图书情报可视化系统认证研究

魏尔啸

（河南省图书馆 河南　郑州 450000）

摘　要：近些年来，图书情报在可视化系统方面快速发展，涌现出大量富有创新的技术应用，随之改进新型研究形式。在日益复杂的各个应用系统之间，如何进行统一规范化的管理、审计、规划，就凸显出单点认证及统一用户系统重要性，除了关乎应用效率，还包括稳定性及安全性问题。本文通过对可视化应用系统现状进行分析，然后探讨认证系统开发的必要性及可行性，并设计出对应框架下的认证管理模式。

关键词：统一认证系统；图书情报可视化

1. 应用系统现状

图书情报领域经过多年的信息化建设，已经形成了一大批比较成熟的应用系统，包括电子著作在线评审、项目共享研究、自动化集成系统（文献处理）、移动终端小程序与 APP 同步响应等等。但随着业务系统的增多和众多分散的数字化项目落地，用户在访问众多可视化编辑分发系统的同时也面临诸多问题。

1.1 由于诸多资源系统的用户接口、认证方式各异，很难做到全局个性定制。

各个商业研发的管理系统也都有自己的用户认证方式，有碍于运维全局用户的管理和权限分配，给当前用户数据分布、异构的系统互连认证带来一定困扰。

1.2 用户为了得到一组数据往往要反复多次进入不同的系统，而每一个系统都需要用户输入用户名和口令才能登录。

随着图书情报业务的发展，将来会增加更多的应用子系统和旁挂系统在服务端运行，而对每一个系统都需要他们进行口令的验证。增加了业务操作的复杂性，工作效率降低，用户信息同步延迟。

1.3 安全问题日益突出，网络攻击明显增加。

由于应用系统开发初期，没有一个统一的身份管理平台，开发商在开发时独立建立自己的用户数据库，随着系统的增多，导致系统管理员面对的用户数据库越来越多，系统管理员对用户的管理不得不辗转于不同应用系统数据库之间，删除或添加用户。而且分散的用户数据库，缺乏统一的针对整体用户帐号和身份信息的安全策略，使得系统管理员难以应对分散用户数据的安全管理。

1.4 用户行为及数据内容审计复杂，工作周期延长。

目前各个应用系统的审计也是相对独立的，缺乏集中统一的访问审计系统。一旦某一个系统应用的用户数据结构更新或重新开发，其他系统用户模块还需要在满足数据上传接口标准的条件下重新对接。

2. 统一身份认证和单点登录需求分析

针对图书情报应用系统多样化的状况，需要通过建立一个统一的身份认证和单点登录平台，为用户提供一个统一的信息资源认证访问入口，使用户只需一次登录就可以根据相关的访问权限和策略设置规则去访问其有权限的不同的应用系统，提高信息系统的易用性、安全性、稳定性；给用户提供简单方便、快捷有效的信息服务。同时，提供一个统一的身份认证和管理平台，设置统一的用户安全管理策略，使得系统管理员通过一个平台来集中管理用户信息。减少安全隐患，方便用户管理。[1]

3. 统一认证和单点登录系统建设方案

3.1 可实施认证方式

当前统一身份认证规范有多种技术实现方式，具体有如下认证方式：

一、数字证书认证方式

在单点登录系统中，普通用户使用传统的用户名+静态口令方式。对关键人员使用基于数字证书的认证方式，数字证书认证方式可以用软证书方式，也可以采用 USB Key 作为认证器，对重要的用户发放数字证书或是 USB Key，UKey 便于携带，且保密性好。结合 CA 数字证书系统或是第三方数字证书系统都可以为身份和单点登录系统提供增强的身份认证。确保用户身份的唯一性和认证信息的机密性。

二、外部源认证

如果总站内建立的 AD 域，可以建立账号同步机制，以及账号引用机制，可以利用 Windows 域认证系统作为本身的认证机制，如果用户通过了它的认证，则认为此用户认证通过。并与 AD 域共用一套用户信息，无需再建立一套账号信息。同时结合 RADIUS 认证和其他第三方 LDAP 认证，通过配置读取 Domino 数据源。

三、动态口令认证

使用 NetPass 动态口令认证系统或者第三方的动态口令认证系统。实现动态口令认证方式。动态口令牌是一种较成熟的方法，在国内外已经成功的使用了多年时间。

四、静态口令认证

静态口令认证是最基本，传统方便的认证方式，对于访问信息机密性不强的用户可以使用此种方式。静态口令作为安全策略，可以设置复杂口令要求，如位数，数字字母组合等。以及定期更改等。认证模式可以灵活支持静态口令+动态短信；静态口令+动态密码等各种方式组合。

五、LDAP 认证方式

使用 LDAP 认证方式，用户名与口令是存储在指定的 LDAP 目录中。当一个用户登录时，提供的用户名与口令若与该 LDAP 目录中指定子树中某一个用户记录的用户名与口令相同，则认证成功，登录者具有 LDAP 目录中该用户记录对应的身份，如 openLDAP、SunLDAP、REDHAT LDAP、南大 LDAP 等。[2]

六、Radius 认证

标准的 Radius 认证服务，可以提供给一些支持 Radius 协议认证的设备实现认证，如 vpn、防火墙等一些网络设备及主机。这样这些设备无需再维护一套自己的用户身份。

在选择身份认证方式时，不同的认证方式具有不同的安全性、易用性和部署成本，因此，针对不同的用户群与不同的应用范围需要对认证方式进行个性化。根据角色、用户指定不同的认证方式，也可以在认证时直接指定认证模块。对于不同组织、角色可以配置个性化的认证方式，满足用户不同级别的安全认证需求。在安全方面，要明确不容易被模仿的原则（包括认证凭证的复制、认证过程的重放）或攻击（包括 DOS

攻击），并针对不同价值的系统以及其中账号权限的保密程度选择不同的认证手段，来降低开发成本，节约系统资源。

3.2 单点登录解决方案

统一身份认证一个很重要的应用是实现 SSO 单点登录。即用户在 SSO 服务器上进行一次登录后，在从 SSO 服务器登出前，访问所有纳入 SSO 管理范围的应用系统时均不需要再次手工登录，而是由 SSO 系统带为登录。

一般用户每天要登录到很多不同的系统和应用中。每个系统都有自己的认证过程，要求用户输入不同的用户名、口令。用户需要进入的系统越多，用户记不住密码的现象可能性就越多。而 SSO 可以解决用户记忆多个口令，登录不同系统需要重复登录的问题，不仅提高了系统的使用效率，而且通过在主帐号认证环节采用强认证技术、或是设置密码策略来增加安全性。（如图 1）

图 1

主流单点登录技术：

一、前置方式

这种解决方案中 SSO 系统提供各种 API，Agent 代理，对原有应用系统进行改造，改变原有应用系统的认证方式，同时采用认证服务器提供的技术进行身份认证。这种解决方案，一般要求用户先统一所有应用系统的用户数据库。把用户的信息统一后，才可实现单点登录功能。

在修改应用的技术方案中，每个应用服务器中都需要安装一个代理程序完成用户的身份认证工作。当用户访问目标应用服务器时，代理程序向 SSO 服务器询问该用户是否已经登录，如果是，则代理程序从 SSO 服务器中取得该用户的用户信息自动登录该应用系统。登录成功后，用户直接访问该目标服务器。如果未曾登录过任何应用服务器，则该应用要求用户进行身份认证，认证结束后，代理程序将认证结果发送给 SSO 服务器。

二、后置方式

这种方式为业务系统直接请求单点登录的登录接口，接口返回登录票据，获取到登录票据后，后续的访问可以通过使用这个票据，实现对用户的验证。票据在整个会话期内有效，一旦用户退出，会话超时后，需要重新登录，生成新的票据。

三、简单代填

即插即用解决方案，它对于内部的各种应用程序不进行修改，通过系统配置的工作来实现。它的实现机制采用二次登录技术，与原有系统的开发语言、操作系统、数据库、应用平台类型等无关。这种解决方案在认证服务器上保存用户所有应用系统的用户名/口令信息列表，认证服务器上采用透明转发机制，自动帮用户实现登录过程。

它的基本工作原理为：首先针对每个应用系统进行配置，产生一个配置文件；用户登录到单点登录服务器上；用户访问应用系统时，单点登录服务器调用对应于该应用的配置文件，将对应该应用的用户认证信息（用户名/口令）取出，代理用户登录应用系统；登录成功后，用户可以访问应用系统。

3.3 账号同步机制

3.3.1 与关系型数据库同步

统一身份管理系统帐号同步模块和关系型数据库，如 SQL Server 等的集成，可以通过 JDBC/ODBC 资源适配器完成的，并在资源方无须代理，通过配置“帐号同步引擎”，完成数据同步。其实质是通过读写操作被同步对象的数据存储设备来实现的。因此这种方式需要提供帐号同步模块各应用系统的数据存储设备的具有管理权限的帐号和密码。

如果不能提供数据库管理权限的帐号和密码，也就是通过帐号同步引擎使不能实现用户帐号同步，或是不能将数据库读写权限交给管理系统，通过编程接口与关系型数据库同步。

3.3.2 与 LDAP 或 AD 进行同步

如果有其他的应用系统底层数据库也是采用的 LDAP，同步引擎可以通过 JNDI 资源适配器完成的，在资源方无须代理。直接通过配置就将总库用户数据与其他 LDAP 目录服务器进行同步。如果已经建立 AD 环境，那么通过同步引擎也可以与 AD 进行同步。

3.3.3 与 Domino 进行同步

Domino 是主流的 OA 开发平台，它有一套独自的用户帐号管理模块，在与 Domino 进行同步时，需要启用 Domino 的 LDAP 服务，Domino 支持 LDAP 访问协议，通过 LDAP 访问协议，实现对 Domino 中的帐号同步。

3.3.4 通过调用 API 进行同步

通过调用应用系统提供的用户管理 API 接口，实现对帐号的同步。

4. 系统部署效益

统一身份认证和单点登录平台，作为图书情报可视化系统的一个基础建设的意义如下：

从用户角度来看，单点登录解决了他们记忆多个用户名、密码的烦恼，解除了使用多个应用系统必须进行多次认证的重复劳动。

从职能价值来看，单点登录系统可以使他们从繁琐的账号密码管理工作中解脱出来，不必每天为用户重置密码而苦恼，使 IT 人员真正的发挥在单位中的管理职能。

从应用系统生产商角度来看，单点登录使他们不必再开发身份认证模块，从而可以把更多精力投入到具体业务中。

从管理角度来看，单点登录提高了工作效率，减少了管理成本，丰富了信息系统的安全性，也节约了后续开发的成本。

综述可见，统一身份认证和单点登录平台，可以方便运维人员后续管理和应用接入。降低整体应用级别的复杂程度，优化图书情报领域的研究效能。

参考文献：

[1] 黄虓.基于 OpenID 的数字图书馆身份认证技术[J].科技情报开发与经济,2011,21(20)

[2] 胡开胜.LDAP 协议在数字图书馆统一身份认证系统中的应用[J].电脑知识与技术,2010, 6(10)

作者信息：魏尔啸 男 1987 年 5 月出生 河南郑州人 研究方向：图书情报 馆员