认证系统、数据库系统和Shibboleth的IdP组件。

##### 4.1.1.1 单点登录认证系统

单点登录认证系统(Single Sign-On Authentication System)是源组织的SSO认证系统,负责响应用户的身份认证请求并生成SSO Token[4]。加入身份联盟的先决条件就是源组织已经可以实现统一身份认证,在此基础上,源组织无须对SSO认证系统做出变动。目前使用较多SSO系统有SUN、Oracle、IBM、Microsoft等厂商推出的统一身份认证系统,身份联盟系统都将提供很好的兼容。

##### 4.1.1.2 认证数据库和用户属性数据库

认证数据库(Authentication DB)是源组织SSO认证系统的一部分,为SSO提供认证数据并直接服务于单点登录认证系统。

用户属性数据库(User DB)主要为Shibboleth的IdP组件服务,它存储了身份联盟系统所需要的用户属性信息。

##### 4.1.1.3 Shibboleth的IdP组件

Shibooleth的IdP组件主要工作单元分为句柄服务器HS(Handle Server)和属性中心AA(Attribute Authority)2个部分。

(1)句柄服务器(HS)

用户通过源组织的SSO认证后，HS根据用户浏览器中cookie值颁发身份联盟的认证句柄作为用户在联盟中的身份凭据。获得认证句柄的过程既可以通过用户浏览器的Browser/POST和Browser/Artifact方式来实现，也可以通过SAML中的身份验证断言(Authentication Assertion)来实现。SAML定义了<samlp:AuthenticationQuery或<samlp:AssertionIDReference>字段的<samlp:Request>消息，通过它可以得到用户身份认证的断言(Assertion)，从中获取句柄信息。用户获得句柄后就获得了访问联盟中服务提供方的合法身份。

(2)属性中心(AA)

AA为服务提供方(SP)提供用户相关的属性信息，这些信息又可分类为用户固有属性信息和用户访问策略信息。用户固有属性信息存储在用户属性数据库(User DB)的数据中；用户访问策略信息则是由属性中心的属性释放策略ARP(Attribute Release Policy)提供的XML配置文件，包含了指定用户是否可以访问指定资源的决策信息。ARP文件定义了一系列的默认策略，同时也支持用户配置策略，用户配置策略的制定工作将统一交由身份联盟中心(FC)负责。

AA与SP通信也是基于SAML系统。服务提供方的属性请求器(Attribute Requester)可以利用SAML中定义的包含<samlp:AttributeQuery>字段的<samlp:Request>消息来发送属性请求，属性中心通过<saml:SubjectConfirmation>来确认属性请求器的身份是否合法(该步骤可选)，如果属性请求器是可信的，属性中心将发送包含<samlp:AttributeStatement>字段的<samlp:Response>断言作为应答。属性请求器解析<samlp:Response>断言就可以得到SP所需要的用户固有属性或访问策略定义。

#### 4.1.2 服务提供方(SP)

SP是提供基于Web的服务、应用或资源的实体，通过安全的途径实现资源的授权访问和个性化服务。主要包含2个模块：mod_shib模块和SHAR模块。

##### 4.1.2.1 mod_shib模块

mod_shib是Shibboleth用于集成到SP Apache服务器的一个扩展模块，负责根据IdP提供的用户访问策略和本地访问控制策略对资源进行访问控制。

##### 4.1.2.2 SHAR模块

SHAR(Shibboleth Attribute Requester)是运行在服务提供方服务器上的一个后台程序，负责向IdP请求用户属性相关的信息并处理响应消息。实际上SHAR是与IdP的属性中心AA配合工作的，当SP需要用户属性信息时，SHAR将以通过认证后获得的句柄(Handle)为凭据，向AA发送属性请求的SAML消息，AA返回属性查询结果，交由SHAR解析作为mod_shib模块实现访问控制的依据。

#### 4.1.3 身份联盟中心(FC)

FC的主要功能是用于用户的源组织选择，即当用户访问非源组织资源需要认证时，将由FC提供源组织定位服务。该功能主要基于Shibboleth的Service Discovery组件，也可称为WAYF服务。另外，本项目中的FC还根据需求提出了资源注册、计费、审计等辅助功能。

WAYF服务在Shibboleth结构中是一个可选组件，采用集中的方式让用户选择自己所在的源组织。

WAYF服务必须支持Shibboleth的认证请求方式，即浏览器Browser/POST和Browser/Artifact认证请求方式或者SAML认证请求方式，目的是为了协调源组织的SSO服务和身份联盟系统中的SSO服务。WAYF实际上充当了各源组织SSO服务的中介，使各源组织的SSO在整个身份联盟系统中都具有有效性。

### 4.2 跨校统一身份认证系统框架

#### 4.2.1 全局架构设计

(1)每个高校都具有双重身份：既是服务提供者(SP)，又是身份提供者(IdP)。

(2)存在一个Discovery服务(即WAYF服务)，当用户没有经过认证而访问SP时，由Discovery确定用户应该到哪个IdP去进行身份验证。

整体逻辑架构[5]说明如图2所示。

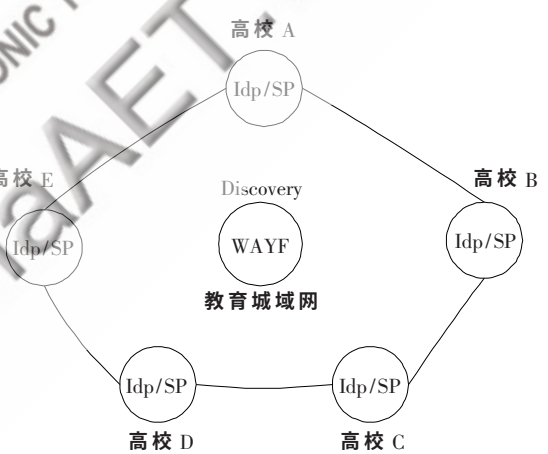


图2 身份联盟系统全局架构

#### 4.2.2 单一高校内部的系统架构设计

为了更清楚地说明整个逻辑架构，图3所示为各个高校的内部逻辑架构图。

高校内部逻辑架构[6]说明：

(1) 高校中的IdP基于原有的身份认证系统，在原有系统基础上加入2个IdP组件：认证凭据和属性凭据。

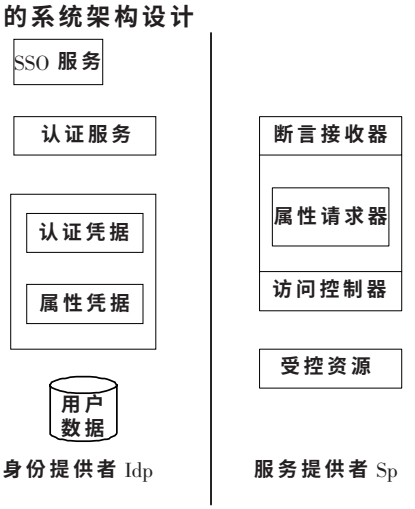


图3 单一高校的内部架构

(2)高校的 SP 提供并保护高校的受控资源,在受控资源之上增加 3 个 SP 组件:断言接受器、属性请求器和访问控制器。1 个 SP 可以保护多个受控资源。

4.2.3 联盟认证过程

4.2.3.1 用户未登录时访问高校 A 的资源(系统视角)

场景:用户第一次访问高校 A 的受控资源如图 4、图 5、图 6 所示。

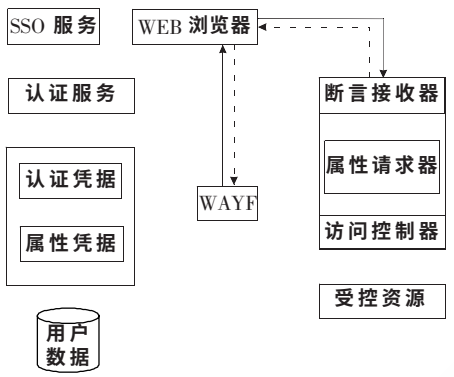


图 4 用户访问某一高校受控资源

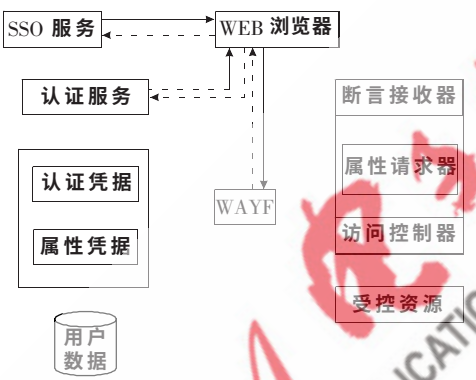


图 5 用户访问某一高校的 Idp

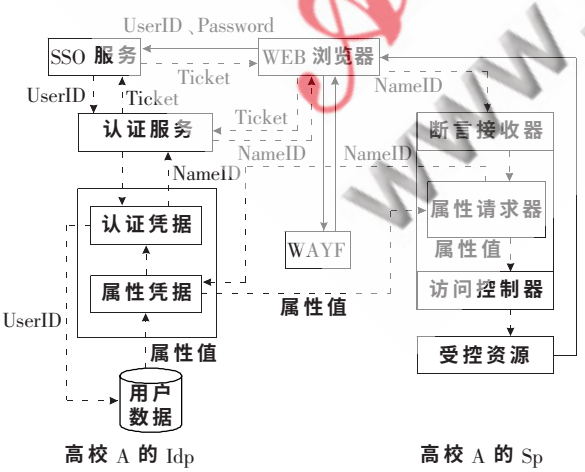


图 6 用户进行身份认证的过程

用户访问某一高校受控资源步骤如下:

(1)用户向高校 A 提出访问请求。

(2)高校 A 的断言接受器发现该用户未认证,将请求重定向给联盟认证中心的 WAYF 服务器。

(3)WAYF 服务器将学校选择界面发送给用户,让用户选择所能认证的 IdP。

用户访问某一高交的 Jdp 步骤如下:

(1)用户选择高校 A 后,提交给 WAYF。

(2)WAYF 重定向到高校 A 的认证服务。

(3)高校 A 的认证服务发现用户尚未登录,将请求定向到 SSO 服务。

(4)SSO 服务向用户发出高校 A 的认证登录界面。

用户进行身份认证的过程步骤如下:

(1)用户输入用户名口令,向高校 A 的 IdP 认证登录。

(2)高校 A 的 SSO 服务对用户认证,通过后生成 Ticket(用户 A 通过认证后的证明),交给浏览器。

(3)请求重定向到高校 A 的认证服务,该认证服务到 SSO 服务上去验证之前生成的 Ticket。

(4)SSO 服务验证 Ticket,通过后将用户的 userId 交给认证服务。

(5)认证服务将 userId 交给认证凭据。

(6)认证凭据为该用户产生一个 nameId,这是整个联盟认证过程中用户的唯一标识,并将该 nameId 返回给认证服务。

(7)认证服务将 nameId 发还给浏览器,浏览器再次访问高校 A 的 SP。

(8)高校 A 的断言接受器接受认证后用户的请求,传给属性请求器。

(9)属性请求器根据来访用户的 nameId,向认证该用户的 IdP 的属性凭据请求用户的属性。

(10)高校 A 的属性凭据根据该 nameId 从认证凭据处获得用户真实的 userId。

(11)属性凭据根据获得的 userId 从用户数据库中获得用户身份信息的属性值,将属性值返回给高校 A 的属性请求器。

(12)高校 A 的属性请求器将属性值发送给访问控制器。

(13)访问控制器根据用户的属性决定用户可访问的受控资源,并将结果返回给用户。

4.2.3.2 用户未登录时访问高校 A 资源(用户视角)

用户可视认证过程如图 7 所示。

访问高校 A 资源的整个过程如下:

(1)用户向高校 A 访问受控资源。

(2)用户收到回复,要求其选择所在的高校。

(3)用户选择其所在的高校。

(4)用户收到其所在高校的登录认证页面。

(5)用户填入用户名密码,并提交。

(6)用户获得所需要的受控资源。

本文参考 Shibboleth 的架构,完成了跨校身份联盟

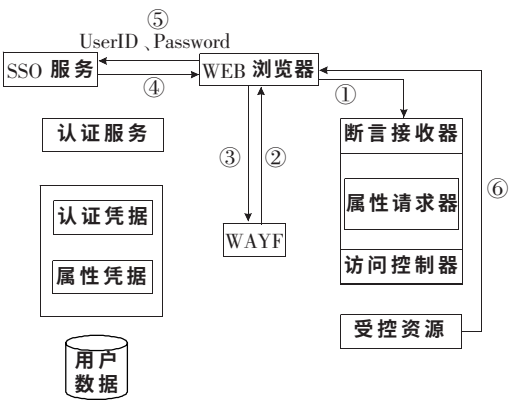


图 7 访问高校 A 资源(用户视角)

系统的设计方案,实现用户“异地访问—本地认证”的功能,避免了异地认证的繁琐,简化了业务流程。身份联盟各子系统交互采用 SAML 标准,有效地保证了系统通信的安全,保障了用户的隐私,很好地满足了应用管理的需求,为高校间的合作和信息交流提供了一个良好的平台。

**参考文献**

[1] Shibboleth support.http://shibboleth.internet2.edu/support,2009.

[2] CANTOR S, HITCH F. Bindings for the OASIS security assertion markup language(SAML)V2.0 S1[M]. OASIS Standard. 2005.

[3] 陈科,余堃,黄迪明.基于安全断言标记语言辅件技术的单点登录系统分析 [J]. 计算机应用,2005,25(11):2574-2576.

[4] CHAO Y Y. Weakest link attack on single sign-on and its case in SAML V2.0 Web SSO [J]. Computational Science and its Applications, 2006,3982:507-516.

[5] 宋志强,陈怀楚,沈锡臣.校园网统一身份认证结构及基于此结构的应用漫游的实现[J].计算机工程与应用,2002,38(10):188-191.

[6] 陈小云.统一身份认证系统的研究与实现[D].成都:西南交通大学,2007.

(收稿日期:2009-09-10)

作者简介:

孙思纬,男,1982 年生,硕士研究生,主要研究方向:交通信息工程及控制。

夏洪山,男,1952 年生,教授,博士生导师,主要研究方向:交通信息工程及控制。