《计算机工程》2000 年增刊

基于 LDAP 目录服务的 PKI 证书库研究与设计

高毓航* 龚俭

（东南大学计算机系，210096 南京）

【摘要】本文提出了一种基于 LDAP 目录服务实现 PKI 管理系统证书库的设计方案。论文通过与传统证书库实现方法的比较，阐述了该方案的优点，并具体给出了在开放的教育网这样的大规模应用环境下的具体实现技术和方法。最后对该方案的进一步使用前途作了总结与展望。

【关键词】LDAP;PKI;证书库;目录

中图分类号：TP393

The Design of PKI Certificate Repository Basing on LDAP Directory

Gao Yuhang, Gong Jian

(Southeast University, Computer Science Dept., 210096 Nanjing, P.R.China)

【Abstract】In this paper, the design of PKI certificate repository is proposed basing on LDAP directory service. Comparisons are made between traditional PKI repository design and this solution to show its advantages. Key technique points and methods are described for how to realize such a repository in large scale network educational application environment. The end of this paper summarizes the design and discusses the further applications of it.

【Key words】LDAP; PKI; Certificate Repository; Directory

随着国内计算机互联网络的用户覆盖范围和信息传输量的迅速增加，各类网络应用也日益增多。由于网络本身的开放性，因而就必然需要有一种安全机制来认证网上敏感数据收发双方的身份，并保证数据传输时的保密性和完整性。从国际的发展和应用趋势来看，目前对这种需求的公认解决方案是

作者简介：高毓航，硕士研究生，主要研究方向为网络安全。

龚俭，工学博士，东南大学计算机系教授、博导，主要研究方向包括网络管理、网络安全、网络体系结构、开放分布式处理等。

建立以非对称密码体制为基础的公开密钥管理框架系统（Public Key Infrastructure－PKI），通过一个可信的第三方——认证中心（CA）来为各用户与应用系统发放遵从 ITU X.509 国际标准格式的数字证书，并保障证书的有效性与可靠性。由于国外网络安全产品的各种出口限制和各种潜在的不安全因素，尽快研究与建立我们自己的 PKI 系统具有重要的意义。象教育网这样大规模的 PKI 管理系统，个人用户和应用系统用户数量大、地域分散性较强，这需要大容量、高可靠性和用户接口友好的 PKI 证书库作为实际应用支撑环境。本文就是在这一背景下，对如何利用 LDAP 目录服务来实现 PKI 证书库的建立与使用方案进行了研究与设计。

1. PKI 与证书库

证书库是 PKI 系统的数据存储中心和发布中心，用于发布所有通过认证中心认可的 X.509 证书和证书撤消列表。数字证书是 PKI 的核心数据结构，包含了证书持有者的个人信息、公开密钥和 CA 的数字签名。依赖于证书上 CA 的签名，用户可以离线地确认一个公钥的真实性和公钥持有者的身份。CA 用数字签名担保证书内容和用户公钥的可靠性与相关性，证书的持有者通过出示证书证明持有对应的私钥，进而证明自己的身份。证书撤消列表列出了仍在有效期内但已不可使用的公钥证书。CRL 和证书一起控制了用户公钥的有效性。

图 1 表示了 PKI 管理系统的基本功能实体和工作机制。在 PKI 系统中，认证中心采用的是离线工作模式，并不参与具体的身份认证和数据加密过程。在一个典型的认证过程中，持证者直接从证书库获取个人证书；验证者通过验证对方证书上 CA 签名的正确性和检查证书库中的 CRL 是否包含该证书来判断对方证书的有效性，从而决定是否建立信任关系。

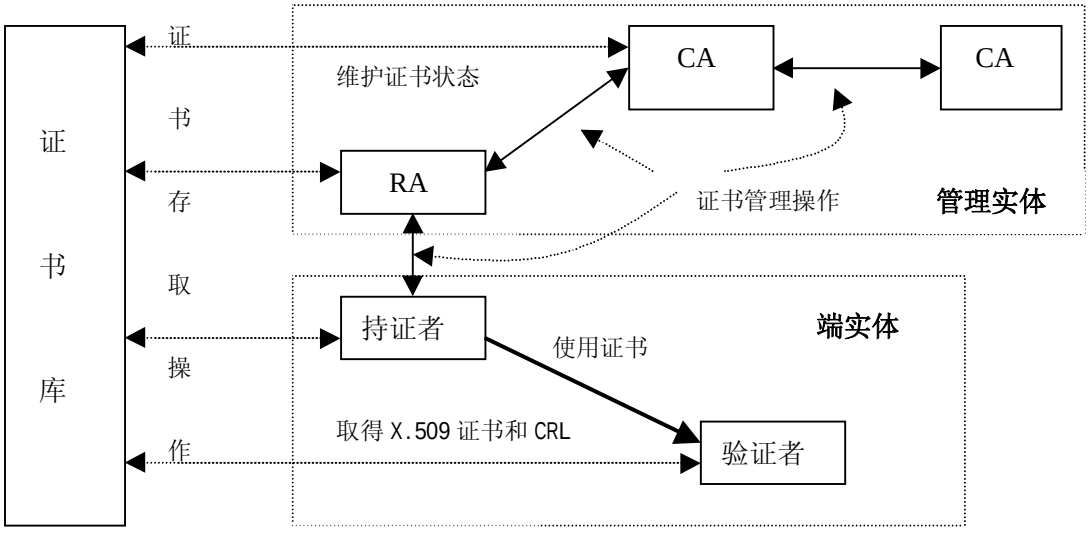

图 1. PKI 基本工作机制

因此设计证书库时，应考虑支持的功能包括，面向一般 PKI 产品用户提供 X.509 证书和证书撤消列表的查询与检索功能；面向管理实体提供支持对证书和证书撤消列表增、删和修改等维护操作。所以不仅需要基于 X.509 证书特点来考虑库中数据管理的可操作和易操作性问题，还应能支持用户与应用系统的不间断在线查询证书状态的功能，并能提供较好的用户查询界面与应用系统接口。在 CERNET 这样的大型应用环境下，用户数量大、应用系统众多、地域分散性强，所以还须注意证书库

定稿日期：2000-05-26

的规模、性能要求和可靠性等问题。

2. 证书库实现方式

最基本的方案是利用操作系统本身的文件系统管理功能来实现证书库，而公共访问协议一般采用 HTTP 协议。因为 X.509 证书各自为一个独立的语义单元，管理实体可以分别对各个证书执行管理操作，所以采用文件方式建立证书库是一种很直观的方法。但是这种方法不易管理，证书检索方式单一，应用系统使用困难。文件方式的证书库整体工作效率不高，只能适用于小型 PKI 管理环境或实验环境。当管辖域逐渐增大时，无论是 CA 的证书状态管理，还是面向用户和应用系统的检索都无法保证运行性能。

另一种方法是在数据库的基础上实现证书库。这种方法所支持的规模显然要比用文件方法大，但是开发的工作量也较大，因为必须要在关系数据库中定义各种的表格和编写大量的操作代码，才能实现对 X.509 证书的各种灵活操作。从面向公共访问服务角度来看，这种方法并没有更多的优势。[1]

LDAP（Lightweight Directory Access Protocol）是目前 Internet 流行的目录访问协议。LDAP 起源于 X.500 目录访问协议 DAP（Directory Access Protocol），是 DAP 的简化版本。LDAP 包含了信息存储格式与模型的定义和对应的检索与操作协议，数据与命名空间从本质上与 X.500 一致。LDAP 取消了 DAP 中较为复杂的操作，可直接运行于 TCP/IP 协议族上，采用是 Client/Server 工作模式。LDAP 由于使用简便，得到了广泛应用，并成为独立的目录服务，市场上已有成熟的商业产品。主流客户浏览器，如 Netscape 和 IE 都支持用 LDAP 协议访问目录；各大型服务器软件也采用 LDAP 目录作为网络数据库；各种基于 LDAP 协议的开发工具包提供了方便的目录数据查询与管理接口，如 Netscape Directory SDK（for C，Java）及 PerlLDAP，Solaris 7 SUNWlldap 软件包中所包含的库函数。

随着 LDAP 标准的日益成熟和 LDAP 目录服务应用的广泛采用，应用 LDAP 目录服务来设计证书库这个思路逐渐现已成为新一代的解决方案。

从数据本身的特性来看，采用目录服务是十分合适的。X.509 标准最早发表是作为目录服务标准 X.500 的一部分，证书名采用了传统的 X.500 的命名标准，而且证书中各种相关信息的存放形式也用的是目录中的“属性—属性值对”。因此，X.509 证书天生就适于存放在目录中。而且，由于 LDAP 目录服务自身带有多种灵活的项目检索、匹配和维护等功能与安全机制，还有众多友好的开发工具，这都使得证书状态的维护操作更为简单和清晰。

从面向公共服务和使用规模的角度看，应用 LDAP 也是合适的。目录服务本身就针对大量的访问操作进行了设计与优化，而且现在的主流浏览器都支持 LDAP 目录访问，一些应用系统也逐渐采用 LDAP 目录来存放网络中各资源与对象的基础信息。通过 LDAP 开发工具，应用系统可以方便地在线获取证书或查询证书状态。LDAP 服务器的目录复制功能（Replica）还可以帮助解决大型分布应用环境中各证书库的数据一致性维护问题。

3. 证书库的设计

下面将从几个工作流程来讨论如何在大规模应用环境下基于 LDAP 实现证书库。

3.1. 证书库的应用背景分析

以教育网为例，入网用户多为高等院校和部分教育机构，入网单位通过地区网络中心和国家中心接入 CERNET。因此在网络中需要保护的信息大致可分为两类：网络管理信息和一些应用系统数据。对网管信息的保护可体现为保障各网络管理中心之间、管理中心与用户单位之间管理信息的安全通信。

应用系统的例子有：在远程教育应用背景下的学生学习、教师答疑和批改作业等都需要通过身份认证。进一步可以为高校学籍联网提供认证和安全服务，为每个学生建立电子学生证和电子文凭。

所以从这样的应用需求来看：应用规模是巨大的，保护网管信息的通信约需要 3000 个证书，远程教育系统中需要的证书量应不少于学生、教职员工和管理机构的数目总和；对性能和可靠性的要求也很高，证书库必须不间断接受大量访问，并具备较好的备份和恢复机制；证书库本身的安全要求高，软件本身要能进行方便的权限设置，操作系统应是稳定、无安全漏洞的，硬件设备要有安全保护措施。

3.2. 证书库的应用结构

通过对应用背景分析，考虑采用集中层次式的证书库结构。图 2 是基于 LDAP 的 PKI 证书库应用结构图。

由中心的 CA 负责签发证书和维护主证书库中的证书状态，各院校有自己的 RA 负责处理用户证书申请和向 CA 提交请求。出于可靠性和一些大型应用系统的性能要求，这里采用双库热备份机制。主库在甲地，从库在乙地，两库之间通过 VPN 高速信道进行连接。CA 对主库的任何修改操作可通过 LDAP 服务器的目录复制功能（Replica）由主库实时地反映到从库中。两库如有一方发生故障，仍然可以保持证书库服务。主库通过 LDAPS 对从库进行访问与数据维护。类似地，各用户单位与应用系统也可自行建立本地备份。本地从库通过定期检查主库更改操作日志或证书库的版本号来保持与主库数据的一致性。

管理实体负责维护主库中的各种数据，主要为 X.509 证书和 CRL；端实体，即个人用户和应用系统，则从证书库获取在安全应用所需的证书和各种证书状态信息。因为证书库中的数据是已采用数字签名来保护数据完整性的公开信息，一般用户可直接用浏览器通过 LDAP 或 HTTP 协议访问，应用系统可通过 LDAP 协议接口来获取 X.509 证书和 CRL; 管理实体则因为需要对库中内容进行添加、修改、和删除等证书状态维护操作，所以要通过 LDAPS 协议访问证书库，通过把各种证书库操作解释为具体的 LDAP 操作流程来实现。

---

[1]为了更好地支持应用系统的查询需求，许多采用上述两种方法的系统还必须提供向 LDAP 目录发布用户证书的功能。

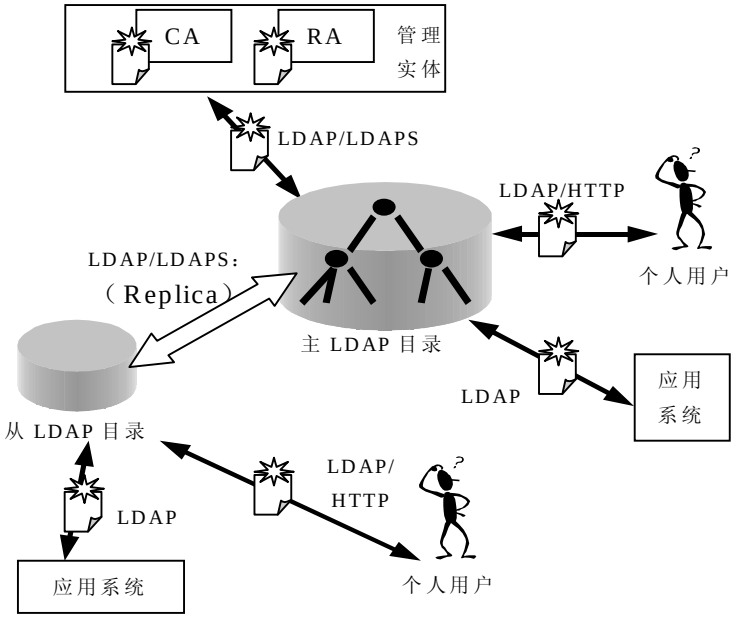

图 2. 基于 LDAP 的 PKI 证书库应用结构

3.3. LDAP 证书库的数据存储模型

IETF 的 PKIX 工作组曾提出一个基于 LDAP V2 的 X.509 PKI 系统应用规划子集（RFC2587），定义了在 LDAP 中存放 PKI 实体所必需的对象类与属性的规划集（Schema），例如：用户（pkiUser）类的定义：

```
pkiUser   OBJECT-CLASS   ::= {
    SUBCLASS OF   { top}
    KIND          auxiliary
    MAY CONTAIN   {userCertificate}
ID    joint-iso-ccitt(2) ds(5) objectClass(6) pkiUser(21)}。
```

这一规划在目前市场上的目录服务器软件中大多已经得到应用，如在 Netscape Directory Server 中的用户类 inetOrgPerson 本身已具有用户证书属性（userCertificate），可以支持一般的应用系统的需求。

但是把该规划应用在上述的证书库目录中就显得过于简单，用户实体只有一个证书属性、CA 实体只有 CA 证书和 CRL，这很容易造成管理和应用上的不便。所以我们在 RFC2587 的基础上，做了一个扩展类型集，扩展的依据是日常数据处理的方便性和用户系统的可用性。在用户类型中，我们增加了证书状态（certificateStatus）、证书名(certificateSubject)、签发者(Issuer)和有效期起止日期等属性；在 CA 类型中增加了证书库版本号（certificateRepositoryVersionNumber）；为了适应分布的 CA 和多个 RA 之间的数据通信，我们增加了证书请求类型（certificateRequest）。

3.4. 证书的访问规程与权限设置

定义好数据模型后，需要确定证书库的各类访问规程，即确定各种访问实体的访问协议。具体涉及到的方面有操作执行步骤和数据匹配原则。IETF 的 PKIX 工作组也分别对这方面提出了相应的标准与草案：操作集——基于 LDAP V2 的 X.509 PKI 系统操作集（RFC2559）和基于 LDAP V3 的 X.509 PKI 系统操作集（draft-ietf-pkix-ldap-v3-01.txt）；匹配规则——raft-ietf-pkix-ldap-v3-01.txt 为 LDAP V3 的使用环境定义了各种证书匹配规则，如 certificateExactMatch 和 certificateListExactMatch 等。RFC2559 中

概括地定义了三种抽象操作：Repository Read, Repository Search, 和 Repository Modify，分别对应证书/CRL 的下载/查询/发布。各抽象操作都是由若干基本的 LDAP 操作按一定顺序组成，如 Repository Read 由三个 LDAP 基本操作实现： BindRequest(BindResponse), SearchRequset(SearchResponse), UnbindRequest。我们根据 IETF 的上述规范，为各种实际的证书库操作制定相应的访问规程，例如 CA 在签发新证书后的保存工作可分解为以下几步：

提取证书中的各种信息-->BindRequest(Bind as CA user)-->查询是否已有同名节点-->生成新节点结构并填写相应的属性值-->AddRequest-->UnbindRequest；

同时根据实际应用增加了部分规程，例如，对特定证书状态的在线查询规程。

规程在具体使用时还需要注意各种实体的操作应与目录中的访问权限一致。目录的主要对外服务是是提供有数字签名机制保护的证书和 CRL，这部分应是匿名只读、管理实体可读可写；如果要支持用户单位建立自己的证书库备份，主库的修改操作日志应允许匿名读；作为 CA 和 RA 协调工作的证书请求部分应只允许 CA 和 RA 读写。下面是具体的权限设置：

（1） 主库：

- 证书和 CRL：可以匿名检索与读取，CA 可以增、删和修改。
- 证书目录树下的修改操作日志：由目录自己生成，可匿名读取。
- 证书请求子树：RA 和 CA 可读、增、删和修改，其它所有用户不可读写。
- 证书库版本号：可以匿名读取，只有 CA 可以修改。

（2） 从库：

- 证书和 CRL：可以匿名检索与读取，CA 可以增、删和修改。
- 证书目录树下的修改操作日志：只有从库管理员和 CA 可以读取。
- 无证书请求子树。
- 证书库版本号：可匿名读取，只有库管理员用户可以修改。

值得注意的是目录管理员对库中内容有全部权限，因此需要有相应的实践规程来进行访问控制，如目录服务器只能由专人从控台登陆管理，机房必须有三防、安全监控系统等保护措施。这对于 PKI 的 CA 和 RA 等管理实体也是一样的。

3.5. 建立证书库服务

证书库的具体建立过程将分为以下几个步骤：

- 确定硬件与软件设施：机房应有安全措施和访问监控，主机采用 E 系列工作站，操作系统应是 UNIX。目录服务器软件定为 Netscape Directory Server 4.x。
- 设置目录服务器：
  （1） 把设计好的数据类型定义和匹配规则应用到 LDAP 目录服务器的配置中。
  （2） 为主库和从库申请服务器证书，确定各自普通服务端口和安全服务端口。
  （3） 在目录中建立管理实体用户（CA 和 RA），绑定各用户与相应的证书。
  （4） 为主、从库建立目录复制关系（Replica），具体方法参见目录服务器管理手册。
  （5） 设定各目录树中的用户访问权限，具体设置类别参考 3.4。
- 根据访问规程为各类确定对证书库的各种访问步骤，将管理实体原有的各种证书库操作 API 替换为用基于 LDAP 开发工具编写的 API，为应用系统提供查询证书、CRL 和证书状态的 API 与具体的访问途径和方法。

- 启动主、从证书库服务和两库之间的目录复制功能。
- 发布服务：将管理实体的证书库访问点指向主目录服务器。对外发布服务器地址和数据类型规划。

4. 结束语

应用 LDAP 目录服务实现 PKI 系统的证书库是目前国际 PKI 证书库设计中的主流趋势。与传统方案相比，现在 PKI 系统中面向管理实体和用户、应用系统的证书库合二为一，这不仅开发实现起来简单、清晰，还能令 PKI 系统中的管理工作变得更为灵活与方便，例如有利于多注册中心和认证中心的协调工作。应用 LDAP 目录为证书库尤其适合象教育网这样的大规模应用环境，LDAP 目录可优化处理大量用户访问，LDAP 本身还较好的支持分布式运行环境与数据备份机制。进一步的应用有：为 PKI 管理系统中的应用各种管理政策，例如设定用户证书名申请规范等。

参考文献

1. http://www.ietf.org/html.charters/pkix-charter.html
2. http://www.netscape.com/eng/servers/directory