基于SAML的联邦身份信任与授权机制研究*

李崴[1]　张华[2]

（1 中国科学院国家科学图书馆武汉分馆，武汉 430071；2 武汉大学计算中心，武汉 430072）

摘 要: 本文首先介绍了 SAML 标准及其模型，然后提出了一种基于 SAML 的联邦身份信任与授权机制。该机制具有平台无关性，松耦合性和信息安全性，能够对合作机构的相关服务进行有效整合，并能够保障用户隐私，从而满足服务提供者和用户的需求。

关键词: SAML； 联邦身份管理； 单点登陆

An Identity-Federated Trust and Authorization Mechanism Based on SAML

Li Wei[1]　Zhang Hua[2]

(1. The Wuhan Branch of the National Science Library, CAS,Wuhan 430071,China

2. Computer Center，Wuhan University,Wuhan 430072,China)

Abstract：In this paper, SAML standards and SAML models are introduced firstly, and then an Identity-Federated Trust and Authorization mechanism based on SAML is proposed. This mechanism is platform independent, coupled loosely, security, and can support related services to carry out effective cooperation and protect user's privacy, meeting the requirements of users and service providers.

Keywords：SAML；federated identity management；single sign-on

0 引　　言

随着网络技术和信息技术的不断发展，越来越多的系统通过 Web 服务、门户和集成化应用程序彼此链接，各应用系统需要为彼此共有的用户群提供联合服务。这些系统各自使用独立的认证授权体系，分别维护着不同的安全策略和用户信息库，导致了业务关系的相对孤立，并浪费系统资源，降低系统执行效率。同时，用户被迫在不同的应用下使用不同身份和口令多次登录，这也造成了孤立的用户体验。对于服务提

*作者简介：李崴（1973-），男，湖北武汉人，副研究馆员，研究方向为数字图书馆技术、网络与信息安全技术。张华（1973-），男，湖北武汉人，博士研究生，研究方向为多媒体网络通讯技术，分布式计算。

供方和用户来说，迫切需要一种便捷、安全的身份认证机制来简化登录多个系统的繁琐过程。消除这种访问孤立和业务孤立的关键是建立一种标准化的、跨管理域的联邦身份访问与授权机制。

单点登录（Single Sign On，简称为 SSO）是目前比较流行的多系统业务整合的解决方案之一。SSO 是指在多个应用系统间，用户只需要登录一次就可以访问所有相互信任的应用系统。在原有单点登录模型中，往往将所有加盟站点的主体及其属性的相关信息集中存储在一个大型中心资料库，形成中心验证站点，为其加盟站点提供身份认证服务。这种集中式的认证模式导致了加盟站点为获得单点登陆而失去了对自己用户信息的所有权。基于安全断言标记语言（SAML）的联邦身份管理模式则通过联合识别、验证和授权的形式克服了这一问题。验证和授权的联合机制允许机构自己拥有并能控制主体身份数据，并能够以结构化的、受控的方式与协作机构共享这些数据。

本文提出了一种基于 SAML 的联邦身份认证与授权机制，能同时满足多项业务联合服务和用户单点登录的需求，并能有效保障认证强度，保护用户隐私。

1 SAML 概况

安全断言标记语言（Secure Assertion Markup Language，简称 SAML）是国际标准化组织 OASIS 发布的一种标记安全断言的 XML 扩展，它是一种在不同的安全域中交换身份验证和授权信息的技术框架。SAML 提供了一个健壮且可扩展的数据格式集，可在各种环境下交换数据和身份识别信息，目前已经被用来解决 SSO（单点登陆）和 Web 服务安全等重要问题。由于 OASIS、自由联盟和 Shibboleth 各个系统最初对 SAML 有相应程度的扩展，修改和扩展了最初的 SAML 1.0 规范来支持不同的用户，因此联邦身份管理存在 5 个不兼容的协议：OASIS 安全声明标记语言 1.0 和 1.1、自由联盟 ID-FF 1.1 和 1.2 以及 Shibboleth。这些联邦协议不能互操作，或者说不向后兼容。OASIS、自由联盟和 Shibboleth 于是联手开发出新的单一标准 SAML 2.0，替换掉他们以前的工作成果。SAML 2.0 消除了阻碍进一步采用联邦身份的最大障碍——多协议复杂性，因而大大改变了联邦身份的局面，同时也使其支持更广范围的应用，包括电子商务等。

SAML 应用的实现主要由三个部分组成：（1）主体（Principals），即用户；（2）服务提供者（Service Providers，以下简称 SP），即各种应用系统，是为用户提供应用或 web 服务的实体；（3）身份提供者（Identity Providers，以下简称 IDP），即身份认证服务器，负责认证用户。

SAML 提供如下三种类型的断言（Assertion）：

（1）认证断言（Authentication Assertion），描述了用户身份验证信息，如认证机构、方式、有效期等；认证断言一般是由 IDP 发出，用于证明已登录用户的身份。

（2）属性断言（Attribute Assertion），定义了某主体具有的属性信息，如主体的所属用户组、访问级别、信用等级等。

（3）授权决定断言（Authorization Decision Assertion），决定是否允许用户对特定资源的访问以及访问权限。

在单点登录过程中，SP 和 IDP 交换信息，以实现用户身份的认证与授权。IDP 负责创建包含用户身份的断言，然后安全地将这个断言发送给 SP。SP 负责在让用户访问之前验证断言的有效性。在实际应用中，很多应用服务器根据所处角色的不同，可以既是 SP 又是 IDP。

SAML 建立了一种独立于协议和平台的验证和授权交换机制，且能够用于集中式的、分散式的以及联合式的部署场景。这样使得 SAML 具有以下特点：它提供单次登陆身份验证的功能，可以大幅度地减少站点之间地复制安全性和身份验证信息地需求；SAML 可令不同类型的安全服务系统之间实现交互；SAML 不依赖于它所交互的任何系统，每个系统都可为用户的身份验证和授权建立自己的策略。

2 联邦身份信任模型

联邦身份管理（Federated Identity Management，FIM）提供一个简单的、松耦合的模型，用于跨管理域或安全域的身份认证和访问权限管理。在这种模式中，多个安全性域之间的应用系统自行负责本系统用户身份的认证，同时基于开放标准来鉴别信任关系，从而建立起可安全交换身份信息的联邦关系。只要用户被联邦内的（也就是可信任的）一个应用所认证，该用户就获得联邦内其他机构的信任（不必再次登陆）。这种机制可以大大地简化机构内和机构间的用户身份管理工作，使认证和授权数据跨越组织界限。

以中国科学院国家科学图书馆（简称国科图）为例，建有随易通、学位论文、机构仓储、集成检索等多个应用；与国科图相关的应用有高校图书馆系统、中科院 ARP 系统、Elsevier 等商业数据库系统。这些系统共同拥有一群用户，但彼此应用上是独立的，难以形成联合服务。由于这些应用是跨地区和跨机构的，且需要自己维护用户信息库，也很难通过集中认证模式来解决单点登陆问题。

上述这些应用系统可形成一个身份联邦，基于对相互联邦身份的信任，可以共享用户身份信息和策略数据，从而将各应用系统耦合在一起，形成联合的服务应用，为用户在联邦站点之间的导航提供更丰富的体验。例如某科研所用户同时具备中科院“学位论文”、“机构仓储”和 Elsevier 数据库的访问权限，在传统模式下他必须分别以不同身份和口令登陆上述 3 个网站来获取资料。在联邦身份模式下，用户登录中科院“学位论文”系统后，即获得了“学问论文”系统对他身份的验证。根据事先约定的多方信任关系，当“机构仓储”或 Elsevier 接受到此用户服务请求时，会自动到“学问论文”系统询问其身份的有效性，此时“学问论文”系统返回断言证实此用户确实是自己的用户。这样“机构仓储”和 Elsevier 数据库也在一定程度上信任该用户，无需用户再次登陆即可按照用户属性授予相应的权限的服务。

国科图及相关应用构成的联邦身份模型如图 1 所示。

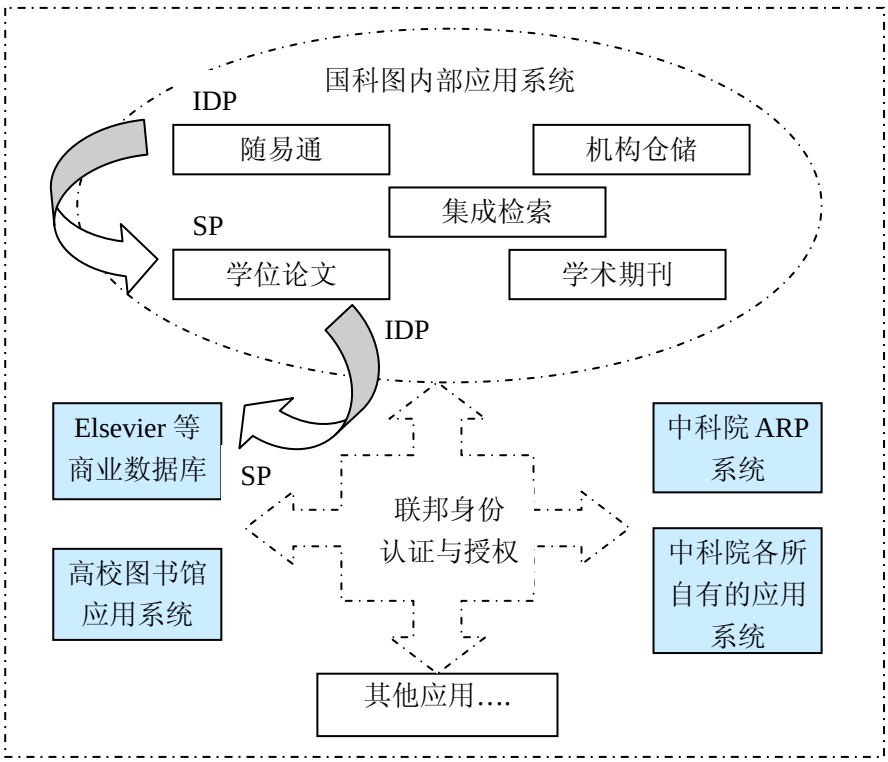

图 1 国科图及相关应用的身份联邦

图 1 中，各应用系统基于对彼此身份的信任组成身份联邦，每个应用系统既可以作为 IDP，也可作为

SP，在不同的访问场景中，同一个系统可分别扮演不同的角色。例如，“随易通”系统的用户想访问“学位论文”系统时，“随易通”系统作为 IDP，负责对该用户的身份进行认证，然后安全地将这个用户的属性断言发送给“学位论文”系统（服务提供者 SP）。“学位论文”系统负责在用户访问之前验证其断言的有效性，并基于用户属性进行相应的访问控制。

当“学位论文”系统的用户要访问“Elsevier”数据库（SP）时，“Elsevier”验证该用户身份来自受信任的联邦站点（学位论文系统），然后根据用户属性提供相应权限的服务。此时“学位论文”系统就变成了身份提供者 IDP。

联邦身份信任模型可以大大地简化用户身份管理的复杂度，降低管理成本，可以为用户提供具有良好体验的联合服务，登陆一次就可以访问机构内部和机构合作伙伴之间（联邦范围内）的其他资源，有效解决大型机构中用户跨地域或跨管理域访问时的用户身份管理工作。

3 认证与授权

SAML 提供了一组有用的机制，可在规模庞大的环境中实现联邦身份管理。在 SAML 中，最重要的环节是 SP 如何获取对主体的断言，根据 SAML 断言传递方式的不同，认证主要有两种方式：一种是 SP 拉方式，一种是 IDP 推方式。SP 拉方式是 SP 主动到 IDP 去了解主体的身份断言，而 IDP 推方式则是 IDP 主动把主体的身份断言通过某种途径告诉 SP。

3.1 SP 拉方式

该方式的主要特点是，SP 获得客户端的凭证（IDP 对用户的一种身份认可）之后，主动请求 IDP 对主体凭证的断言。如图 2 所示，用户是根据凭证去访问 SP 的。

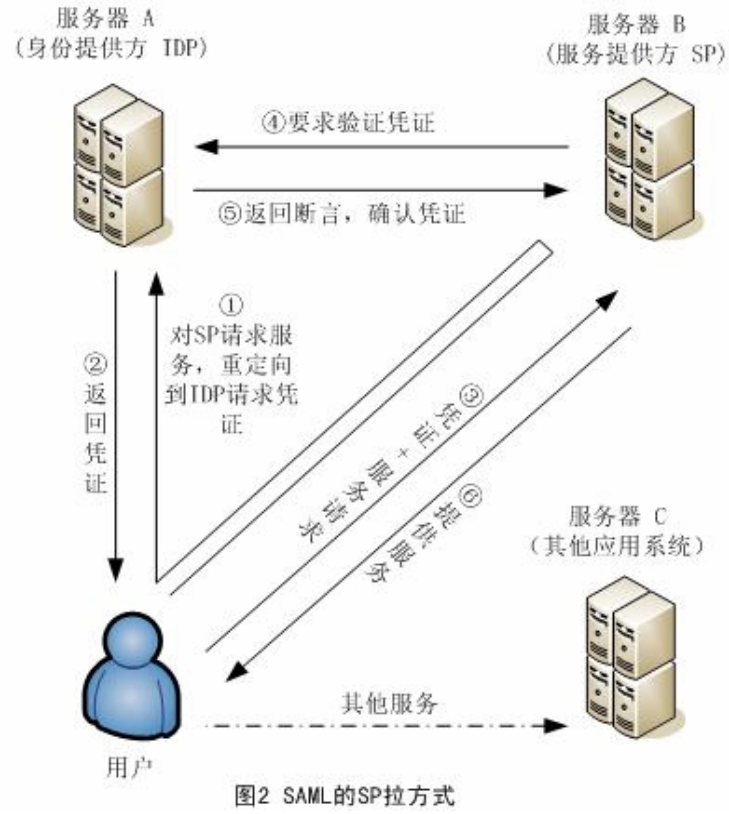

图2 SAML的SP拉方式

SP 拉方式工作机制：

① 用户访问 SP 的受保护资源，SP 发现用户请求中没有包含任何的授权信息，于是它重定向用户访问 IDP；
② IDP 通过验证用户提供的信息（账号、密码），来确定是否发放凭证。认证通过后，IDP 生成一个认证断言和一个凭证（此凭证是一个全局唯一的标识符，通过它可以找到相对应的服务器，进而建立断言和凭证的一一对应关系），然后将此凭证作为参数返回给用户；
③ 用户将获取的 IDP 凭证和服务请求同时提交给 SP；
④ SP 接受到用户的凭证，它在提供服务之前必须验证该凭证，于是它产生了一个 SAML 请求，要求 IDP 对凭证断言；
⑤ IDP 根据对应关系将断言返回给 SP，并删除断言与 Artifact 之间的对应关系；
⑥ SP 信任 IDP 的 SAML 断言，它根据认证断言判断用户的身份，确定是否为用户提供服务；根据属性断言来判断为用户提供哪些授权服务。

3.2 IDP 推方式

该方式的主要特点是，IDP 交给 Subject 的不是凭证，而是断言。过程如下：
① 用户首先登录 IDP，或者访问 SP 的授权服务时被 SP 重定向到 IDP 的登录界面；
② IDP 验证用户身份；
③ 与 SP 拉方式不同，IDP 对用户身份进行验证后，并不生成凭证，而是直接将用户断言和服务申请重定向到原来 SP；
④ SP 根据此断言判断用户的身份，如果合法则将为该用户提供相应权限的服务。

以上两种方式各有优点，IDP 推方式可以减少 SP 与 IDP 之间的交互，节省网络带宽，但往往被认为是不够安全的。因为当 SAML 断言被 IDP 发出后，在断言的有效期限内，站点无法队断言的状况进行跟踪。相对而言 SP 拉方式则安全性更高，断言被保存在 IDP，供 SP 实时查询，可确保断言的时效性；发送给用户的只是凭证，SP 查询过凭证后，IDP 立即删除凭证与断言的对应关系，可有效防止重放攻击。

3.3 信任模型的逻辑结构

从逻辑上联邦身份信任模型的各项应用可分为应用服务器、认证服务器、身份数据库和资源服务器。他们之间的逻辑结构见图 3。

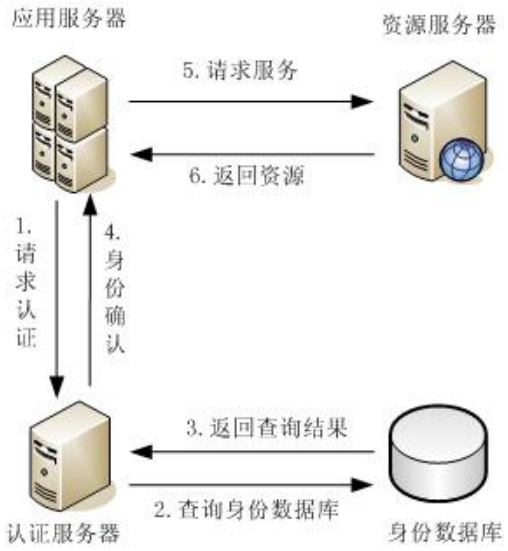

图3 信任模型的逻辑结构图

模型中，认证服务器可以被多个应用服务器所共用。应用服务器也可根据用户来源选择不同的认证服务器。根据应用服务器收到请求的性质不同，可分为如下几种情况：收到用户发来的认证请求时，直接转向认证服务器，按照图 3 中 1-4 的步骤进行身份验证然后提供服务；当应用服务器收到一个带有 SAML 断言的请求时，则依照策略对 SAML 进行校验，根据验证结果和自身策略提供相应服务；收到的请求如果带有凭证，则可根据凭证反向找到认证服务器，并请求对该凭证的断言。然后根据返回断言结合自身策略来作出相应处理。

3.4 联邦身份信任模型的特点

分布式认证的单点登录

在这种分布式认证机制中，用户由本域的 IDP 进行身份认证，基于联邦站点间的相互信任实现了单点登录，简化了用户登录多个系统的繁琐过程，有效解决了集中式认证中用户信息过于集中、用户信息不能自主拥有等诸多问题。

适用性强

联邦身份认证机制基于 SAML 规范，屏蔽了不同平台和架构的特殊性，可灵活在各种平台上选择 B/S 或 C/S 架构；这种简单的、松耦合的认证模式有效避免了用户信息的同步更新等复杂的实现，还具有较强的开放性，能与其他协议如 SOAP，SMTP 绑定，为各种联合服务提供安全认证，具有较广的适用范围。

隐私保护

这种认证授权方式由 IDP 和用户决定用户自身信息的哪些部分可以提供给 SP。提供给 SP 的往往并非用户姓名、年龄等确切信息，而是关于用户身份属性的断言，如请求学位论文时提供用户的属性断言为某研究所博士生（并非真实姓名），这样用户隐私得到了较好的保护。

4 安全性

由于联邦身份的认证机制是基于 SAML 在多个站点间建立的信任关系，所以安全性是需要考虑的一个非常重要的因素。SAML 断言在网络传输过程中必须的安全性受到保证，因此必须采用一批制定完善的安全标准（包括 SSL 和 X.509）来保护 SP 和 IDP 之间通信的安全。

联邦身份管理是一种统一身份认证的机制，在整个访问过程中客户端只进行了一次身份认证，因此需要在 IDP 保证身份认证的强度。存储在数据库中的用户信息应采用有效的加密措施，确保即便有人打开数据库，也无法获得用户的个人信息和的密码。

SAML 断言一旦发出就不在发出者的控制之内了。比如，可能在未定的时期内持续使用断言，或者选择与最初的发出者不知道的第三方共享这些信息。 为防止重发攻击，通常需要在每个消息中嵌入一个时间标记（或消息序列号）令牌，并对其进行 XML 签名。

5 小　　结

本文使用 SAML 实现联邦身份管理机制，能方便地实现单点登陆功能，减少了用户在多个安全域中重复登录的负担，带来良好的用户体验。同时也有效地实现了合作机构间的联合服务，有效降低管理工作成本，提高系统可靠性。可以预见，随着 SAML 规范的发展，这种模式的适用范围及安全性也将更加完善。

参考文献:

[1] Assertions and protocols for the OASIS security assertion markup language(SAML) v2.0 [EB/OL].

http://docs.oasis-open.org/security/saml/v2.0/,2008-4-20.

[2] Security and privacy considerations for the OASIS security assertion markup language (SAML) V2.0 [EB/OL]. http://docs.oasis-open.org/security/saml/v2.0/,2008-4-20.

[3] Shin D, Ahn G, Shenoy P. Ensuring information assurance in federated identity management[C]. Proceeding of IEEE International Performance Computing and Communications Conference,2004:821-826.

[4] 梁昌勇，李劳.基于 SAML 的信任移植模型[J].微计算机信息，2008，24（3）：162-164.

[5] 王洪生，袁捷，曹春生，董媛媛..基于 SAML 的身份联盟建立的研究[J].计算机工程与设计，2007，28（21）：5122-5124.