第34卷 第14期 计 算 机 工 程 2008年7月
Vol.34 No.14 Computer Engineering July 2008
·网络与通信· 文章编号：1000—3428(2008)14—0121—02 文献标识码：A 中图分类号：TP393

# 可插入式单点登录技术的应用

赖慎禄[1,2]，李 新[1]，及俊川[1]
(1. 中国科学院计算机网络信息中心，北京 100080；2. 中国科学院研究生院，北京 100049)

**摘 要：**以统一的用户接口作为实现单点登录(SSO)的配置接口，在SSO服务过程中动态配置并生成新的应用服务接口，实现SSO服务接口的可扩展性。以安全的票据共享方式实现SSO多个应用的身份跨域共享，利用双重票据作为单点登录的安全增强机制，通过插件式应用确保SSO的快速实施和灵活调整。

**关键词：**单点登录；插入式；票据；身份认证

# Application of Pluggable SSO Technology

LAI Shen-lu[1,2], LI Xin[1], JI Jun-chuan[1]
(1. Computer Network Information Center, Chinese Academy of Sciences, Beijing 100080;
2. Graduate University, Chinese Academy of Sciences, Beijing 100049)

**【Abstract】** This paper uses the uniform user interface as the config interface to realize Single Sign-On(SSO). New interfaces for a new application are generated during the SSO service process, and SSO is implemented as self-extended. Secure tickets sharing pattern guarantees the security of cross domain identification in SSO, and twofold ticket is used to strengthen that. Pluggable implication reinforces the quick start and the adjustment of the SSO.

**【Key words】** Single Sign-On(SSO); pluggable; ticket; authentication

## 1 概述

随着网络技术和信息技术的发展，信息化已深入社会的各个领域。在同一部门内通常有多个功能不同的应用信息系统。用户每天需要登录到不同应用系统进行业务处理，如网络、邮件、数据库和各种应用服务器等。传统应用系统中各用户的认证信息相互独立，在各系统中独自处理。单点登录技术[1]通过用户的一次性鉴别登录获得需访问系统和应用软件的授权，在此前提下，管理员无须修改或干涉用户登录便可方便地实施希望得到的安全控制，或在分布式计算环境中安全地鉴别用户。可插入式单点登录是基于统一认证协议的活动框架。各应用服务以插件形式部署于单点登录中，在进行一次认证后，各应用系统充分信任单点登录服务票据信息的正确性，不再主动参与其他身份认证过程。各应用系统共享相同的认证库，对用户信息进行统一管理，从而减少出错几率并增强系统安全性。

## 2 SSO原理

单点登录(Single Sign-On, SSO)又称为一次登录，可插入式[1]单点登录在单点登录的基础上提高用户对管理的敏捷性。用户在访问不同业务系统时需要独立访问该业务系统并在各系统间频繁切换，操作较复杂，无法快速获取相关业务信息并加以利用。而在安全性和系统管理方面，企业需要大量IT技术管理人员，分别管理和维护不同系统(如ERP、统计分析、OA、财务、Notes系统等)的用户信息。因此，需要建立可靠、安全、保密的业务系统网络环境，以保证企业业务不受破坏和干扰。

本文通过实现插入式单点登录为企业用户提供统一的信息资源认证访问入口，建立统一的、基于角色的和个性化的信息访问、集成平台，使用户只须一次登录就可根据相关规则访问不同的应用系统，提高了信息系统的易用性、安全性、稳定性，并在此基础上实现了企业用户高速协同办公和企业知识管理功能。由于企业的业务系统通常采用异构系统(在不同平台上建立不同应用服务器的业务系统)，因此在确保业务系统独立运行的前提下，要解决单点登录、安全防护和信息保密等相关技术问题。

## 3 SSO的关键技术

### 3.1 单点登录协议

本文描述的单点登录协议简单实效，且足够安全。此协议通过请求生成共享的TGT(Ticket Granting Ticket)信息[2]，该TGT信息在多次访问或多个应用系统切换时被共享，TGT本身不服务于具体应用，只作为共享的用户信息在网络中安全传递，是获取ST(Service Ticket)[2]的途径，用户通过ST来访问服务。TGT只与Server相关，解决了单点登录无法跨域实现的局限性。与TGT相反，ST是服务的一个具体应用，每个应用可能有相同的TGT但各自的ST唯一且只能用于本应用，因为ST只服务于单独的应用，所以能以任意方式在网络中传输而无须考虑重放等安全性问题。单点登录本身有相应TGT和ST的实体，虽然它们保护TGT的方法有区别，但最终都可以实现一次登录多个应用访问。在整个协议中，Server与Client的通信都基于XML来传递，协议过程如 图1所示。用户从Web浏览器中向应用系统发送业务请求，业务系统检查用户是否通过认证，若不存在票据凭证，则转入单点登录服务(即SSO Server)中进行认证。得到相应凭证票据后转到请求的业务系统中，业务系统对票据进行确认以生成用户在SSO

**作者简介：**赖慎禄(1982－)，男，硕士研究生，主研方向：信息管理技术；李 新，副研究员、博士后；及俊川，高级工程师
**收稿日期：**2007-09-24 **E-mail：**laishenlu@gmail.com

Server中的ST信息及验证ST。业务系统对用户进行业务权限授权工作及业务处理。

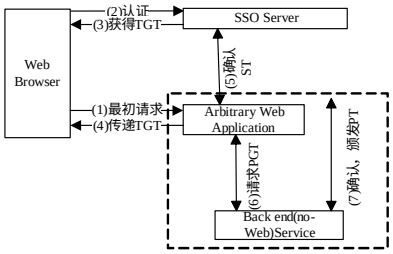


**图 1　单点登录协议**

在图 1 中，对单点登录协议作了代理机制的改进，以支持对非 Web 应用的服务。整个协议过程都围绕凭证票据的生成、管理、传递和检验来完成。在图 1 中，(6)～(7)只在代理模式下进行。

在结构体系上，单点登录协议包含如下 2 方面的内容：

(1)服务器。SSO Server负责完成对用户的认证工作，CAS Server需要单独部署。SSO Server负责处理用户名/密码等凭证[3]，其认证方式可以是到认证库检索一条用户的认证信息或在XML文件中检索用户密码，后一种方式可以实现灵活且统一的接口分离，SSO用何种认证方式与单点登录协议相分离，认证的实现细节可以自己定制和扩展。

(2)客户端。SSO Client 负责部署在客户端(具体应用系统)，SSO Client 的部署通常表明有对本地应用系统的受保护资源的访问请求，并需要对请求方进行身份认证。应用系统不处理任何用户名密码等类似的 Credentials，而是简单地把请求重定向到 SSO Server 进行认证。由 SSO Server 统一对认证进行处理。

### 3.2　即插即用技术

可插入性能提高用户对单点登录的体验并减少对SSO系统管理人员的技术要求，系统管理人员能根据应用需要对SSO 进行调整和修改，而不必关心单点登录协议的实现过程，提高了单点登录应用的可维护性。通过对应用管理系统的动态集成，在不影响单点登录业务操作的前提下，对新的应用管理系统进行热部署，并以自动化采集用户信息代替手工维护，以减少出错几率。

### 3.3　认证库

本文实现了单点登录协议与后端认证库的松散耦合，从配置文件中加载读取与认证库的连接信息，完成与后端凭证库的连接。单点登录协议实现了与多个认证类型库接口支持，包括 LDAP 目录服务、MS-SQL Server, Oracle, DB2 等多种常用数据库。后端认证库与单点登录协议的实现相独立，只与SSO 服务的认证方式衔接，各个认证方式可以选择合适的认证库为存储凭证库，管理人员可以根据业务需要选择认证库和认证方式，也可以在使用过程中更改设置，实现对认证库和认证方式的即插即用。

### 3.4　多种认证方式

单点登录协议为基本用户名密码对认证、使用表单认证机制的认证、基于IP地址认证、基于数字证书认证、基于令牌认证、基于传输协议认证及递进式多重认证机制组合等多种用户认证方式提供灵活插入接口[4]。应用Spring框架的反转控制(IOC)机制可灵活地实现与认证方式之间的连接。认证方式、认证库、单点登录协议在完成SSO服务中以SSO组件形式相互独立，实现可插拔。

应用系统的插拔设计使 SSO 更接近用户习惯，在应用系统的部署中，为用户提供浏览器作为用户统一的 UI，能在页面中添加参数提交请求，在 SSO Server 端动态生成与应用有关的接口信息。在整个部署应用的过程中 SSO 正常处理其他单点登录请求，部署过程不影响服务器端对其他应用请求的处理。在 Server 端可根据应用请求的参数为应用系统生成接口表，以完成与应用系统授权的异步协同。网络管理人员和系统管理员可以通过浏览器在任何地方进行远程访问管理。

### 3.5　代理机制

SSO Proxy[4]的目的如下：当浏览器用户访问应用X时，应用X引用应用A和应用B的授权性资源，并试图代表用户去访问应用A和应用B，因此，应用X需要告诉应用A和应用B当前用户是谁，以便应用A和应用B对用户的Request请求进行授权，这就是SSO代理。为了完成代理，SSO增加代理票据 Proxy Grant Ticket(PGT) 和代理服务票据 Proxy Ticket(PT)[2]，它们被应用X用来代理浏览器用户去访问其他更多的应用凭据，应用X向SSO Server提交ST和PGT，ST是应用X的应用服务票据，PGT最终让应用X获得PT，PT跟ST的作用一模一样，它也是一次性的票据，X传PT给后端的Back-end application[4]，Back-end application就可以根据这个PT获得X现在代理的用户的认证信息了。

在单点登录实际环境中，SSO 仅依赖信任证书的部署和双向 SSL 来实现信任关系的建立和核实。应用 X 和应用 Back-end application 是完全不同的 2 个应用，它们之间没有建立信任关系，如果 X 告诉 Back-end application 关于用户的认证信息，Back-end application 也不会相信，Back-end application 只信任 CA Server，最终问题仍需要 X 通过 SSO Server 向 Back-end application 提交一个用户的认证信息。

### 3.6　异步授权协同

各应用系统对授权机制要求差异较大，为了减少对应用系统原型的修改，单点登录协议实现了各应用系统认证授权的分离[4]。在单点登录中完成对用户的统一认证，处理具体应用请求前按各应用系统的具体要求对用户进行相应授权。

为了减少单点登录的响应时间，采用异步方式完成用户认证信息与用户授权信息的协同工作。当用户发出业务请求时，应用业务系统判断是否已认证用户，若用户未被 SSO 认证，则转入 SSO 进行认证，若已获得 SSO 的认证凭证，则应用业务系统根据SSO的凭证信息对用户进行各自的授权工作。认证和授权异步完成，体现了统一认证的共性和授权机制的个性，满足了各应用授权机制的个性化实现。认证授权的异步协同必须保证SSO服务与各应用系统的用户认证信息及授权信息的完整性和统一性。在插入新应用时，由 SSO 服务动态生成与各应用的接口信息，服务器客户端通过更新对应系统的接口信息完成协同，由 SSO 服务生成对应用系统可访问的权限信息并植入接口信息中，应用系统增加对应用户的业务应用权限以实现最后业务处理的授权工作，并返回握手成功信息到 SSO 服务接口中，由 SSO 服务对用户信息作最后的更新。在相同用户信息具有多个应用的访问权限时，每修改一次用户对应用系统的访问权限，就要进行一次协同。

异步认证与授权和单点登录协议提供了即插即用的可能性[4]。单点登录协议实现认证与授权的分离，异步认证与授权实现认证与授权的再结合。插入的应用系统作为SSO的一个服务对象由SSO提供服务，而各应用系统仍保留各自对业务需求的权限控制。

(下转第 125 页)