# 数字图书馆用户单点登录机制与技术研究

王昉[1]，姜恩波[2]，张晓雁[3]
(1. 中国科学院文献情报中心，北京 100190；2. 中国科学院成都文献情报中心，成都 610041；
3. 北京大学外国语学院图书分馆，北京 100871)

摘要：总结分析了用户统一认证技术在数字图书馆应用的需求与现状，讨论了应用系统设计中涉及的关键技术解决方案和管理政策需求，以及国内外数字图书馆对统一认证和授权实现的模式，并在最后讨论了我国实践中存在的问题与未来的发展方向。

关键词：分布移动用户；统一认证和授权；单点登录
中图分类号：G250
DOI：10.3772/j.issn.1673—2286.2014.07.006

## 1 前言

用户单点登录是指认证系统通过技术和管理机制等手段对物理上分散的用户进行统一、可信任的身份识别，进而根据用户身份和相关资料提供有差别的资源授权和服务。该技术在互联网有着广泛的应用，目标在于解决在不同用户环境下用户身份认证和信息安全、隐私保护（如云环境下用户统一认证技术与应用[1]）、多个系统间的单点登录和无缝跳转，以及对用户环境和设备的自适应（如有线网络与无线网络之间，计算机与手机、平板电脑等移动设备之间[2,3]）等，并被用于电子数据交换（如eTrust电子信任联盟[4]）、网上银行、目录访问服务等。而数字图书馆的用户统一认证主要用于解决分散、移动用户对图书馆购买电子资源的IP地址限制、图书馆多个网络服务的集成认证和访问等问题。

与其他系统提供认证和访问的目标资源多为自主知识产权资源相区别，数字图书馆面临的主要困境是对购买商业电子资源的认证和访问服务需要得到资源提供商的许可和支持。就相关问题国内外数字图书馆界已进行了长期的探索和实践，并形成了许多实施框架和建设标准、应用成果，影响较大的单点登录系统如Athens访问管理系统[5]、InCommon（美国）[6]、中科院国家科学图书馆随易通[7]、CALIS统一认证系统等，以及知名开源项目及工具如Shibboleth[8]、CAS[9]（耶鲁大学）、JOSSO单点登录开源项目（Java Open Single Sign-On）[10]、SourceID开源联合身份认证管理（Open Source Federated Identity Management）[11]等。国内许多图书馆也通过购买成熟软件如OCLC EZproxy[12]或基于OpenID、CAS、SSL VPN等技术自行研发并在本馆或机构服务中应用[13-15]。国内版权和知识产权保护的环境的现实使得相关正式合作与国外相比存在很大差距。本文旨在应对上述矛盾，通过对国内外数字图书馆界该技术的研究与应用现状进行分析，总结实践中需解决的关键技术与管理问题，探索其未来发展方向。

## 2 应用需求与现状

数字图书馆应用单点登录的原因可归纳如下：

（1）为购买电子资源的远程访问提供安全、灵活的用户身份认证和授权

图书馆购买的电子资源（如文献数据库、科研工具等）由于知识产权和出版商权益保护等原因，往往并非向所有公众开放，而是将获取范围限制在特定地域的特定用户群，如购买某电子资源的大学所在校园园区的学生和教师、职员。基于IP地址认证用户身份是一种简单有效的办法，也是目前最常用的用户访问控制方式。它的弊端在于限制了合法用户获取电子资源和服务的地理范围，一旦用户离开了该资源或服务授权的IP地址范围，访问则被视为非法访问而无法获取服务。图书馆通常的解决方案是通过用户名/密码对、数字证书等

用户身份认证+远程网络资源代理访问的方式，提供对基于用户网络地址进行身份认证的有效补充，使用户在外地、野外和休假时等也能获取相应的服务。而用户单点登录系统可以根据不同用户的身份（所属机构、院系等）、类别（学生、教师、研究人员、访问学者等）、学科性质、认证方式（如强用户认证、弱用户认证）等为用户授予不同资源、不同深度的访问权限。以某高校学位论文数据库的访问控制为例，通过分布移动用户认证和单点登录服务可根据用户身份定义论文获取权限为：该校所有用户检索并获取论文文摘、前16页，教师和同系别学生可获取论文全文。

国外图书馆利用代理为用户提供远程访问订购的电子资源非常普遍（如EZproxy在全球的用户包括60多个国家的400多个机构[12]），但在我国由于知识产权和版权保护等现实原因，代理软件通常并不得到电子资源出版商的许可，需要拿出有力的证据证明用户账号只分发给授权用户使用而不被散发，以及对用户批量下载行为的有效防止和管理。

（2）提供多种服务的集成认证和单点登录

许多数字图书馆服务（如电子资源、参考咨询、文献传递、跨库集成检索、学科门户、科研工具等）的功能需要用户注册、登录后才能使用，并根据用户身份、学科、兴趣偏好、付费信息等为其提供个性化的定制服务。然而繁琐的注册阻碍了用户进一步使用服务的兴趣，也为用户记忆各种注册信息造成了困难。用户单点登录技术为用户提供了多种服务的统一认证和授权，用户只要从集成认证中心或单个系统登录，就能无缝地使用各种资源和服务，无需单独向各个资源和服务注册和登录。这类服务通常通过统一认证和授权技术实现对不同的用户访问控制策略，同时根据认证中心传递的用户信息为用户提供个性化服务。如某高校物理专业研究生在该校分布移动用户认证中心注册，通过验证后，认证中心根据用户注册信息的专业、系别、身份为用户分配相应电子资源和服务的访问权限，如开放针对该专业、教学进度设置的教参、课程资料、数据库的访问，提供符合该专业和用户偏好的个性化服务，如推送物理学科门户、物理学科数据库等。

（3）网络访问代理

当用户受所在网络访问限制无法访问广域网、或某特定网络由于安全、管理策略等因素只针对特定用户群开放时，用户单点登录服务可作为代理网关，为用户提供万维网（WWW）或虚拟专用网（VPN）访问代理。当用户暂时离开校园或所在机构时，可通过分布移动用户认证和单点登录服务实现系统的远程登录。它区别于普通代理网关之处在于可实现基于用户身份的访问授权和控制、用户行为管理和审计。

## 3 单点登录模式分析

实现安全、可信赖的单点登录服务涉及两个问题：用户身份认证和基于用户角色的资源访问授权。其中用户身份认证方式除了常见的用户名/密码方式，根据系统对安全强度要求不同可在此基础上增加不同的验证手段如动态口令、数字证书等；对于基于用户角色的资源访问授权，业界面临的主要问题是非自有知识产权的远程资源，其主流方案主要有以下两种：

（1）基于IP地址身份认证（如VPN、HTTP代理）方式，即采用目标服务端认可的IP地址对远程资源进行访问或访问代理。这种方式适用于单个图书馆独立部署的单点登录服务，其优点在于无需与远程资源就单个使用用户的身份认证进行交互，同时也带来一些弊端，包括本地代理负担重、访问速度比直接访问慢；用户访问授权和行为管理由资源提供服务者转为代理服务提供者控制，需要制定妥善的用户访问行为控制策略以保证对资源的合理使用，等等。

（2）与远程资源建立基于通用标准（如SAML、SSL、LDAP等）的合作身份认证和授权，通过传递用户的身份属性等信息，由目标服务端根据用户角色对用户的访问进行授权。其优点在于对远程资源的访问授权由目标服务直接提供，本地管理压力小、用户访问速度快。其问题在于需要逐一与众多的商业资源提供商协商谈判以取得其许可和授权、并支持不同的提供商遵循的认证方式，对于单个图书馆而言实现难度较大，更适用于认证资源授权和角色复杂、用户类别和数量较多的信任机构联盟（如高校图书馆联盟）。

我国多采用前一种方式实现用户的单点登录，而后一种方式在欧美等发达国家多通过联盟或政府组织的方式实现。实际应用中根据对用户认证方式和服务授权的管理模式不同，可将它们分为以下两种模式：

（1）集中式用户认证和授权

其特点是用户认证所需的身份信息、访问授权策略和信息集中保存在集成认证中心，用户从集成认证中心登录获取授权访问的资源和服务。典型的代表有

Athens、随易通。它们都采用了分级式管理，服务的访问授权由认证中心根据内容提供商提供的一份订阅该服务的机构清单为相关机构授权，注册的机构可自动获得本机构订阅的网络资源的访问权限，而无需与内容提供商交涉访问控制的细节；注册机构自行维护本机构用户帐号和资源授权，机构管理员可通过建立资源访问控制策略，为不同身份用户设置不同的资源访问权限。Athens与随易通相比，由于Athens与英国教育部与卫生部官方长期合作，对服务提供商而言可信任度高，因此集成认证的网络服务数量、服务种类多，如电子全文数据库（如Ebrary、Ebsco、IEEE、Elsevier ScienceDirect等）、电子期刊（如Cambridge Journals Online、Oxford Journals）、远程教育资源（如Proquest Learning、Education Media OnLine等）、在线数据服务（如Census Interaction Data Service、Economic and Social Data Service等）、数字图书馆网站（如NHS National Library for Health）、网络服务（如Oxford Reference Online）等。Athens提供了网络服务器插件、各类开发接口等方式，可方便网络服务提供商将Athens认证集成到他们的系统；随易通目前只提供对中国科学院集团购买的电子文献资源远程访问的统一认证和授权，以及部分其他数字图书馆服务的统一认证和单点登录（如中科院跨库集成检索）。其远程访问方式目前已开放SSL VPN代理方式的测试并与中科院统一认证登录集成（之前采用反向代理技术），与Authens相比需认证中心维护资源访问控制，配置较复杂、维护成本较高。其用户认证与授权模块目前基于SSL的用户名/密码、用户名/密码＋随易通E-key或SSL VPN的两级强度的用户认证方式，资源授权方式灵活、支持用户访问在线预警、离线分析安全策略等。

（2）联盟式管理

其特点是共享资源的机构间建立联盟和信任度网络，由请求资源的机构自行负责本机构用户身份的认证，向目标机构发送的用户信息为用户属性的断言，基于用户属性进行访问控制，并根据目标资源要求由请求机构提供关于用户属性的断言，而用户属性由用户所在机构注册信息生成。这种认证授权方式有较好的用户隐私管理，由发送请求机构和用户决定关于用户自身信息的哪些部分可以提供给目标机构。往往需要提供给目标机构的并非用户姓名、年龄等确切信息，而是关于用户身份属性的断言，如对请求某一课程资源时提供用户的属性断言为某专业二年级学生。同时，基于SAML、SSL、LDAP等标准的开发，使认证系统易于与同样采用了这些标准的应用之间进行互操作。Shibbloleth、SourceID同属这类模式。以Shibbloleth为例，它主要被应用在大学、图书馆及其联盟共享远程教育资源、图书馆电子资源、机构学术资源和公共信息等提供用户的集成认证和单点登录，如俄亥俄州立大学用于建立访问该校所有网络应用的统一认证入口，包括学生服务网站、课程管理系统、人力资源、员工研究资源门户等；马里兰大学及其附属机构联盟用于共享图书馆资源和服务，如Metalib、用户目录服务、SFX等。在世界范围内建立基于Shibbloleth框架的联盟有美国的InCommon、英国的SDSS[16]、瑞士的SWITCH[17]、法国的Éducation-Recherche[18]和芬兰的HAKA。支持Shibbloleth的网络应用和服务包括CSA（剑桥科学文摘）、ExLibris-SFX、Elsevier ScienceDirect、OCLC的EZproxy、NSDL（美国国家科学数字图书馆）等。

## 4 关键技术解决方案和相关管理机制

根据上述应用需求在我国的实践需要，单点登录系统在设计中需要考虑以下三个主要问题：

### 4.1 提供安全、可信的认证和授权机制

用户单点登录服务的工作模式是：认证中心对注册用户提交的登录信息进行验证，确认用户声称的身份信息真实有效后，为用户分配可访问资源或服务的授权，并将必要的用户资料（资料详细程度根据不同系统需求而有区别）提交给用户访问的资源，为用户提供个性化服务。这个流程中可能出现的问题包括：由于在互联网上传输的数据对公众是可见的，可能产生传输数据被恶意截获、修改或延迟；用户口令被盗、散发；用户对资源和服务的恶意使用（如批量下载），等等。为保证统一认证和单点登录服务的安全性和可靠性，目前各类系统采取的解决方案主要有：

（1）提供不同的认证强度支持安全、可靠的用户访问控制

单点登录服务系统可根据应用对安全性能所需的不同级别提供不同强度的认证。如网上银行对普通用户进行帐务查询等操作采用用户通行词（如身份证号/查询

密码）的简单认证方式，而进行转帐、网上交易等对安全性要求高的操作则采用数字证书认证的强认证方式。

根据认证方式的认证强度可分为：①简单认证，即用户向系统提交用户名/密码对的方式，它的缺陷在于容易破解，而系统无需向用户证明自己的身份；②受保护的认证，即用户和认证中心共有秘密，但不依赖于秘密的明文交换，例如X.509受保护密码、Kerberos认证、一次性生成口令等；③强认证，即采用公钥和数字证书的加密技术，例如X.509数字证书、PEM信任模型、PGP信任模型等[19]。随易通系统即采用了简单认证与强认证结合的方式以应对用户对二次文献数据库与全文数据库的访问需求，并结合随易通E-key与用户使用绑定、用户行为的在线监测与离线分析等方法，防止用户账号散发。

（2）采用加密技术保证通信的机密性

机密性是指通信时确保只有信息发送者预定的信息接收者能够理解发送信息的内容。在分布移动用户认证系统中要求用户认证信息的数据加密传输，如通过SSL（Secure Socket Layer）对通讯内容进行高强度的加密，以防止黑客监听通讯内容甚至是用户密码。

（3）采用数字签名保证数据一致性和防抵赖

数字签名是指用户用自己的私钥对原始数据的哈希摘要进行加密所得的数据。信息接收者使用信息发送者的公钥对附在原始信息后的数字签名进行解密后获得哈希摘要，并通过与自己用收到的原始数据产生的哈希摘要对照，便可确信原始信息是否被篡改，并保证了数据传送的不可抵赖性[20]。在统一认证系统中通常对用户传输的认证信息进行数字签名。

（4）跟踪和分析用户日志对用户行为进行管理

根据预定义的规则通过实时或离线的方式对用户活动记录进行的跟踪和分析，发现用户违规行为，如用户口令散发、过量下载等。同时通过对用户访问资源的日志的统计分析可得到关于资源和服务使用情况等数据，帮助图书馆员更好地改进服务。

## 4.2 提供稳定、可靠的网络资源的远程访问和管理

为分布用户提供远程访问图书馆购买的电子资源的方式通常有四种：正向代理（Forward Proxy）、反向代理（Reverse Proxy）、IPsec VPN 和SSL VPN。其中反向代理的典型代表是EZproxy。这4种方式的区别与特点本文归纳总结如下（见表1）。由分析可见，正向代理、反向代理和SSL VPN 3种方式访问权限控制细粒度较高，能满足基于URL的规则过滤，当遇到类似同一电子资源采购集团中不同机构对同一数据库中选订的期刊不同（同一网络地址、URL不同）时显得尤为必要；正向代理和IPsec VPN都需要客户端进行一定配置或安装软件，对客户端设备适应性而言，除IPsec VPN外其他3种访问方式都支持不同操作系统及上网设备，用户端维护成本较低。而反向代理由于采取了URL重写技术，对与URL变化无关的网页脚本（如JS）支持较差，代理维护成本高。笔者认为SSL VPN是将来远程访问代理的发展方向，已有图书馆及企业尝试该种方式在本领域的应用[21]。

表1 4种远程访问代理方式的特点

| 代理方式 | 所处互联网协议层 | 访问权限控制粒度 | 客户端所需配置 | 支持代理应用/设备 | 安全性 |
|---|---|---|---|---|---|
| 正向代理 | 应用层 | 基于URL | 需要配置客户端网页浏览器代理 | 基本支持所有上网类型如HTTP GET、Connect GET、SOCKS4、SOCKS5等 | 取决于代理是否对数据加密 |
| 反向代理 | 应用层 | 基于URL | 客户端无需配置 | 基本支持所有上网类型如HTTP GET、Connect GET、SOCKS4、SOCKS5等 | 取决于代理是否对数据加密 |
| IPsec VPN | 数据链路层或网络层 | IP地址或域名 | 需安装VPN客户端软件 | 对IP应用高度透明，支持包括浏览器在内的其他网络应用 | IP安全体系架构协议 |
| SSL VPN | 应用层 | 基于URL | 无需安装客户端软件，认证用户通过Web浏览器接入网络 | 某些高端的SSL VPN产品支持文件共享、网络邻居、Telnet 、Vtp、Oracle等TCP/UDP的C/S应用 | SSL安全套接层协议 |

### 4.3 制定有效的管理政策保证系统的可靠性

用户单点登录的安全、可信并不仅仅是技术问题，更是政策问题。制定完善可执行的管理政策，并保证管理政策的可靠实施才能实现系统真正的可信赖。其对认证和授权系统的要求包括：①保证正确的用户得到正确的资源授权，如用户身份的真实有效性、授权的准确性等，并可通过相应的用户注册信息验证、用户管理和维护、认证中心注册资源和服务的授权管理和维护等措施保证，如高校通过校园一卡通、中科院通过E-key与用户账号绑定，可有效防止用户账号的散发；②保证用户的违规行为得到有效的防止和管理，可通过制定用户违规行为监控方法、相关责任追踪措施（如停止相关账号、通报）等。

## 5 结语

我国数字图书馆中用户单点登录技术的应用与国外同行比较，标准规范应用程度及应用推广规模仍有较大差距，体现在：①对资源的集成访问多采用代理方式，缺乏与资源提供商的合作，增加了资源的访问和控制的实现难度和维护成本，难以实现在不同资源之间的无缝转移；②对图书馆服务系统的集成认证和单点登录多采用在集团内自定义的集中用户认证和授权模式，系统之间耦合度高，不支持开放的身份认证和授权协议，不利于与其他支持开放标准的资源与服务的互联。上述问题的解决不仅仅依赖于技术的更新，除在系统框架上进一步向开放标准靠拢外，更需要建立完善的服务政策和管理机制，增强资源提供商对系统的认证和授权机制的信任度；在更大范围内建立图书馆之间联盟和认证信息交换机制，在增进不同认证与授权系统之间互操作的同时，也能增加我们与资源提供商进行相关谈判的话语权。

#### 参考文献


[1] 季一木,康家邦,等.一种云计算环境下的用户统一认证方法:中国,CN103259663 A [P/OL]. (2013-08-21) [2014-03-07]. http://www.google.com/patents/CN103259663A?cl=zh.

[2] 高飞.西安交大推出“云计算”统一认证平台学生手机可查空闲教室[N/OL].人民网,2012-12-29 [2013-08-21]. http://sn.people.com.cn/n/2012/1229/c226647-17941090-1.html.

[3] lightRadioWiFi [EB/OL]. [2014-03-07]. http://www.alcatellucent.com/solutions/carrier-wifi.

[4] The Electronic Trust foundation [EB/OL]. [2014-03-07]. http://www.etrust.org/.

[5] Eduserv - OpenAthens [EB/OL]. [2014-03-07]. http://www.athensams.net/.

[6] InCommon [EB/OL]. [2014-03-07]. http://www.incommon.org/.

[7] 中科院国家科学图书馆随易通[EB/OL]. [2014-03-07]. https://ras.csdl.ac.cn/.

[8] Shibboleth [EB/OL]. [2014-03-07]. https://shibboleth.net/.

[9] Central Authentication Service project.

[10] Java Open Single Sign-On [EB/OL]. [2014-03-07]. http://www.josso.org/.

[11] SourceID [EB/OL]. [2014-03-07]. http://www.sourceid.org/.

[12] EZproxy [EB/OL]. [2014-03-07]. http://www.oclc.org/ezproxy.en.html.

[13] 许雁冬,李宇.国家科学图书馆单点登录系统设计与实现[J].现代图书情报技术,2009(10):28-33.

[14] 黄娆.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).

[15] 申飞驹.基于SSL-VPN的数字图书馆资源共享服务平台研究[J].图书馆理论与实践,2010(8).

[16] Shibboleth Development and Support Services (SDSS) [EB/OL]. [2014-03-07]. http://edina.ac.uk/projects/sdss/.

[17] SWITCH [EB/OL]. [2014-03-07]. https://www.switch.ch/aai/about/shibboleth/.

[18] Éducation-Recherche [EB/OL]. [2014-03-07]. https://services.renater.fr/federation/en/index.

[19] YOUNG A, et al. Technologies to Support Authentication in Higher Education [EB/OL]. [2014-03-07]. http://www.ukoln.ac.uk/services/elib/papers/other/scoping/.

[20] Digital Signature & PKI Assessment Guidelines [EB/OL]. [2014-03-07]. http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html.

[21] VPN的原理及SSL VPN方案的优势[EB/OL]. [2014-03-07]. http://www.60vpn.com/post/102.html.

## 作者简介

王昉，女，1977年生，硕士，中国科学院文献情报中心副研究馆员，研究方向：开放资源的利用、互操作，E-mail：wangfang@mail.las.ac.cn。
姜恩波，男，1972年生，硕士，中国科学院成都文献情报中心副研究馆员，研究方向：信息组织。
张晓雁，女，1978年生，北京大学外国语学院图书分馆馆员，研究方向：图书馆理论与实践。


Application Research on Single Sign-On in Digital Library


WANG Fang[1], JIANG EnBo[2], ZHANG XiaoYan[3]
(1. National Science Library, Chinese Academy of Science, Beijing 100190, China; 2. Chengdu Library, Chinese Academy of Sciences, Chengdu 610041, China; 3. The Branch Library of School of Foreign Languages at Peking University, Beijing 100871, China)



Abstract: This paper deals with the applications for technology of user unified authentication and single sign-on in digital library. Technology and policy problems concerning on system design and application examples on digital library at home and abroad are discussed and analyzed. Finally, the problems in practice and future direction are explored.



Keywords: Distributed and transferred user; Authentication and authorization; Single sign-on

（收稿日期：2014-03-10）


## 书讯

# 《中国高被引分析报告2012》

在您所关注的研究领域中，哪些论文最受同行关注？哪些研究主题最为热门？哪些学者最具学术影响力？哪些期刊最获同行认可？又有哪些机构占据领域研究的制高点？上述问题请您参考近期出版的《中国高被引分析报告2012》。

该书将理、工、农、医、人文、社科等领域划分为51个学科，综合分析了各个学科的研究热点与前沿、高影响力论文、高影响力作者、高影响力期刊和高影响力科研机构，并以关联图谱的方式展现各种学术关系，有助于科研人员及时发现并跟踪研究热点，可为科研管理机构评估科研能力提供依据，还有利于期刊编辑部监测本刊学术影响力，是高等院校、科研院所及期刊编辑部等相关单位和人员参考工具书。

该书以“中国知识链接数据库”为依托，数据样本覆盖我国6000余种期刊的论文及引文，分学科揭示高影响力的学者、研究机构（大学、研究所、医院等）、地区（省/自治区/直辖市）、学术期刊、图书、外文期刊和会议录，并采用共词分析、共被引分析和合著分析等方法绘制出各学科的前沿主题分布以及作者、机构和期刊间关联的知识图谱。

《中国高被引分析报告2012》由中国科学技术信息研究所编著，科学技术文献出版社出版，全书86万字，定价298.00元。