数字化图书馆引入 PKI 的思考

温汉荣 郑 婷

（广东药学院图书馆 广州 510006）

〔摘要〕 介绍数字化图书馆的特性以及 PKI 技术的概念、构成，指出引入 PKI 能解决图书馆数字化过程中出现的版权保护、信息安全、馆际合作等问题。但我国 PKI 技术发展水平不高，将其应用于图书馆中仍面临人员、技术、成本方面的困难，促进技术的应用仍需更多努力。

〔关键词〕 数字图书馆；PKI；版权保护；信息安全；馆际合作

Thinkings on Introducing PKI into Digital Library *WEN Han – rong, ZHENG Ting, Library of Guangdong College of Pharmacy, Guangzhou 510006, China*

〔**Abstract**〕 The paper introduces characteristics of digital libraries as well as the connotation and structure of PKI technology, it points out that introducing PKI technology can solve the problems which have emerged in library digitalization process, such as copyright protection, information security and interlibrary cooperation. However, the development level of PKI technology in China is not high, adopting PKI in library is still facing obstacles including lack of technical staffs, key technology and cost, the application of promoting technology still needs more endeavors.

〔**Keywords**〕 Digital library; PKI; Copyright protection; Information safety; Interlibrary cooperation

现代信息技术的发展对数字化图书馆中信息的所有权、使用权和拒绝权等也提出了新一轮的挑战。引入公开密钥基础设施（Public Key Infrastructure，简称 PKI）能在开放各种数字资源的同时，较好地解决信息安全、信息管理、知识产权、馆际互借等数字化图书馆急需解决而又比较棘手的问题。

1 数字化图书馆的特性与 PKI 技术

1.1 数字化图书馆的特性

1.1.1 *资源数字化* 资源数字化是数字化图书馆的基础，目前大多数图书馆通过购买、数字化、信息挖掘 3 种方法进行数字资源采集：调整图书采购计划，在保证传统纸质文献在馆藏中占一定比例的前提下，加大购买电子文献的比例；文献数字化，通过计算机技术，对馆藏文献进行有重点、有计划的数字化，填补传统图书馆馆藏数字资源的空缺，确保馆藏资源具有一定的连续性；信息挖掘，在网络时代，有许多有价值的信息，但这些信息不是现成的，需要对其进行筛选、确认、组织、补充等后期信息挖掘加工工作。

1.1.2 *管理自动化* 几乎所有传统图书馆的工作内容都能利用计算机完成，采访有采集器，编目、借还文献有图书管理系统，信息服务可通过计算机网络完成。有些图书馆在复印、打印和还书等服务中还能实现自助化，而这些服务的范围随着计算机技术的不断发展而不断扩大。

1.1.3 *传递网络化* 资源数字化和操作自动化后，

〔收稿日期〕 2009 – 12 – 14

〔作者简介〕 温汉荣，馆员，发表论文 4 篇，参编著作 1 部。

读者可以脱离图书馆实体而享受到图书馆的服务。如文献传输，读者可以在办公室或家里通过计算机终端访问图书馆，查找需要的文献并提出借阅请求，工作人员就会在规定的时间内把所需求文献的电子版通过网络发送给读者，实现了文献传递的网络化。

1.1.4 资源共享化 图书馆要真正满足广大读者的信息需求就必须共享数字化资源，它具有复制容易、传递方便、可塑性强、不受时间与空间的限制等特点。资源共享打破了传统图书馆在信息服务上受时空约束的瓶颈。

1.1.5 结构连接化 在资源数字化、传输网络化的平台上，建立一套标准操作程序，制定相关资源数字化和传输标准，结合数字化图书馆本身的计算机技术和资源整合技术，综合性开发利用本馆馆藏、馆外资源以及其它网上资源，文献资源共享将更加便捷，使不同图书馆在网络上形成统一整体，相互连接，资源利用最大化。

1.2 PKI 的概念与构成

PKI 是一个用非对称密码算法原理和技术实现的、具有通用性的安全基础设施。简单地说，PKI 是提供公钥加密和数字签名服务的系统，目的是为了自动管理密钥和证书，保证网上数字信息传输的机密性、真实性、完整性和不可否认性。一个完整的 PKI 至少包括以下几部分。认证机构（CA）：是很多大规模 PKI 的关键组成部分（在一个图书馆这样范围有限并且相对封闭的环境中，图书馆可以作为自己的认证机构）；证书库：必须存在某种鲁棒的、规模可扩充的再现资料库系统，以便用户能找到安全通信需要的证书；证书撤销：需要用一种撤销的方式来宣布证书不再有效；密钥备份和恢复：由于丢失密钥造成被保护数据的丢失是完全不可接受的；自动密钥更新：当失效日期到来时，启动更新过程，生成一个新证书来代替旧证书；密钥历史档案：当一个用户几年前加密或其他人为他加密的数据无法用现在的密钥解密，那么该用户需要从他的密钥历史档案中找到正确的解密密钥来解密数据；交叉认证：例如图书馆联盟等由多个机构联合以实现多项服务功能，如馆际互借、资源共享等，由于没有一个统一的 PKI 环境，交叉认证是一个可以接受的机制，能够保证一个 PKI 团体的用户验证另一个 PKI 团体的用户证书；支持非否认：一个 PKI 本身无法提供真正、完全的非否认服务，然而，PKI 必须提供所需要的技术上的证据，支持决策，提供数据来源认证和可信的时间数据的签名；时间戳：时间值必须被安全地传送，PKI 中必须存在用户可信任的权威时间源；客户软件端：应用程序通过标准接入点与客户端软件连接，但应用程序本身并不与各种 PKI 服务器连接[1]，即应用程序使用基础设施，但并不是基础设施的组成部分。

2 PKI 解决图书馆数字化问题的机制

2.1 版权保护

在数字化图书馆中，通过网络传输数据文件或作品时，非法个人或团体对数字作品的侵权更加容易，篡改也更加方便。因此，如何充分利用网络传输的便利，又能有效地保护知识产权，已成为一个迫在眉睫的现实问题。通常侵权行为包括 3 种情况：一是非法访问，二是故意篡改，三是版权破坏。目前版权保护技术有很多，如信息隐藏、密码学、数字水印等，但这些技术都具有一定的局限性和片面性。PKI 能针对以上 3 种侵权行为，较好地实现版权保护[2]。

2.1.1 PKI 身份认证服务 PKI 比在本地环境中的非 PKI 操作的初始化认证具有更强的认证服务，包括口令、生物特征扫描设备的单个或多条件认证，它采用了数字签名的密码技术。用户要访问数字化图书馆，首先要进入系统登录平台，由证书认证服务器进行身份认证，以确定访问用户的合法身份，杜绝了非法用户的访问。数字化图书馆利用这样一个安全、可靠并易于维护的用户身份管理和合法性验证机制来确保应用系统的安全性。

2.1.2 PKI 完整性服务 PKI 完整性服务可以采用两种技术实现。第 1 种是数字签名、时间戳，既可以提供实体认证，也可以保证被签名数据的完整性，验证信息在传送或存储过程中是否被篡改、重放或延迟，如果签名通过，接受方就认为收到的是

原始数据；第 2 种技术是消息认证码（MAC），通常采用对称分组密码或密码杂凑函数。通过 PKI 的完整性服务，在数字作品中加入适当的版权保护技术，可防止故意篡改、版权破坏的侵权行为。

2.2 信息安全

主要是针对图书馆数字化信息资源共享和传递过程中由于网络的特性而造成的问题，主要有以下两点：一是窃取数据资料，大部分数字化图书馆不仅拥有丰富的馆藏特色数字资源，还保存着大量的会员私密信息，这些投入大量人力财力的数据库资源以及会员个人信息成为被窃取的主要对象；二是信息传输过程缺乏安全保护意识，传输通道的监管力度不够[3,4]。信息安全问题与版权问题是密切相关的，没有安全的信息保障就谈不上版权的保护，所以利用 PKI 的身份认证服务和完整性服务同样可以解决信息安全的身份认证、登录等部分问题[5]。另外，为了更全面地保障信息的安全，还利用到 PKI 的其他服务。

2.1.1 PKI 密钥管理服务 一个密码系统的安全性取决于对密钥的保护，而不是对系统或硬件本身的保护。所谓的密钥管理包括密钥的产生、存储、装入、分配、保护、更新、销毁以及保密等内容。利用 PKI，可以将身份认证和图书访问功能模块设置于系统安全隔离区内，与外部网络是安全隔离的，以保证整个数字化图书馆系统的安全性和可靠性，防止了窃取数据资料的各种非法攻击。此外，图书馆在保存各种数字资源的同时，还要存储大量用户的信息，这样能使图书馆摆脱用户管理这项繁重的工作，更加专注地建设各种特色馆藏和提高图书馆数字化服务水平。

2.2.2 PKI 机密性服务 PKI 的机密性服务采用了类似于完整性服务的机制，具体过程如下：A 生成一个对称密钥，用对称密钥加密数据，将加密后的数据以及 A 的公钥或用 B 的公钥加密后的对称密钥发送给 B。利用密钥交换和密钥传输机制，在 A 与 B 之间建立了一个对称密钥[6]。这样 PKI 就能很好地控制信息的流向，数字作品可以用合法用户的公钥加密，经过传递后再用该用户的私钥解密，这种做法对远程访问更加安全和方便。它与代理服务器相比，除了大大提高安全性外，还引入了数据库的访问控制；与 VPN 相比，它能实现用户的需求分析，资源利用率分析等多项功能。

2.3 馆际合作

数字化图书馆除了图书馆本身数字化程度的提高外，还意味着利用数字化环境的建设使馆与馆之间的信息交流更加密切，更好地利用各馆的特色馆藏。从广义上说馆际合作是图书馆数字化发展的未来，图书馆通过合作增大规模，逐渐提高信息服务能力与价值，最终成为提高核心竞争力的有效手段和途径。但目前馆际合作遇到的问题很多，主要有利益平衡、资金障碍、人文障碍和合作的相关理论与方法等。这里只谈技术方面的问题，就是如何管理用户和执行统一的用户管理标准。由于各馆的情况不同，在馆际合作中，为了利益平衡等原因，他们各自所开放或者共享的资源有相应的限制，这样对用户使用权的管理难度就大大增加，而且涉及了跨地区和版权保护问题，让图书馆靠本身的管理系统难以解决多层次用户的管理问题。通过 PKI，可以实现用户管理与资源管理的分开，而且 PKI 具有交叉认证技术，利用数字证书标识密钥持有人的身份，通过对密钥的规范化管理，为组织机构建立和维护一个可信赖的系统环境，透明地为应用系统提供身份认证、数据保密性和完整性、抗抵赖等各种必要的安全保障，满足各种应用系统的安全需求。这样就在技术上解决了馆际合作用户管理这个大难题，为以后的发展打下了安全、稳妥的技术基础。

3 数字化图书馆引入 PKI 的问题与对策

3.1 我国 PKI 发展水平不高

在我国 PKI 最早应用于电子商务和电子政务中，自 1998 年中国出现第一家 CA 认证中心（CTCA）以来，经过多年的发展，我国的 PKI 技术已经具备了一定基础，形成了一定规模，积累了运营、管理经验，探索了应用模式，并培育了一些专业人才。但与西方国家相比，我国的 PKI 发展还存在不

少问题：不同技术标准和管理规范并存；各 CA 基本处于互相分隔状态，成为互不相连的信息孤岛；已建成的 CA 规模小，利用率低，距离可商业化运作的规模还相差很远；已经建立的 CA 自身安全考虑不够；缺乏国家统一指导，管理问题突出，政出多门，没有权威的管理部门；缺乏有力的法律支持，至今国家尚未出台和 PKI/CA、数字签名等相关的政策和法律法规。这样一种情形，导致在数字化图书馆中引入 PKI，没有现成的系统，没有统一的管理部门，更没有法律的支持，因此在现阶段不可能大范围地实现引入。在缺乏可持续发展的大环境下，图书馆要实现 PKI 的引入，必须采取自主研发、自我管理的模式，而其中要投入的资金与人力不是一般高校或公共图书馆所能承担的。

3.2 PKI 实施中的问题与对策

3.2.1 人员问题 PKI 对于大部分图书馆工作者来说是一个比较新的技术，在人员的技术与管理培训方面短时间内不可能得到很大的提高，毕竟一部分图书馆工作者计算机方面的知识相对薄弱，要让他们了解掌握一项新的技术，而且是相对复杂的技术需要较长一段时间。虽然图书馆都设有技术部门，但让 PKI 完全嵌入数字化图书馆不是一个部门的事情，是整个图书馆每个环节配合改进的过程。

3.2.2 技术问题 包括可信模型、资源引进与资源外包、建立与购买、封闭环境与开放环境、X.509 与其他证书格式、目标应用与综合解决方案、标准与专用解决方案、实现互操作需要考虑的因素、证书和 CRL、符合的业界标准、PKI 支撑的应用、策略问题、在线与离线操作、外围设备支持、设备要求、人员要求、证书撤销、密钥回复、资料库问题、安全保障、风险缓解等[7]。只有在建设的过程中把障碍清除，才能保障 PKI 的成功实施和顺利运作。目前在我国高校图书馆，还没有一家能真正引入 PKI 技术。

3.2.3 成本问题 PKI 包含了想法、谅解、惯例、协议、合同、法律、法规、机构、人，当然还有人与人之间的信任，因此可以用公钥信封及电子证书代替从前用笔签在纸上的手签名。数字化图书馆 PKI 的引入关系着整个图书馆的各项业务流程，要求图书馆去架构一个可以让 PKI 嵌入的平台，而且是整体的平台，这是一项成本开支很大的项目。目前很多新旧体系间的磨合问题需要解决，在讨论 PKI 能较好地解决上述问题的同时，还得慎重思考开展 PKI 项目存在的风险，认真计算其成效与成本之间的关系。按目前图书馆数字化的发展趋势看，单凭一个馆或几个馆的能力很难实现 PKI 的引入，无论是设备、资金、人力，还是法律法规，都不能满足 PKI 嵌入平台的构建要求，要真正实现 PKI，图书馆应该以联盟的方式，由政府主导、投入，图书馆负责管理、法规制定，这样一方面减轻图书馆的成本压力，另一方面还可以借鉴电子政务领域的有关经验，为数字化图书馆引入 PKI 提供可行方案和相对成熟的技术。

我国图书馆对 PKI 的研究很大程度上处于理论层面，大部分学者从不同角度论述 PKI 技术在图书馆运用的可行性，而很少有相关方面的实证研究。PKI 技术符合图书馆数字化的发展需求，但却迟迟未能有效解决知识产权、信息安全、馆际合作等问题。因此希望更多专家学者努力克服引入 PKI 的困难，投入更多精力在实证研究方面，促使 PKI 技术早日在实践中发挥应有的作用。

参考文献

1 段述明，张文金. 基于 PKI 的图书管理系统研究〔J〕. 通讯技术，2008，(5)：121－124.

2 周军. 数字化图书馆的版权保护技术的比较研究〔J〕. 图书馆论坛，2006，26 (3)：104－106.

3 黄新民，刘旺泉. VPN 技术综述〔J〕. 计算机安全，2003，(5)：9－11.

4 杨新，申功璋，文传源. 代理服务器在 Internet 中的应用〔J〕. 计算机工程与应用，2000，(10)：148－149.

5 夏志方. 远程访问图书馆电子资源技术综述〔J〕. 图书情报工作，2006，(3)：123－126.

6 张焕国，郝彦军，王丽娜. 数字水印、密码学比较研究〔J〕. 计算机工程与应用，2003，(9)：63－67.

7 Housley R. Internet X.509Public Key Infrastructure，Certificate and CRL Profile〔S〕. RFC2459. 1999.