文章编号: 1001- 2486(2003) 01- 0026- 05

基于 CA 的电子印章系统设计与实现*

刘世栋[1], 杨 林[2], 侯 滨[2], 王建新[2]
(1. 解放军理工大学通信工程学院, 江苏 南京 210016; 2. 总参第 61 研究所, 北京 100039)

摘 要: 针对分布式层次化网络安全应用, 提出了一种分布式简化严格层次结构的 PKI 信任体系模型, 为网络应用提供有效的认证、访问控制、授权、机密性、完整性、非否认服务。在该信任体系模型基础上, 提出并建立了由 CA 签发的发章证书概念, 来保证 CA 所辖域中印章文件的安全。系统通过 CA 签发的电子印章来对网络中电子公文和印章文件进行数字签名、验证, 并由加密证书保护电子公文加密密钥, 通过授权服务器管理用户打印印章权限。

关键词: 网络安全; 域; 签发中心; 注册中心; 电子印章
中图分类号: TP393.08 文献标识码: A

Design and Realization of the Secure CA-based Electronic Seal System

LIU Shi-dong[1], YANG Lin[2], HOU Bin[2], WANG Jian-xin[2]
(1. College of Communication Technology, PLA, Nanjing 210016, China; 2. The Sixty-first Academy, General Staff, Beijing 100039, China)

Abstract: To solve the distributed hierarchical network security problems, a distributed simple strictly hierarchical (DSSH) PKI trust model is presented. This model provides effective network security services such as authentication, access control, integrity, confidentiality, non-repudiation and so on. On the basis of the trust model, the concept of the issue-seal certification is presented and established to ensure the security of the seal file in the CA domain. The system implements the digital signature and verification of the electronic documents by the electronic seal. The key, which encrypts and decrypts the electronic documents, is protected by the encryption certification. Finally, the system implements the management of printing seal files abilities through the authority server.

Key words: network security; domain; Certificate Authority (CA); Register Authority (RA); electronic seal

随着计算机和网络技术的发展和广泛应用, Internet 正逐步影响着人们的生活和工作方式, 信息安全性也越来越受到人们的普遍关注, 网络攻击现象也愈加频繁。在提供分布式网络安全服务的机制中, 公开密钥基础设施(Public Key Infrastructure, PKI) 作为一种重要安全机制在近些年有很大发展, 在 PKI 提供的框架中, 各种各样的构件、应用、策略等组合起来为网络应用提供认证、访问控制、机密性、完整性、不可抵赖性服务[1]。

1 分布式简单层次信任模型

公开密钥基础设施作为利用公钥体制提供安全服务的具有通用性的支撑性基础设施, 主要是用来可靠有效地产生、发布和管理密钥与证书等安全凭证, 实现和管理不同实体之间的信任关系。PKI 作为一种符合 X.509 标准的密钥管理平台, 与传统的基于对称密钥的 KDC 相比, 可以实现密钥的私有性, 在实施认证的过程中, 无需 KDC 的参与, 可以工作在离线方式, 具有数字签名功能, 扩展性强, 在分布式网络安全应用中建立 PKI 可以实现鉴别、认证、访问控制和授权等功能[2, 3]。

在 PKI 机制中, 信任关系模型是网络上双方相互信任的基础。ITU-T X.509 标准中认为: 如果实体 A 认为实体 B 严格按照 A 所期望的那样行动, 则 A 信任 B。目前主流的信任模型主要有四种, 分别

* 收稿日期: 2002- 06- 27
基金项目: 国家部委资助项目(413150703)
作者简介: 刘世栋(1976—), 男, 博士生。

是CA 的严格层次结构、分布式信任结构、Web 模型、以用户为中心的信任[4,5]。不同的信任模型适用于不同的环境, 针对分布式层次化网络安全应用, 结合严格层次结构和分布式信任结构, 提出了分布式简化严格层次(DSSH) PKI 信任结构模型。该模型的信任体系结构如图 1 所示。

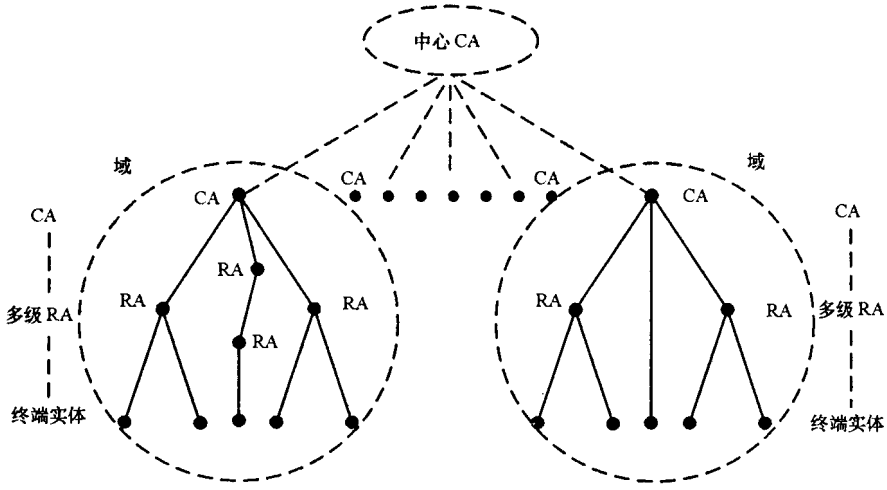

图 1 分布式简化严格层次 PKI 信任结构模型

Fig. 1 Distributed Simple Strictly Hierarchical (DSSH) PKI trust model

在 DSSH PKI 信任模型中, 根据部门或机构将不同的实体划分在不同的域中, 每个域里只有一个 CA, 称为部门 CA, 所有部门 CA 是相互独立的同位体, 进而将网络中分布式信任机构分散到多个 CA 上。而在 CA 和用户之间, 采用了简化的层次信任模型, 即部门 CA 下面没有子 CA, 但可以有一级或多级 RA。这样减少了 CA 的路径处理及其可能带来的安全问题, 并通过一级或多级 RA 注册, 分担了 CA 的部分功能, 增加了可扩展性, 并降低了 CA 的负担[5,6]。

每个部门 CA 管辖不同的域, 并具有不同证书, 在每个域中, 层次结构中所有实体都信任本域惟一的部门 CA。各 CA 域之间通过中心 CA(Bridge CA) 进行交叉认证, 中心 CA 的作用在于沟通任何一对 CA 之间的联系, 这样 n 个部门 CA 完全连接时仅需要 n 个交叉认证协议[6]。在模型中, 每个域内设有一个授权服务器, 用于异域之间授权访问。与其它信任模型相比, 该模型具有以下特点:

(1) 将不同的实体按照一定的规则划分成不同的域, 各域设置自己的部门 CA, 这样可以避免采用单一的 CA 带来的潜在威胁, 即使一个域中 CA 不可信并不影响其它 CA 的工作。

(2) 在每个域中仅有一个认证机构(CA), 而有多个 RA, 适合具有严格层次、有组织性、级别比较明确的机构, 减少了认证过程的路径处理, 各级层次 RA 的建立可以降低 CA 负担, 使 CA 运行更有效。RA 主要提供证书的注册服务, 包括接收审核用户的申请, 注册和管理用户数据, 证书存档服务, 目录服务等。

(3) 通过中心 CA 认证各域的 CA, 可以将不同的 CA 域信任联系起来, 并且减少交叉认证次数。

(4) 对于终端用户是透明的, 用户可以与本域其它用户通信, 也可以通过授权服务器授权访问其它域中的服务。

2 电子公文与电子印章安全模型及其实现机制

通过 DSSH 信任模型建立起来 PKI, 通过公钥密码体制来实现了分布式层次结构网络应用的机密性、完整性、认证和非否认服务[7]。电子印章系统是该模型基础上的一个实际安全应用系统。随着网络的发展以及网上办公的需要, 各级机构之间需要频繁传递公文文件, 特别是一些重要敏感度高的公文和印章, 更需要严格的保护。电子印章系统主要包括以下内容: (1) 电子公文完整性的验证; (2) 对发送电子公文的单位进行验证; (3) 电子公文机密性保护; (4) 完善的密码管理机制; (5) 印章文件加密存储; (6) 持有电子印章的用户可以验证印章文件的真假; (7) 只有合法用户才能阅读公文; (8) 只有经过授权

的合法用户才有权查看或打印所带的印章, 杜绝电子公文的非法流转; (9) 使用专用密码算法, 各域之间通过标准证书互连互通; (10) 支持异域用户授权。

在讨论电子公文和电子印章安全体系模型之前, 首先介绍一下在系统中定义和使用的印章文件、发章证书、加密证书、电子印章证书、用户证书以及授权、证书服务器的概念。

(1) 电子印章文件: 对应实际印章的图形文件, 其存储介质可为软盘等。

(2) 电子印章证书: 印章持有者为自己的印章所申请的证书, 由各部门 CA 签发, 电子印章证书的载体为智能 IC 卡。

(3) 加密证书: 由 CA 为发送电子公文用户产生的证书。通过加密证书加密通信中使用的对称密钥, 该对称密钥用于加密电子公文, 实现电子公文的机密性保护。

(4) 发章证书: 为了保证印章文件的安全传递的完整性, 各域 CA 均产生一个相对应的发章证书, 在印章文件下发之前, 使用该发章证书的私钥对印章文件进行签名。将签名结果作为印章文件的一部分, 同时将发章证书的公钥写入存放电子印章证书的 IC 卡中, 然后将印章文件及电子印章证书同时下发给印章使用者, 这样印章使用者即可在使用印章之前, 首先验证印章文件的真伪。为了保证对电子印章文件认证并保证其机密性、完整性, 在印章文件下发之前, 对印章文件的操作步骤如下:

(a) 对印章文件进行压缩后, 作消息摘要运算, 以防止对印章文件的篡改。

(b) 对摘要通过发章证书的 IC 卡进行数字签名, 防止私刻公章现象的发生。

(c) 将签名结果以及通过通信密钥加密的印章文件再进行消息摘要运算, 防止在传输过程中被篡改。

(d) 将文件头信息以及以上内容写入文件, 存入软盘, 并下发印章使用者。

(5) 用户证书: 由 CA 为电子公文用户签发的证书。用户证书写入 IC 卡, 用户的信息由 RA 审核, 由 CA 进行签发, 确保用户信息的正确性和可信性。

(6) 授权服务器: 可以给印章使用者授予使用权利的服务器。印章使用者通过连接查询服务器可以获取对电子印章的使用权限。

(7) 证书服务器: 存放证书信息及其历史档案的服务器, 通常采用 LDAP 或 X.500 协议来实现。

采用 DSSH PKI 模型建立的电子公文和电子印章安全系统体系, 满足了电子印章系统的安全需求。系统安全体系模型如图 2 所示。为了描述简洁, 在该图中, 略去了注册中心、审计服务器等功能模块, 仅示意了在同一个域中电子公文及电子印章系统涉及的关键部分, 不同域之间示意图可以类推。通过建立的公开密钥基础设施, 使域中用户有本域部门 CA 签发的证书, 相互之间可以互相信任, 传递电子公文以及共享数据。使用电子印章系统, 可以通过以下 4 个步骤完成:

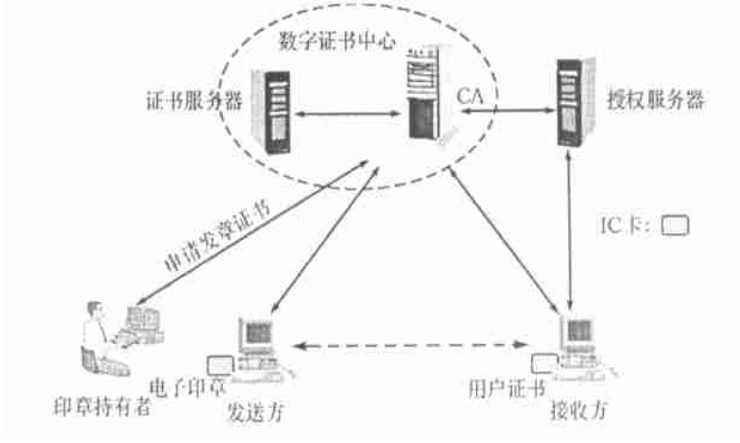

图 2 电子印章系统示意图

Fig. 2 Electronic seal system architecture

(1) 印章持有者申请电子印章。为了使用电子印章, 印章持有者必须向 CA 申请它的电子印章。

只有申请印章通过后, CA 安全管理员才能下发该持有者的电子印章并交付使用者使用。

(2) 发送电子公文及电子印章。印章使用者采用对称密钥对电子公文文件进行加密, 该对称密钥使用加密证书进行保护。利用电子印章对电子公文进行数字签名, 将签名结果、加密后的电子公文以及印章文件发送到接收方, 从而实现对电子公文的数字签名、机密性以及接收方对发送方的验证。

(3) 接收方进行验证。接收方收到发送的数据之后, 通过用户证书向发送方发送签收证明, 只有发送方收到接收方签收证明后, 利用加密证书对公文加密密钥进行加密后发送给接收者, 接收方利用加密证书的私钥恢复出公文加密密钥, 并通过用户证书验证电子公文的完整性, 从而实现对电子公文的非否认机制。

(4) 接收方获取打印权限。接收方通过连接授权服务器, 查询授权信息来获取对印章的打印权限。

图 3 给出了电子公文与电子印章流转的基本步骤, 略去了许多涉及对 IC 卡、读取证书公钥、证书服务器操作、收发双方之间的交互操作以及对会话密钥产生使用等。整个电子印章安全保密系统通过基于 PKI 体制实现了对电子公文和印章文件的机密性、完整性保护, 数字签名、非否认服务等, 并实现了通过授权服务器管理用户打印印章权限。对于印章使用者, 仅涉及在发送或接收公文时, 系统需要读取 IC 卡, 并提示用户输入 IC 卡口令。基本不改变用户现有工作流程, 具体操作步骤对印章使用户透明。

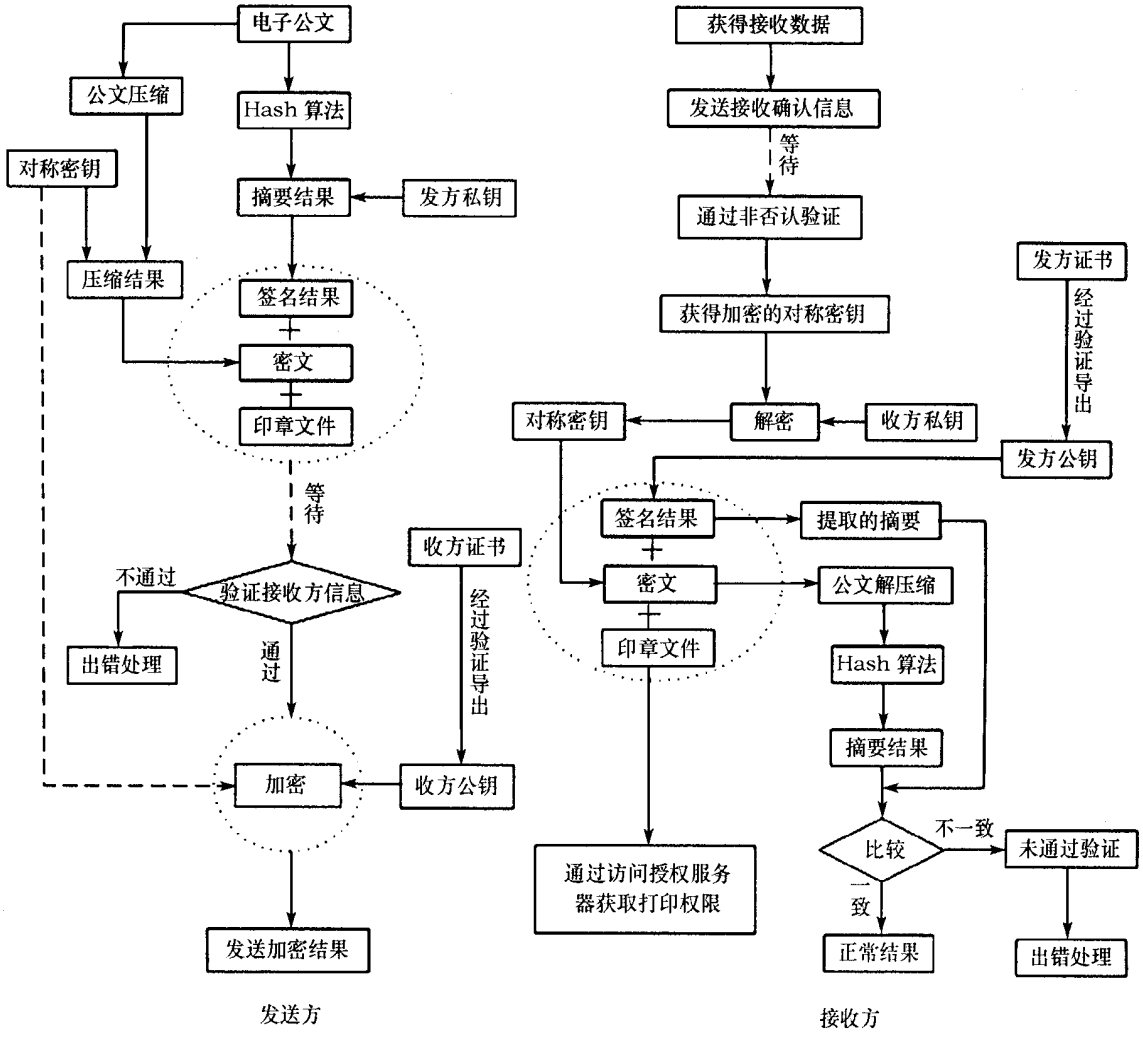

图 3 电子公文与电子印章流转步骤简要示意图

Fig. 3 Electronic documents and electronic seals transaction workflow

3 系统实现的其它考虑

电子印章系统采用PKI体制实现了分布式层次网络电子公文通信的机密性、完整性、认证和非否认服务,PKI体制主要对证书进行操作管理,使网络上相互通信的双方能够相互确认对方的身份。系统在实现时采用了更多的安全机制来保障系统的顺利运行,主要包括:

(1) 采用IC卡技术鉴别用户身份。登录系统时,需要使用者插入所对应登录的IC卡,并输入相应的IC卡口令。在制作证书以及分发密钥时,系统采用IC卡技术进行数字签名,在域中用户登录服务器或者系统时,都需要插入IC身份卡验明身份,防止未经授权的访问。另外,用IC卡存储私钥,保证私钥的安全[8]。

(2) 采用审计服务器记录对系统的操作。通过审计系统,可以了解系统签发证书情况以及在事后查看用户或安全管理员对系统的操作,防止内部人员的恶意动作。

(3) 采用PCI卡对证书进行签名,验证和生成证书,提高了签发的效率和安全性。

4 结论

通过提出的分布式简化严格层次信任模型并利用该信任模型建立的PKI体制,能提供分布式层次网络环境下的机密性、完整性、认证和非否认服务。在分析用户对电子公文和电子印章的需求前提下,在建立的公开密钥基础设施上设计和实现了电子印章系统,通过提出的电子印章框架模型,实现了对印章的完整性和使用权限的保护,保证了电子公文的完整性、机密性,通过建立授权服务器,可以对电子印章使用者进行授权,实现对电子印章的查看或者打印权限管理。电子印章系统是PKI支撑下的一个实际系统,利用PKI可以扩展实现其它多种安全服务。

参考文献:

[1] 冯登国. 计算机通信网安全[M]. 北京: 清华大学出版社, 2001.

[2] 王育民, 刘建伟. 通信网的安全——理论与技术[M]. 西安: 西安电子科技大学出版社, 1999.

[3] 陈彦学. 信息安全理论与实务[M]. 北京: 中国铁道出版社, 2001.

[4] Adams C, Lloyd S. Understanding Public-key Infrastructure: Concepts, Standards, and Deployment Considerations[M]. Macmillan Technical Publishing, 1999.

[5] Houseley R, Polk T. Planning for PKI[M]. Wiley Computer Publishing, 2000.

[6] Blaze M, Feigenbaum J, Lacy J. Decentralized Trust Management[C]. Proceedings of the IEEE Conference on Security and Privacy, May 1996.

[7] Schneier B. Applied Cryptography[M]. 2nd ed., John Wiley & Sons, Inc., 1996.

[8] Kaliski B S, Jr. An Overview of the PKCS Standards[R]. RSA Laboratories. 1993.