CA认证中心的系统设计与实现

国防科技大学计算机学院 韩伟红 贾焰 王志英

摘要：电子商务的安全是通过在网络上使用加密手段来达到的，目前最常用的加密方法是非对称加密算法，CA机构就是用来解决非对称加密算法中公钥的合法性检验问题。我们设计CA认证中心系统的目的是在中国公众多媒体通信网上建立覆盖全国的基于CA体系的安全基础结构，为用户上网使用创造安全环境，为电子商务的应用创造安全环境。

关键词：CA（Certificate Authority）证书认证中心 RA（Registry Authority）审核机构 CP（ertificate Processor）证书操作部门 RS（Registry Server）证书授理服务器

概述

随着网络技术的迅猛发展和国内网络的日趋完善，在网上开展的各种业务活动正如雨后春笋般蓬勃地发展起来。从广义上来看，其中的很多业务都可以归入电子商务的业务范畴。因此如何更好地保证网上电子商务业务的顺利开展是一个不容忽视的问题。

电子商务的安全是通过在网络上使用加密手段来达到的。在使用加密技术时，密钥分配是密钥管理中最大的问题。传统的对称密钥加密算法的密钥必须通过安全的通路进行分配，但随着用户的增多和通信量的增大，特别是在Internet这样的环境下，为了在任意两个地理上可能相距遥远的广域网用户之间建立彼此信任的保密通信几乎是不可能的。非对称加密算法的出现，为密钥管理带来了新的解决途径。

在非对称加密算法的使用中，每个用户都有一对密钥，一把自己保存，称为私人密钥（或秘密密钥），一把对外公布，称为公开密钥。因此，这种体系也称为公钥体系。这两把密钥互为加解密：用一把密钥加密的内容，必须用另一把密钥解码。在这种体系中，必须有一个查找其他人的公开密钥和公布自己的公开密钥的途径。然而，在开放的网络环境中，如何鉴别公钥的真实性成为公钥体系所要解决的主要问题，否则攻击者就能篡改他人的公开密钥导致保密通信机制的崩溃。

CA机构就是用来解决公钥体系中公钥的合法性检验问题。CA机构，又称为证书授权(Certificate Authority)中心。证书授权中心为每个申请公开密钥的用户发放一个证书，该证书证明了该用户拥有证书中列出的公开密钥。证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。CA的数字签名使得攻击者不能伪造和篡改证书，证书的作用是向接收者证实某人或某个机构对公开密钥的拥有。

证书包含一个公开密钥、名称以及证书授权中心的数字签名。证书中还包括密钥的过期时间，发证机关(证书授权中心)的名称，该证书的序列号等信息，证书的格式遵循X.509国际标准。

CA机构的设置包括两大部门：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。另一个是证书操作部门（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。

我们设计CA认证中心系统的目的是在中国公众多

媒体通信网上建立覆盖全国的基于CA体系的安全基础结构，并与各行业合作在网上构造安全的业务应用系统，为用户上网使用创造安全环境，为电子商务的应用创造安全环境。

CA系统的实现有两种模式：一种是由用户在自己的机器上产生密钥对，另一种是由“可信的第三方”，即CA机构为客户产生密钥对。前一种方式由于用户自己产生密钥对，在申请证书时只传递公钥，因此私钥的安全性要高。但这种方式往往会与国家安全产生冲突（如政府需要监听犯罪集团的通信时需要取得其密钥），会给实施带来困难。后一种方式由于密钥对由第三方生成，一旦政府实施密钥管理法，它能较好地适应。因此，后一种方式具有更强的可实施性。目前，国际国内的CA系统主要是采用第二种方式，因此我们进行CA认证中心的系统设计时也采用了第二种方式。

系统结构

CA认证中心的系统结构如图1所示，整个系统由两个部分组成：一是CA认证中心；二是CA业务受理点。

1.CA认证中心

CA中心负责制作证书、签发证书作废表、审核高级别的证书申请、管理和维护中心CA系统。

CA中心主要由证书管理服务器（以及其备份服务器）、证书签名服务器、作废证书签发服务器、作废证书查询服务器、高级别的证书审核处理机、加密服务器、防火墙以及业务管理服务器组成。

·证书签名服务器：负责证书的制作，并维护本地日志记录

·作废证书签发服务器：负责证书作废表的签发

·证书管理服务器：负责接收各业务受理点上传的各种请求（证书申请、挂失和下载）；向证书签名服务器转发证书签名请求；向证书签名服务器发送作废证书签名请求；向作废证书查询服务器发送作废证书更新消息。

·证书管理备份服务器：负责系统的备份，保证CA关键部分运行可靠。

·作废证书查询服务器：负责处理各种证书状态查询服务。

·证书审核处理机：主要用于处理高级别的证书请求审核。

·加密服务器：负责CA认证中心的加密、解密、签名以及根证书密钥的存放。

·防火墙：负责隔离CA认证中心网络与公网的连接，保证CA中心网络的安全。

·业务管理服务器：实现CA管理系统与业务系统的衔接，主要体现用户利用证书所能使用业务的权限，此服务器由业务系统自行管理，CA中心集中维护。

2.CA业务受理点

CA业务受理点由录入终端、审核终端、证书发行终端和证书受理服务器组成。

·录入终端：用来录入客户证书申请、挂失资料。由IC卡完成操作员身份鉴别。

·审核终端：用来对客户提供的资料进行审核和证书制作授权，并完成本受理点的数据管理和维护功能。由IC卡完成操作员身份鉴别。

·证书发行终端：用来将客户的私人密钥和证书灌入IC卡或磁盘，发放给客户。由IC卡完成操作员身份鉴别。

·证书受理服务器：负责密钥的生成、与CA中心证书处理服务器的保密通信。

高级别的证书申请由受理点来受理，审核由CA认证中心来完成，受理点检测CA中心反馈的情况，并生成证书。受理点也采用防火墙，保证CA业务受理服务器的安全。另外，所有系统软件的使用都使用IC卡证书认证的方式。

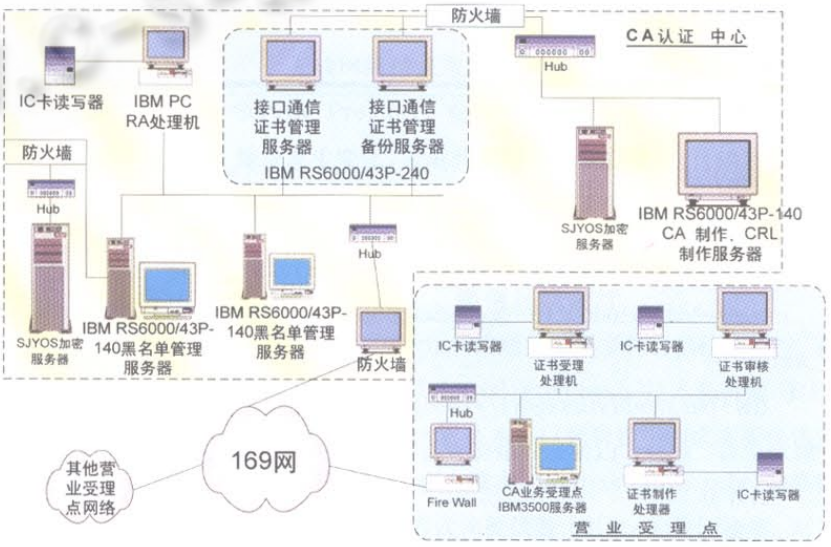

图1 CA认证中心体系结构

系统功能与特点

我们设计和实现的这个CA认证中心主要具有如下功能：证书管理功能；黑名单管理功能；用户OCSP证书状态查询服务管理功能；业务受理点证书管理功能；能够接收个人、企业和服务器的证书请求；验证申请者身份的功能；处理和管理本地证书功能；提供查询证书办理的状态功能；暂缓、认可、拒绝证书授权的功能；对本地证书办理的审计跟踪功能；密钥管理、用户密钥恢复管理功能；系统远程管理，业务统计管理功能；系统维护，IC卡制作管理功能。

本系统主要有以下几个特点：

1. 采用国家密码管理委员会认可的加密设备和加密算法

目前，国内的很多加密产品都在使用国外的加密产品或自己研制的、未经国家密码管理委员会认可的加密产品，虽然政府还没有执行严格的密码管理法规，但是，一旦政府从国家安全考虑，执行严格的密码管理法规，就需要改造、更新、甚至替换现有系统，这样会带来很多不便，甚至会影响已有的业务系统。现在就采用国家密码管理委员会认可的加密设备和加密算法，避免了日后可能出现的麻烦。

2. 具有独立的RA功能

传统的CA软件系统中，RA往往作为CA的一部分，而不单独作为一个独立的软件。这样审核授权与证书制作需要同一机构担任，不便于实际使用。将RA独立，有助于将审核授权与证书制作管理指派给不同机构处理，能较好地适应各种不同的需求。

3. 采用OCSP作为作废证书查询系统，具有更高的实时性。

传统的作废证书查询方式采用CA机构签发作废证书查询表的方式，由于作废证书表的签发只可能定期更新，无法满足对实时性要求较高的应用（考虑实际可行性，作废证书表最快为一天签发一次）。而OCSP（在线证书状态查询协议）能够实时反映作废证书状态，而且由于数据包内容较少，也不会给网络带来负担。

4. 对所有操作员都有身份鉴别机制

为防止非授权用户操作CA系统，在每一个操作终端上都有操作员身份鉴别系统，只有授权的用户才可以通过IC卡在CA终端上操作。

5. 对所有操作都有日志记录。对操作员的每次操作都有日志记录，可用于跟踪、审计。

6. 支持X.509(V3)标准

7. 系统密钥均放在加密机和加密卡中，安全强度高，不易泄露，即使系统被破坏，也不会泄露密钥。

8. 根证书的生成需要三个人同时使用自己身份IC卡，从而保证系统根证书操作的安全强度。■

参考文献

1 IETF SET V1.0 (1997.5) 安全电子交易 Secure Electronic Transaction

2 IETF SSL V1.1 (1996.1) 安全套接层 Secure Socket Layer

3 ITU-T X.509 (1993.11) 关于认证框架的介绍 Information technology-open systems Interconnection the directory: authentication framework