基于 Shibboleth 的企业信息系统统一身份认证①

杨光露

(河南中烟工业有限责任公司 南阳卷烟厂，南阳 473007)

摘 要：主要介绍企业信息系统中的统一身份认证研究和实践情况。对于一些大型企业而言，其信息系统往往是由不同的业务系统组成的，而且具有分布式的特点，其统一的身份认证就是提高系统运行效率，保证安全性关键之一。就以烟草行业信息系统为例，利用 Shibboleth 构建了一个统一身份认证系统，对相关的系统建设具有一定的借鉴作用。

关键词：Shibboleth；企业信息系统；统一身份认证；单点登陆

Unified Identity Authentication in Enterprise Information System Based on Shibboleth

YANG Guang-Lu

(China Tobacco Hennan Industrial Co. Ltd, Nanyang 473007, China)

Abstract: This paper introduces the unified identify authentication research and some practices in enterprise information system. For some large companies, the information system normally includes many subsystems. These systems are also distrusted. The unified identify authentication is just the key technology to ensure the efficiency and security. This paper uses the Shibboleth to build the unified identify authentication system for information system in tobacco industry. It could give the useful reference for the related system construction.

Key words: Shibboleth; enterprise information system; unified identity authentication; single sign on

1 介绍

随着企业信息化建设的不断推进，各种基于 Internet/Intranet 的业务系统快速增长，这类系统的业务性质一般都要求实现用户管理、身份认证、授权等必不可少的安全措施，但由于应用系统众多，而新的系统不断增加，多个身份认证就会增加整个系统的管理工作成本，为管理使用的各个方面都带来很多不变，这在烟草行业企业信息管理系统中就非常突出[1]。

烟草企业信息系统的目前现状是每个部门都有自己开发的系统，各自按照自己的使用习惯开发，造成信息化标准不一致和信息处理工作不规范，从而难于进行信息交换和实现信息共享;各自的身份认证系统也各不相同，这就显现了一些突出问题：

①对用户而言，需要记忆多个帐户和口令，使用非常不便，同时由于用户口令遗忘而导致的支持费用也不断上涨；

②从管理角度来看，由于无法实现统一的认证和授权，安全策略必须逐个在不同的系统内进行设置，因而造成修改策略的进度可能跟不上策略的变化，无法统一分析用户的应用行为，而且多个身份认证系统还会增加整个系统的管理工作成本；

③从长远发展来看，每个系统都开发各自不同的身份认证系统，势必将造成信息资源的浪费，消耗开发成本并延缓开发进度。

因此，实现统一的身份认证系统就成了企业信息系统发展的关键之一，该系统需要能够对用户进行统一认证管理和系统集成平台，即用户只需要注册登陆一次就可以拥有不同权限使用不同的应用系统[2]。

本文则以烟草行业的信息管理系统建设实践为例，对统一身份认证系统的需求进行了分析，并对目前典型的统一身份认证技术进行了简介，最终选择利用 Shibboleth 进行了统一身份认证的研究与实现。

① 收稿时间:2011-03-17;收到修改稿时间:2011-04-12

2 相关统一身份认证技术简介

由于应用系统本身的复杂性，目前统一身份认证还没有哪一种占据统治地位，很多软件企业都有各自不同的方案，适用于不同的应用环境。而更多的应用单位，如企业高校等则是结合自己的情况进行了相应的开发设计。总体上讲，目前的统一身份认证系统可以分为以下几种构架模式[3]。

首先是采用 ERP(企业资源计划)模式，这是一个全局的、自上而下的过程，不仅身份认证系统统一，各种应用系统数据库也进行统一设计，这种方案实施简单，但系统之间的藕合度太高，数据库统一设计，各部门的信息交织在一起，系统升级非常困难。

另外一种则是应用系统直接与统一身份认证系统松耦合的方式，系统采用一个身份认证注册中心，提供给各个应用系统使用。用户要登录网络，必须先到身份认证系统认证身份，然后才可以访问网络资源。采用这种体系结构的典型技术方案如下所述：

①基于 LDAP 和 Kerberos 的统一身份认证系统。这类系统采用了 LDAP(轻量级目录访问协议)存储用户信息，以提高系统可用性和可靠性，同时缩短响应时间。而采用 Kerberos 认证机制将所有相关网络实体，支持双向认证，极大地提高系统安全性。

②基于 SAML 的统一认证系统。单点登录过程中，应用系统之间通过共享安全信息来避免用户多次登录。利用 SAML 技术，可以构建出能够跨越安全域和管理域、具有良好互操作性的单点登录系统。

③与浏览器相关的认证服务体系。本类系统主要基于浏览器 Cookie 的设置，利用 Cookie 保持用户的身份信息，这在很多网站系统中得到了广泛的应用。

3 需求分析

企业信息系统一般都涉及人事、财务、资产等各个业务的应用系统，在企业的信息化建设时，由于各自的需求不同，而且也缺少一个统一的规划。因此各系统的体系结构也各不相同，而各个系统一般都已经有自己的身份认证系统，因此在设计统一的身份认证系统时，应当能达到下面几个目标：

1)安全可靠。由于企业的所有应用都可以通过该统一身份认证系统访问，该系统的安全性便处在首要的位置。

2)管理者和用户使用方便。对管理者而言，新系统应当能够建立一套有效管理网络资源、日常用户的安全管理机制，保证用户身份验证的准确性和便利性，实现用户权限分配的安全性和灵活性。对用户而言，由于目前企业办公自动化系统都逐渐 Web 化，应当重点实现“一点登录、多点漫游”的目标，也就是实现单点登陆功能[3]。

3)具有良好的扩展性和可集成性。系统应不仅能支持现有的应用系统及其现有的用户系统，当有新的企业应用系统被部署或开发的时候，这个统一身份认证服务可以作为它的身份认证模块的形式工作。

4 基于Shibboleth的统一身份系统应用

4.1 Shibboleth 简介

Shibboleth 源自于 Internet2，是一个中间件产品，其目的是开发一个基于 SAML 标准体系结构和策略框架及一套开放源代码软件,以用于支持机构间的、需要存取控制的 Web 资源共享。Shibboleth 系统从 1999 年开始开发，目前的最新版本是 1. 3 版本[5]。

它利用了“身份和访问管理基础设施”来控制个人的身份验证，它实质上是一个代理服务，资源提供者可以连接到这个服务，用其中的资源来验证请求者是否满足访问标准。Shibboleth 系统由身份提供者、服务提供者和可选的 WAYF 服务以及各种交互子组件组成。Shibboleth 的特点主要表现如下几个方面：

1)极好的隐私保密性和安全性。标识用户身份的是一个不透明的句柄，只有在用户访问资源时，并不是一次将所有的信息全部暴露出来，而是在需要的时候部分暴露。

2)充分解决了单点登录问题。SAML 规范主要是针对单点登陆问题，而 Shibboleth 参照了 SAML 规范，极好地解决了单点登陆问题。

3)灵活的访问控制方式。该系统具有灵活的访问控制的能力，允许用户方通过属性有效地控制访问，继而控制使用代价，而不需要授予不必要的访问。

结合企业的基本需求以及 Shibboleth 的特点，可以看到其基本适合作为企业信息系统统一身份认证的基础系统。

4.2 具体应用

综合企业信息系统建设的情况和 Shibboleth 的特点，首先确定了用户数据中心逻辑上统一、授权管理分布式进行，应用系统多种形式耦合的统一身份认证系统建设方针。

在用户资料数据中心建设方面,目前有两种不同的做法，一种是设置一个集中式数据库，各个节点可以通过计算机网络访问这个数据库。另一种方式是各部门建立自己的数据库。由于本单位的很多部门已经有了各类的身份认证数据库，而且很多的身份记录只

在自己的业务系统内应用，针对这种情况我们采用了第二种方式建立用户数据库，具体的用户库则采用“LDAP+关系数据库”的模式，LDAP 存放用户名和密码等简单信息，而关系数据库则存放比较复杂的用户身份信息，这样就可以利用 LDAP 目录对分布数据操作的良好支持，实现用户信息库总体上逻辑统一，而原有的身份认证库则不需要改变，两类数据利用外部程序定时做数据同步，以保持数据的高度一致性。

访问权限的控制和身份管理方面和用户库设计中遇到的问题一样，各应用系统一般是在不同时间阶段进行开发，并且每个应用系统都有自己的访问控制方式，而且各业务系统对用户身份信息理解不同，从而造成用户身份信息的不一致。如果要采用理想的方式，则必须对现有的应用系统进行改造，需要对应用系统本身的用户、权限等模块进行大规模的改造，工作量和难度都会很大。这里就根据用户库的建立模式，对于一些本部门使用的服务，则仍使用原有的权限管理模式，而另外建立一个中心数据库，与各个 LDAP 数据库进行映射，该数据库则负责一些全公司范围内使用的信息服务的访问权限管理。

与现有应用系统的整合方面，则依照 Shibboleth 系统的推荐模式进行设计，Shibboleth 实际上是基于 SAML 标准，建立了用户数据库与各种应用系统之间的联结关系。Shibboleth 本事可以支持传统的关系数据与 LDAP 等目录数据库，因此只用一些基本的配置即可与身份数据库连接。而对于应用系统而言，Shibboleth 主要关注于浏览器用户，其主要通过 CA 数字证书认证等具体方式支持 Web 应用系统的单点登陆，多点漫游。而对其它一些非 Web 应用系统，则需要自行编制接口，基于 Web Services 技术的统一身份认证系统体现出了自己的优势，特别是在 Internet 环境下，因此可以将 Shibboleth 统一身份认证(身份提供者)封装为一个专门的服务，其它应用系统只需按照一定的规范调用这个服务即可。

为了防止解决了已有的“信息孤岛”问题之后，又带来了新的“信息孤岛”现象，采取了基于松藕合架构的 Web Services 集成，提供了一种循序渐进的方法。对原有系统不需要作大的修改，这就解决了各部门在提出新的信息需求时，面临的是修改还是重新开发系统的两难选择。这一做法让系统开发可以从较简单的模块开始，直到建立起复杂的集成化应用系统。此外，从条件较成熟的领域或部门先行推进;信息中心做好系统分析、项目组织管理;结合软件公司合作开发等做法，都是该统一身份认证系统建设的特色所在。

4.3 效果分析

本系统总体上采用了分布式与集中式相结合的方式来构建基本的用户身份及其角色权限信息库，这样在到达身份信息统一管理的同时避免了对原有系统的更改，然后以 Shibboleth 系统为核心实现了与各个应用系统的联结，并使用了 Web 服务形式发布各类认证服务，以方便系统的开发和修改，基本上实现了统一身份认证的基本要求，但是同时也可以看到一些具体的问题，如在用户数据管理方面，该模式就存在数据更新等问题。对于烟草行业等大型企业的统一身份系统，由于企业本身的结构复杂等原因，很难找到一种各方满意的完美方案，因此在系统设计过程中始终保持应用集成方法的简易性和一致性。

5 总结

随着 Web Service/SOAD 以及云计算等新技术在企业信息管理系统中逐步得到广泛应用，可以为企业节省成本、提高工作效率。但另一方面系统安全问题就变得相对复杂一些，用户统一身份认证就是解决这个问题的关键之一。由于企业系统复杂多样，目前还很难找到一个通用而成熟的认证技术和标准，我们利用 Shibboleth 系统进行企业统一身份认证系统的设计，就是在这方面做了一些有益的尝试，对未来相关技术的开发有一定的借鉴作用。

参考文献

1 华晓丽.基于登录代理的统一身份认证服务平台构建.铁道科学与工程学报,2005,(10):80−84.
2 尹文平,兰雨晴,等.基于 LDAP 的用户统一身份认证管理系统的设计与实现.计算机系统应用,2005,14(10):18−21.
3 许鑫苏,新宁.数字化校园中统一身份认证系统的分析.现代图书情报技术,2005,(3):50−56.
4 曹敏年,张玮.统一身份认证平台的数据交换机制与实现.上海理工大学学报,2006,(3):293−298.
5 江淇,王群.Shibboleth 系统应用实例分析.现代图书情报技术,2007,(9):44−48.