证书服务器的设计与实现

刘建航
（东南大学计算机科学与工程系，南京 210096）

【摘要】非对称密码体制的广泛使用迫切需要提供可靠的公钥获取途径，为此 PKI 建立了一个公开密钥的管理框架，向网络中需要使用公钥机制的应用提供公钥管理服务。作为 PKI 的核心组件，CA 实现了大部分的 PKI 操作。本文描述了华东北地区网络中心设计并实现的证书服务器的功能框架，简单介绍了该服务器在两个项目中的具体应用。

【关键词】X.509 证书 CA 非对称密码体制

一. 背景介绍

1976 年 Diffie 和 Hellman 在《密码学的新方向》一文中提出了公开密钥的思想.由于大大简化了对称性密码体制繁重的密钥管理任务，非对称密码体制，如离散对数，RSA 等得到了广泛的应用。对公开密钥体制而言，如何安全地获得通信对方的公钥是系统安全性的前提。1978 年 Loren Kohnfelder 提出了证书的概念，使用由第三方签名的证书作为可靠传递公钥的方法，以解决集中存储公钥带来的性能瓶颈。作为 X.500 目录服务的一部分，X.509 证书将一个 X.500 节点名 DN(Distributed Name)和一个公钥绑定起来用于控制对目录的访问操作。虽然 X.500 的全局目录并未真正建立起来，但 X.509 却得到了一定的发展。IETF 的 PKIX 工作组致力于建立一个全局的公开密钥管理框架（PKI），使用 X。509V3 证书和证书撤消列表 CRL V2，向网络中需要使用公钥机制的应用程序提供公开密钥管理服务。

当要在 Intranet 环境中（如校园网）建立 PKI 时，有两种选择，一是依赖外部 CA 公司，如 Verisign,GTE 等提供的证书服务；二是建立自己的 CA。在华东北地区网络中心承担的两个九五攻关课题---“基于内部网的网络管理系统”和“网络安全监察系统”中都需要使用公钥机制保护浏览器与 Web 间的交互信息，考虑到安全因素及系统自身的独立性，我们不能使用外部 CA 服务；我们还考察了国外的商业化产品，如 Netscape,Microsoft 等公司的证书服务器，发现这些产品除价格昂贵外，系统开销非常大，不适合我们的要求。考虑到 CA 作为网络安全基础设施的重要性，我们设计并开发了该证书服务器，实现了 PKI 框架中的 CA 功能。

二. 证书服务器的系统功能

作为两个九五公共项目－－“基于内部网的网络管理系统”和“网络安全监察系统”的一部分，该证书服务器的设计目标是在中小规模的网络（如校园网）环境中建立一个公钥管理平台，使各项应用程序能够使用公钥机制保护重要的数据传送。

作为 PKI 框架的核心部分，作为 CA 的证书服务器应具有以下基本功能:

1.接收用户（个人浏览器，Web 服务器等）的证书请求，管理请求队列；

2.管理员可对证书请求进行查询，批准，驳回等操作；

3.管理员可查询证书库，对其中的证书进行查询，校验等操作；

4.用户可从服务器下载自己及 CA 的证书，可查询他人证书的状态。

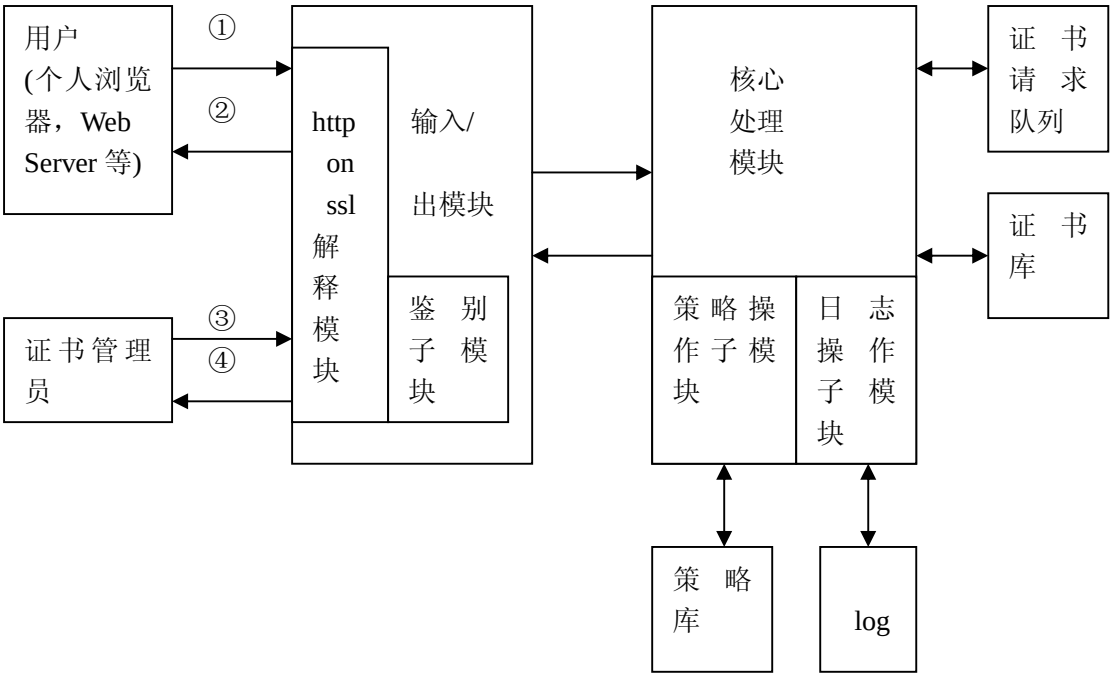
证书服务器仅限于向各应用程序提供公开密钥的管理服务，使用公钥的各项操作如签

名，协商会话密钥等都需要由应用程序自己完成的，因此证书服务器的用户是那些实现了公钥处理模块的应用，如浏览器，商业 Web 服务器，目录服务器等。为保证能和上述应用程序协同工作，证书服务器必须支持开放性的标准：

1. 支持 X.509 V3 证书，可根据需要添加用户扩展；
2. 支持 RSA 及 PKCS 系列标准;
3. 支持 HTML，HTTP，SSL，S/MIME，LDAP 等应用协议。

三．证书服务器的系统结构

按功能上分，本服务器可分为输入/出模块，核心处理模块，策略库，请求队列，证书库等几部分，具体框架见下图：



1. 输入/出模块

输入/出模块的主要作用是理解证书请求用户所使用的传输协议，将各种操作请求传给核心处理模块。PKI 框架并未指定具体的传输协议，故可以使用 http,ftp,smtp 等。考虑到浏览器已成为最广泛使用的客户端软件，我们选择 http 作为用户与证书服务器之间交互的传输协议。用户通过浏览器访问证书服务器，提交证书请求（图中①）,下载自己及 CA 的证书（图中②）。为保证证书请求(PKCS10)和验证信息的完整性和隐蔽性，输入/出模块使用 http on ssl，通过 SSL 协议提供的安全通道透明地保护 http 协议报文。

由于管理员同样使用浏览器进行各项操作，输入/出模块必须能够确认操作发起者的真实身份，为此我们引入了鉴别子模块。系统初始建立时将产生一管理员证书并下载至指定的机器上。当管理员进入系统时（图中③）,输入/出模块使用 SSL V3 的客户证书鉴别机制确认管理员的身份，通过鉴别后即可进行各项管理操作。

在证书批准后，用户登入系统以下载证书（图中②）,通过定义两个特殊的 MIME 类型，application/x-x509-ca-cert，application/x-x509-user-cert,浏览器可识别出下载的内容为 CA 证书或个人证书，确认有效性后存在证书表中。

2.核心处理模块

核心处理模块的主要作用是根据管理员指示和安全策略对证书请求及证书作查询，批准，撤消等操作。根据操作的性质和输入/出模块的鉴别结果，核心处理模块将操作分为两

大类：

(1)用户操作：由证书服务器的用户提交的操作，包括证书请求，下载证书，查询证书状态；

(2)管理员操作：由证书服务器的管理员提交的操作，包括批准或驳回证书请求，发布，删除证书，校验请求有效性。

在以上各项操作中，核心的操作是证书批准操作，其工作流程如下：

策略是证书服务器限制证书操作的一组规则，如限制只能发布某特定 DN（Distributed Name）子树下的证书，限制用户提交的请求中必须带有 Email 地址或电话号码，限制证书库中所有的证书不能出现相同的公钥或 DN，限制最长有效期，等等。策略是 CA 安全政策的体现，不加任何限制的 CA 是毫无意义的。 策略子模块对各项操作进行过滤，只有符合策略的才予以执行。管理员可以通过策略子模块修改策略库以适应新的需求。

对任一个操作，核心处理模块都将给出成功或失败的响应，并使用日志子模块将该操作记录在日志中，以反映证书服务器运行的历史状态。

(三)证书请求队列和证书库

这两项是证书服务器的核心数据，反映了证书从请求提交，批准，发布至过期的整个生命周期。证书请求队列共有三个子队列，分别为待处理请求队列，已驳回请求队列和已批准请求队列。核心处理模块根据请求的不同状态将其置入不同的队列中，管理员可观察，校验处于不同状态的请求内容。 证书库中维护着服务器发布的所有证书，包括个人浏览器证书及应用服务器证书。证书库中的每个实体可处于有效，无效或过期状态，核心处理模块将根据证书库的内容响应用户的下载及查询请求。

四．系统应用及进一步的改进

该证书服务器完成后首先应用于前面提到的两个攻关项目中，用于向 Web 服务器和系统用户发布证书。项目中使用基于证书的双向鉴别机制，提高了鉴别的强度。通过试验，我们开发的证书服务器能够和现在流行的商业产品，如 Netscape Enterprise Server, Proxy 等服务器协同工作，可用于内部网中建立安全应用的基础平台。

限于时间，目前我们仅实现了 CA 的基本功能，下一步希望对证书服务器的功能做以下扩展：

1.支持 CRL：CRL 是 PKI 框架中重要的证书状态校验机制，尽管目前商业产品大多还不支持 CRL 验证操作，但我们认为作为完备的 CA，证书服务器应具有 CRL 的产生和发布功能。用户可随时提交证书撤消请求，管理员根据用户请求撤消证书并将其置入 CRL 中；

2.支持 CA 间互授证书：大规模网络中往往需要域间信任，通过 CA 间互授证书形成证书链，证书服务器可应用于更为复杂的信任模式中；

3.支持 LDAP 目录服务：证书，CRL 都是公开信息，适合发布在开放性的 LDAP 目录中，这样可缓解证书服务器的负载压力；此外，LDAP 目录还具有集中管理，查询效率高等优点。

4.采用数据库维护证书及请求信息。目前我们采用文件系统管理数据，当网络规模较大，证书数量很多时查询等操作速度较慢。

五．结束语

随着 Internet 的逐渐商业化，网上数据的重要性正日益增强。Intranet,电子商务等领域都需要引入数字认证服务。PKI 提供了大型网络中公钥管理的框架，研究 PKI 的各项关键技术，如 CA 的实现，是有一定意义的。我们在攻关课题项目实施过程中根据需要设计并开发的这个证书服务器虽然还不很完善，但已具备了 CA 的基本功能。以此为基础，可以实现许多基于公钥体制的安全应用。

参考文献

【1】IETF PKIX Working Group ,"draft-ietf-pkix-*.txt"
【2】MasterCard,Visa "SET:Secure Electronic Transaction Specification"
【3】龚俭:《计算机网络安全概论》
【4】Netscape Corp: "Security White Paper"

【Abstract】With the spread use of unsymmetrical cryptography, we need a method with which one can get another's public key reliably. PKI is such a management infrastructure whose main function is to provide public key managering service. As the essential component of PKI , CA(Certificate Authority) implement most of PKI operations. This article described the infrastructure of the Certificate Server which was designed and implemented by NENC, then introduced the application of this server in two projects.

【Keywords】X.509　Certificate　CA　unsymmetrical cryptography