Broadview
www.broadview.com.cn

安全技术大系

公钥基础设施 PKI及其应用

关振胜 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

公钥基础设施PKI及其应用

关振胜 编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

公钥基础设施 PKI（Public Key Infrastructure）是利用公钥概念和加密技术为网上通信提供的符合标准的一整套安全基础平台。公钥基础设施能为各种不同安全需求的用户提供各种不同的网上安全服务，主要有身份识别与鉴别（认证）、数据保密性、数据完整性、不可否认性及时间戳服务等。用户利用 PKI 所提供的这些安全服务进行安全通信，以及不可否认的安全电子交易活动。无论是国内还是国外，PKI 都已得到广泛的应用，如安全电子邮件、Web 访问、虚拟专用网络 VPN 和本地简单登录认证，以及电子商务、电子政务、网上银行和网上证券交易等各种强认证系统都普遍应用了 PKI 技术。

本书共分 18 章，主要介绍 PKI 的概念、PKI 的主要内容、PKI 的理论基础、PKI 体系及其所提供的服务功能，重点论述 PKI 在各种领域的应用，如电子商务和电子政务、网上银行、网上证券和网上税务，以及企业内部的信息安全管理等。本书是作者多年来工作经验的总结，既有理论又有实践；本书内容丰富、新颖、技术性强，所涉及的技术都是目前国内外 IT 前沿的技术领域。

本书既可供从事 CA 设计、建设、运营和 PKI 应用，如网上银行、网上证券、电子商务和电子政务技术人员学习和参考，也可供电子认证服务行业人员学习和参考，还可作为大专院校相关专业的学习教材以及电子政务、电子商务的培训教材。

图书在版编目（CIP）数据

公钥基础设施 PKI 及其应用 / 关振胜编著. —北京：电子工业出版社，2008.1
（安全技术大系）
ISBN 978-7-121-05228-6

I. 公… II. 关… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字（2007）第 162006 号

责任编辑：葛 娜
印 刷：北京市天竺颖华印刷厂
装 订：三河市金马印装有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×980 1/16 印张：32.5 字数：722 千字
印 次：2008 年 1 月第 1 次印刷
印 数：5000 册 定价：65.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

总　序

公钥基础设施 PKI 是符合标准的网络安全基础平台，它能为网络通信、网上交易提供普适性的安全服务，如网上身份认证服务，即完成网上用户身份的鉴别；网上数据传输的完整性保护，即保障数据不被非法篡改；网上数据的保密性，即保证非授权用户不能读懂传输的数据；数据的公正性服务，即在对处理过的数据发生争端时，可提供数据处理的事后审计、仲裁功能及时间戳服务。

随着国内的网上银行、电子商务、电子政务的飞速发展，对 PKI 提供服务的需求越来越广泛和迫切。特别是我国在 2005 年 4 月 1 日公布并执行《电子签名法》以来，对国内 PKI/CA 市场进行了整顿，国家有关主管部门同时出台了《电子认证服务管理办法》，使国内 PKI 服务业逐渐走向正规。

由于工作关系，我十分关注国内网络认证体系的研究和建设。中国金融认证中心（CFCA）技术总监关振胜先生应电子工业出版社《安全技术大系》专家委员会的邀请，编著《公钥基础设施 PKI 及其应用》一书是很有必要的，也是很适时的。

该书除了论述 PKI 一般技术原理之外，还用较大篇幅论述了 PKI 的应用，理论与应用紧密结合。PKI 建设的目的是应用，是为了保障网络信息系统的安全。

在中国，PKI 数字证书应用最广泛的是金融界的网上银行。网上银行的开办，是我国银行家看准并及时抓住了互联网络及其安全的这一新生科学技术，在短短不到十年的时间内，就大规模地应用了这项新生科学技术，改变了银行的传统业务和经营方式，建立了新的机构和制度。在 PKI 等安全技术的保障下，银行利用互联网在国内和国际间传递电子货币，提高了工作效率，降低了银行成本。目前，PKI 不仅对金融界网上银行起到保驾护航的作用，而且对日益兴起的电子政务也将起到毋庸置疑的安全保障作用。

当然，一个国家的网络信任体系结构、PKI 的总体结构，应该有一个统一的建设规划，才能使我国的网上银行、电子商务、电子政务等做到有序、健康地发展。作者在这方面，也提出了自己的看法。

在国内，有关 PKI 的论著不多，电子工业出版社组织编著的包括 PKI 在内的《安全技术大系》丛书，无疑将对我国信息安全建设有很好的推动和促进作用。

衷心祝愿我国的信息安全事业飞速健康发展！

中国工程院院士　周仲义

二 OO 七年六月

序

不知道互联网是否是美国人拨动世界经济的一个战略，总之，伴随互联网发展的二十多年来，地球人都在忙不迭地提升自己的概念、武装自己的家当，催动互联网和美国IT经济的发展。

从1995年开始，从没有什么事物像互联网这么迅猛地在中国生根开花。一个个“.com”如雨后春笋般地冒出、发展、上市。不知道那时的市场是否那么需求互联网和网站，当2000年纳斯达克综合指数在摸高后又急转直下，全球互联网市场跌入低谷，破灭……

几度风雨，几度春秋，十年后的今天，互联网发展趋于理性——尽管还掺杂着直觉和风潮。爱也好，怪也好，毕竟，互联网的高速发展影响、改变了人们的生活方式和企业的运营方式。商业模式越来越丰富、新颖：短信、搜索、游戏、即时通信……当互联网提供了除新闻、聊天外更实际的东西时，一个关键问题出现了，“互联网上不知对方是人还是狗！”——一语道出了关键所在——安全。

互联网上的交易或者信息传输，必须解决4个问题：身份认证、数据保密性、数据完整性和不可否认性。PKI（Public Key Infrastructure）就是建立在公钥理论基础上的一种安全体系，它确实能够保证网上交易和信息传输的身份证认、数据保密性、数据完整性和不可否认性，为网上银行、电子商务和电子政务提供安全保障。

本书作者关振胜先生是中国金融认证中心的技术顾问，长期从事IT理论研究和实践工作，对PKI理论有着深入的研究，具有丰富的实际经验。相信本书是一本对于从事相关工作的朋友有价值的好书。

中国金融认证中心　总经理

2007年6月

前　言

本书主要论述 PKI（Public Key Infrastructure），PKI 是普适性的安全基础设施，它是为网络通信和网上交易提供身份认证，以及数据完整性、数据保密性、数据公正性、不可否认性及时间戳服务的安全基础平台。

本书共分 18 章：第 1~3 章论述 PKI 的理论基础与基本概念；第 4~6 章和第 8 章论述 PKI 的结构和功能，以及信任模型和交叉认证技术；第 7 章专述 CPS，即 PKI/CA 对外证书认证业务声明，属 PKI 的管理范畴；第 9 章论述 PMI 权限管理基础设施及应用；第 10 章和第 12 章详细讲述 PKI 的核心元素数字证书的结构及应用，特别是电子签名法中进行数字签名的原理、签名过程及其应用；第 11 章全面介绍 PKI 的所有标准；第 13~18 章除了集中讲述 PKI/CA 的常规应用外，还重点论述了 PKI 在各种领域的成功应用，特别是网上银行的应用是本书应用论述的重点之一。

本书在电子工业出版社策划的《安全技术大系》中占一席之地，是国内科技图书创新、技术更新之作。作者通过多年来从事 PKI 理论及应用实践编著此书，其特点是理论与实践相结合，既适合于从事 PKI 设计、应用和运营工作者学习参考，也适合于作为大专院校有关专业学生的学习教材，还适合于相关专业的研究生学习参考。

在本书编写过程中得到了中国工程院周仲义院士和中国金融认证中心李晓峰总经理等的帮助和指导，在此一并表示感谢！

由于时间关系，书中有不当之处，敬请读者批评指正。

作　者

2007 年 7 月

目　录

CHAPTER 1

第1章 概 述

有两种创新改变人类的生活方式，一是新技术的发明，如蒸汽机、电力、通信、计算机及其网络和计算机密码学等；二是服务业的创新，如银行、邮电和保险公司等。在计算机密码学方面，由于非对称密钥算法的发明，完全改变了传统的对称密钥算法。非对称密钥算法，也称公钥算法，是计算机密码学方面的一次重大革命和创新，从而改变了信息通信和信息安全的前景。

公钥基础设施（PKI，Public Key Infrastructure）在过去的几年里，在全世界，特别是在中国引起了人们的极大关注，PKI 得到了广泛的应用。美国建立了联邦桥 CA-EMA2000，欧盟也建立了欧洲桥 CA，在日本有一半的企业采用了 PKI，主要进行身份认证。在中国，截至 2006 年已建立 CA 100 余家，还不算企业级自建的 CA。在中国颁布了国家《电子签名法》，于 2005 年 4 月 1 日执行，为此，信息产业部颁发了《电子认证服务管理办法》规范了市场准入，到目前为止，已批准了 19 家 CA，作为第三方认证机构，可向社会公众提供电子认证服务。

几乎所有的新技术，创新的新事物，都有一个不断完善的发展过程，一般说来，都不是“直线”前进的，都要经过“波浪式”的前进过程。在前几年，我们看到了 PKI 的蓬勃发展阶段，但近时期发展速度减缓。但 PKI 的使用宣传报导，在各种媒体上有所强化，这是因为建立 PKI 的目的是在于应用。在互联网和其他网络的应用中，公钥/私钥密码技术和其他加密技术的有机结合，能够满足电子商务、网上银行、电子政务等网上交易和网上办公的一切安全需求。公钥技术与其他加密技术相结合，就可以开发出适用性很强，与具体应用相对独立的证书机制，以及与此相关的、丰富多彩的适用于电子商务、电子政务安全新需求的双强因子认证、数字签名和数字信封的数据完整性、数据保密性和交易不可否认性机制。

PKI 技术和其他新技术一样，在人们的使用早期，会感觉到它还不能达到其最初所承诺的某些功能和特性，结果使一些人对 PKI 的可用性和集成性感到失望。然而，事实给业界指出了希望，由于 PKI 技术和其他安全技术的进步，近几年来，使 PKI 应用大踏步前进了，使它在计算机和网络环境中得到了广泛的应用。如可信计算机中的本机认证、电子商务、网上银行、网上证券、网上保险；电子政务中的网上办公、网上税务、网上工商、电

子海关、电子病历管理等，都引入了 PKI 的应用。我们可以相信，在不久的将来，PKI 完全可以达到和计算机网络一样的集成性和易用性的水平，还要显示出它易实现、互操作的特点。

1.1 信息安全的发展趋势

信息安全是一个永久的话题，因为信息已成为一种资产，像其他重要的业务资产一样，对一个组织单位是有价值的，需要保护。信息安全在 ISO 17799 中定义为："在技术上和管理上为数据处理系统建立的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和泄露。"根据这一定义信息安全的概念，就不只是保护集体数据不被非法访问的问题，其中最大的问题还是如何阻止那些想摧毁信息系统，或者想窃取机密隐私信息的人进入你的系统。

计算机网络的广泛应用开始于 20 世纪 80 年代的早期，网络系统的广泛应用创建了一个新的虚拟世界环境，特别是 90 年代互联网的飞速发展，使网络环境中的信息达到充分共享。比如，我们可以通过使用拨号连接和声音耦合器的接入方式来访问这些网络，这样就为一个全新行业的成长创造了机遇，这个全新行业的任务就是专门保护这些接入点。在使用专用线路连接远程站点并随后将它们连入 Internet 的同时，我们也为各种各样的不法分子进行范围广泛的访问创造了机会。

随着网络访问的日益普及，安全问题就变成了如何在比较柔软、脆弱的内部信息系统的周围，建立起坚固防范围墙。信息安全的主要内容和措施就是如何阻止不法分子攻击破坏企业网内部的文明。常用的安全防范措施或称安全机制，在 OSI 或 TCP/IP 网络协议的网络层，通常采用的是防火墙、安全路由器、入侵检测 IDS 及防黑客软件等机制；而在应用层上，目前最佳的防范机制就是基于 PKI 的数字证书机制。

因此，一个全新的防卫策略语言产生了，我们构建了基于"要塞"思想和边界防御的模型；开发了认证产品以便城镇的居民能够向守门的卫兵证实身份；构造了非军事区（DMZ，DeMilitarized Zones）以区分那些允许从外部访问的由不太敏感的设备组成的区域，以及那些我们准备誓死保卫的区域（堡垒主机）；建立了防火墙，将网络城市内部划分成数个区域，当侵略者夺取系统、毁坏我们的数据时，可以限制他们造成的破坏；建立了入侵检测系统（防御墙）和陷阱（城堡外墙），单位内部的信息大本营必须保证安全无恙。

信息已成为企业的资源，信息的核心是数据，所以，保护信息、数据的安全其发展趋势将越来越重要。

1.2 现今的电子商务和电子政务的安全

TCP/IP 协议的创建者和互联网的发明人，他们一定没预想到，在多少年之后，会在互联网上除传输信息流之外，还会传输资金流。也就是说，如今在互联网上除办理电子政务

之外，还可以办理电子商务。从原来的封闭式、局域性的网络，发展成为广域的、开放式的环境。一些 B2B、B2C 的主要商务交易活动和在线资金支付，可以在这个环境中进行。

在这种情况下，公司企业的数据安全固然重要，但重点还要关注到公司商品贸易最大化的需求，商品信息及商品的流通，需要资金货币的流通做保障，商品流通到哪里，货币支付就应及时流通到哪里。现代的商品流通已全球化了，所以信息安全问题不是如何限制对信息系统的访问，而是如何提供最大化的访问，去面向那些电子商务环境中的各种角色，如客户、商家、支付平台、银行和物流公司等。

当然，传统的信息安全机制还仍然需要，如在网络层上面装置的所谓“老三样”（防火墙、路由器、入侵检测 IDS）。但是有个明显区别，就是在互联网情况下，那些信息系统严守的边界将不再存在了。因为，你允许合作伙伴访问公司数据；允许客户访问公司数据，而客户可能分布在全球各地；允许公司的分销商和代理商访问公司数据……你的数据中心可能外包托管到某一个 ASP 设备管理公司；网络连接和网络管理是互联网服务提供商提供的，甚至有些单位的应用系统也是由应用服务提供商来代替运营的。

所以，安全问题遇到了新的挑战，对网上的电子商务提出了新的安全需求。这就是网上身份的真实性认证，对网上各种角色的身份进行鉴别与识别；网上交易订单信息要保护其私密性；交易支付信息的完整性及交易各方对其交易和支付结果的不可抵赖性。

1.3 电子商务、电子政务的安全需求

电子商务是将传统的商务活动移到网络环境中来，特别是建立在互联网上的商务活动，其安全问题备受关注。基于互联网上的电子商务和电子政务，其发展制约之一就是安全问题，安全是电子商务的基础保证。所谓电子商务的安全，主要是网络安全问题，需要从电子商务对网络系统的安全需求分析出发，采取安全技术措施，提供安全服务，以满足电子商务的各种安全需求。其中，首要的问题是制定安全策略。

1.3.1 安全策略

所谓安全策略，就是实施计算机信息系统的安全措施及安全管理的指导思想，是在计算机信息系统内，用于所有与安全活动相关的一套规则。这些规则是由这个系统中新设立的一个安全权力机构建立的，并由安全控制机构来描述、实施和实现。

安全策略是一个很广的概念，这一术语以许多不同的方式用于各种文献的标准中。据一些有关的分析表明，安全策略有以下几个不同的等级。

（1）安全策略目标。它是某个机构对所要保护的特定资源要达到的目的所进行的描述。

（2）机构安全策略。这是一套法律、规则及实际操作方法，用于规范某个机构如何来管理、保护和分配资源，以达到安全策略的既定目标。

（3）系统安全策略。它所描述的是如何将某个特定的信息技术系统付诸工程实现，以支持此机构的安全策略要求。