全国组织机构代码CA认证实用教程

全国组织机构代码管理中心　编

中国标准出版社

全国组织机构代码CA认证实用教程

[redacted]

全国组织机构代码CA认证实用教程

全国组织机构代码管理中心　编

主　编　顾迎建　殷文波　柯志勇　王旻

编著者　孙　镇　张建民　王傲巍

中国标准出版社

内 容 提 要

本教程从介绍PKI/CA的基本概念入手，系统地介绍了电子商务与PKI/CA的标准、PKI/CA的应用、组织机构代码CA设计与建设、组织机构代码CA的安全管理规范以及国家有关CA的一些法律、法规等方面的内容。该教程理论与实践相结合，由浅入深，通俗易懂，实用性强，是广大组织机构代码管理人员、技术人员学习和了解组织机构代码CA知识较为全面的读物。

本教程可供从事组织机构代码CA技术研究和应用的有关人员阅读。

图书在版编目(CIP)数据

全国组织机构代码CA认证实用教程/全国组织机构代码管理中心编. —北京：中国标准出版社，2006
ISBN 7-5066-4129-1

Ⅰ. 全… Ⅱ. 全… Ⅲ. 组织机构-代码-CA认证-教材 Ⅳ. F208-39

中国版本图书馆CIP数据核字(2006)第045876号

中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码：100045
网址 www.spc.net.cn
电话：68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 787×1092 1/16 印张 12 字数 270千字
2006年9月第一版 2006年9月第一次印刷
*
定价 **24.00** 元

前　言

随着信息技术的不断发展和Internet互联网应用的普及，网络安全、信息安全问题日益突出。网络安全隐患随时存在，诸如重要的数据、文件资料等在传输过程中容易被篡改或泄密，假冒或抵赖等网络欺诈行为时有发生。特别是随着电子政务、电子商务的逐步开展，网络安全、授权访问（包括身份识别）、加密传输等显得尤为重要和迫切。基于PKI（公钥基础设施）的CA认证系统是顺应这种网络安全的需要，为电子政务、电子商务的开展提供安全保障措施的基础设施之一。

安全认证，是指一个具有权威性、公正性、惟一性的机构，利用密码技术，向参与电子政务、电子商务和其他网上业务的各个主体颁发符合国内、国际安全协议标准的电子安全数字证书，并对其真实身份进行验证，对数据进行加密，以保障主体之间在网上传递信息的安全性、真实性、可靠性、完整性和不可抵赖性。

随着我国的电子政务、电子商务活动的不断增多，许多电子商务活动已经受到了安全问题的困扰，特别是在金融领域，网上业务没有安全认证作为安全的屏障，受到了很大威胁，严重地制约了电子商务活动安全有效地进行。为了改变这种状况，一方面是采取必要的法律手段，加大打击网上犯罪的力度；而更为重要的另一方面是，必须要采用更加先进的、可靠的、具有自主知识产权的高技术手段来应对这种挑战，CA认证技术正是适应这一形势发展的需要、有效解决这一问题的最佳途径。

我国的组织机构代码作为惟一标识企业、事业单位、机关、社会团体和其他合法组织机构的标准代码，在国民经济建设和社会发展中正在发挥着巨大的作用。目前组织机构代码已在银行、税

务、海关、外汇、商贸、统计、工商、人事、社保、公安、国有资产、财政、质检等十多个领域和部门得到了广泛应用，成为现实生活中标识社会组织经济活动主体的身份识别码，具有极高的社会认知度和权威性。组织机构代码的统一性、惟一性和终身不变性的特点，决定了以组织机构代码作为主体惟一标识的组织机构代码数字证书可以作为互联网上的企业和政府部门进行身份识别、授权管理和实现数据安全传输的重要手段。

以全国组织机构代码管理中心为核心、覆盖全国2600多个县以上地区的庞大的组织机构代码管理体系，已具备了开展CA认证工作的良好基础条件和综合优势。

本教程系统地介绍了PKI/CA技术的基本概念、PKI/CA的技术标准、PKI/CA在电子商务中的应用、组织机构代码CA的概念、代码CA认证系统的设计、代码CA安全认证管理规范、代码CA认证的责任、代码CA机房设计、代码数字证书的应用和PKI/CA的法律、法规等内容，对于初次接触PKI/CA技术和希望了解组织机构代码CA认证工作的有关人员将会有所帮助。

本教程适合于全国从事代码CA技术推广与应用的技术人员阅读，也适合于社会其他应用代码信息的各类单位和个人使用，特别是对希望了解代码CA建设与发展现状，并积极应用组织机构代码数字证书的个人和单位来说，会有一定的借鉴作用。由于编著者水平有限，在本教程中难免出现纰漏和问题，望广大读者不吝赐教。

编　　者

2006年5月

目　录

第 1 章

PKI/CA 的基本概述

1.1 PKI/CA 技术及其发展概述

随着信息技术的不断发展和 Internet 互联网应用的普及，网络安全、信息安全问题日益突出。网络安全隐患随时存在，诸如重要的数据、文件资料等在传输过程中容易被篡改或泄密，假冒或抵赖等网络欺诈行为也时有发生。随着电子政务、电子商务的不断开展，网络安全、授权访问（包括身份识别）、加密传输等问题就显得尤为重要和迫切。

为解决 Internet 的安全问题，世界各国对其进行了多年的研究，初步形成了一套完整的 Internet 安全解决方案，即目前被国际上广泛采用的公钥基础设施（PKI）。PKI 是“Public Key Infrastructure”的缩写。PKI 技术是利用公开密钥理论和技术建立的提供信息安全服务的基础设施。公钥体制是目前应用最广泛的一种加密体制，在这一体制中，加密密钥与解密密钥各不相同，发送信息的人利用接收者的公钥发送加密信息，接收者再利用自己专有的私钥进行解密。这种方式既保证了信息的机密性，又能保证信息具有不可抵赖性。目前，公钥体制广泛地用于 CA 认证、数字签名和密钥交换等领域。

PKI 几乎可以解决绝大多数网络安全问题，它是基于公开密钥理论和技术建立起来的安全体系，是提供信息安全服务的具有普适性的安全基础设施。该体系在统一的安全认证标准和规范的基础上提供在线身份认证，是 CA 认证、数字证书、数字签名以及相关安全应用组件模块的集合。作为一种技术体系，PKI 可以作为支持认证、完整性、机密性和不可否认性的技术基础，从技术上解决网上身份认证、信息完整性和不可抵赖等安全问题，为网络应用提供可靠的安全保障。但 PKI 绝不仅仅涉及到技术层面的问题，还涉及到电子政务、电子商务以及国家信息化的整体发展战略等多个层面的问题。PKI 作为国家信息化的基础设施，是相关技术、应用、组织、规范和法律法规的总和，是一个宏观体系，其本身就体现了强大的国家实力。PKI 的核心是要解决信息网络空间中的信任问题，确定信息网络空间中各种经济、军事和管理行为主体（包括组织和个人）身份的惟一性、真实性和合法性，保护信息网络空间中各种主体的安全利益。

PKI 是 20 世纪 80 年代由美国学者提出来的概念，实际上，授权管理基础设施、可信时间戳服务系统、安全保密管理系统、统一的安全电子政务平台等的构筑都离不开它的支持。数字证书认证中心 CA（Certificate Authority）、审核注册中心 RA（Registration Authority）、密钥管理中心 KMC（Key Management Center）都是组成 PKI 的关键组件。作为提供信息安全服务的公共基础设施，PKI 是目前公认的保障网络社会安全的最佳体系。

1.2 PKI 在中国的发展

目前，我国的电子政务、电子商务活动正在以前所未有的规模不断增加，许多电子商务活动已经开始受到了安全认证问题的困扰，特别是在金融领域，网上业务没有 PKI 作为安全的屏障，受到了很大威胁，严重地制约了电子商务活动的有效进行，网上盗窃用户密码的非法活动尤为猖獗，对正常社会经济生活造成了严重危害。对于这种情况，既要采取必要的法律手段，加强对违法行为的打击力度，同时要积极采用更加先进的、可靠的、具有自主知识产权的新技术手段来应对这种挑战，PKI 技术正是适应这样的条件，应运而生的有效技术手段。

自 1998 年中国出现第一家 CA 认证中心 CTCA(中国电信 CA 认证中心)以来，标志着 PKI 技术正式开始应用到我国的电子商务领域。据不完全统计，全国已经有超过 100 家 CA 中心存在。现有 CA 中心主要为行业性 CA 和地方区域性 CA，并已开始在电子商务和面向公众服务的电子政务应用中发挥作用。我国 PKI 体系的研究与建设有了良好的开端，具备了一定的技术基础。PKI/CA 建设已经成为信息安全产业的亮点。

我国的 PKI/CA 中心大体上可分为三类：一是以中国金融 CA、中国电信 CA、中国海关 CA 等为代表的行业 CA；二是以地方政府与公司共建为主的区域性 CA，如北京 CA、上海 CA、陕西 CA、天津 CA、广东 CA、西部 CA 等；三是一些完全商业化的 CA，如天威诚信 CA、颐信科技 CA、国投安信 CA 等。

比较早建立的 CA 认证机构主要有：

中国金融认证中心(CFCA)，2000 年 10 月开始运行，是一个由十三家银行参与建设和运行的 CA 认证体系，主要市场是企业与银行间的资金转帐和往来服务业务。

中国电信认证中心(CTCA)，1999 年 6 月开始运行，是一个全部由中国电信集团建设和运行的 CA 认证体系，主要市场是企业与个人的电子商务应用。

海关认证中心(SCCA)，是一个由国家海关总署建设和运行的 CA 认证体系，主要市场是报送企业的电子报关业务应用。

地方政府建立的 CA 认证机构主要有：

南方认证中心(NFCA)，1999 年 6 月开始运行，是一个由广东电信数据局建设和运行的 CA 认证体系，主要市场是企业和个人的电子商务应用。

上海认证中心(SHECA)，是一个由上海电信数据局等部门建设和运行的 CA 认证体系，主要市场是政府、企业、个人的电子商务应用。

另外，近几年又陆续出现了一批区域性的 CA，如浙江 CA、重庆 CA、陕西 CA、山东 CA、福建 CA、广东 CA、江苏 CA、新疆 CA、湖北 CA、辽宁 CA 等。

行业性的 CA 多集中于自身的行业应用，而区域性的 CA 则以地方的电子政务应用为主。从整个应用情况看，目前整个市场还是处于起步阶段，虽然有数字表明，CA 数字证书发放总量已超过 500 万张，但真正的应用还没有形成规模，CA 还有很大的发展空间。

由于 Internet 普及程度，商家对电子商务的认知程度，银行、税务、社保等金融部门的配合力度等方面的限制，使得我国的 CA 认证市场到目前为止仍处于市场培育时期，具体体现

为签发证书数量少、证书使用场合少等情况。

1.3 PKI的市场前景

由于PKI体系结构是目前比较成熟、完善的Internet网络安全解决方案，国外的一些大的网络安全公司纷纷推出一系列的基于PKI的网络安全产品，如美国的Verisign、IBM、Entrust等安全产品供应商为用户提供了一系列的客户端和服务器端的安全产品，不仅为电子商务的发展提供了安全保证而且为电子商务、政府办公网、EDI等提供了完整的网络安全解决方案。

美国在2000年就有了《全球及全国商业电子签名法》。作为美国历史上第一部联邦级的电子签名法，它意味着网上炒股、网上签约、政府网上采购等大宗交易都可以通过电子签名来完成，而不再需要传统的纸笔签名。德国、日本、新加坡和韩国等国家也已经相继通过电子签名法。随着Internet应用的不断普及和深入，政府部门将利用PKI来支持管理；商业企业内部、企业与企业之间、区域性服务网络、电子商务网站将使用PKI的技术和解决方案。在不久的将来，政府以及大企业将会建立自己的PKI平台，而中小企业以及个人则会需要社会提供的商业性PKI服务，可见PKI的市场需求是非常巨大的。

中国作为目前全球最大的市场和产品、服务提供地，无疑为PKI市场的发展提供了更大的想象空间，目前通过国内网络市场近几年的快速发展就足以说明。2004年10月中华人民共和国人大常委会通过了《中华人民共和国电子签名法》，进一步为PKI在中国的规范发展提供了法律依据，新一轮的PKI建设和应用高潮即将到来。

1.4 PKI的基本知识和构架

1.4.1 什么是PKI

PKI(Public Key Intrastructure)即“公开密钥体系”，是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，简单来说，PKI就是利用公钥理论和技术建立的提供安全服务的基础设施。PKI技术是信息安全技术的核心，也是电子商务的关键和基础技术。

PKI的基础技术包括加密、数字签名、数据完整性机制、数字信封、双重数字签名等。

1.4.2 如何构建PKI

构建PKI必须建立起如下系统：典型的PKI系统由五个基本的部分组成：证书申请者(Subscriber)、注册机构(Registration Authority，RA)、认证中心(Certificate Authority，CA)、证书库(Certificate Repository，CR)和证书信任方(Relying Party)。其中，认证中心、注册机构和证书库三部分是PKI的核心，证书申请者和证书信任方则是利用PKI进行网上交易的参与者。在具体应用中，各部分的功能是有弹性的，有些功能并不在所有的应用中出现，PKI的许多详细功能要根据业务的操作规程确定。

1.4.3　PKI 的功能

一个完整的 PKI 产品应具备以下功能：根据 X.509 标准发放证书，产生密钥对，密钥备份及恢复，证书密钥对的自动更换，加密密钥和签名密钥的分隔，管理密钥和证书，支持对数字签名的不可抵赖性，密钥历史的管理，为用户提供 PKI 服务——如用户安全登录、增加和删除用户、恢复密钥、检验证书等。其他相关功能还包括交叉认证、支持 LDAP(轻量目录访问)协议、支持用于认证的智能卡等。此外，PKI 的特性融入各种应用(如防火墙、浏览器、电子邮件、群件、网络操作系统)也正在成为趋势。

1.4.4　PKI 的性能

PKI 的性能要求可扩展性能满足电子商务不断发展的需要，方便用户，保证其安全和经济性，支持远程参与者的通信通行无阻，因此必须具有以下性能。

1.4.4.1　支持多政策

用户可能信赖某个认证机构 CA，但未必信赖另一个 CA。因此，应允许不同用户接受不同 CA 的政策。

1.4.4.2　透明性和易用性

作为网络环境的一种安全基础设施，PKI 必须具有良好的透明性和易用性，这是对 PKI 的最基本要求，PKI 必须尽可能地向上层应用屏蔽密码服务的实现细节，向用户提供屏蔽复杂的安全解决方案，使密码服务对用户而言简单易用，同时便于单位、企业完全控制其信息资源。

1.4.4.3　互操作性

PKI 互操作性是电子商务通信的关键，建立对 Internet 交易保密性的信任，是电子商务发展所面临的最重要以及最具挑战性的问题之一。

PKI 是在 Internet 上建立信任的一种技术选择，但是，部署 PKI 并不容易。保证多厂商 PKI 环境的互操作性是在电子商务交易中建立信任的关键。不同企、事业单位的 PKI 实现可能是不同的，这就提出了互操作性要求。要保证 PKI 的互操作性，必须将 PKI 建立在标准之上，这些标准包括加密标准、数字签名标准、HASH 标准、密钥管理标准、证书格式、目录标准、文件信封格式、安全会话格式、安全应用程序接口规范等。

1.4.5　简单的风险管理

任何基础设施都需对所面临的风险有全面的了解，并适于在参与者之间进行分配。

1.4.6　支持多平台

PKI 是遵循一系列标准的，它必须适合于不同的开发环境和不同的开发平台，例如 Windows、UNIX、MAC 等。

1.4.7 支持多应用

PKI应该面向广泛的网络应用，提供文件传送安全、文件存储安全、电子邮件安全、电子表单安全、Web应用安全等保护。

1.4.8 数字证书和PKI解决的问题

互联网(Internet)电子商务系统必须保证具有十分可靠的安全保密技术，也就是说，必须保证网络安全的四大要素，即信息传输的保密性、数据交换的完整性、发送信息的不可否认性、交易者身份的确定性。而利用数字证书恰好能够解决这些问题，就像通行证一样时刻伴随着电子商务的整个过程。数字证书和PKI结合可以解决电子商务中的安全问题。在传统的安全解决方案中，密码服务与应用紧密地结合在一起，每一种网络应用都有自己的一套密钥管理，功能大量冗余，管理维护工作复杂，费用高，而且这种分散的、插件式的安全解决方案存在安全隐患，互操作性也得不到保证；而PKI以统一的方式来解决所有应用的共同问题，提供通用的管理，无疑是一种更为合理的安全解决方案。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，能够安全地从事商务活动。不难看出，建立以PKI为基础的安全解决方案，无论是对于在内部互联网(Intranet)上开展无纸办公等内部业务，还是对于开展电子商务、网络银行等Internet商业应用，都是一种好的选择。

在开放式的互联网上，登录者可以匿名上网，无法确认其身份；而且网上传输的信息也极易被窃取。从外部网络看，网上欺诈、网上偷窃和各种网上恶意行为层出不穷。从内部网络看，盗用口令、篡改数据时有发生。

数字证书正好解决了以上问题，它使我们可以确认网上用户的身份，利用数字证书进行签名，确保信息不被篡改以及所发送信息的法律效力。