维普资讯 http://www.cqvip.com



# CA系统中RA中心的设计及实现

李冬梅

（上海交通大学计算机科学与工程系　上海200030）

**摘　要**　本文就CA系统的RA系统的功能进行了介绍，详细分析了RA中心与CA中心的接口关系，软件设计上，通过运行环境、软件结构、算法说明、数据库结构、出错处理这五个方面解释了具体设计结构，本系统已在政府部门、武警部门使用，系统运行良好。

**关键词**　RA中心，CA，PHP，数字签名

## Design and Implementation of RA Center in CA

LI Dong-Mei

(Department of Computer Science & Engineering, Shanghai Jiaotong University, Shanghai 200030)

**Abstract**　This paper presents the functions of the RA center in CA, analyzes the interface relation between RA center and CA. In software design , we elaborate the material design structure through five aspects below: runing entironment, software frame, algorithm , database structure and the error handling. This system has been applied in department of government and armed police , and running stably .

**Keywords**　Register authority, Certification authority, Hypertext preprocessor, Digital signature

为了加强政府的各职能部门内的信息安全，我们利用CA系统又称为认证中心，它是负责产生、分配并管理数字证书的可信赖的第三方权威机构。通过CA系统给各个用户及设备发放证书，利用PKI可以方便地建立和维护一个可信的网络计算环境，从而使得人们在这个无法直接相互面对的环境里，能够确认彼此的身份和所交换的信息，能够安全地从事信息交换活动。可以实现无纸办公等内部业务、安全访问等。认证中心通常采用多层次的分级结构，上级认证中心负责签发和管理下级认证中心的证书，最下一级的认证中心直接面向最终用户。其中证书受理点RA(Register Authority)中心是在CA系统中完成与用户最直接的一层，是证书管理系统的一类特殊端实体，是CA的证书发放、管理的延伸，它对申请证书的用户的身份、地址等信息进行登记录入，对用户身份进行核实，代理用户向证书管理中心申请证书，并且将签发的证书写入证书存储介质，最后交给用户。RA是CA系统中的证书申请发出点和用户得到证书的终止点，是整个CA中心得以正常运行不可缺少的一部分。

## 1　CA系统总体框架

密钥管理中心(KMC)为独立运行，设在CA中心所在地。密钥管理中心负责管理根中心以下的各类密钥(通信加密密钥、CA签名密钥、密钥加密密钥、用户证书加密密钥等)。密钥管理中心与CA中心之间采用网络隔离器连接，采用非标准协议纯数据交换，确保密钥管理中心提供实时在线服务的同时，又能保证自身的安全。

CA中心直接为最终用户(个人、团体、设备等)签发支持各种应用的证书，并负责管理所签发的这些证书。负责管理RA中心的设立。其中CA中心包括实现证书发放的多种服务器模块主要有：

·RS：Register Server，注册服务器。完成证书申请的复审工作，并向证书管理服务器发送证书申请。

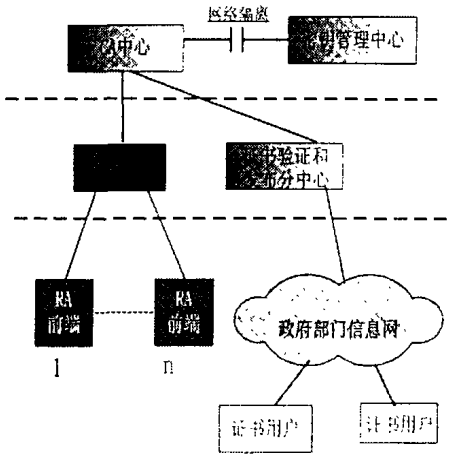


图1　CA认证系统总体构架图示

·CMS：Certificate Management Server，证书管理服务器是对所有证书的生成、作废等操作实现控制的核心，维护所有证书库、作废证书库、证书状态库、权威CA证书CRL等有关信息。

·SAS：Safety Audit Server，安全审计服务器。记录证书生成、撤销和重签过程中常规或违规的安全事件。

·MMS：Man Management Server，人员管理服务器。控制人员登录，操作证书管理界面。提供人员验证模块及各系统管理员和操作员的权限设置，限制授予各系统人员的权限。

·SS：Signature Server，证书签名服务器。接收来自证书管理服务器的申请，按规则对待签名CA证书和权威CRL进行数字签名，用签名密钥对用户的基本信息签名。

证书注册受理点(RA)根据统一的认证策略和管理规范的规定对用户提交的身份信息进行审查，以决定是否为用户发放证书，并代用户向CA中心申请签发证书，制作已签名的证书并分发。LRA为隶属于所在RA的证书申请终端，负责证书信息的录入和申请的递交。

李冬梅　工程师，主要研究方向为计算机安全。

维普资讯 http://www.cqvip.com

## 2 RA 中心与 CA 中心各服务模块的接口关系

RA 中心与 CA 中心各个模块的接口关系包括：

1. RA 与 MMS 人员验证服务模块之间完成管理员验证功能，由 RA 中心将管理员信息从管理员 IC 卡中读出，并将信息提交到 CA 中心的人员验证服务模块，由该模块验证管理员的合法性并授予该管理员权限返回应答给 RA 中心。

2. RA 与 RS 注册受理服务模块之间完成证书的申请、撤消、更新功能，由 RA 中心将用户的基本信息填好后提交给注册受理服务模块，该模块受理证书的各种请求后，符合条件发放相应的证书并通知 RA 中心，RA 中心可取得证书。

3. RA 与 OCSP 服务器之间完成证书的状态查询，由 RA 中心将需要查询状态的证书的证书序列号发给 OCSP 服务器，服务器根据证书序列号查找相应证书状态后，将证书状态(有效、无效)传回给 RA 中心。

4. RA 与 LDAP 目录服务器之间完成证书的下载，由 RA 中心填入用户基本信息后发给 LDAP 目录服务器，目录服务器根据信息查找相应证书后，将符合条件的证书传回给 RA 中心。

5. RA 与 SAS 安全审计服务模块之间完成 RA 审计事件的发送和入库处理，由 RA 中心将各类审计事件发给安全审计服务模块，安全审计服务器模块收到后根据相应的类型将审计事件入库并完成统计。

图2为接口示意图。

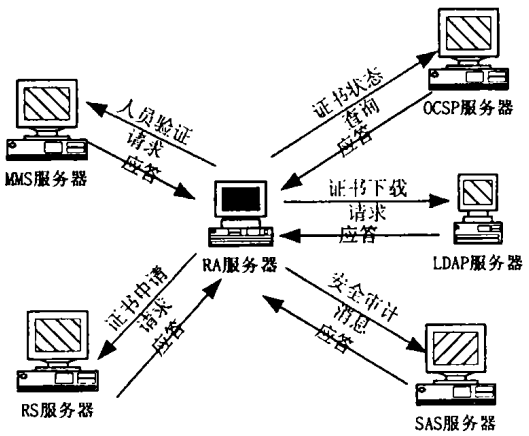


图2

## 3 RA 中心功能设计

### 3.1 录入用户信息

·调用人员验证单元
·信息写入申请表及入库
·信息从申请表提交审核表
·记录录入事件

### 3.2 审核用户信息

·调用人员验证单元
·查询待审核信息
·审核通过，密钥生成
·调用与 RS 之间的消息处理软件单元
·审核未通过，记录原因，更改合格标记
·记录审核事件

### 3.3 证书及私钥的制卡

·调用人员验证单元
·根据输入的制卡信息查询相应的审核表
·向 RS 申请下载用户证书，调用 RA 与 RS 之间的消息处理软件单元，对加密证书还必须从密钥管理中心下载相应的用户密钥
·验证用户 IC 卡口令，并将证书和相应的用户密钥写入用户 IC 卡
·制卡信息记入制卡信息表
·记录制卡事件

### 3.4 管理员身份验证

·调用人员验证服务器模块提供的公共验证单元，验证管理员身份，取得对相应网页的操作权限

本系统采用数字签名技术进行身份认证，在服务器前端的代理服务器完成对管理员身份验证的工作。一个基本的签名及验证过程如图3所示。

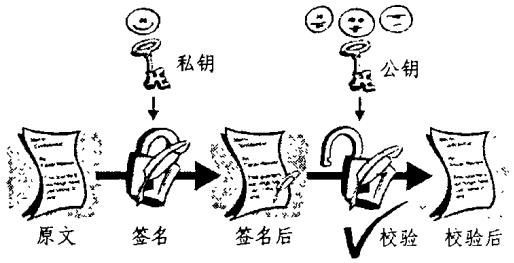


图3

RA 客户端与 MMS 服务模块之间是通过如下的操作来完成身份认证的工作的。RA 客户端向 MMS 服务模块发送申请时，首先使用 Hash 函数对要签名的信息进行摘要处理，然后用自己的签名私钥对 Hash 运算得出的摘要数据进行签名；MMS 服务模块收到客户端的签名消息后，根据管理员的基本信息从 CA 中心下载管理员的证书，并向 OCSP 验证其证书的有效性，再使用证书中的公钥对签名消息进行解密，得到解密后的 Hash 运算结果。此时，MMS 服务模块只需要计算出该消息的 Hash 运算结果并与解密得到的 Hash 值进行比较，如果相同，就可以确认管理员的身份和权限，否则将拒绝管理员的操作。

### 3.5 与上层各服务模块之间的消息处理

·构造 PKI 消息
·生成数字信封
·发送消息
·接收消息
·处理应答消息

### 3.6 审计事件记录和发送

·记录审计事件如：录入事件、审核事件、制卡事件
·将 RA 端的审计事件通过审计事件记录客户端模块发送给安全审计服务模块。
·发送审计事件

## 4 RA 中心软件设计

### 4.1 软件运行环境要求

操作系统：Redhat Linux7.3
数据库系统：Sybase ASE12.5 for Linux
Web 服务：Apache3.9 for Linux

### 4.2 软件结构说明

在 RA 系统中，系统服务器主要采用 Web 服务器-功能服务器-数据库服务器的三层次结构，在此基础上增强了密码处理功能。服务器平台采用增加安全功能的 Linux 操作系统，ApacheWeb 服务器和 Sybase 数据库。Web 服务软件采用

维普资讯 http://www.cqvip.com

PHP 语言和 CGI 技术实现，为用户提供功能强、操作方便的使用界面。RA 系统与 CA 内部各服务模块之间采用安全加密封装协议进行消息通信，同步各服务模块之间的业务处理流程。RA 中心的各项功能操作管理均采用 Web 方式，内部用户操作通过 IE 浏览器进行，客户端与服务器间传输的信息采用本地控件进行加密签名。因此由 RA 前端(RA Client)向 RA 服务器提交申请、撤消、更新证书的请求，RA 服务器接收请求后自动进行身份审核，也可以等待操作员进行人工审核，将审核通过的请求提交给 CA 进行处理，将处理结果返回给 RA 前端。

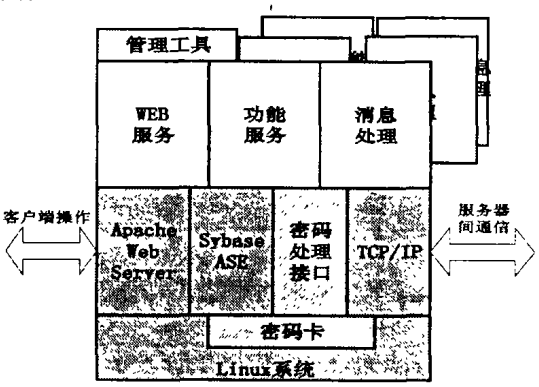


图4

### 4.3 算法种类说明

·RSA 算法：用于非对称密钥的加密、签名运算。数字签名、密钥加密等使用该算法。非对称密钥的加、解密运算是指用数字证书中绑定的密钥对完成数据的加、解密运算。包括四个函数：公钥加密、公钥解密、私钥加密、私钥解密。在一般情况下，私钥的加密运算和对应公钥的解密运算提供数字签名/验证，保证信息的完整性；公钥的加密运算和私钥的解密运算用于提供数据加密，主要指密钥加密，如制作数字信封。

·专用密码算法：对称密钥加/解密算法，用于数据内容的加密和制作数字信封时，利用该算法实现。

·MD5摘要算法

函数原形：unsigned char * MD5

(unsigned char * data,

unsigned long datalen,

unsigned char * md);

参数描述：data：需要摘要的原始信息(输入)、datalen：data 数据的长度值(输入)

md：摘要信息输出串(输出)

返回值：0：表示摘要生成成功；其它：操作失败。

说明：该函数根据输入参数提供的原始信息，生成16字节 MD5消息摘要。

·SHA1算法

函数原形：unsigned char * SHA

(unsigned char * data,

unsigned long datalen,

unsigned char * sha);

参数描述：data：需要摘要的原始信息(信息串的 DER 编码)(输入)；

datalen：data 数据的长度值(输入)；

sha：摘要信息输出串(输出)

返回值：

0：表示摘要生成成功；其它：操作失败。

说明：该函数根据输入参数提供的原始信息，生成 SHA-1消息摘要。

### 4.5 数据库结构

该库含有四种类型的表，该库的名称为：RA_DB。共有如下几类表：

第一类表申请表：该表存放用户申请的基本信息

申请表：个人证书 manaly 设备证书 eqaly

撤消表：个人证书 mancal 设备证书 eqcal

更新表：个人证书 manresign 设备证书 eqresign

第二类表审核通过表：该表存放审核通过后的各类型信息，如审核员信息、审核时间等。

审核表：个人证书 ManNopass 设备证书 EqNopass

第三类表审核不合格表：该表存放审核不通过的各类型信息，如不合格原因等。

审核不合格表：个人证书 ManNopass

设备证书 EqNopass

第四类表：制卡表：该表存放制卡后的信息，如制卡员工号、卡号、制卡时间等。

制卡信息表：write_IC_info

### 4.6 出错处理

可能出现的错误情况及解决措施如下：

·网络不通：检查网线、网络设备，在尽可能不断电的情况下排除故障。如果不能排除故障，则断电重起或更换设备。

·数据库错误：先查看系统/opt/sybsase-12.5/ASE/install/目录下的日志文件，根据日志文件检查数据库运行情况，排除故障。如果数据库日志和数据需要备份可进入 master 数据库将数据备份完毕后，数据库运行即可正常。如果数据库遭到破坏，恢复数据库，如果数据库软件崩溃，停止服务软件，重装数据库软件。

·IC 卡读写错误：检查 IC 卡设备，如果是 IC 卡没插好或者 IC 卡损坏，重插 IC 卡或更换 IC 卡，如果是 IC 卡读写设备或连线问题，则更换设备。

·系统硬件平台故障：测试加密卡、加密机，测试错误，可停止服务后重起服务，还无法正常，可更换设备，重新开机运行软件。

·服务程序出错：查看系统/usr/ca/ra.log 日志文件，重启服务程序。

**结束语** RA 中心是整个 CA 认证系统中证书生成的起始点和终止点，系统的友善性在 RA 中心表现突出，因此 RA 中心的界面必须操作简便、使用容易、稳定性好，使用户的操作快捷、方便。而且 RA 中心是 CA 系统外围的核心部门，它与 CA 中心的接口比较多，所以系统必须设计可靠，能很好地满足用户的需求，还必须有一定的安全保障。该 RA 系统已在政府、武警内部实施过，运行良好。

## 参 考 文 献

1 [美]Nash A，等. 公钥基础设施(PKI)实现和管理电子安全. 北京：清华大学出版社，2002

2 ITU-T (former CCITT) Recommendation X.509 (1988), The Directory - Authentication Framework

3 Worden D J(美). Sybase 开发者指南. 清华大学出版社