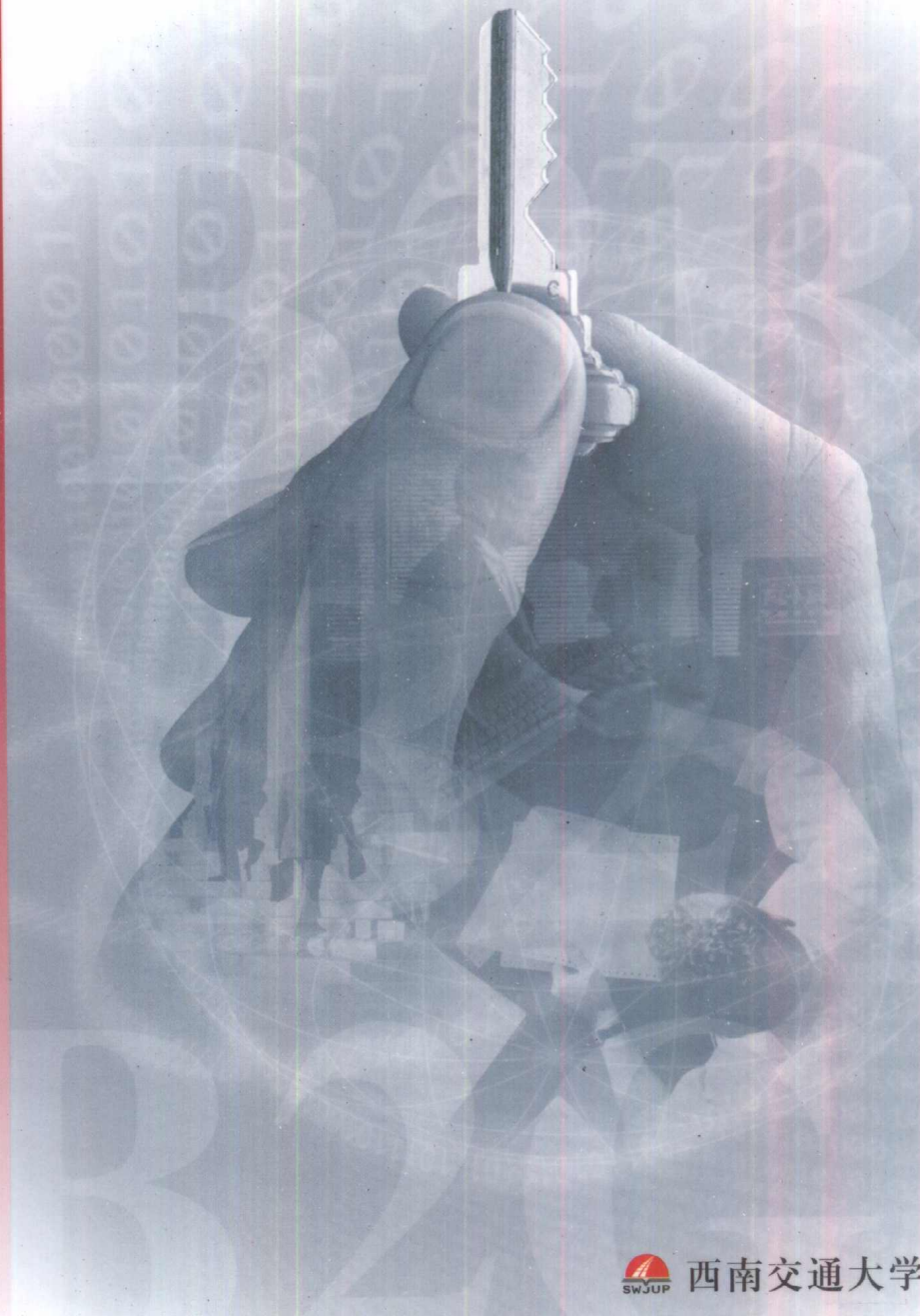
电子商务安全与PKI技术

帅青红　匡　松　编著



西南交通大学出版社

电子商务安全与 PKI 技术

帅青红　匡　松　编著

西南交通大学出版社

·成　都·

内 容 简 介

本书主要介绍电子商务基础、电子商务对社会的影响、网上银行与网上支付；PKI的信任模型与PKI的基础理论；网络系统的安全、电子商务的安全、常用的安全技术、数字证书技术及证书运作规范；主要的PKI产品、PKI技术的应用以及PKI在中国电子商务中的应用。

本书可作为大专院校电子商务方面的教材及参考书。

图书在版编目（CIP）数据

电子商务安全与PKI技术 / 帅青红，匡松编著. —第1版. 成都：西南交通大学出版社，2001.6
ISBN 7-81057-556-2

Ⅰ. 电… Ⅱ. ①帅…②匡… Ⅲ. 电子商务－安全技术 Ⅳ. F713.36

中国版本图书馆CIP数据核字（2001）第26409号

电子商务安全与PKI技术

帅青红 匡 松 编著

*

出 版 人 宋绍南
责任编辑 秦 薇
封面设计 肖 勤

西南交通大学出版社出版发行
（成都二环路北一段111号 邮政编码：610031 发行科电话：7600564）
http://press.swjtu.edu.cn
E-mail: cbs@center2.swjtu.edu.cn
成都飞机工业公司印刷厂印刷

*

开本：787 mm×1092 mm 1/16 印张：10.625
字数：240千字 印数：1～3000册
2001年6月第1版 2001年6月第1次印刷
ISBN 7-81057-556-2/F · 051
定价：13.00元

前　言

近年来，信息安全成为极度热门的话题，特别是电子商务的兴起使信息安全问题更为突出。人们已经从现实世界进入了电子世界，并通过网络进行交流和商业活动，而如何建立起相互之间的不可否认性则是我们面临的急需解决的最大问题。PKI就是解决这一系列问题的技术基础。

PKI是“Public Key Infrastructure”的缩写，意为“公钥基础设施”。简单地说，PKI技术就是利用公钥理论和技术建立起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。

本书分四篇介绍有关电子商务安全与PKI技术方面的基本知识、基本理论、技术应用及其主要产品。

第1篇介绍电子商务基础、电子商务对社会的影响、网上银行、网上支付。包括电子商务的基本概念、电子商务的分类、电子商务的组成，特别是电子商务对银行业的影响及其对策。

第2篇从互联网时代的信息安全开始，讲述了网络系统的安全、电子商务的安全、常用的安全技术、数字证书技术以及证书运作规范。

第3篇介绍PKI的信任模型与PKI的基础理论。

第4篇介绍世界上主要的PKI产品、PKI技术的应用以及PKI在中国电子商务中的应用。

目　　录

第1篇　电子商务基础

第2篇 电子商务的安全技术

第 3 篇 PKI 技术

第 4 篇 PKI 的应用

第1篇　电子商务基础

本篇分为 4 部分

- 电子商务基础
- 电子商务对社会的影响
- 网上银行
- 网上支付

包括电子商务的基本概念、电子商务的分类、电子商务的组成，特别是电子商务对银行业的影响及其对策。

第1章

电子商务基础

全球经济发展正在进入信息经济时代，知识经济初见端倪。作为21世纪的主要经济增长方式——电子商务，将给世界各国和世界经济带来巨大的变革，产生深远的影响。电子商务通过大幅度降低交易成本、增加贸易机会、简化贸易流程、提高贸易效率、提高生产力、改善物流系统等，并最终推动企业和国民经济结构的改革。与此同时对电子商务的关注和投入可以发展新兴产业，创造就业机会，推动国家和全球经济的发展。

电子商务(Electronic Commerce)就是指贸易活动各环节信息的电子化，它涵盖了三方面的内容：一是政府贸易管理的电子化；二是企业级电子商务；三是电子购物。因此电子商务涉及商务活动的所有环节，其中包括组织和个人，这些活动都是基于数字数据的处理和传递，包括文本、声音和图像信息。电子商务的实现主要有三个环节：信息流，电子货币流和物质流。电子商务是一个新兴市场，而且是一种替代传统商务活动的新形式。它有可能彻底改变贸易活动的本质，形成一套全新的贸易活动框架。

电子商务的最初形式电子数据交换（EDI）起源于20世纪60年代。20世纪80年代末，发达国家的电子数据交换已形成规模，向商业数据的无纸化处理迈出了一步。其后，一些专门的数据交换系统逐渐形成并投入运行。在增值网络服务推出以后，此类专用信息交换系统得到了更大的发展。随着网络技术的发展，特别是国际互联网在全球的日益普及，电子商务得到了迅速发展。

正是由于电子商务的巨大潜力和电子商务活动的本质特征，世界各国政府都对此给予高度重视。为了能够创造性地和及时有效地抓住电子商务迅速发展的机会，一些国家提出了本国的电子商务框架和发展战略，积极推动电子商务。OECD、APEC、WIPO和UN等相关国际组织和论坛专门成立了电子商务工作组，并提出了一些报告或规范。

现在，电子商务的潮流已经进入国内，并在外经贸、海关、金融、商业等许多领域中得到应用，同时，各种专业网和增值网络发展迅速，电子商务成为各方关注的焦点，电子商务发展和应用的环境正在逐步形成。

中国政府非常重视电子商务的应用和发展。1998年11月，在吉隆坡举行的APEC领导人非正式会议上，中国国家主席江泽民指出：**“电子商务代表着未来贸易发展的方向，其推广将给各成员国带来更多的贸易机会”**。在世界经济全球化、信息化时代，电子商务对世界各国都是一个重要的机遇，也是一个挑战。中国是世界第十大贸易国，国民经济持

续稳定增长，对外贸易在国民经济中所占比重越来越大，中国需要建立自己的电子商务框架，推动电子商务的应用和发展，为下一个世纪中国国内经济发展和参与全球经济贸易奠定基础。

电子商务的应用、推广和发展，需要政府的推动、指导和协调，需要良好的法规环境，需要统一的标准和有效的管理。为了促进电子商务的发展，并且最大限度地开发和利用电子商务，中国政府正在按照江泽民主席的指示，加强政府部门对发展电子商务的宏观规划和指导，不断改善法律法规环境。同时中国政府也重视私营、工商部门在电子商务发展中的推动作用，并发挥政府的作用，促进工商业的信息技术应用和参与电子商务。

1.1 电子商务基础知识

1.1.1 电子商务的定义

所谓电子商务就是借助计算机技术、网络技术和远程通讯技术，使得交易各方当事人通过电子方式联系，摒弃传统的纸面文件、单据的传输，实现整个交易过程的电子化、数字化、网络化。所以，现代电子商务将通过网络，在网上形成信息流、物质流和资金流的统一。

广义的电子商务(Electronic Commerce，E-Business)，是指利用简单、快捷、低成本的电子通讯方式，买卖双方不谋面地进行各种商贸活动；随着 Internet 技术的日益成熟和发展，通常人们所说的电子商务则是特指**通过 Internet 进行的各种商贸活动**。

电子商务是在 Internet 开放的网络环境下，基于浏览器/服务器（Browser/Server）应用方式，实现消费者的网上购物、商户之间的网上交易和在线电子支付等的一种新型的商业运营模式。目前，国内外对电子商务还没有统一的定义，有的叫 Electronic Commerce；也有的叫 Electronic Business。

1.1.2 电子商务的特点

简便、快捷、高效、低成本、电子通讯、买卖双方不谋面、全球性、开放性等是电子商务的主要特点。

电子商务具有鲜明的特点，正在世界范围内方兴未艾。电子商务将生产企业、流通企业以及消费者和政府带入了一个网络经济、数字化生存的新天地；电子商务所具有的全球性、开放性的特点，为企业和消费者提供了更多的机会；电子商务突破了时间和空间的限制，使得交易可以随时随地进行，从而大大提高了效率；同时电子商务也为中小企业提供了与大企业进行平等竞争的机会。

1.1.3 电子商务的实现方式

依据电子商务实现的环节，可分为：较低层次的电子商务，如电子商情、电子贸易、电子合同等；高层次的完全在 Internet 网上完成全部贸易活动的电子商务。即在网上将信息流、商流、资金流和部分的物流完整地实现，也就是说，你可以从寻找客户开始，一直到洽谈、订货、在线付（收）款、开具电子发票一直到电子报关、电子纳税等通过 Internet 一气呵成。

从交易类型来说，电子商务可分为：企业与个人（即 B to C），企业与企业(即 B to B)等多种方式。

网上购物就是一种典型的 B to C 方式。

1.1.4 电子商务涉及的实体（参与者）

买方（包括个人消费者或企业）;

卖方（包括销售商、制造商等）;

银行（包括发卡行、开户行）;

认证中心 CA（Certificate Authority）。

电子商务认证中心（CA）专门为参与网上交易的各方发放网上身份证（买方、卖方、银行）——数字证书，并不具体参与交易。

目前，中国已经建成的 CA 有：中国金融认证中心(CFCA)，上海市、广东省、天津市、海南省、深圳市等地方性的 CA，各商业银行的 CA 以及电信、邮政的 CA 等。

三大 CA：中国金融 CA，上海 CA，电信 CA，网址分别为：

www.cfca.com.cn; www.sheca.com; www.cnca.net.

1.1.5 网上支付

网上支付是电子商务的关键环节，也是电子商务得以顺利发展的基础条件。如何保障电子商务网上支付的安全，一直是电子商务的核心。目前，它是通过认证中心（CA）发放数字证书来实现的。采用数字证书可以对交易各方的身份进行验证，并且可以对要传输的信息进行加密和签名，保证了信息的机密性、真实性、完整性和不可否认性。

为了保证网上支付的实现，由中国人民银行联合中国工商银行、中国银行、中国农业银行、中国建设银行、交通银行、招商银行、中信实业银行、华夏银行、广东发展银行、深圳发展银行、光大银行、民生银行等十二家商业银行共同建成了中国金融认证中心（CA），这个系统专门为参与网上交易（网上银行、网上购物等）的各方提供数字证书服务，保证了网上交易各方能够实现网上支付。

1.1.6 实现电子商务的三个方面

信息流、物质流和资金流是实现电子商务的三个方面。

Internet 上的电子商务可以分为三个方面(信息流、物质流和资金流)，即：信息服务、交易和支付。主要内容包括：电子商情广告、电子选购和交易、电子交易凭证的交换、电子支付与结算以及售后的网上服务等。

电子商务只是商务模式的改变，它不能代替传统企业，而仍属于服务领域；电子商务离不开物资的流动，这就需要传统企业的积极参与，特别是配送系统的建立就显得至关重要；资金的流动则可以通过电子货币来实现。

总而言之，作为一种商务活动过程，电子商务将带来一场史无前例的革命。其对社会经济的影响会远远超过商务的本身，电子商务不仅将改变商务活动的方式，改变企业的生产方式和人们的消费方式，它还将对就业、法律制度以及文化教育等带来巨大的影响。电子商务会将人类真正带入信息社会。

电子商务是 Internet 迅速发展的直接产物，是网络技术应用的全新发展方向。Internet 本身所具有的开放性、全球性、低成本、高效率的特点，也成为电子商务的内在特征，并使得电子商务大大超越了作为一种新的贸易形式所具有的价值，它不仅会改变企业本身的生产、经营、管理活动，而且将影响到整个社会的经济运行与结构。

① 电子商务将传统的商务流程电子化、数字化，一方面以电子流代替了实物流，可以大量减少人力、物力，降低了成本；另一方面突破了时间和空间的限制，使得交易活动可以在任何时间、任何地点进行，从而大大提高了效率。

② 电子商务所具有的开放性和全球性的特点，为企业创造了更多的贸易机会。

③ 电子商务使企业可以以相近的成本进入全球电子化市场，使得中小企业有可能拥有和大企业一样的信息资源，提高了中小企业的竞争能力。

④ 电子商务重新定义了传统的流通模式，减少了中间环节，使得生产者和消费者的直接交易成为可能，从而在一定程度上改变了整个社会经济运行的方式。

⑤ 电子商务一方面破除了时空的壁垒，另一方面又提供了丰富的信息资源，为各种社会经济要素的重新组合提供了更多的可能，这将影响到社会的经济布局和结构。

要实现完整的电子商务还会涉及到很多方面，除了买方、卖方外，还要有银行或金融机构、政府机构、认证中心、配送中心等机构的加入才行。由于参与电子商务活动的各方在物理上是互不谋面的，因此整个电子商务过程并不是物理世界商务活动的翻版，网上银行、在线电子支付、数据加密、电子签名等技术在电子商务中发挥着重要的不可或缺的作用。

1.2 电子商务的基本术语

▶ **证书 [Certificate]**

CA 根据其 CPS 颁发的，包含客体的标识信息和私钥，并用颁发者的私钥进行数字签名，用以证实客体身份信息的电子记录和该信息的载体。

▶ **证书颁发 [Certificate Issuance]**

生成证书并将细节通报给证书中所记录的申请者的行为。

▶ **证书撤销 [Certificate Revocation]**

在发生私钥失密或泄密的情况下，或在证书的重要属性（如申请者姓名）已经改变的情况下，在证书有效期内使证书失效。

▶ **证书废止列表（或：证书黑名单）[Certification Revocation List（CRL）]**

认证机构已经签署的印有时间的撤销证书目录。

▶ **证书所有者 [Certificate Subscriber]**

已收到由认证中心颁发证书的人员。除非另外标注，在本指南中证书所有者简称为“属主”。

▶ **证书暂停 [Certificate Suspension]**

在证书有效期内将证书临时撤销。

▶ **证书用户 [Certificate User]**

使用证书的人员，如证书所有者或证书验证者。除非另外标注，证书用户被简称为“用户”。

▶ **证书运作规范 [Certification Practice Statement（CPS）]**

证书运作规范指的是认证中心进行发布、撤销、更新和访问证书等操作时应遵循的规则。

▶ **认证 [Certification]**

为个人、组织、设备等生成证书的过程。

▶ **认证中心 [Certification Authority（CA）]**

认证中心作为一个权威的、可信赖的、公正的第三方信任机构，专门负责为各种认证需求提供数字证书服务，为参与网上交易的各方提供安全的基础，建立彼此信任的机制。认证中心为负责授权和发布证书的实体。认证中心能够履行 RA 的职能和进行证书制定授权。

▶ **失密 [Compromise]**

私钥及相关保密信息已被或可能被偷窃，或被外泄，或者由于第三方解密已经或可能使秘密暴露的情况。

▶ **交叉认证 [Cross Certification]**

两个认证中心相互认证的过程。交叉认证使得由两个认证中心颁发的证书可以通用，扩大了用户证书的使用范围。

▶ **密码模块 [Cryptographic Module]**

用来保障在生成、存贮和使用密钥时的安全性，它包含了软件、固件或硬件。

▶ **数字签名[Digital Signature]**

被签发数据的哈希值，经过私钥加密后的结果。通过把使用公钥对数字签名解密得到的值与原始数据的哈希值相对照，就能验证数字签名。

▶ **多重控制 [Dual Control]**

把控制功能分布至多个人员，直至所有人员都完成了其控制功能后才执行某项特定功能的一种工作制度或控制制度，以防止在访问秘密信息或运行系统时的不当行为。

▶ **哈希（或：散列）[Hash]**

通过对数据作数学运算得到的定长的数据串。在“单向哈希”中，无法从哈希值还原出原始数据。

▶ **标识与鉴别 [Identification & Authentication]**

验证个人、组织、设备或其他方信息的真实性的行为。

▶ **密钥对 [Key Pair]**

在公钥密码体制中使用的公钥以及与此公钥相对应的私钥。

▶ **操作手册 [Operation Manuals]**

详细规定根据证书运作规范（CPS）操作的文档。

▶ **策略 [Policy]**

关于认证中心服务与运行的条例与标准。

▶ **私钥 [Private Key]**

在公钥密码体制下使用的一对密钥中，由用户自己保管不对外公开的密钥。

▶ **公钥 [Public Key]**

在公钥密码体制下使用的一对密钥中，对外公开供通信其他方使用的密钥。

▶ **公钥密码体制 [Public Key Crypto System]**

使用两个密钥（公钥和私钥）的一种非对称密码算法。当用一个密钥（公钥）加密数据后，可使用另外一个密钥（私钥）来将其解密。并且，当用一个密钥（私钥）对数据签名后，接收者能够使用另外一个密钥（公钥）来鉴别签名者。这一对密钥所具有的属性使得即使已经知道公钥，也无法通过计算而找到私钥。

▶ **公钥体系（或：公钥基础设施）[Public Key Infrastructure]**

使用公钥密码体制来保障信息系统和通信系统安全的一系列技术和服务。

▶ **注册审批机构 [Registration Authority（RA）]**

对申请证书者的资格、能力、权限等进行审核，并决定能否颁发证书，但并不签署和发布证书，只将审核通过者资料传送给 CA。

▶ **证书验证者 [Relying party]**

接收证书并在执行交易时，依赖该证书的人员。

▶ **加密秘钥对**

指两个数学关联的秘钥具有以下特性：解密秘钥只能用于解密一条用加密秘钥加密的信息。

▶ **目标识别符（OID）**

目标识别符为一国际标准组织认可的特殊格式化的数字形式。

▶ **证书有效期**

证书具有有效期，其有效期始于证书签发日（或是在证书中注明的日期），终止于证书中标明的过期时间或提前撤销的时间。

▶ **证书的中止**

在证书的有效期内，暂时中止该证书的效力。中止的原因消失后可恢复效力。

▶ **证书制作**

从受权持证人接受私钥和识别信息，到创建数字证书（包括其他有关的信息及数字签名证书）的过程。

▶ **人员**

人员（指正常人）、团体、有限责任公司、其他司法机构或由另外一个人控制的数字驱动程序。

▶ **签名**

为达到确认某记录的目的，由某人签署或认可的符号、方法。

▶ **电子签名**

附加在电子记录之后或与其有逻辑联系的、数字形式的标识符号、其签署和认可的目的在于对电子记录的认证。

▶ **数字签名**

由电子记录经哈希函数和非对称加密体制的转换而产生的电子签名。

▶ **数字签名的验证**

准确确认数字签名、记录和私钥的关系。

▶ **签名秘钥对**

非对称加密体制中的私钥及其在数学上对应的私钥，私钥可以验证由私钥签署的数字签名。

▶ **私钥**

秘钥对中用于创建数字签名的秘钥，本秘钥需秘密保存。

▶ **公钥**

指秘钥对中用于校验数字签名的秘钥。任何从秘钥对持有者手中收到数字签名信息的人都可自由使用私钥。通常，认证中心发布的证书提供的私钥可通过访问目录器来获得。私钥用于校验相关私钥的持有者发送的信息。

▶ **可靠的第三方**

在适用证书政策以内依靠证书的受权人。

▶ **根 CA（RCA）**

最高层 CA，用于制定 CA 的政策，审批、颁发下层 CA 的证书，并负责与其他 CA 系统进行交叉认证。

▶ **支持机构**

受权持证人附属的组织（如雇员、服务用户、业务伙伴、客户等）。

▶ **主体**

其私钥在证书内被鉴定的实体，也包括持证人。

▶ **持证人**

拥有与证书上的私钥对应私钥的证书的持有者。

▶ **有效证书**

指的是符合下列条件的证书：①认证中心已发布的；②列出了已接受的持证人的；③未过期的；④未撤销的。只有该证书由认证中心发布并被持证人接受才有效。

▶ **校验公开秘钥**

签名秘钥对的私钥部分由第三方用于校验终端用户数字签名。

▶ **记录**

指在有形介质描述、存贮的信息。