数字证书授权机制 网络建 Internet用 (10)

计算机科学2000Vol. 27№. 11

数字证书授权机制的研究与实现

Study and Implementation of a Digital Certificate Authority Mechanism

39-42

宣 蕾 吴泉源 王怀民
(国防科技大学计算机学院 长沙410073)

TP393.408

Abstract We studied and implemented a Certificate Authority (CA)server software to issue the Digital Certificate which uses for secure authentication over Internet in this paper, includes: generating the RSA key pair and management of the Digital certificate, e. g. generating a certificate request, generating a certificate, signing/verifying a certificate and revoking a certificate. Now the CA server that we implemented has passed the test. The conclusion is that the CA server measures up the correlative international standard and it can offer the practical applications.

Keywords Digital certificate, Certificate authority (CA), Authentication, Public key cryptography, Key pair

1 引言

进入21世纪，网络安全问题已不再停留在认识阶段，而是进入了实施阶段。随着网络安全投资的不断增加，网络安全技术应用越来越广泛，从电子商务、事务处理到软件发布、电子邮件，任何安全系统都离不开认证，数字签名是目前应用最广的认证系统。数字证书提供了一种在 Internet 上进行身份认证和数字签名的方式，在网上进行事物处理、电子商务等活动时，双方需要使用数字证书来表明自己的身份，并使用数字证书来进行有关操作。

数字证书(Digital Certificate)是公钥体制的一种密钥管理媒介，它是一种权威性的电子文档，用于证明某一主体(如用户、服务器、软件代码等)的身份以及其公钥的合法性。

为了防止证书假冒，数字证书需要一个具有权威性和公正性的第三方机构发放，于是产生了证书授权机构 CA(Certificate Authority)。

2 PKI 模型

证书授权机构(CA)是网络中的专用证书目录服务器系统，具有数字证书生成、证书名称分配、证书发布、生成 PKI 管理信息加密的密钥，密钥分配、密钥对存储、用户身份鉴别、证书目录服务等功能，同时为用户提供验证证书的功能。

目前，国外有许多权威 CA 机构，提供在线或离线签发证书、验证证书等服务，商业 CA 机构如 Verisign、Cybertrust、CommerceNet、Thawte 等，政府 CA 机构有美国邮政局等，各大电脑公司也建立了自己的 CA 机构，如 IBM、AT&T、Microsoft 等。国内也在纷纷建立 CA 机构，如263. Net、上海市、外经贸部、南方电子商务中心、长沙电子商务中心等，可以为单位或个人有偿提供不同级别、不同用途的数字证书服务，但规模比较小，尚无全国的根认证中心(PCA)。据悉，国内金融界1999年已开始共建基于公钥基础设施 PKI 的金融权威认证中心(PCA)，作为电子商务信息安全的基础设施。

PKI(Public Key Infrastructure)是一种遵循标准的密钥管理平台，能够为所有网络应用透明地提供采用加密和数字签名等密码服务所必需的密钥和证书管理。PKI 必须具有：认证机构(CA)、证书存储服务器(Repository)、PKI 证书管理协议、证书注册机构(RA)、证书用户(客户端证书处理系统)等五个基本成分，PKI 将围绕着这五大系统来构建，CA 是 PKI 的核心。图1给出了证书管理、应用系统的一个模型。

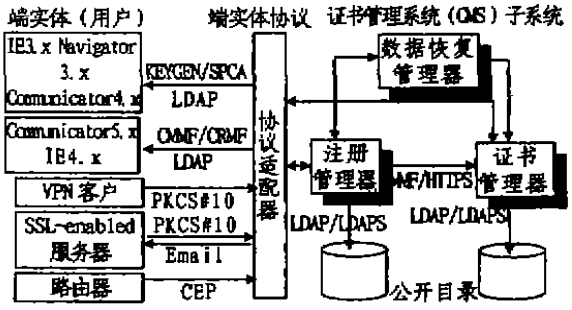

图1 Netscape 证书管理系统体系结构

端实体(用户):各种各样的端实体(End Entity)可以向证书管理系统(CMS)申请证书:

·浏览器,如 Netscape Communicator 或 IE;

·支持 SSL 的服务器,如 Oracle Application Server;

·虚拟私有网络(VPN)客户方:如 RedCreek;

·路由器,如 Cisco routers。

端实体协议:证书管理系统(CMS)支持的允许端实体与服务器进行交互的各种各样的协议。

证书管理器(CA):是一个签发与撤销证书并产生 CRL 列表的服务器,它能够从端实体直接接收证书申请,也能从注册管理器接收证书申请,注册管理器已经担负了一些证书管理功能,如鉴定端实体。

注册管理器(RA):是一个据有充分资格的证书管理器 CA 的远程注册前端,加强了证书发布、更新、撤销请求,密钥更新与恢复,以及综合功能的管理策略。多重注册管理器可以汇总到一个证书管理器。一旦用户注册成功,该证书用户便获得了对证书和 CRL 的存取权限。

数据恢复管理器:处理加密私钥业务,如密钥档案和密钥恢复。

内部数据库:在 CMS 中建立的一个遵从 LDAP 协议的持久稳固的存储系统,这个数据库是预设的目录服务器。

公开目录:用于公布证书和 CRL 列表,CMS 可以公布任何遵从 X.500系列协议的目录。

PKI 信息管理是对证书用户和 PKI 服务器(CA 和 RA)之间信息交换的管理,主要包括:请求公钥证书,CA 响应证书请求,CA 为 PKI 用户生成密钥对,请求作废一个证书,查看 CRL,直接从 PKI 服务器中接收有关 CA 密钥或证书的更新、CRL 刷新和用户废弃证书通告等信息。

PKI 管理信息的通信通常可利用 FTP、基于 TCP 的通信协议(套接字)、Email、HTTP 或目录存取协议(DAP、LDAP)等。

PKI 支持安全套接字层(SSL)、安全 IP(IPsec)、虚拟私有网络(VPN)、安全电子商务(SET)及安全电子邮件(S/MIME)等协议。

3 CA 管理模型

CA 是一个受一个或多个用户信任的发证机构,负责生成和分配证书,也可以为没有密钥对生成工具的用户生成密钥对。CA 用自己的私钥签发证书,用户用 CA 的公钥验证证书。验证证书有效性包括四个方面:确定用户和发行者的名字是否有效;检查证书的有效期限,确定是否过期;确定证书是否已被撤消;确定证书中的签名是否有效。

在增强的私密电子邮件 PEM(Privacy Enhancement for Internet Electronic Mail)标准(RFC1422)中,定义了 CA 的层次结构,如图2所示的树状模型:根结点 IPRA(Internet Policy Registration Authority)确定全球证书管理策略。在 Internet 仅此一个根结点;PCA(Policy Certification Authority)由 IPRA 验证,是特殊的 CA,一般由政府或总公司管理定义。制订下属 CA 的安全原则;CA 由 PCA 验证,为端实体或下属 CA 组织签发、验证证书。

证书可以通过 CA 的树状结构得到验证:每一个证书都与为它签名的 CA 的证书相连,使用验证路径就可以追溯到一个著名的可信赖的 CA,从而确定证书是有效的。

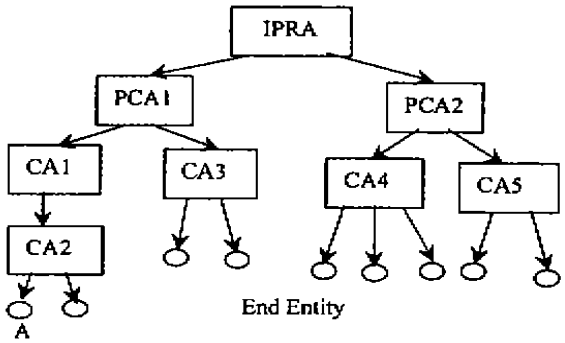

图2 CA 的树状结构模型

IPRA-PCA-CA1-CA2-A 五张证书连在一起,便形成了一条证书链。它是从根结点证书到端实体证书的一条有向路径,用户进行验证时,不需要查找每级 CA 的证书,只要查到根结点的证书(公钥)即可验证。证书链存放的第一张证书为端用户证书,最后一张证书为根 CA 证书。

4 密钥对产生

目前最常用的是 RSA 公钥证书。RSA 是把明文转换成密文的一种块密码,它有两个密钥:公钥和私钥,用一个密钥加密的消息只能用另一个密钥解密,任何人都无法通过公钥确定私钥,也没有人能通过加密消息的密钥解密。创建两个协同工作的密钥是 RSA 的最重要的特性。RSA 系统的构造是:

1)选择两个大素数 p 和 q(保密)。

2)计算它们的乘积 $n=pq$(公开),和 $\Phi(n)=(p-1)(q-1)$(保密)。其中 $\Phi(n)$为欧拉函数,n 被称为模。

3)随机选择一个整数e，它小于n并满足(e，Φ(n))=1，1<e<Φ(n)，即e与Φ(n)互素，除了1以外没有公因子(公开)。

4)求出另一个整数d，满足(ed－1)能够被(p－1)(q－1)整除，即ed≡1modΦ(n)，1<d<Φ(n)，(保密)。

e和d的值各自被称为公开指数和私有指数，因子p、q与私钥一起保存或被销毁。RSA系统的公开密钥为k=(n，e)，私有密钥为k'=(n'd)，一旦产生了这个密钥对，就可以采用单向陷门函数进行加密和解密：明文消息m满足0≤m<n，加密过程和解密过程分别为：

加密算法：$E: m \rightarrow c = E_k(m) = m^e \bmod n$

解密算法：$D: c \rightarrow D_{k'}(c) = D_{k'}(E_k(m)) = c^d \bmod n$

将加解密的顺序反过来，RSA算法还可用于数字签名。因为私钥加密的信息任何人都能找到他的公钥来解密，所以只能起到证明身份的作用。

从RSA算法分析可以看出产生RSA密钥对是实现RSA算法的关键，根据上述RSA密钥对的构造过程，可逐步求出RSA密钥对及其相关参数，处理过程如图3所示。

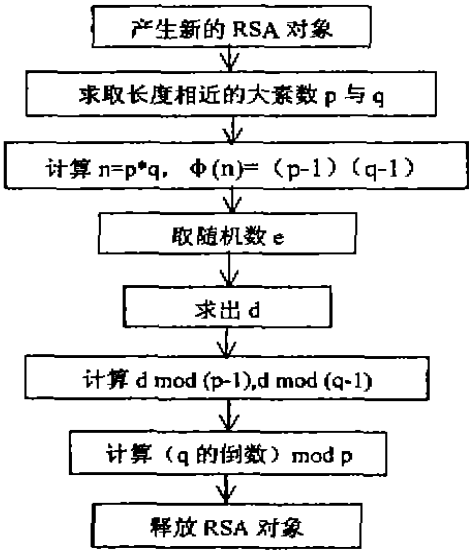

图3　产生RSA密钥对的流程

申请数字证书依据RSA密钥分配类型分为两种模式：集中式和分布式(详见参考资料[9])。

5　证书的结构

目前通用的证书以X.509版本3(基于公钥证书的目录鉴别协议)作为数字证书标准，X.509规范中定义了一种通用的数字证书格式，其数据结构如表1所示。

表1　X.509V3证书数据结构

域	说明
版本号	定义证书的版本，主要用于表明是否与X.509v3兼容，
证书序列号	一个CA发布的每张证书具有唯一的序列号，
证书签名算法	定义了签发证书采用的加密算法。
发证机构名称	定义了证书签发者(通常是一个CA)的名称。
证书有效期	定义了该证书的有效期限，起始日期到终止日期。
证书持有者名	定义了该证书持有者的名字及其详细资料。
证书持有者公钥	存放证书持有者的公钥信息。
版本3扩展项	允许往证书里加入扩展信息，如发证机构别名、证书管理策略等。

证书还有多种编码方式如：ANS.1的DER编码二进制格式证书、PKCS＃7格式证书链、Netscape证书序列格式、base-64编码预包装的证书或证书链等。

在查看证书内容时，我们经常会看到数据类型中所没有的密钥指纹，它是一个公钥的密钥参数的密码散列(哈希函数值)，在密钥创建时产生，交给密钥所有者记录下来。

证书没有过期并不一定就是有效的，比如私钥失密或证书持有者离职，证书就需要撤销。X.509标准中定义了证书撤销列表CRL(Certificate Revocation List)，用于存放已撤销的证书并向网上传播，直到撤销证书签发时给定的失效时刻，再从CRL中删除到期证书。

CRL列出了被撤销的证书，带有CA的签名，由CA负责定期更新。在验证证书的有效性时，必须检查最新的CRL以确保证书未被撤销。

一张证书只能由签发它的CA机构撤销，每个CA机构都应维护自己的CRL列表，通过目录向外公布。

6　CA服务软件的实现

为了给基于SSL的安全系统提供证书，本人通过对PKI体系结构、证书管理机构(CA)、证书申请和证书结构等模型的分析，设计了一个层次结构的、离线式CA服务软件，可以进行集中式证书申请及签发证书，也可以为分布式证书申请签发证书，它能够产生RSA密钥对和X.509v3标准证书，包括CA机构的自签名根证书和客户、服务器等端实体证书、PKCS＃10证书申请、PKCS＃7证书响应等。

这个CA服务软件实现的一个CA机构应具备以下基本功能：产生RSA密钥对；产生自签名的CA根

证书；产生证书申请；为证书申请签发证书；导出证书，交给用户；查看证书；用新证书更新证书库，程序的基本流程如图4所示。

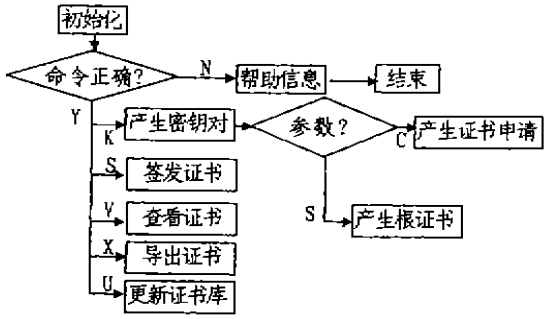

图4 CA 基本服务流程

为实现以上基本功能，需要一些基本函数的支持。下面简单介绍一些程序中对证书进行操作的常用基本函数的功能：

GenerateKeyPair：用于产生新的 RSA 密钥对。这属于集中式证书申请方案，为没有密钥对的证书申请者产生密钥对。若证书申请者有自己生成的密钥对并提交了公钥，属于分布式证书申请，就不必执行这一操作，程序直接从证书申请文件中提取公钥。本 CA 服务软件支持这两种方式的证书申请。

CreateCertObj：用于创建一个新的证书对象，可以是一个证书、证书申请、证书链、CRL 或其它证书类对象。新创建的证书对象域值是空的，需经下列函数对各个域进行赋值或修改。

AddCertComponent：用于向证书对象中加入域值信息。如证书持有者名称、证书发布者名称等可用本函数进行赋值。

DeleteCertComponent：用于从一个证书对象中删除一个成分。当证书的某些域值需要修改时，可先删除该域值，再赋予新的域值。

GetCertCompnent：用于从证书对象中取出域值数据。当需要显示查看证书时，使用本函数取出各种字符串类型的域值。

SignCert：用于为证书对象中的公钥证书、CA 证书、证书申请、CRL 等进行数字签名。一旦经过签名，证书对象就不能再用上述证书操作函数进行修改或更新，如果须修改该证书，就要另外产生一个新的证书对象。调用该函数时，须要指定用于签名的私钥，若是要自签名的 CA 机构的根证书，就用证书对象中的公钥对应的私钥进行签名；若是端实体证书，就用指定的 CA 机构的私钥进行签名。

ExportCert：用于从一个包含证书的对象中导出各种编码格式的公钥证书、证书申请、CRL 等。导出证书之前必须对每个要求赋值的域赋好值并经过 SignCert 签名。

ImportCert：用于把一个证书、证书申请、CRL 等导入到包含证书的对象，以便对其进行各种操作。

CheckCert：用于检查一个证书对象的签名或者验证一个证书对象是否在 CRL 中。

DestroyCertObj：当对证书对象操作完毕后，用于销毁一个证书对象，它清除证书对象使用的全部密钥信息与各种其它保密信息，释放证书对象使用的所有内存，以免攻击者从中搜索到与证书相关的保密信息。

结束语 目前，WWW 系统被广泛应用于开发事务处理、工作流等业务网，WWW 系统采用 Client/Server 模式工作，浏览器基本上使用 IE 或 Netscape Navigator，服务器也大部分采用国外软件，这些软件虽然支持 SSL 协议，但证书必须花钱到厂商指定的 CA 机构申请，等于系统地安全由他们托管，这是任何一个安全 WWW 系统都不希望的方案。因此，基于 SSL 协议进行加密和认证的安全 WWW 系统，在不能通过可靠渠道从可信赖的 CA 机构取得数字证书时，可以建立自己的 CA 服务器，从而成为整个 CA 机构上的一个结点或作为一个独立的 CA 机构，为单位内部员工分配、管理证书以利于工作和保密。

我们分析、设计了发放数字证书的 CA 服务软件的模式，并系统地实现了它，使其满足基于 SSL 的数字证书要求，并能兼容符合标准的通用安全软件的证书需求。目前通过测试验证，表明我们实现的 CA 服务软件符合相应的国际标准，可提供实际应用。

参 考 文 献

1 Kent S. Privacy Enhancement for Internet Electronic Mail. Part Ⅰ. Certificate-Based Key Management. RFC1422. BBN. February 1993
2 Linn J. Privacy Enhancement for Internet Electronic Mail: Part Ⅰ. Message Encryption and Authentication Procedures, RFC1421, February 1993
3 Kaliski B. Privacy Enhancement for Internet Electronic Mail: Part Ⅳ: Key Certification and Related Services, RFC1424, Februry 1993
4 Kaliski B. PKCS # 10: Certification Request Syntax Version 1.5, RFC2314, March 1998
5 Kaliski B. PKCS # 7: Cryptographic Message Syntax Version 1.5, RFC2315, March 1998
6 Housley R, et al. Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC2459, January1999
7 Gutmann P. Cryptlib Security Toolkit, Version 2.1, April 1999
8 韦卫，王行刚. PKI-X.509公钥证书及其 CA 的研究进展. 通信保密，1999(2)
9 金晓秋，郭巍，金亿平，张世永. PKI 中的证书和发证机构. 计算机科学，1999，26(7)
10 宣蕾，滕猛，吴泉源. SSL 协议实现与 CA 的支持. 信息和通信安全—CCICS'99第一届中国信息和通信安全学术会议论文集. 科学出版社，1999
11 宣蕾. 安全通信协议 SSL 及其数字证书机制的研究与实现：[硕士学位论文]. 国防科技大学研究生院，2000