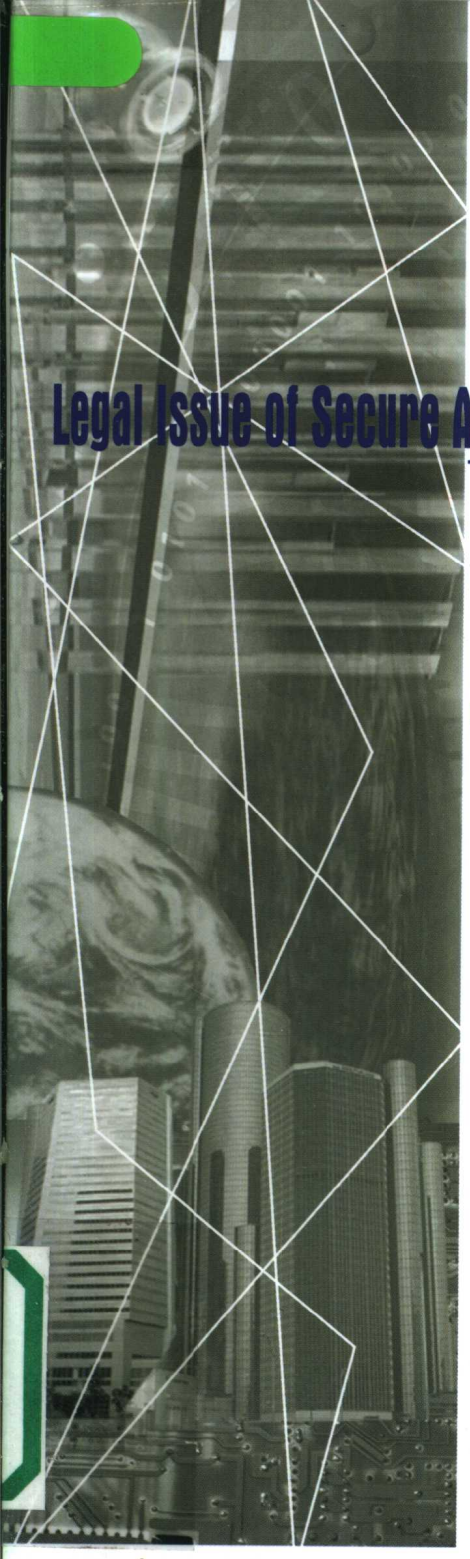


电子商务法系列丛书

Legal Issue of Secure Authentication in Electronic Commerce

电子商务认证法律问题

胡静 编著

Series of
E-Commercial Law

北京邮电大学出版社
www.buptpress.com

电子商务认证法律问题

——电子商务安全与CA认证

胡 静 编著

北京邮电大学出版社
·北京·

内 容 提 要

随着 Internet 的发展，电子商务逐渐成为一种新型的商务模式，其发展前景十分诱人；电子商务的安全问题也因此越来越突出。如何建立一个安全、可靠、便捷的电子商务应用环境，以对电子商务活动提供保障，已成为人们十分关心的话题。

本书专门就电子商务安全所涉及到的电子商务安全认证技术和法律问题进行了研究。全书共分七章，第一章概述了电子商务安全，后六章分别介绍了电子商务安全与电子商务安全认证的技术和法律体系。为方便读者了解电子商务安全认证的相关知识，书中还提供了典型案例及其分析。

图书在版编目(CIP)数据

电子商务认证法律问题/胡静编著. —北京：北京邮电大学出版社，2001.8
(电子商务法系列丛书)
ISBN 7-5635-0485-0

Ⅰ.电… Ⅱ.胡… Ⅲ.电子商务—安全技术—研究 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2001)第 17832 号

出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号(100876)
电话传真：010-62282185(发行部)/010-62283578(传真)
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京源海印刷厂
印　　数：1—3 000 册
开　　本：787 mm × 960 mm　1/16
印　　张：19
字　　数：287 千字
版　　次：2001 年 8 月第 1 版　　2001 年 8 月第 1 次印刷

ISBN　7-5635-0485-0/F.36　　定　　价：35.00 元

电子商务法系列丛书

序　言

亲爱的读者，我非常高兴为展现在广大读者面前的这本《电子商务认证法律问题》撰写序言。

电子商务安全认证系统是保证电子商务安全的基础设施。电子商务安全认证，就是由权威的安全认证机构通过签发数字证书，对利用通信网络从事商业和其他业务活动的各主体进行事先的验证和识别，并采用数字安全认证技术实现各业务主体之间在网上进行的业务操作和信息传递的安全性、真实性、可靠性、完整性和不可抵赖性。

电子商务是新世纪世界商务发展的潮流。随着电子商务的蓬勃发展，安全问题越来越显得重要和突出。因此，制约电子商务发展的一大瓶颈——"安全认证"便成为业界专家关注的焦点。

根据我国密码安全产品开发的有关政策，属于专控产品的密码安全产品既不出品，也不进口，必须完全自主开发。考虑到电子商务安全认证体系是电子商务的制高点和核心，应用最有效的安全技术建立电子安全体系结构，已成为电子商务建设中首先需要解决的问题。国际上提出了基于公开密钥体系（PKI）的数字证书解决方案，现已被普遍采用。电子中安全措施的实现主要围绕数字证书展开。

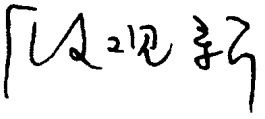
基于上述电子商务安全认证的需要，我们成立了广东省电子商务认证中心（注册名为：广东省电子商务认证有限公司）。它是目前广东省唯一一家政府认可的安全认证机构，是向全社会提供安全认证与信任服务的专业机构。它作为电子商务活动中可信任的中立的第三方，主要为电子政务、电子商务活动提供电子身份认证、数字证书签发、密钥与证书管理服务，同时还提供政府、企业安全解决方案、网上安全支付、电子商务顾问咨询、客户培训等服务。

从我们目前的安全电子认证业务发展情况和问卷调查结构来看，不论是企业还是个人，对于电子商务安全认证涉及的有关法

律、法规方面的需求是非常迫切的，比如认证机构的法律地位，电子签名、数字证书和电子认证法律效力如何等诸多法律问题，这均向传统法律提出了新的课题。

作为电子商务安全认证业界的实践者，我们感到非常有必要开展这方面的理论研究。因此，我将本书的研究成果推荐给读者，期望本书的问世能给读者提供理论上的参考和帮助，也期望本书能够引发各界人士加入到关心电子商务安全的行列中来，一道为开创崭新而又安全的电子商务时代出力献策！

广东省电子商务认证有限公司董事长



编者的话

电子商务是一个充满机遇和挑战的新领域，作为一种全新的商业机制，它以高效率、无疆界、无时限和低成本等特点受到全球各国政府和企业界的广泛重视，并获得迅速发展。人们普遍认为，电子商务将成为21世纪全球经济最大增长点之一。

随着Internet的迅速发展，电子商务开始应用到各个方面。但是，由于Internet的开放性、共享性和动态性的特点，任何人都可以自由接入Internet，一些怀有恶意者就可以采取各种手段进行破坏活动，对电子商务系统的安全构成一定威胁。因此，在Internet上发展电子商务的首要问题就是要解决电子商务的安全问题，而且，电子商务能否在不久的将来逐步取代传统意义上的商业形式，主要取决于电子商务能否在可靠的机制上安全地运行。电子商务的安全问题是一个涉及范围极广的社会问题，要使电子商务能够健康、蓬勃地发展，就必须用全面的电子商务安全解决方案来提供电子交易的信任保障。目前，电子签名和安全认证已被普遍认为是网上比较成熟的安全手段之一。

笔者是广东省电子商务认证中心（网址：http://www.cnca.net，注册名为广东省电子商务认证有限公司）的一名从业人员，从事电子商务安全认证方面的工作，在切身的工作实践中，深刻体会到电子商务安全是电子商务获得发展的重要前提。因此，开展电子商务安全认证技术与法律方面的研究非常有必要。不久前，笔者参编了广东科技出版社出版的《电子商务法律热点》一书，对电子商务领域亟需立法的热点法律问题进行了研究；本书是在北京邮电大学张楚博士的推荐与指导下编写的，目的是期望对想了解电子商务安全认证工作和对电子商务安全认证工作感兴趣的朋友们有所帮助。

由于电子商务安全与CA电子认证方面的资料不多，且时间有限，故本书只是对其作粗浅的探讨，值得深入研究的地方还很

多。

本书在编写过程中，曾得到广东省电子商务认证有限公司技术部的技术咨询，特别是得到了广州大学的方稳根先生的指导与大力帮助，在此一并表示深深谢意！本书参考了国内外有关资料，在此向提供支持和帮助的朋友们致谢！同时，更要感谢北京邮电大学出版社的支持与厚爱！

限于作者水平，可能存在一些欠妥当的地方，敬请各位专家指正！同时也欢迎读者对本书提出宝贵意见，并希望有越来越多的各界人士加入到关心电子商务安全的行列中来，一起为开创崭新而又安全的电子商务时代出力献策！

胡　静

2001 年 2 月于广州天河

目　录

1　电子商务安全概述

2　电子商务安全认证技术概述

3 安全电子认证概述

4 电子商务安全认证立法概述

5 电子商务安全认证法律分析

6 电子商务安全法律规范

7 典型案例与分析

1 电子商务安全概述

Internet 在拉近人们的距离，改变着人们的生活、生产和生存的方式。人们已从传统的面对面的交易和作业，变为跨越时空互不见面的网上操作。当人们在尽情享受数字化的生活、利用互联网资源和工具的同时，也面临着被攻击的危险。当人们在网上工作时，其正在作业的系统可能会遭到攻击者的非法访问甚至破坏，部门机关的机密资料、个人隐私、交易的敏感信息、支付信息等等都可能遭到窃取、盗用或篡改。可见，互联网络并不太平。黑客的攻击和电脑病毒的爆发也常常造成网站的瘫痪、信息的丢失，给蓬勃发展的电子商务带来极大的安全隐患。因此，解决电子商务的安全问题成为电子商务发展的首要问题。据国际数据公司统计预测，全球电子商务交易额到 2003 年将高达数万亿美元。如果不解决网络安全问题，预测恐怕难以变成现实。

随着电子商务的发展，安全问题越来越显得重要和突出。概括地说，电子商务的安全主要体现在：交易的有效性和可执行性、交易机制的可靠性、交易过程中信息的完整性和保密性。目前，电子商务安全问题的解决，可分为技术和法律两方面。

从技术方面来讲，建立电子商务的安全认证机构（CA：Certification Authority），确认用户身份的真实性，信息和数据的保密性、完整性和不可抵赖性，同时利用现代密码技术、加解密技术和电子签名技术，可以保证电子商务的安全。

从法律上讲为电子商务提供安全保障，也就是在电子商务出现差错时，用法律手段解决有关交易方的责任和权利等问题。电子商务使用现代电子通讯手段所产生的法律问题，最终还是要通过立法来解决。

“安全”是一个相对的词语，电子商务的发展也将促使人们对安全技术和电子商务法律问题进行不断探索研究和开发应用，以建立一个相对安全的电子商务环境。

第一节 电子商务与安全

一、关于电子商务的科学定义

随着 Internet 热潮席卷全球，电子商务日益成为当下时髦的词汇之一。各国政府、学者、各界人士根据自己所处的地位和对电子商务的参与程度，曾给出了一些表述各异的电子商务定义与各种理解。

电子商务一词源于英文 Electronic Commerce，简写为 EC，指的是利用简单、快捷、低成本的电子通讯方式，买卖双方互不见面地进行各种商务活动和事务活动。由于电子商务真正的发展是建立在 Internet 技术上的，所以也有人把电子商务简称为 IC（Internet Commerce）。

何谓电子商务？目前存在着各种各样的说法，例如，一些人认为，电子商务是从售前服务到售后服务的各个环节全部实现电子化和自动化；也有人认为，电子商务是一种在商业运作过程中实现无纸化、直接化的操作；更多的人认为，电子商务就是利用电子手段的购物活动，或者说是利用计算机网络进行的购物活动；还有人认为，电子商务有广义和狭义之分。广义的说，电子商务是指在计算机与通信网络的基础上，利用电子工具实现商业交换和商业作业活动的全过程，亦称作电子商业（E-business），如市场分析、客户管理、资源调配、企业决策等。而狭义的电子商务也称作电子交易（E-commerce），主要是指利用 Web 提供的通信手段在网上进行的商业贸易活动和事务活动。

各异的说法时常会令希望了解这一新生事物的人们无所适从。实际上，电子商务并不神秘。它在全球各地，包括中国在内，已经有着许多成功的实践，人们可以通过这些成功的实践来了解它和熟悉它。虽然人们对电子商务的概念有不同的理解，但从计算机与商业结合的角度，我们可以给出一个较为科学的定义。

所谓电子商务就是指整个事务活动和贸易活动的电子化。它将信息网、金融网、物流网结合起来，把事务活动和贸易活动中发生关系的各方有机地联系起来，使得信息流、资金流、实物流迅速流动，极大地方便了各种事务活动和贸易活动。

电子商务完备的双向信息沟通、灵活的交易手段和快速的交货方式将给我们带来巨大的经济效益，促进社会生产力的大幅度提高；电子商务的广泛推行，将大大加速整个社会的商品流通，有助于降低企业的成本，提高企业的竞争能力；电子商务也将为消费者提供更多的消费选择，使消费者得到更多的实惠。这是一场商业领域的根本性革命，它打破了时空的局限，改变了贸易形态。

随着电子商务的迅速发展，电子商务在给人们带来便利与经济效益的同时，其安全性问题也更为突出。

二、关于安全电子商务的内涵

对于安全的概念有不同的解释，但从本质上讲，互联网络的安全性一般包括访问控制安全和信息传输安全。从互联网络信息的层次来分，安全性包括网络层的安全性、传输层的安全性、应用层的安全性。按照实施安全措施的对象来看，可以分为物理安全、运行管理安全、数据库资源的安全等等。

安全电子商务的提出，是由于电子商务中的支付环节是将传统方式下的信用卡消费转移至公共信息网——Internet，于是就对网上支付系统的安全机制提出了更高的要求，国内大多数人士认为，从具体方面来讲，实现安全电子商务要解决以下四个问题：

(1) 应有足够的技术手段来保证数据（特别是信用卡号与付款金额）在传输作业中不被非法截获，帐户中的现金不被窃取。

(2) 应有足够的技术手段来验证传输数据的完整性，如防止交易双方按照不完整数据来处理交易。

(3) 应有足够的技术手段来确认交易双方的身份，例如，客户要通过身份认证来确认他选购商品的商店是否具有合法身份，是不是真实的商店等。

(4) 应有足够的技术手段来保证交易各方对所做过的交易无

法进行抵赖。

能够满足上述安全机制的电子商务即称之为安全电子商务。

三、电子商务的主要安全隐患

从国内相关资料的分析中了解到，目前开展电子商务的主要安全隐患有：

(1) 恶意中断系统——破坏系统的有效性

电子商务以电子形式取代了纸张，网络故障、操作错误、应用程序错误、硬件故障、系统软件错误及计算机病毒都能导致系统不能正常工作。因而有必要对由此所产生的潜在威胁加以控制和预防，以保证贸易数据与信息在确定的时刻、确定的地点是有效的。

(2) 窃听信息——破坏系统的机密性

攻击者可能通过互联网、公共电话网搭线或在电磁波辐射范围内安装截收装置等方式，截获传输的机密信息，或通过对信息流量和流向、通信频度和长度等参数的分析，推断出有用信息，如消费的银行帐号、密码等。

(3) 篡改信息——破坏系统的完整性

电子商务简化了贸易的过程，减少了人为的干预，但同时也带来了如何维护贸易各方商业信息的完整和统一的问题。这是因为，数据输入时的意外差错或欺诈行为，都可能导致贸易各方信息的差异。此外，数据传输过程中信息的丢失、重复或传送的次序差异也会导致贸易各方信息的不同。而贸易各方信息的完整性将影响到贸易各方的交易和经营策略。因此，很有必要预防对信息的随意生成、修改、删除或者插入，并要防止数据传送过程中信息的丢失和重复，保证信息传送次序的统一。

(4) 假冒他人身份

电子商务可能直接关系到贸易双方的商业交易，如何确定要进行交易的贸易方正是所期望的贸易方则是保证电子商务顺利进行的关键。在传统的纸上贸易中，贸易双方通过在交易合同、契约或贸易单据等书面文件上手写签名或印章来鉴别贸易伙伴，确定合同、契约、单据的可靠性并预防抵赖行为的发生。这也就是