电子政务内门户单点登录系统的实现

Realization of Single Sign – on System in E – Government Inner Portal

徐福仓　蔡玲玲　吴 敏　（中南大学信息科学与工程学院 湖南长沙 410083）

摘要：介绍了一个电子政务内网门户单点登录系统的实现。系统基于凭证映射的方法，把用户的主认证身份同后台应用中的凭证相对应，应用端的认证由系统自动完成，并采用 LDAP 目录服务对门户用户进行统一管理和访问控制。它无缝集成采用标准认证机制的原有 web 政务应用系统，为公务员提供统一的信息资源认证访问入口，提高了政务效率效能和信息系统的安全性。

关键词：门户　单点登录　凭证映射　LDAP

1　引言

电子政务内门户是一个面向政府公务员的内部门户网站。它是政府各部门的办公平台，在此实现在线办公、统一审批、信息沟通和知识管理。同时，它提供对"三网一库"体系中的政务专网[1]的入口，在多年的电子政务系统建设中，专网上已建立了多个应用系统，今后，更多的应用系统也需要集成到内门户中。因此，这里就存在着两个问题：第一，用户在访问不同业务系统时需要独立访问该业务系统，往往需要在各系统间频繁切换。第二，用户帐号或密码遗忘现象时有发生，或者一套简单用户名和密码多系统使用，造成保密强度低等问题。

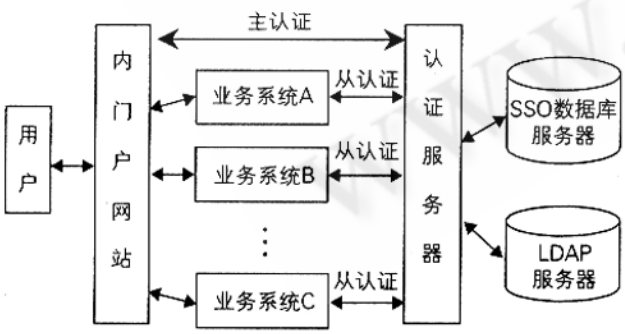

图 1　SSO 系统总体结构图

因此，我们通过在内门户中提取出一个基础性服务子系统：单点登录服务（Single Sign On，SSO），为公务员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展示、集成平台。从而提高政务效率效能和信息系统的安全性。

目前有多种单点登录系统的实现，在这些系统中，其实现方法分为两种：一种是建立在 PKI，Kerberos 和用户名/口令存储的基础上[2,3]，一种是建立在 Cookie 的基础上[4]。但是实施这两种方法的一个前提是必须修改原应用的认证模块，使其符合新的认证机制的要求。本文则采用一种基于凭证映射的 SSO 系统，它针对那些已经存在的且采用标准认证机制（如 basic 认证或 form – based 认证）的 web 政务应用系统而设计，不需要对应用系统的原有认证模块作任何修改，因此能够实现与原有系统的无缝集成。

2　系统总体结构

系统的总体结构如图 1 所示：政务专网上已经存在有 A、B、C 等不同业务系统，而且会随着电子政务的深入而不断增加，用户对这些已有的和以后将新增的业务系统的访问都通过内门户网站这一个入口进行，各业务系统同时与认证服务器进行连接。认证服务器是整个系统的中心，用户对门户中业务系统的访问都被转到认证服务器，认证服务器与 LDAP 服务器进行通信，对该用户进行主认证，即该用户是否拥有进入门户的权限，LDAP 服务器中保存了所有用户相关信息，实现对内门户的所有用户进行统一的管理。

同时，在 SSO 系统中建立了一个加密的凭证库，存

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn

放在 SSO 数据库中，其中存储了每个内门户用户在各个业务系统中的身份凭据。对于通过主认证的人员，该用户身份的二次认证都将交给各个业务系统，用户在每个业务系统中的权限由各自的系统进行控制，最后提供给符合用户身份的应用。

3 单点登录系统的实现

3.1 内门户用户的主认证

整个单点登录系统是应用在内门户上，它是一个 Intranet 环境，其中的用户和 Web 服务器计算机都在同一个域中，而且客户端浏览器为 IE 2.0 以上版本。因此我们可以采用 windows 集成身份验证，集成 Windows 身份验证是一种安全的身份验证形式，因为用户名和密码在通过网络发送之前就进行了散列处理。启用集成 Windows 身份验证时，用户浏览器通过与 Web 服务器进行加密信息交换（包括散列算法）来证明自己知晓密码。

集成 Windows 身份验证使用 Kerberos? v5 身份验证或 NTLM 身份验证，采用共享密钥加密系统，能够满足电子政务内部门户的高安全性要求。

3.2 基于凭证映射的单点登陆过程

用户通过了 portal 的主验证以后，若其要求进一步访问某个后台的集成的业务应用，SSO 系统能够代替用户完成应用端的认证。其过程如图 2 所示。

（1）凭据存在判断。用户访问门户的业务应用系统入口，认证服务器检查所需要的应用程序的用户凭据是否存储在 SSO 数据库中。如果用户是初次访问，没有为该用户存储所需要的业务应用的凭据，用户的浏览器将被重定向到这个业务应用的登录表单，转第（2）步；如果凭据存储在该数据库中，将直接转到第（4）步进行。

（2）凭据存储。用户提供与业务应用定义的配置文件相吻合的凭据，所提供的凭据被映射到该用户的主认证身份，并存储在 SSO 数据库中。

（3）用户被重定向门户的业务应用系统入口。

（4）从认证。认证服务器调用凭证管理组件从 SSO 数据库中检索用户凭据，然后再以合适的认证逻辑将内含的认证信息送到业务系统，并与其认证接口进行交互。

（5）建立连接。后台的业务系统对用户的认证信息进行验证，认证成功后，则向用户发回响应并建立连接会话，用户就能进入到该应用中或检索到所需的信息。

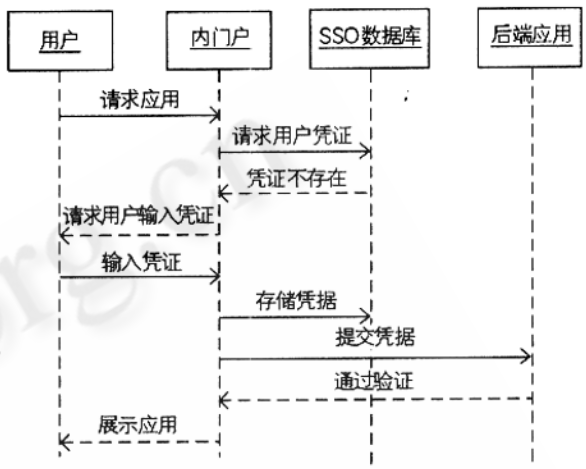

图 2　单点登陆顺序图（初次访问）

下面从业务应用定义、凭证库和凭证管理组件、凭证映射实现机制及基于 LDAP 的人员管理几个主要部分对该系统的实现作具体的介绍。

3.3 业务应用定义

对于内门户所连接到的每个业务应用，都有一个对应的、可配置的业务应用定义。应用程序定义向 SSO 系统提供了该业务应用的相关信息，包括业务应用名称、认证方式、认证需要提供的信息类型、该应用的用户凭据存储数据库等。认证服务器使用该业务应用定义来检索凭据，用于与企业应用程序集成。这个定义由网站的管理员完成，对内门户网站的用户是透明的。业务应用定义保存于一个.xml 配置文件中。

3.4 凭证库和凭证管理组件

用户凭证是用户用以登陆到业务系统的认证信息，比如用户名和密码等，不同的业务应用系统有不同的用户凭据定义。SSO 系统中的用户凭据存储在 SSO 数据库中，并使用单点登录加密密钥来加密。为了增强系统的安全性，需要在一定时间段后更改原密钥，重新生成密钥并重新加密凭据存储区。

凭证管理组件封装了用户对凭证对象的创建、存储和管理逻辑。它由一个 Credentials 类实现，该类的主要方法有：SetCredentials（）方法根据业务应用定义

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn

的来传入用户在该业务系统中的原始凭证信息，加密后存储；GetCredentials( ) 方法能够从根据用户身份从数据库中取得用户解密后的凭证；DeleAllUserCredentials( ) 和 DeleUserCredentials( ) 对用户的凭证进行删除。

3.5 凭证映射实现机制

当一个用户登录门户后，认证服务器从 LDAP 服务器中取得该用户信息，然后根据其需要访问的业务应用，从 SSO 数据库中取得凭证，从而实现由用户身份到业务应用系统用户凭据的映射。

在 SSO 系统实现中，我们把用户在门户中的身份封装成一个 PortalUser 类，把用户在后台业务应用系统中的身份信息封装在另一个类 ApplicatioUser 中，并作为 PortalUser 类的一个内部属性。

每个用户在成功进入内门户后，系统就维护了一个 PortalUser 对象，该对象由唯一的一个 UserId 来进行识别，当该用户访问不同应用系统时，PortalUser 的 ApplicationUser 属性获取应用的 AppId，并通过 Credentials 对象就能获取数据库中用户凭证。图 3 用类图清楚地显示了上述映射关系。

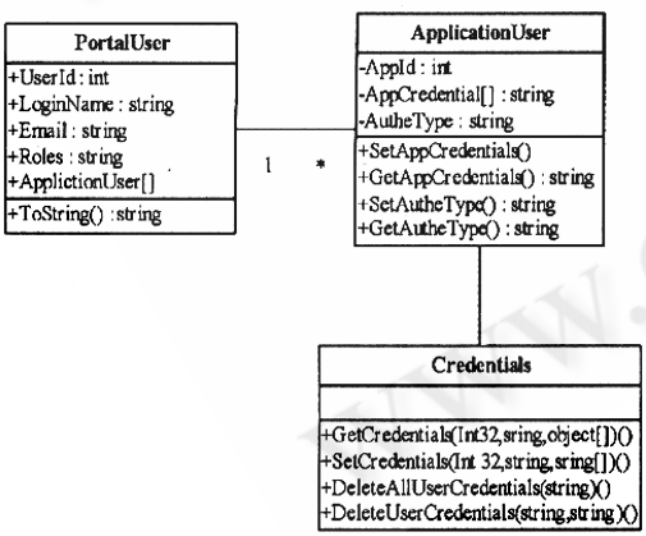

图 3　凭证映射类图

3.6 基于 LDAP 目录服务的人员管理

LDAP 的英文全称是 Lightweight Directory Access Protocol（轻量级目录访问协议），它是基于 X.500 协议标准的，但进行了相应的简化。它具有查询效率高、树状的信息管理模式、分布式的部署框架以及灵活而细腻的访问控制等优点。

内门户中涉及到几万个公务员，几百个部门，既要对人员进行统一规划，又要实现分级管理，因而需要有一个能够实现分布式人员管理的机制。在本系统中，我们采用微软的 Active Directory 建立人员基础信息管理系统：针对整个内门户系统在活动目录里建立一个域，其下创建直属部门的的组织单元（Organizational Unit），在组织单元下创建具体的人员（user），从而形成“域—组织单元—用户”的三级模式的目录管理系统。

通过 AD 的标准 LDAP 访问接口 ADSI（Active Directory Service Interfaces，活动目录服务接口），可以访问目录中的各种对象，提取存储在目录中对象的各种信息，实现对人员的身份信息和权限进行灵活的控制。

4 结束语

本单点登录系统采用基于凭证映射的方法，把用户的主认证身份同后台应用中的凭证相对应，应用端的认证由系统自动完成，并采用 LDAP 目录服务对门户用户进行统一管理和访问控制。系统已在某省的电子政务内网门户上实现，它无缝集成了原有的办公自动化等 web 政务应用，取得了预期的效果。

参考文献

1 全国政府系统政务信息化建设 2001－2005 年规划纲要（摘要），国务院办公厅秘书局，http://news.chinabyte.com/365/1851365.shtml.

2 李小平、阎光伟、王轩峰等，基于公开密钥基础设施的单点登录系统的设计[J]，北京理工大学学报，2002，22(2)：209－213.

3 任 栋、刘连忠，Web 应用环境下安全单点登录模型的设计[J]，计 算机工程与应用，2002，38(24)：174－176.

4 谭立球、费耀平、李建华，企业信息门户单点登录系统的实现[J]，计算机工程，2004，31(17)：102－104.

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn