基于国产加密产品的 CA 安全认证系统的研究与实现

Research and Realization on CA Security Authentication System Based on National Encryption Products

兰丽娜　（北京邮电大学 网络教育学院 北京 100088）
刘辛越　杨涛海　（信息产业部电信研究院 北京 100083）

摘要：本文分析了 CA 安全认证系统功能模型，提出并阐述了 CA 系统总体架构，包括 CA 子系统和 RA 子系统。详细阐述了关键技术实现，包括应用软件功能模块结构设计，以及一种通过控制进程数来优化服务器软件性能的方法。

关键词：CA（证书授权） RA（审核授权） CRL（证书作废表） 系统架构

1　引言

CA 安全认证系统为网上的各种电子商务用户发放数字证书，最好地解决了公网上电子商务应用中公钥的分发和合法性检验问题。因此，要实现完整的安全电子商务，就必须有一个 CA 安全认证系统。而安全问题涉及国家安全，因此自主开发基于我国国产加密产品的 CA 安全认证系统具有重要意义。

2　CA 系统功能模型

CA 机构一般包括两大部门：一是审核授权部门（简称 RA，Registry Authority），它负责对证书申请者进行资格审查，并决定是否同意给该申请者发放证书，并承担因审核错误引起的、为不满足资格的证书申请者发放证书所引起的一切后果，因此它应由能够承担这些责任的机构担任。另一个是证书发放管理部门（狭义的 CA，有时也简称 CP，Certificate Processor），负责为已授权的申请者制作、发放和管理证书，并承担因操作运营错误所产生的一切后果，包括失密和为没有获得授权者发放证书等，它可以由审核授权部门自己担任，也可委托给第三方担任。

由图 1 的 CA 系统功能模型可以看出，CA 系统从功能模块来划分，大致可分为以下几部分：接收用户证书申请的证书受理者 RS、证书发放的审核部门 RA、证书发放的操作部门 CP（一般称这部分为 CA）、以及记录作废证书的证书作废表 CRL。

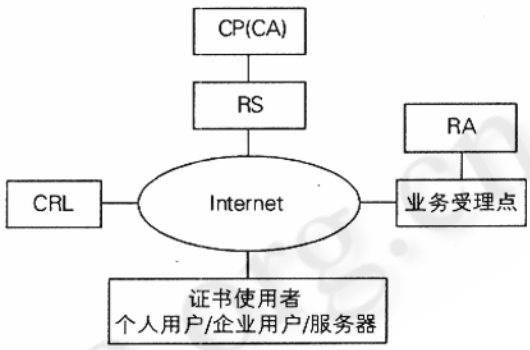

图 1　CA 系统功能模型

各部分具体功能如下：

RA：即证书发放审核部门，它负责对证书申请者进行资格审查，并决定是否同意给该申请者发放证书，因此它应由能够承担这些责任的机构担任；

CP：即证书发放的操作部门，负责为已授权的申请者制作、发放和管理证书，它可以由审核授权部门自己担任，也可委托给第三方担任；

RS：即证书受理者，它用于接收用户的证书申请请求，转发给 CP 和 RA 进行相应的处理；

CRL：即证书作废表（也称黑名单表）4 其中记录尚未过期但已声明作废的用户证书序列号，供证书使用者在认证与之通信的对方证书是否作废时查询；

业务受理点：作为 CA 系统对外提供服务的一个窗口，为用户提供面对面的证书申请和发放服务，同时

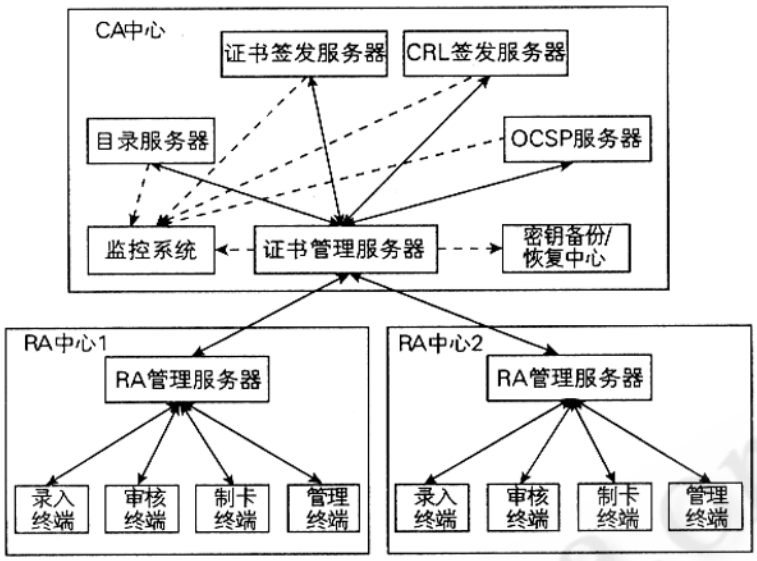

图 2　CA 系统总体架构图

业务受理点可以担任用户证书发放的审核部门，当面审核用户提交的资料，决定是否为用户发放证书。

依据 CA 系统功能模型，并考虑系统应能够尽可能满足国内各种业务的不同要求，CA 安全认证系统必须满足如下功能：

(1) 为各类用户发放数字证书，包括：个人用户，企业用户，服务器，系统管理员

(2) 证书申请、受理、审核、签发

(3) 证书作废和更新

(4) 证书信息发布

(5) 黑名单实时发布

(6) 证书管理和归档

(7) 系统管理和审计

(8) 系统运营维护管理。

3　CA 系统总体架构

CA 系统总体架构如图 2 所示。

CA 系统由一个 CA 中心子系统和多个 RA 中心子系统组成。CA 子系统与 RA 子系统之间通过 Internet 通信，采用加密通信方式。

3.1 CA 中心子系统

CA 中心子系统主要功能有：

(1) 负责证书的签发，CRL 签发，以及所辖 RA 的所有用户资料的管理；

(2) 授权设立 RA 管理中心；

(3) 处理各 RA 管理中心发来的各种业务请求；

(4) 负责维护全网的 CRL。

CA 子系统由证书管理服务器、证书签发服务器、CRL 签发服务器等服务器组成，各服务器功能如下：

CRL 签发服务器：负责接收证书管理服务器发送的 CRL 制作请求并制作 CRL，保存操作日志。

证书签发服务器：负责接收证书管理服务器发送的证书制作请求并制作证书，保存操作日志。

目录服务器：采用 LDAP 协议的证书及 CRL 发布服务器。接收证书管理服务器发送的数据更新信息，并更新数据；接收并处理客户端的使用 LDAP 协议对证书和黑名单的查询请求。

OCSP(Online Certificate Status Query Server)服务器：即在线证书状态查询服务器，接收证书管理服务器发送的数据更新信息，并更新数据；接收并处理客户端使用 OCSP 协议发送的证书作废状态实时查询请求。

证书管理服务器：负责接收各 RA 发来的业务请求并作相应的处理，是 CA 管理中心与各 RA 中心的唯一接口。同时保存各 RA 发来的用户资料，是全系统的用户资料的备份。

监控系统：接受 CA 中心主要服务器以及各 RA 服务器发来的服务器状态信息，通过表格或图表显示出来，用于对整个 CA 系统进行实时监控。

3.2 RA 中心子系统

RA 中心子系统主要功能有：

(1) 负责本地用户资料的录入、审核，以及为客户制作证书 IC 卡；

(2) 维护本地用户资料库；

(3) 与 CA 管理中心进行通讯，完成各种业务操作。

RA 子系统由 RA 管理服务器和各种终端组成，各部分具体功能如下：

RA 管理服务器：保存和维护本地用户资料库，并与 CA 中心管理服务器通讯，完成所需的各种业务功能。

管理终端：用于对 RA 系统的操作员进行管理，并

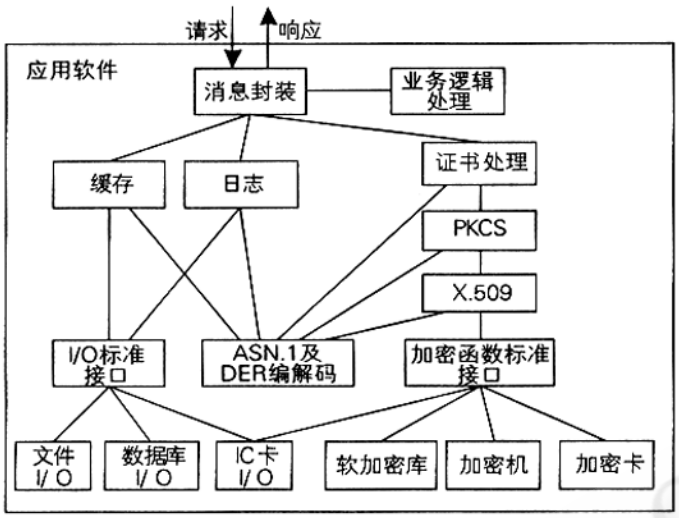

图 3　应用软件功能模块结构图

对 RA 业务数据进行查询和统计。

录入终端：用于操作员录入用户资料，具备操作员控制功能。

审核终端：用于操作员对用户申请进行审核，具备操作员控制功能。

制卡终端：用于操作员制作证书卡，具备操作员控制功能。

3.3 证书申请和发放流程

电子商务用户的数字证书申请和发放流程如下：

(1) 用户携带自己的相关证明到当地或就近的业务受理点(RA 中心)申请证书；

(2) 用户填写证书申请表格，RA 中心操作员通过录入终端录入用户数据；

(3) RA 中心通过离线方式认证用户的身份、能力和信誉等；

(4) 验证通过后，RA 中心操作员通过审核终端执行审核通过，将该用户的信息提交给 CA 中心，向 CA 中心发出用户证书申请请求；

(5) CA 中心证书管理服务器响应证书请求，通过证书签发服务器为该用户制作证书，并发布在目录服务器上；

(6) RA 中心将 CA 中心为该用户制作的证书通过制卡终端复制到 IC 卡上交给用户；

(7) 用户用申请得到的证书在中国公众多媒体通信网或 Internet 网上享受各种电子商务服务。

4 关键技术实现

4.1 开发平台选择

CA 系统中服务器选用 UNIX 主机 + 加密机，RA 中心的管理终端采用 PC 机 + Windows NT/2000/XP + 加密卡。其中加密机、加密卡采用国家密码管理委员会办公室鉴定的国产商用密码硬件加密机和加密卡。

应用软件为 C/S 架构，开发语言为 C + +，服务器端软件采用 UNIX 多进程机制实现并发访问。

数据库采用大型关系数据库系统，如 Oracle，DB2 等。

4.2 软件功能模块结构设计

CA 系统各服务器软件采用相同的功能模块结构，如图 3 所示。各功能模块说明如下：

(1) 消息封装。它负责处理各种协议规程及消息封装、解包处理。收到请求进行解包，发送响应前进行打包(消息封装)。

(2) 证书处理。为简化程序设计，优化结构，将证书处理设计为一个独立的模块，即证书处理模块，供其它模块调用。

(3) PKCS 系列处理。PKCS 系列标准(Public Key Crypto Standard，公共密钥加密标准)是被广泛接受和使用的有关密码方面的标准，PKCS 处理模块实现 CA 系统中所需要的一系列 PKCS 标准处理。

(4) X.509 封装处理。ITU－T 的 X.509 标准是 X.500 系列中的认证框架。X.509 模块实现 X.509 所定义的系列封装。

(5) 加密函数封装。用于屏蔽底层加密模块，为上层应用提供一个统一的函数调用接口，保证应用系统的相对独立性。

(6) 日志处理。负责记录各种操作记录和程序运行状态，便于审计和跟踪。

(7) 缓存处理。缓存的抽象接口，负责保存一个会话期间的数据，以及其他需要临时保存的数据。缓存处理模块可减少信息交换次数，提高运行效率。

(8) ASN.1 及 DER 编解码。此模块完成将 ASN.1 描述的数据结构转化成编程语言所表示的内部数据结构。DER 编码规则(Distinguish Encode Rule，唯一编码规则)是为了保证互通使用的。此模块完成系统所需各种数据类型的 DER 编码/解码工作。

(9) I/O 标准接口。此模块提供一个抽象的、一致的标准输入输出接口，用以屏蔽具体的输入输出操作。

(10) 业务逻辑处理。此模块实现具体业务逻辑的处理。各服务器软件中此模块功能不同，需根据业务功能需求独立开发。

4.3 服务器软件性能优化

CA 中心的 OCSP 服务器需接收并处理大量客户端使用 OCSP 协议发送的证书作废状态实时查询请求。但经测试发现，对 OCSP 服务器进行大数据量访问，经过一段时间后，OCSP 服务器没有任何响应，检查主机，发现其原因是由于该服务器产生大量的进程，将系统资源耗尽，导致系统瘫痪。

因此，需对服务器软件进行改造，设置最大进程数，增加进程数控制，防止进程过多引起资源耗尽而死机。具体方法如图 4 所示。

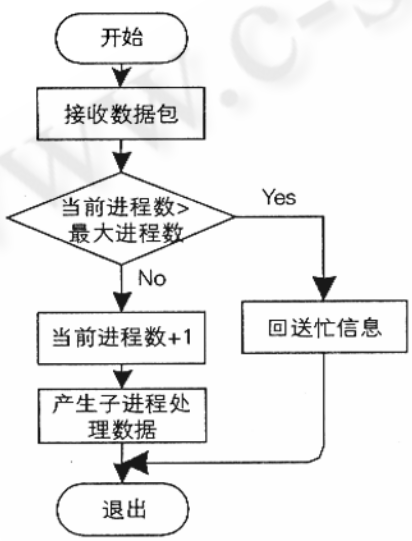

图 4　服务器主程序进程数控制流程

服务器主程序在产生子进程前首先检查目前的子进程数是否达到规定的最大进程数，如果已达到最大进程数，则拒绝该请求。否则，将当前子进程数加一，产生新的子进程，处理该数据请求。在子进程退出前，向主程序发送退出信号，主程序收到该信号后将当前子进程数减一，以便允许产生新的子进程。

最大进程数可通过配置文件进行配置。最大进程数的设置可根据系统软硬件处理能力和支持并发访问数指标等因素综合确定。

该方法适用于系统中所有的服务器软件，有效解决了因进程数过多而死机的问题，提高了系统的稳定性，优化了系统性能。

5 结束语

采用本方案开发的 CA 安全认证系统遵循国际 PKCS、PKIX 系列标准，在证书发布上采用分布式的 X.500 目录服务，符合国际标准，可以发放符合 X.509 标准的 SSL 证书、S/MIME 等格式的证书。系统通过了与 Netscape 证书、IE 证书的兼容性测试，证书能够与标准的 WWW 服务器和 Web 浏览器互通。通过了安全 Email 收发测试。

本系统已通过中国信息安全测评认证中心的严格测试和鉴定，功能齐全，性能稳定。系统已成功应用于中国电信湖南 CA 安全认证中心。

参考文献

1 PKCS #1: RSA Encryption Standard. Version 1.5.
2 PKCS #3: Agreement Standard. Version 1.4.
3 PKCS #5: Based Encryption Standard. Version 1.5.
4 PKCS #6: Certificate Syntax Standard. Version 1.5.
5 PKCS #7: Cryptographic Message Syntax Standard. Version 1.5.
6 PKCS #8: Private – Key Information Syntax Standard. Version 1.2.
7 PKCS #10: Certification Request Syntax Standard.
8 RFC 1321: The MD5 Message – Digest Algorithm. April 1992.
9 RFC 1421: Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures.
10 RFC 1422: Privacy Enhancement for Internet Electronic Mail: Part II: Certificate – Based Key Management.
11 RFC 1423: Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers.
12 RFC 1424: Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services.
13 X.208: Specification of Abstract Syntax Notation One (ASN.1).
14 X.209: Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).