随着基于企业应用系统的普及，越来越多的应用系统被开发出来，但由于

各种客观条件的因素，这些应用系统开发时期和使用的技术各不相同，且每个

系统都有各自独立的身份验证机制，这就造成了在实际应用中，用户将花费大

量的时间来输入验证信息(用户名和密码)，影响了工作效率，而且当企业员工

进行调整时候，需要对所有系统的身份信息进行人工调整，这无疑增加了系统

管理员的负担，且容易出错，所以研究这一问题的解决方案具有很强的现实意

义，单点登录(Single Sign On)，简称为SSO，是目前解决上述l’口J题的流行

解决方案，SSO的简单定义是在多个应用系统中，用户只需要登录一次就可以

访问所有相互信任的应用系统。它把实际用户映射成一个电子票掘，当用户登

录时，获得其电子票据，用户登录其它站点时，不需要重复登录。

本文主要围绕建立目前企业应用系统需要单点登录功能而展开，首先，简

要介绍了单点登录需要用到的信息安全方面的理论进行了一个简要的介绍，并

对现在流行的单点登录模型Kerberos、Microsoft Passport和SAML模型的特

点和原理作了详细的分析和比较。在这基础上，分析了现在企业应用的实际，

设计了较为灵活的基于SAML协议和RBAC协议原理的单点登录模型，该模型充

分考虑了企业的业务实际要求，对RBAC协议进行了一定的改进，以保证权限

控制的灵活性，最后，根据设计出的模型，结合ASP．NET和数据库相关技术给

出了一个企业单点登录系统的具体实现，该系统充分考虑了功能和安全方面的

要求，对企业的单点登录改造有一定的积极意义。

关键词：