第 19 卷第 4 期 广西科学院学报 Vol. 19, No. 4
2003 年 11 月 Journal of Guangxi Academy of Sciences November 2003

Web 服务环境下基于 SAML 的联合单点登录系统设计*

SAML-Based Federated Single Sign-On System in Web Services Environment

刘 利 苏德富
Liu Li Su Defu

(广西大学计算机与信息工程学院 南宁 530004)
(Coll. of Comp. & Info. Engi., Guangxi Univ., Nanning, 530004)

摘要 根据 Web 服务的特点，设计一个适用于 Web 服务要求的联合单点登录系统。该系统的用户声明采用安全声明标记语言 (SAML) 描述，消息间的保密性由 WS-Security 保证。该系统具有跨越平台的特性，可以减少用户注册、认证次数以及企业管理用户信息的开销。
关键词 联合单点登录 Web 服务 SAML
中图法分类号 TP393
Abstract According to the characteristics of Web service, a SAML-based federated single sign-on system that secrecy by WS-Security is designed, and it may reduce the login frequency and manage cost of enterprise.
Key words federated single sign-on, Web service, SAML

Web 服务[1]的出现使得企业与它的合作伙伴、客户以及员工之间的关系变得更加紧密，企业也更能根据后者的需求提供实时的服务。但是，现在认证用户（或者获得用户属性）的机制普遍要求用户先注册，访问站点时用户首先要认证自己（一般是通过用户名/密码），才能调用不同的站点（可能位于不同域）提供的服务。这样用户需要在每个自己感兴趣的站点注册，每次使用站点服务时都要先认证自己。用户必须记住许多用户名和密码，非常的不方便，如果用户对用户名密码管理不当丢失的话，还会给系统带来威胁；对企业来说需要管理大量用户的用户名和密码等个人信息，开销也不小。

针对这类问题出现了“单点登录”[2]这个概念。是指用户在一个域登录后可以使用不同域里的资源，而无需再次认证自己。现在已有的单点登录系统有 Novell 公司的 SSO 系统，微软的 TrustBridge 系统等，但是这些单点登录系统受应用环境的限制，如后者就只能用于 Windows 平台。本文在文献 [3] 提出的联合单点登录概念及其理论框架的基础上，根据 Web 服务的特点及要求，设计一个适用于 Web 服务具体环境的联合单点登录系统。此系统最主要

2003-06-09 收稿。
* 广西壮族自治区教育厅科研项目(桂教科研[2001]401 号)资助。

的一个特点是基于 SAML[4]，因此，可以跨越平台的限制，克服现有单点登录系统的不足。

1 安全声明标记语言

安全声明标记语言（Security Assertion Markup Language，SAML）是一种完全基于 XML1.0 的描述语言，因此，它继承了 XML 跨越平台的数据表述特性。它的主要设计目标之一是单点登录，用它可以描述系统在不同站点之间传输的用户“声明”，就可以跨越平台、语言、计算机体系结构等的限制。

SAML 是一种描述语言，而并非一种新的认证或者授权技术。它定义一个基于 XML 的用于交换安全信息的框架，这里的安全信息是指对一个主体的声明。声明是 SAML 的基本数据对象，是对主体（人或计算机）的身份、权限、属性等的描述。现阶段定义了 3 种声明的格式：认证声明、授权决议声明、属性声明。认证声明是描述与身份鉴别相关的信息，如被认证主体的 DNS 域和 IP 地址、认证采用的方法、认证时间等；授权决议声明是描述根据指定的证据，对一个请求者对一特定资源的所授权行为的决定（允许、拒绝、无法确定）；属性声明是描述与授权相关的信息，如主体的系统用户标识、所属用户组、角色，以及可访问的资源及权限）。除了这 3 种声明外，用户可以自己定义声明元素，但考虑到互操作以及一致性，用户要慎重使用。

SAML 规范的协议部分定义了通过请求/响应方式的请求和响应格式。它需要和具体协议的绑定（把 SAML 请求/响应的消息交换映射成标准的消息或者通信协议称为“SAML 协议绑定”或“绑定”），才能实现声明的生成和交换。在 SAML 规范中描述了 SAML 如何与 SOAP 以及 HTTP 绑定。

2 联合单点登录系统的设计

联合的前提是企业或站点之间相互信任，可以共享用户信息。联合单点登录使企业可以构建一个安全 B2B 和 B2C 的电子商务框架，而不光只是 B2C 的；系统可以实现用户在其源注册站点登录后就可以访问联合组织内不同站点提供的服务。根据应用要求以及 Web 服务特点，系统设计时考虑如下 3 个问题。

（1）互操作性。不同站点（企业）提供服务的平台，实现服务的语言可能互不相同，但是用户在源站点验证身份通过后，源站点产生的“声明”必须能够被其它站点理解才能达到系统本身的目的。这就需要采用统一的且能跨越平台的描述语言。我们设计采用 SAML 实现这一功能。

（2）隐私问题。由于用户个人信息由用户所注册的源站点管理，有时候其它站点一样需要知道一些关于此用户的信息。这需要由用户来决定。我们设计采用 WS-Policy[3]来描述用户的隐私策略，共享用户信息的时候必须满足此策略。

（3）消息的安全问题。由于 Web 服务环境下，一个消息从请求方到接收方可能会通过多个中介，这要求有端到端的安全机制。我们设计采用 WS-Security[5]来提供单个消息端到端的安全，确保不同站点提供服务之间交换消息的安全。

2.1 系统用例

图 1 是系统的用例，其中：（1）注册是参与者用户执行。一个新的用户要使用联合组织内某个站点上的服务时，如果该用户从未在此联合组织内注册过，那么需要首先注册，以后

用户的信息就由用户注册的站点管理，并根据用户的隐私策略同其它站点共享用户信息。系统返回用户名/密码。(2) 请求声明是参与者用户执行。用户请求源注册站点产生一个认证此用户的声明，以后用户调用其它站点的服务时，就在请求消息中包含此声明即可，而不用再次输入用户名/密码认证自己。(3) 管理个人信息是参与者用户执行。用户可以修改个人信息，以及个人隐私策略。(4) 验证声明是参与者系统代理。这里的系统代理只是一个代理程序，也是系统的一部分，它负责处理用户的请求，当用户请求调用服务，若消息中含有声明时，它便请求用户注册的源站点验证此用户声明的有效性。

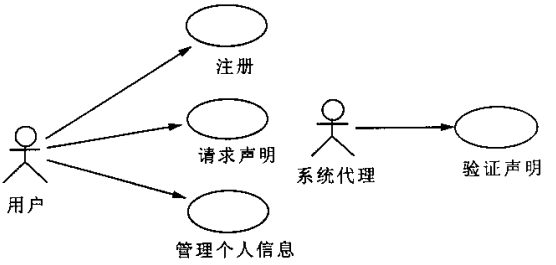

图 1　系统用例

2.2　用户调用服务的顺序

企业 A 和企业 B 相互联合信任，且其站点里都装有联合单点登录系统。现有一个用户已经在企业 A 站点注册，现在用户想调用企业 B 站点服务的顺序（图 2）如下：(1) 用户输入用户名和密码，请求用户“声明”，系统验证用户名/密码，验证通过则产生用户声明，否则拒绝请求；(2) 系统返回用户声明给用户；(3) 用户请求调用企业 B 的服务，请求消息中包含用户 A 产生的声明；(4) 企业 B 请求企业 A 验证此声明的有效性；(5) 企业 A 返回验证结果给 B；(6) 企业 B 根据 A 的验证结果处理用户请求（验证通过则允许用户请求，否则拒绝）。

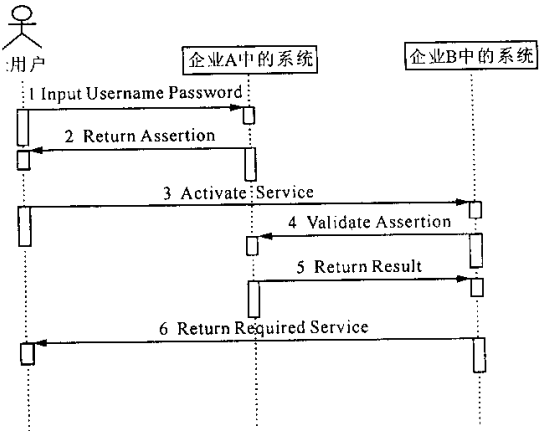

图 2　用户调用服务的顺序

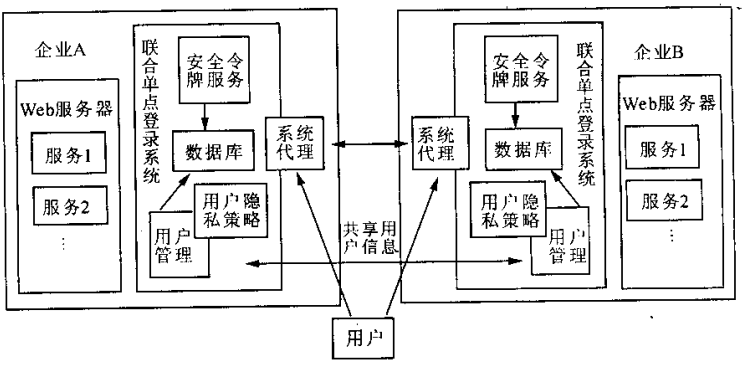

图 3　单点登录系统结构

上面的 (4) 和 (5) 对用户来说是透明的。请求消息中若含有敏感信息（如用户名/密码

等)，需用 WS-Security[5]里面提供的加密方式对敏感信息加密。企业中提供的服务也可充当用户的角色，只是它代表一个或几个用户而已，其处理过程与单个用户的时候一样。以上只给出了 2 个企业的联合，实际应用中可以是很多个企业联合，只要他们之间相互信任。

2.3 系统结构

联合单点登录系统主要由安全令牌服务、用户管理、数据库以及系统代理组成。每个用户在调用企业服务时，都首先经过系统代理，系统代理根据用户的请求，作相应的处理（调用用户管理或安全令牌服务），通过认证后才允许用户调用服务。

系统代理：负责处理用户请求，根据用户请求调用相应的服务。用户没有被认证时要求用户认证自己。若用户请求注册，则调用注册服务，若用户请求认证“声明”或者其它企业的系统代理请求验证声明时，系统代理调用安全令牌服务；安全令牌服务：验证用户名/密码，产生用户“声明”，验证来自联合组织内其它企业的系统代理请求验证的“声明”；用户管理：注册新的用户，管理用户信息（包括取回密码，修改密码，注销，修改自己的隐私策略）；用户隐私策略：根据用户隐私要求，用 WS-Policy[6]描述用户隐私策略；数据库：存储用户信息及用户隐私策略。用户与企业、企业与企业之间的通信可以采用标准的通讯协议（HTTP 等）。他们之间的消息格式都采用 SOAP 格式，然后与下层的通信协议（HTTP）绑定传输。其中请求/返回用户声明(用 SAML 描述)，在 SAML 中定义请求/响应的消息格式，并在 SAML 的协议绑定部分说明了如何同 SOAP 绑定，再通过 HTTP 传输。SAML 声明的传输可以采用在 SAML 中定义的方式，也可以采用文献[7]中定义的在 WS-Security 中传输 SAML 声明的方式。

3 结束语

联合单点登录系统的用户声明采用 SAML 描述，而 SAML 继承了 XML 跨越平台的优点，使系统克服了以往单点登录系统受平台限制的缺陷，并适用于 B2B 和 B2C 的情况。系统消息之间的保密性由 WS-Security 保证，满足了 Web 服务环境下端到端安全级别的要求。系统是以 Web 服务的形式提供给用户。如果要减少企业间因为验证用户“声明”的通信，企业可以在本地加个用户“声明”的缓存。联合单点登录系统可以减少用户注册、认证自己的次数，以及企业管理用户信息的开销，具有很好的应用前景。

参考文献

1 柴晓路. Web 服务架构与开放互操作技术. 北京：电子工业出版社，2003. 1.

2 Chamberlin N. A Brief Overview of Single Sign-On Technology，Http://www.gitec.org/assets/pdfs/pdf2000/Single%20Sign-On.pdf，2000.

3 IBM Tivoli Federated Identity Management and Secure Web Services. Http://www.rv-nrw.de/Koop/TivoliIdMgr/FederatedIdentity_technicalWP.pdf，2002-11.

4 Hallam B P，Maler E. Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)，Http://www.oasis-open.org/committees/security/docs/，2002-12-05.

5 Kaler C. WS-Security. Http://msdn.microsoft.com/library/default.asp? url=/library/en-us/dnwssecur/html/securitywhitepaper.asp，2002-04-05.

6 Kaler C，Hondo M. WS-Policy. Http://msdn.microsoft.com/ws/2002/12/Policy/，2002-12-18.

7 Kaler C. WS-Security Profile for XML-based Tokens. Http://xml.coverpages.org/WS-Security-XML-Tokens.pdf，2002-08-28.

（责任编辑：邓大玉 曾蔚茹）