文章编号：1005-8451（2004）10-0032-03

单点登录技术在铁路信息系统中的应用探讨

张 勇
（上海铁路局 电子计算技术中心，上海 200071）

摘 要：主要针对目前铁路信息系统用户管理各自独立的现状，介绍了单点登录技术及 SAML 的原理，并提出了单点登录技术在铁路信息系统中的实现方案，使得用户进行一次身份认证就可达到对多个应用系统进行访问，提高了用户工作效率，增强了系统整体安全性。

关键词：单点登录；SAML；铁路信息系统；实现
中图分类号：U29-39 **文献标识码**：A

Discussion on application of single sign-on technology in Railway Information System

ZHANG Yong
(Electronic & Computing Technology Center of Shanghai Railway Administration, Shanghai 200071, China)

Abstract: Aimed at the independent situation of user management work in Railway Information System, it was introduced the principle of single sign-on and SAML technology, proposed the solution of single sign-on technology in Railway Information System. It could make the users interview a lot of application systems with an identity authentication, improve user's working efficiency, strengthen the whole security of the system.

Key words: single sign-on; SAML; Railway Information System; implementation

铁路内部信息系统构架庞大而复杂，应用系统彼此之间缺乏联系。随着 Internet 和电子商务的发展，铁路必须不断地突破自身限制，需要向客户和合作伙伴开放更多的信息系统，为他们提供对其内部系统及应用程序的访问，安全和管理方面的挑战更为严峻。因此，应该设计一种协同工作使得可以只需进行一次身份认证就可达到对多个应用系统进行访问，来统一管理各类用户对应用系统的安全访问。

收稿日期：2004-09-02
作者简介：张 勇，工程师。

积分管理分 3 部分：积分卡办理，积分统计和积分奖励兑现。

（1）在旅客办理积分卡时要把相关信息录入内网数据库，并且把这些信息通过数据传输程序传到外网数据库，这样持有积分卡的旅客就可以通过电子商务平台直接用积分卡号登录，进行订购车票；

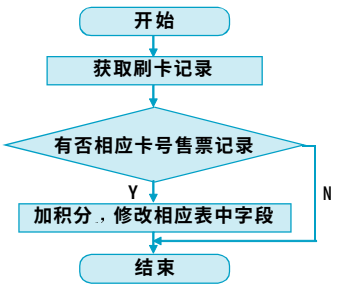

图 6 积分管理流程图

（2）按照旅客买票乘车的积分规则，结合旅客在列车上刷卡记录进行积分统计，并传输到外网数据库；根据积分卡用户的积分情况，车站的工作人员为旅客兑现积分奖励，同时扣掉相应积分。

3 结束语

目前我们的网上订票系统还只是与铁路的客票系统相结合，只发售京沪直达庞巴迪列车的车票。很多旅客都通过 e-mail 或留言对我们网上订票的开通表示欢迎和肯定，同时迫切希望能通过铁路电子商务平台买到更多其它车次的车票。由于铁路的运能与运量的矛盾比较突出，全面推广网上订票这一售票方式在客观上有一定的难度。对此我们现在在对旅客的回复中只能表示遗憾。但我们的系统已充分考虑了可扩展性。我们有理由相信，随着铁路建设跨越式地发展，我们的网上订票系统将为人们提供更多更好的服务！

1　单点登录

1.1　传统的单点登录

采用单点登录（Single Sign-On，SSO）方式时，系统需要从用户那里收集所有必要的证明和用户凭证信息，用以支持可能会与之发生作用的其他应用时对用户的认证。SSO并不是J2EE（一种利用Java 2平台来简化企业解决方案的开发、部署和管理相关的复杂问题的体系结构）中的标准实现，而是各家中间件提供商在提供J2EE应用服务器集群时提供的一种认证信息共享的机制，所以各家厂商提供的实现方式不一样。

通常情况下，实现SSO的流程如图1所示，用户就可以按照系统安全策略的规定，访问那些（也只有那些）授权访问的资源，无需进一步登录到这些不同的系统、资源、应用和网络上。

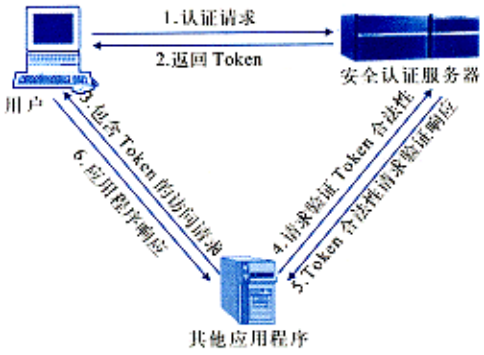

图1　单点登陆模型

1.2　SAML介绍

前面所讲的是在一个企业安全域内的单点登录，用户可能还有跨企业安全域访问的需求。铁道部下属的各铁路局，不同铁路局之间需要互相访问对方的资源，而且随着电子商务的发展，铁路商务网站（货物物流中心、客运网上售票、EDI集装箱电子数据交换等）与其他合作伙伴之间也经常需要通过网络来交换机密的资料或数据，两者往往采用不同的安全系统。如何提高跨越企业边界的安全信息互操作性，使各不相同的安全系统身份认证达到一体化是一个极具挑战性的问题。

OASIS组织发布了单点登录安全标准“Security Assertion Markup Language（SAML）V1.0”。SAML针对不同的安全系统提供了一个共有的框架，允许企业及其供应商、客户与合作伙伴进行安全的认证、授权和基本信息交换，能够在多个企业运营的站点之间实现单点登录等基于网络的安全相互连接功能。

SAML是一种基于XML语言用于传输认证及授权信息的框架，以与主体相关的断言形式表达。在这里，主体是一个实体（人或计算机），这个实体在某个安全域中拥有一个特定身份，断言可传递主体执行的认证信息、属性信息及关于是否允许主体访问其资源的授权决定。一个SAML断言包含着有关何时、以什么方式、对什么资源允许访问的信息。SAML提供认证断言、属性断言、决定断言和授权断言这几种不同类型的安全断言。

1.3　SAML的工作原理

（1）用户向认证机构提交证书。

（2）认证机构对用户的证书进行断言，并且产生一个认证断言以及一个或更多的属性断言。用户立即就会得到由SAML断言的认证和识别令牌。

（3）用户使用这个SAML令牌尝试访问受保护的资源（比如一个需要认证的站点）。

（4）用户对保护资源的访问请求被策略实施点PEP截取，同时用户的SAML令牌（认证断言）被PEP提交给策略决策点PDP（Policy Decision Point）。

（5）PDP负责根据已有的安全策略作出决策。使用相关安全策略作出授权决策后，PDP返回一个授权决策断言。如果声明表示可以接受某种级别的授权，一个属性断言就被追加到用户的SAML令牌中，用户就能够以单点登录方式呈现给信任的伙伴，访问受保护的资源了。如果断言表示不接受任何级别的授权，客户在访问受保护的资源前将被重定向到重新登录窗口。

2　单点登录在铁路信息系统的实现方案

2.1　B/S应用的单点登录实现方案

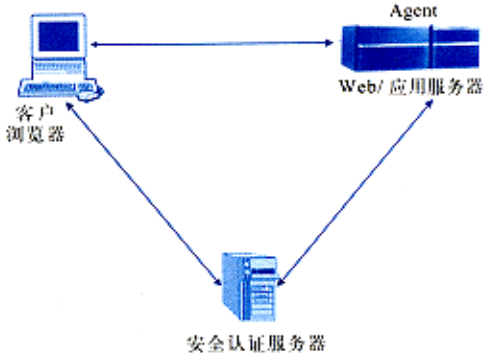

图2　B/S应用的SSO实现方案

B/S应用的SSO实现过程：

（1）客户浏览器请求访问位于Web/应用服务器上的受保护的URL资源。

（2）Agent截获访问请求，并检查是否有有效的身份认证标识（Token）。

（3）如果没有有效的身份认证标识（Token），Agent将其重定向到安全认证服务器进行认证。如果有有效的身份认证标识（Token）则执行6。

（4）浏览器随即到安全认证服务器进行身份认证。身份认证成功后，将身份认证标识（Token）返回给浏览器。

（5）用户通过身份认证后，被重定向到最初请求的资源上。

（6）Agent截获访问请求，并在缓存中检查用户的权限(允许与拒绝访问列表)。

（7）如果没有用户的权限，则向安全认证服务器发请求。

（8）安全认证服务器取得用户的权限，回复Agent。

（9）Agent根据用户权限决定用户是否可以访问Web/应用服务器上的受保护的资源，并缓存用户权限。

（10）用户有访问权限则可以访问其所请求的资源。

一旦身份验证成功，用户可以不需要重新认证就可以在同一会话期间访问被安全认证服务器和Agent保护的其他资源和应用，从而实现单点登录。

2.2 C/S应用的单点登录实现方案

C/S应用由客户端和数据端组成，应用逻辑分散在客户端和数据端。C/S应用客户端功能强大，但显示逻辑与应用逻辑混在一起。对于铁路内部存在的大量C/S应用程序，必须开发一个专用的基于标准的Web服务，在安全认证服务器和应用程序之间交互，实现单点登录。实现过程与B/S模式大致相同，在此不再作赘述。

2.3 跨路局的单点登录实现方案

采用SAML可以实现跨越路局边界的单点登录，有2种实现方式：即浏览器/辅件（Artifact）档案和浏览器/POST档案。在使用浏览器/Artifact时，一个SAML Artifact作为一个URL查询串的组成部分传输。SAML Artifact是指向一个声明的指针。在使用浏览器/post时，SAML声明在一个HTML表格内被上载给浏览器，并作为一次HTTP post的有效载荷的组成部分传送给目的站点。

下面给出浏览器/Artifact档案方式中用户与铁路内部Web网站互动的过程：

（1）用户的浏览器通过HTTP/安全套接层(SSL)访问源站点（站点起到SAML认证管理机构的作用）；（2）源站点要求浏览器提供用户ID和口令；（3）浏览器通过输入用户ID和口令，回答源站点的询问；（4）源站点调用外部认证服务器（如轻型目录访问协议目录）认证浏览器；（5）浏览器通过点击源站点上的通用资源标识（URI），请求保存在目的服务器上的特定资源，从而重新定向到源站点的“站点间传输服务”URL上；（6）源站点保持会话并生成一个生存期暂短的SAML认证，来声明一个事件已经发生（根据认证声明上的条件以及被请求的目的服务和资源定义的策略）；（7）源站点将声明信息保存在本地缓存中；（8）源站点利用SSL将一个包含SAML Artifact（一种8字节Base64串）的URI返回给浏览器，这个附加的SAML Artifact指向认证声明并将浏览器改向连接到请求的目的站点和资源；（9）目的站点使用SAML Artifact从源站点请求/索取这个引用的认证声明（通常通过SSL会话）；（10）目的站点保持会话，解析/验证认证声明信息，并批准浏览器对请求资源的访问。

要实现跨越铁路局边界的单点登录，各铁路局应事先达成合作协议，且各铁路局的安全系统都可以识别SAML 数据，可根据SAML声明判断用户的身份，或决定用户在本局内的访问许可权。

3 结束语

单点登录SSO使得可以只需进行一次身份认证就可达到对多个应用系统进行访问，提高了用户工作效率，增强了系统安全性，减轻了繁重的管理负担，降低了高昂的成本。采用SAML实现的SSO同时提高了跨越企业边界的安全信息互操作性，使各不相同的安全系统身份认证达到一体化，优化了网络系统的安全管理控制。单点登录SSO必将在铁路内部信息系统和电子商务（货物物流中心、客运网上售票、EDI集装箱电子数据交换等）中得到广泛应用。

参考文献：

[1] H.M.Deitel,B. DuWaldt. WEB服务实用技术教程[M]. 北京：机械工业出版，2004.