企业信息门户单点登录系统的设计与实现①

Design and Implementation of Single Sign – on in Enterprise Information Portal

陈观林　张　泳　（浙江大学城市学院 计算机科学与工程学系 浙江 杭州 310015）

摘　要：本文介绍了一个企业信息门户中单点登录系统的设计与实现。系统实现了一个基于 Java EE 架构的结合凭证加密和 Web Services 的单点登录系统，对门户用户进行统一认证和访问控制。论文详细阐述了该系统的总体结构、设计思想、工作原理和具体实现方案，目前系统已在部分省市的广电行业信息门户平台中得到了良好的应用。

关键词：单点登录 企业信息门户 Web 服务 认证 访问控制

1　引言

随着计算机信息技术的迅猛发展，Web 技术应用已在全球范围内普及。信息技术不仅实现了企业内和企业间信息的共享，而且改变着企业的经营运作方式。企业信息门户（Enterprise Information Portal，简称 EIP）就是近年 IT 领域一项重要的新技术，也是企业信息化的重要发展方向。

EIP 将企业的所有应用和数据集成到一个信息管理平台之上，并以统一的用户界面提供给用户，使企业可以快速地建立企业对部门、企业对员工的信息门户。EIP 是一个基于 Web 的系统，它通过唯一的访问入口，将企业各种不同的管理系统、数据库系统以及网络共享资源集成在一起，为用户提供形式多样的信息和统一安全管理机制。EIP 的构建涉及 Portal、内容管理、数据集成、单点登录等多方面的内容和技术，单点登录则是其中尤为重要的功能。

2　单点登录技术

单点登录（Single Sign On，简称 SSO）是一种认证和授权机制，主要目的是为了方便用户访问多个系统。用户只需在登录时进行一次注册，就可以在多个系统间自由穿梭，不必重复输入用户名和密码来确定身份，从而实现“一次登录，全网访问”。单点登录的实质是安全上下文（Security Context）或凭证（Credential）在多个业务系统之间的传递或共享。当用户登录系统时，客户端软件根据用户的凭证为用户建立一个安全上下文，安全上下文包含用于验证用户的安全信息，系统用这个安全上下文和安全策略来判断用户是否具有访问系统资源的权限。

SSO 登录方式减少了用户在不同系统中登录耗费的时间，避免了处理和保存多套系统用户的认证信息，缩短了系统管理员管理用户权限的时间，增加了管理的便利性。通过 SSO 功能，使得操作人员在企业信息门户的统一界面中，通过一次登录，可以了解到各个不同系统的信息，而且可以随意切换到相关的功能系统进行专业的业务处理。另外，SSO 系统从根本上抛弃了传统认证中用户名密码以明文传输的方式，而是采用了结合密码学技术的新的认证机制，从而大大提高了整个系统的安全性。

单点登录的原理如图 1 所示，具体的登录验证过程如下：

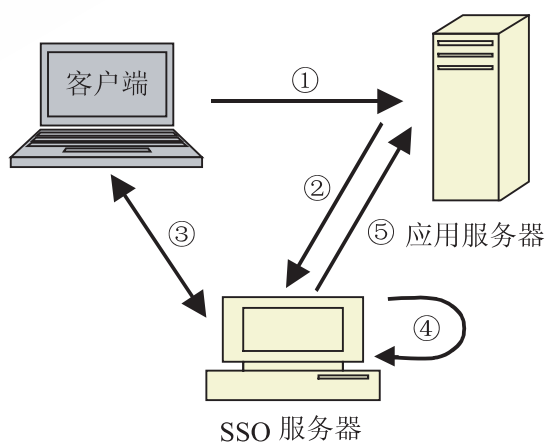

图 1　单点登录原理

① 基金项目：浙江省教育厅高校科研计划项目（20061290）

① 客户端向应用服务器请求访问某资源；

② 应用服务器重定向到 SSO 服务器请求凭证；

③ 如果用户未登录 SSO 安全域，SSO 服务器将请求重定向到身份认证服务；

④ 用户通过身份认证服务后，SSO 服务器为其生成身份标识，并签发身份凭证；

⑤ SSO 服务器重定向到应用服务器，后者验证凭证有效性，从而获得用户身份信息。

目前单点登录系统的实现有多种方法：一种是基于 ticket 凭证加密的认证，如 PKI、Kerberos 系统等；一种是建立在 Cookie 的基础上，如 IBM WebSphere、Bea WebLogic 等；另外一种是采用 Web Services 架构，将统一认证模块做成 Web 服务的方式。

本文通过凭证加密和 Web Services 相结合的方式提出一种 SSO 的解决方案，利用 Java EE 平台的 Servlet 技术提供 Web Services，将权限管理和认证授权进行抽象，集中在 Web 框架中，供所有的业务程序共享，从而提供企业信息门户中不同业务程序的单点登录功能。

3　系统总体设计

下面给出企业信息门户中单点登录系统的总体设计方案，该 SSO 系统通过 Web 服务传递用户身份信息，提供对已有业务系统的安全集成，可以访问门户内所有业务系统和数据，同时利用加密机制保证单点登录的安全性。图 2 为系统的总体结构图，主要包括用户注册/注销、用户登录以及与其他业务系统的验证等功能模块。

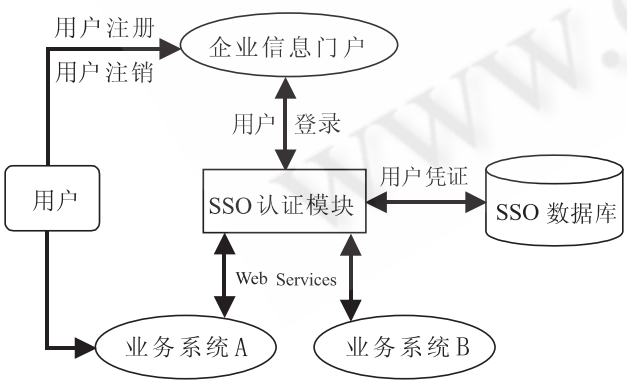

图 2　系统总体结构图

(1) 用户注册/注销流程：

①SSO 服务器管理员在 SSO 服务器上添加注册用户，保存该用户的统一登录名和密码；

②业务系统 A 的管理员在业务系统 A 的管理模块中选择所需注册用户，保存该用户在业务系统 A 的唯一识别字和用户名；

③SSO 服务器管理员可以根据用户的要求选择业务系统 A 对 SSO 的信任级别。信任级别分为三级：始终信任、验证通过时信任和始终不信任(默认为验证通过时信任)。如果选择始终不信任，则可以加强业务系统的安全性，防止其他用户利用单点登录的便利直接登录到安全性要求强的业务系统；

④用户需要在业务系统中注销时，SSO 中的相关信息一并注销。

(2) 用户登录/验证流程：

①用户登录 SSO 服务器时，会生成该用户的数字签名密钥对，并将该密钥对保存在 SSO 数据库中，以后用户登录 SSO，都会用该密钥对对用户名和密码进行签名验证；

②用户在计算机 A 上登录 SSO 服务器后，SSO 服务器会标识该用户已经通过单点登录认证，并进入门户平台。当用户要求启动业务系统 B 时，系统向 SSO 服务器发送请求用户的 SSO 用户名、待启动的业务系统 B 的标识代号，SSO 服务器判断用户是否已经通过 SSO 认证，确认通过验证后，SSO 服务器在用户计算机 A 上启动业务系统 B 的认证程序；

③业务系统 B 的认证程序通过 SSO 服务器的 Web Services 生成此次会话的密钥对，并将该密钥对保存到 SSO 数据库中，然后用其中一把密钥对用户对应的业务系统 B 的登录用户名进行加密，接着 Web Services 将解密密钥、密文和此次会话的 SessionID 发送至请求端。请求端程序用解密密钥将密文进行解密，获取用户对应的业务系统 B 的登录用户名，最后请求端程序验证该登录用户名，如果验证通过，则根据该用户的权限启动业务系统 B，并返回 Web Services 一个 Success 信息；如果验证不通过，则返回一个 Failure 信息。

系统具体认证流程如图 3 所示。

4　SSO 系统的数据库设计

SSO 系统的数据库负责存储 SSO 平台关于单点登录帐号、用户系统绑定、登录信息记录以及帐号加密等数据，主要包括 SSO 用户表、SSO 业务系统表、用户系