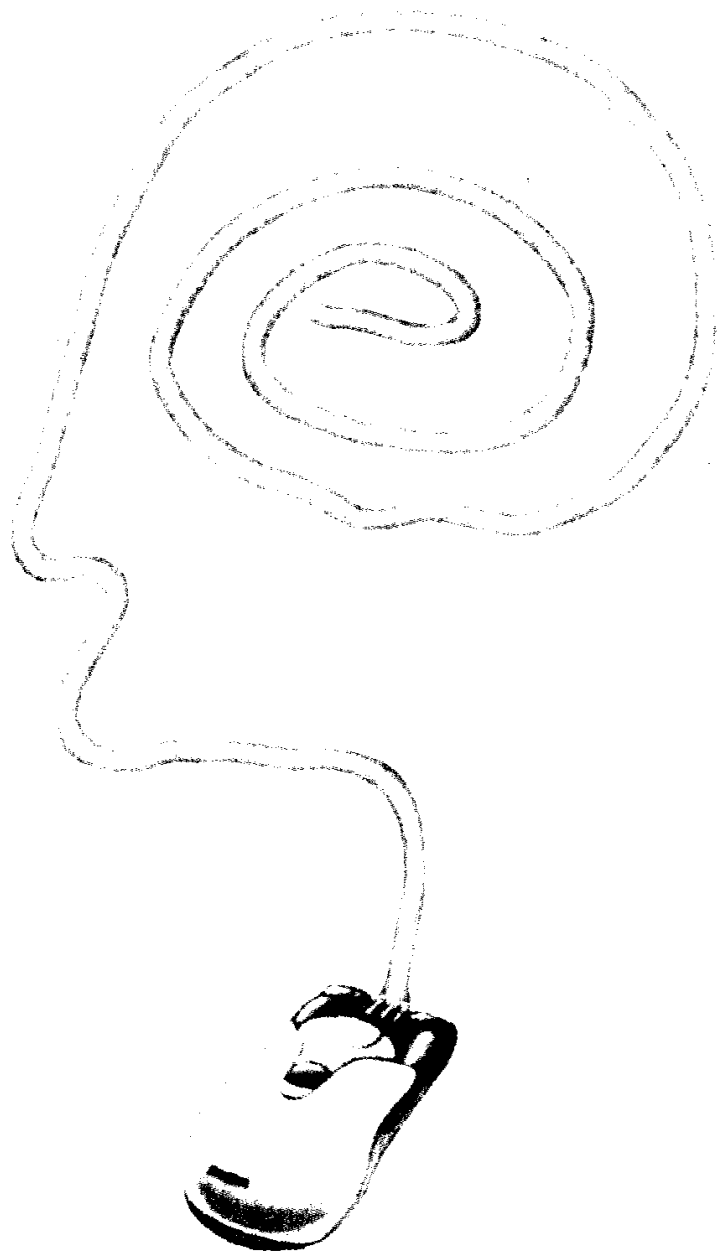
电子商务核心理论与技术实现



刘志凌 编著

国防工业出版社
·北京·

图书在版编目(CIP)数据

电子商务核心理论与技术实现/刘志凌编著.—北京：国防工业出版社，2001.7
ISBN 7-118-02537-2

Ⅰ.电… Ⅱ.刘… Ⅲ.电子商务 Ⅳ.F713.36

中国版本图书馆 CIP 数据核字(2001)第 23035 号

国防工业出版社出版发行
(北京市海淀区紫竹院南路 23 号)
(邮政编码 100044)
北京奥隆印刷厂印刷
新华书店经售
*
开本 787×1092 1/16 印张 20½ 474 千字
2001 年 7 月第 1 版 2001 年 7 月北京第 1 次印刷
印数：1—3000 册 定价：29.00 元

内 容 简 介

电子商务是目前计算机界最热门的话题之一。一方面，它具有巨大的市场潜力；另一方面，它也存在许多安全性问题。本书旨在向有心在电子商务方面做研究或开发的读者提供电子商务的运作原理和开发技巧及方法。全书共分两大部分：第一部分是电子商务的原理篇，它介绍了电子商务的基本运作过程和目前在电子商务中最流行的两个安全问题解决方案 SET 和 PKI。书中还对 SET 和 PKI 中都涉及到的安全协议 SSL 进行了详细的介绍。原理篇旨在帮助读者了解电子商务的内部机制，并且为开发做一个充分的准备。第二部分是实践的内容。它着重介绍了在电子商务中有重要作用的目录的体系结构和编程接口。书中重点介绍了目录的 C 语言接口和 SDK，同时也对 JAVA 接口作了简单介绍。

本书是理论和实践相结合的参考书籍，是那些想了解电子商务并希望在这方面有所作为的人士的理想选择。

前　言

随着计算机、网络、信息技术的发展和日益融合，Internet 已进入我们社会生活的各个领域和环节。尤其是基于 Internet 的电子商务(E-Commerce)的出现，更是给传统的交易方式带来了一场革命。电子商务除了具有使得市场变得全球化，降低了生产成本，提高了效率，减短了生产周期等特点之外，它还提供了支持服务，网上供货等新的产品和服务，从而以高效低价的模式给消费者和商家带来全新的世界。

21 世纪将是电子商务的时代，这是勿庸置疑的。而且发达国家已经将这一技术充分运用到现代商务活动的各个环节中去。专家预测网络零售到 2002 年的销售额就将达到 260 亿美元，而企业之间的电子商务往来将达到 2680 亿美元。Gartner 集团总裁 BruceGuptill 曾说："如果一家公司到 1998 年年底还没有制定出一个企业级电子商务战略的话，那么它在未来 5 年的销售中将不具备丝毫的竞争力。"世界范围的电子商务就如一场竞争激烈的竞技比赛，而对于角逐这场比赛的企业来说，无论多么令人振奋的数字预测都是次要的，重要的是如何在这块巨大的蛋糕中分得一块。

电子商务的问题集中体现在安全问题上。电子商务要求个人隐私和金融信息的严格保密及高可靠性，这与 Internet 的广泛互联性和开放性有所矛盾。这样，商户和客户之间的信任需要借助特殊的技术和一个权威的、可信赖的第三方来得以建立。数字证书(Certificate)认证是通过运用对称、非对称密码体制，及数字签名等密码技术而建立起一套严密的身份认证系统。它可为电子商务提供技术保障。而证书认证中心(Certificate Authority，简称 CA)则是我们需要的第三方，它专门负责数字证书的发放和管理，确保网上信息的安全，它在电子商务中的作用至关重要。

CA 的运作是公钥基础设施(Public Key Infrastructure，简称 PKI)的一部分。PKI 的核心是对数字证书生命周期的管理。数字证书的生命周期，包括了密钥生成、证书申请、证书签发、证书使用、证书审核、证书销毁等一系列过程。在整个周期中，数字证书担负着保证网上信息安全交流的责任。具体而言，它应提供：

- 保密性(Confidentiality)
- 访问控制(Access Control)
- 身份认证(Authentication)
- 数据完整性(Data Integrity)
- 不可否认性(Non-Repudiation)

同时具备：

- 开放性
- 高效性
- 可扩展性

• 通用性

对于一个企业来说，电子商务意味着运作模式和运营技术方面的革新。本书讨论的内容是电子商务运营技术的核心：安全技术。对于这些安全技术，有许多书籍从应用一面对它们进行过介绍。但对于技术本身而言，却鲜有介绍。然而，要想成为一个得心应手的应用开发人员，必要的原理是必须了解的。当你读完本书，会发现它能使你对电子商务有更深一层的认识。

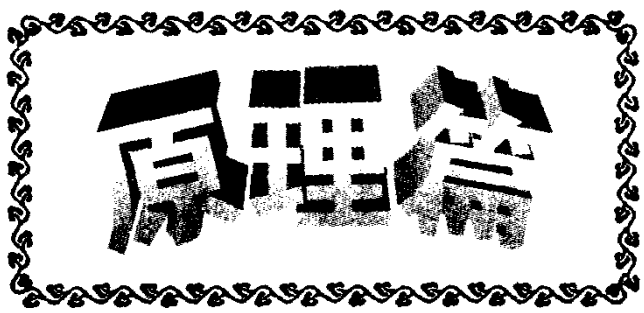
本书我们假定读者已经掌握了至少一种编程语言以及具有中级编程能力，这能使你很容易地理解书中的内容。如果你熟悉 C 语言，那么你可以从本书中得到更多的收获。

本书主要由刘志凌编写，同时参加编写的人员还有：徐佳、黄舒、刘宝锋、吴铮、胡皓、罗远华、林琼、蒙文荣、黄建森、康永宏、郑国鸿、张劲松、郑清初、林振宁、周成福、陈培、黄强等，在此表示感谢。

目　录

原　理　篇

实 践 篇



第1章 概 述

1.1 电子商务简介

有人指出，信息时代就是缩略语的时代。从历史性的 PC 开始，到数据库（DB）、网络计算机（NC）、即插即用（PnP），以及 HTML、ADSL、ATM、TCO 等等，缩略语的数量可以说是按几何级数增长的。可怜的用户，就像苦苦赶考的书生一样，不停地结识、搬弄、记忆、吞咽着大量“压缩饼干”似的名词和术语。不过最近的风向有所不同，如果说以往出现的词汇，尚有“先上车后买票”的迹象的话，现在的风格则多属于“先买票后上车”，电子商务当属一例。

随着 Internet 进入我们社会生活的各个领域和环节，无论是机关、单位还是个人，都可以通过 Internet 获取信息资源，实现资源共享。当基于 Internet 的电子商务（E-Commerce）出现的时候，标志着 Internet 的影响力已深入到了交易这一人类最重要的社会活动之一。并且，它正给传统的交易方式带来一场革命。据一些媒体在 1998 年引用某些预测公司的数据和说法，电子商务的销售额将从现在的 30 亿美元上升到 2001 年的 2200 亿美元，在线购物的比重将从现在的 12%上升到 2000 年的 30%；1998 年末，Internet 用户达 9000 万，2000 年超过 2 亿；1998 年，Web 在线交易达 200 亿美元，是 1997 年（70 亿）的 3 倍。下面的这张来自 PSI Global Consulting 的图可以看出人们支付手段的电子化趋势。

IBM 已经荣膺“当代电子商务开山鼻祖”的雅号，其观点的公式是：Web＋IT=电子商务。但是按照一些持不同观点者的看法，电子商务早在 20 年前商贸界鼓吹“电子单证”的时代就有了。所不同的是，后来给电子商务起名字的时候流年不利，ElectronicCommerce 的称呼没有获得众人的青睐。据说，电子商务的概念并不是 IBM 拍脑门拍出来的，而是经过了一番调查研究：IBM 完成了企业界有史以来最大规模的“电子商务与企业经营”调查研究，包括对全球银行、保险、公共事业、零售及信息服务等行业的 170 位以上的最高决策主管进行访谈，对 550 位以上的高级主管进行问卷调查，以及举行超过 400 人次的各种工作座谈会。经过详细的分析，IBM 发现，电子商务策略的确已经为若干企业带来了革命性的竞争优势。IBM 认为，电子商务简单地说是一种存

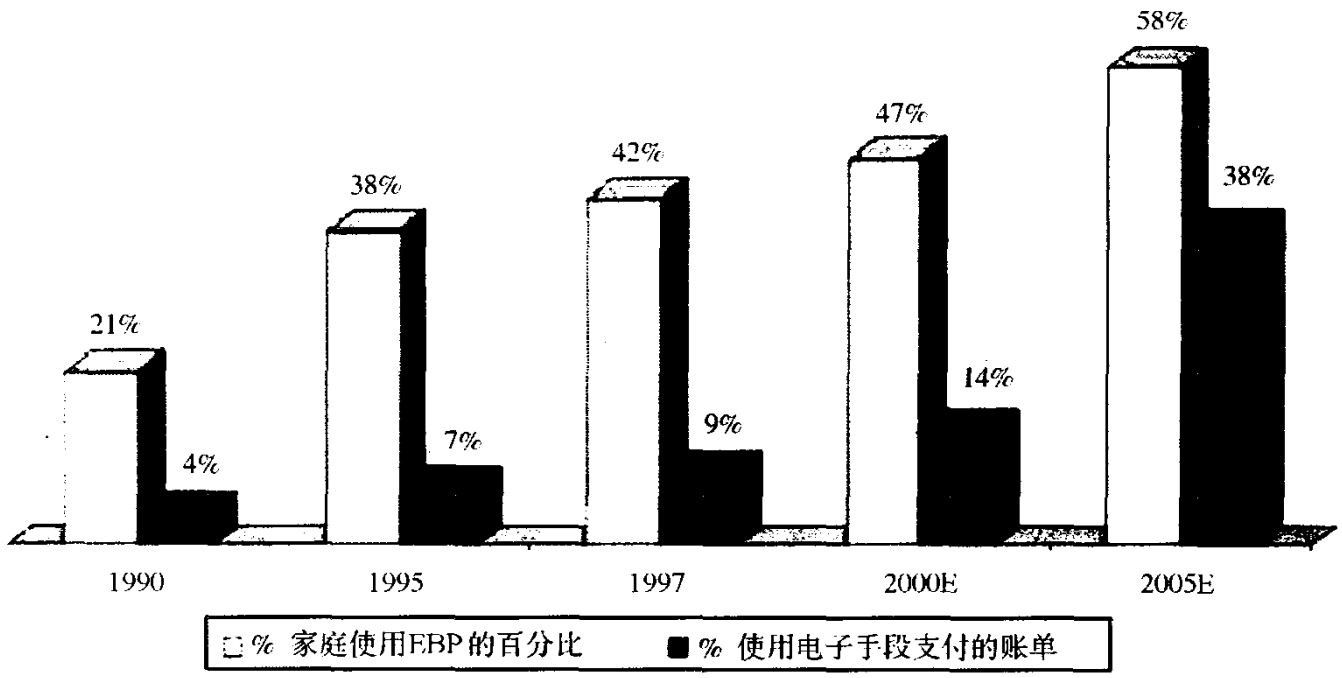


图 1.1　电子化趋势

在于企业与企业之间、企业与客户之间、企业内部的联系网络；Internet 为企业和客户提供相互沟通的新渠道；Intranet 是企业内部网，共享程序与信息、增强员工之间的协作，简化工作流程；Extranet 则涵盖企业和协作厂商之间的联系。电子商务始于网络计算，网络计算提供了技术平台，电子商务则是网络计算的最新应用和最终目标。

电子商务究竟是 ElectronicCommerce，还是 ElectronicBusiness？有人认为 EB 涵盖 EC，EC 强调的是有交易意识的、直接的电子商业行为，范围比 EB 小，但却是 EB 的主要和精华部分。有观点认为，EC 包括早一些的电子数据交换（Electronic Data Interchange, EDI）和相对新一些的 Internet 商务，如在线商店等 Web 业务。电子商务的非 EDI 部分称为 Internet 商务，如 Internet 数据库、在线商店、在线目录、电子邮件等，电子商务的平台是 Internet。那些关心电子商务能带来多大市场和潜在客户的公司已经脚踏实地地做出一番行动。微软与 NCR 达成协议，开发集成化数据仓库、电子商务、高可用性技术和应用程序等。再比如 HP 提出以现代扩展型企业为信息技术基础结构，建立由电子商务 EC，电子业务 EB，电子消费 E-Consumer 为基础的电子化世界 E-World。HP 认为，变换企业业务运作模式、改变企业竞争策略、提升企业间业务合作伙伴关系，是企业在 EW 中获得成功的关键。通过与微软合作，HP 将对现有平台 PA-RISC、IA-32 和未来 IA-64 的 HP 产品全线优化，与 Intel 合作开发 64 位计算微处理器结构，并联合定义了新型并行事务处理技术 EPIC。除此之外，HP 还提出了具体的性能指标：保证用户平均开机率达到 99.99%以上，即每年停机时间不超过 4.5 小时。

到底为什么那么多商家对电子商务感兴趣呢？E-Commerce 究竟有什么好处？现在看来，电子商务给交易活动带来了以下几点主要的变革：

（1）市场变得全球化。商家和客户之间的关系再也不受限于地域和国家边界，而只受到计算机互联网络覆盖范围的限制。

（2）降低了生产成本。由于获取信息成本下降，致使厂商一方面可以更多地了解原材料价格，从而选取价格较低的原材料；另一方面，厂商的产品信息面向的是互联网上的所有用户，其涉及面之大是任何媒体无法比拟的，而其成本之低，也是其他媒体望而兴叹的。

（3）缩短了生产周期、供求反应，提高了效率。通过电子商务，商家几乎是直接与用户进行沟通，使得它们更加“贴近消费者”，从而更有竞争力。在价格每周下降5%的PC市场上，竞争十分残酷，商家每多一天的存货就意味着多一部分损失。Compaq在收购了Digital公司之后一跃成为IT界第二大厂商，仅次于IBM。然而，由于稳定保持一周左右的存货，Compaq公司在PC市场上竞争力逐渐下降，股票价值下跌不止。相比之下，较小的Dell公司由于采取了网上直销方式，使其存货基本为零，抢占了大部分市场份额。

（4）提供了新的产品和服务。电子商务提供了支持服务、网上供货等新的产品和服务。消费者处于一个全新的世界，而厂商则面对着更多的契机。

Internet的蓬勃发展，为电子商务开启了方便之门，但是，要通过Internet全面地开展电子商务，还面临着诸多实际问题。主要体现在如下几个方面：

- 付款认证问题
- 安全问题
- 商品投送保证
- 缺乏统一的国际标准
- 法律法规不健全
- 国家之间的经济冲突妨碍电子商务的全球化进程

1.2 如何实现网上交易

1.2.1 传统交易和网上交易

传统的交易与网上交易有两点最明显的不同：

（1）传统交易中，交易双方间的信任关系比较容易建立，而在电子商务中，交易双方之间要通过特殊的手段来建立相互间的信任。

传统的交易是发生在现实生活中的，它具有可检验性。当你去买苹果时，你可以看到苹果的大小、颜色；你可以仔细检查它是否腐坏了；你甚至可以先尝一尝味道再决定购买。当你把钞票交给商人的时候，你手中已经拿到了你所想要得到的苹果。网上交易是发生在虚拟世界（Virtual Reality）中，交易双方是通过互联网相互沟通的。这种情况下，问题就不那么简单了。作为消费者，你首先要确信对方商家“确有其人”。这听起来很滑稽，但仔细一想，如何面对终端来检验对方的身份确实是个问题。其次，你必须能确定在付出钱后会收到你所需要的东西。最后，你还必须确信商家不会否认其行为。这样，当你收到的是坏苹果时，你可以根据记录寻求赔偿。同样的，对于商家而言，也面临类似的问题。并且，商家可能还要跟银行等金融机构打交道，因为你不会当面把钱

交给他，这个过程将通过金融中介来完成。

（2）传统的交易是面对面的，双方间几乎没有通信安全性问题；而对于网上交易，安全问题成为了交易是否成功的关键。消费者还必须有信息传输方面的安全保证。只有当信息可以安全送到目的地，而没有被篡改或是截取时，双方间可信的通信才能成为现实。在这个黑客横行的世界中，安全问题变得更加棘手而重要。

下面，将典型的网络交易过程做一个描述：

（1）客户上网浏览商家网页，选择想要的商品，并把购买命令发送给商家。

（2）商家激活用户的电子钱包软件，进入安全电子购物状态。

（3）客户的电子钱包软件自动索取并验证商家的数字证书、网关数字证书。如果通过，则向商家系统发送附有订单指令和付款指令的购物请求。

（4）商家系统接收客户的购物请求，验证其数字证书。如果验证通过，则向客户返回“订单收到”信息。

（5）商家系统将客户的付款指令转送支付网关系统。

（6）支付网关系统根据付款指令，通过金融网络向客户的授权金融机构（如：银行）验证客户的账户余额，如果余额允许，则完成支付授权。

（7）商家系统得到支付网关发回的响应后，从中获取支付令牌（Captoken），然后发送货物。

（8）客户进行查询请求。当从商户处得知“支付已授权”，表明商家已按要求发送出货物，客户只需等待货物到达。

（9）商家系统在恰当的时机（因为业务是批处理的），使用支付令牌，向支付网关请求完成从客户授权银行到商家获款银行的划款。

（10）支付网关得到商家的划款请求，验证通过支付令牌，实现银行划款。

（11)在交易的过程中，商家系统还可以向支付网关提出授权更改、划款更改，甚至退款。

（12）交易双方保留交易记录，以备查证。

1.2.2 网上交易的技术保障

电子商务要求个人隐私和金融信息的严格保密及高可靠性，这与 Internet 的广泛互联性和开放性有所矛盾。日益严重的电脑安全问题构成了对电子商务系统的威胁。常见的网络犯罪有：

- 窃听敏感信息
- 截断信息传输
- 伪装身份
- 篡改传输中的信息
- 恶意抵赖
- 对信息进行重发

因此，要使电子商务正常运行，从技术上必须保证：

(1) 保密性（Confidentiality）：数据经过加密，以防止未经授权的他人访问或修改。

(2) 访问控制（Access Control）：数据经过压缩处理，只有用特殊的压缩格式才可访问加密过的数据。

(3) 身份认证（Authentication）：用户可以在网上向其他客户证明自己的身份而不用通过网络发送私有信息（如密码，密钥等）。

(4) 数据完整性（Data Integrity）：收方所得数据正是发方所发的原文，而没有经过篡改。

(5) 不可否认性（Non-Repudiation）：客户一旦发出数据，无法否认其发送行为。

要实现这些，就必须有一个系统，来提供安全技术支持。数字证书（Certificate）认证是通过运用对称、非对称密码体制，及数字签名等密码技术而建立起的一套严密的身份认证系统，它可为电子商务提供技术保障。

1.2.3　网上交易信任的建立

除了安全问题外，网上交易最重要的一点就是建立买卖双方间的信任关系，这也是交易的基础。由于网络世界是虚拟的，“信任”在其中出现了新的问题。本节在理论上对“信任”和“信任模型”进行了阐述。这些枯燥的理论对今后认证中心的体系结构及实现有很大的帮助。

1. 数字认证中心(CA)和 PKI

1) 什么是数字证书(Certificate)

为实现信息安全要求，除了在通信传输中采用更强的加密算法之外，必须建立一种责任及信任验证机制，即参加电子商务的各方必须有一个可以被验证的标识，这就是我们所说的数字证书。

回想一下我们正常意义下的证书。它们是由某个机构，如政府、学校等颁发的，作为某种凭证的东西。当我们去招聘会上想谋求“一官半职”的时候，我们拿着大学毕业证给用人单位，希望通过它来表明我们具有工作的能力。同样的，用人单位也纷纷拿出自己的资质证明，希望以此树立其良好的形象，从而能有更多优秀毕业生应聘。可见，证书的目的是用来对自身的某种属性、特点给以证明的客观凭证。当你出示你的毕业证并被对方认可之时，你们之间已经建立了某种信任关系。

那么，为什么人们仅仅凭着一张写有字迹的纸就可以建立信任关系呢？实际上，这个关系来之并不容易。这张纸上，不仅仅有对你已经毕业这个事实的说明，而且还有你毕业学校的印章，或许还有你的校长签名。这些，都表示“你毕业”这个事实是被校方认可的。当用人单位看到证书的时候，它和你之间的信任是通过校方而建立起来的。这是一个典型的通过第三方建立信任的例子。当双方无法进行足够的检验活动以了解对方时，双方的信任必须通过双方都信赖的第三方来实现。在我们的例子中，学校、政府都是扮演着第三方的角色。

回到我们的网络世界中，数字证书也和普通意义上的证书一样起到证明某种性质，帮助建立某种信任关系的作用。由于网络世界是虚拟世界，信任更加需要可靠的第三方来帮助实现。虽然数字证书和普通的证书表面是一致的，但在具体实现上，数字证书面

临着很多新的问题。首先，数字证书必须是唯一的，而普通的证书却没有明确的要求。如果你的学校里有人和你同名，这并不影响你们俩的毕业证颁发，而且证书上你也不会被迫改名。其次，普通证书是实实在在的“白纸黑字”，它看得见、摸得着；就其内容来说，它明确记载了需要证明的特性，容易被人理解。而数字证书存在于以 0 和 1 为基础的计算机世界中，它到底是什么东西？再者，普通证书上最重要的一点是要有可靠的第三方的签名，这实际上是信任传递的工具。当接受方看到第三方签名时，他才会确信这份证书是有效的证书。同样，数字证书也需要这样的工具来传递信任，那么在计算机中是怎样做的呢？这些问题在学习完 PKI 时将得到解答。读者在读完关于目录一部分内容时，会对它们有更现实的了解。

2) 通过第三方证明自己的身份

正如上面所述，信任是通过第三方建立的。这就意味着应有一个在网上大家都信任的机构，专门负责数字证书的发放和管理，确保网上信息安全，这个机构就是数字认证中心（Certificate Authority, 简称 CA）。CA 是整个网上电子交易安全的关键环节。它主要负责产生、分配并管理所有参与网上交易的个体所需的身份认证数字证书。每一份数字证书都与上一级的数字签名证书相关联，最终通过安全链追溯到一个已知的并被广泛认可为安全、权威、足以信赖的机构。

CA 是有一定区域性的，不同的 CA 以某种结构方式（如：层次（Hierarchy）结构、交叉（Cross）结构等）形成不同级别。各级 CA 认证机构的存在组成了整个电子商务的信任链。具体的 CA 体系结构是我们下面要讨论的。

电子交易的各方都必须拥有合法的身份，即由数字证书认证中心机构签发的数字证书。在交易的各个环节，交易的各方都需检验对方数字证书的有效性。CA 涉及到电子交易中各交易方的身份信息、严格的加密技术和认证程序。基于其牢固的安全机制，CA 的应用可扩大到一切有安全要求的网上数据传输服务。

3) 什么是 PKI

随着 Internet 的普及，越来越多的单位和个人开始使用这一新兴的通信媒体。Internet 的主旨之一就是尽可能地让所有用户共享信息资源，这就决定了它固有的高度不设防性。由于众多的网络相互连接，使得 Internet 又有管理松散的特点。正因为这样，它被称为非安全网络（Insecure Network）。这意味着在 Internet 上传递的应该是一些公众可以共享的、不具有任何敏感性的信息。当人们要在 Internet 上作交易的时候，上述特点和交易的私有性、个人信息不可侵犯性发生了矛盾。为了解决这个问题，我们将求援之手伸向了密码学。通过密码学中一些可靠的算法把将在 Internet 上传送的内容加密后再送出，以此克服原来的安全缺陷。

在众多的加密算法之中，公钥加密算法（也称为非对称加密算法）是被比较广泛使用的一种。由于它具有良好的性质，可以保证网络的安全传输、身份认证等问题很容易地解决，现在，以公钥加密算法加密为数字签名提供网络安全性的机制已广泛为人们所接受。

基于非对称算法的公钥基础设施（Public Key Infrastructure, 简称 PKI）是提供公钥加密和数字签名服务的标准，其核心是对密钥生命周期和数字证书的管理。它是解决互

联网络安全问题的基础机制。有关 PKI 和加密算法将在第 2 章详细讨论，在这里，我们仅仅将非对称加密算法当作是用一个“保险箱”把“贵重物品”锁在其中，而所谓的密钥则是打开“保险箱”唯一的钥匙。

密钥的生命周期，如图 1.2 所示，其中包括了密钥生成、数字证书申请、数字证书签发、密钥使用、数字证书审核、密钥销毁等一系列过程。在整个周期中，密钥担负着保证网上信息安全交流的责任。

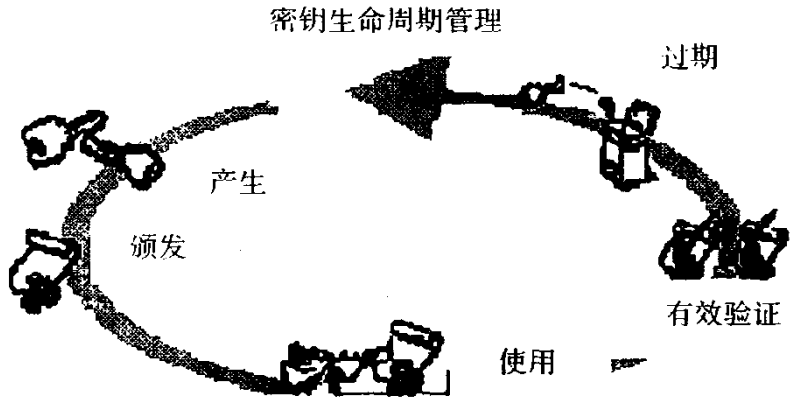


图 1.2 密钥的生命周期

不同厂商根据 PKI 的功能要求所开发出的系统大相径庭，但是仔细研究各厂商的产品后会发现他们的系统中有两个最重要的功能模块都是非常相似的。其一是负责签发和管理数字证书的 CA；另一个则是负责存储和管理密钥的目录。实际上，PKI 的大多数功能都是基于目录的应用，因此，在 PKI 的实现上目录是核心问题。CA 给每个用户唯一的公钥,它就像是一把“保险箱”的钥匙，是打开“保险箱”的唯一正常途径。每当我们收到加密信息的时候，我们都需要它来对密文解密。值得注意的是，此处所谓的“惟一”不仅仅是在当前环境下的惟一，在整个历史中也应有惟一性，因为每次颁发的公共密钥不可以和曾经使用过的公共密钥相同。至此，我们可以回答上面提出的问题。我们可以把数字证书视为将 CA 的公开密钥和持证实体本身联系在一起的数据结构，它具有对于实体的惟一性。具体一点，数字证书是一段经过加密的数据，其加密前的内容是一些关于认证 CA 的信息和持证实体的公共密钥。而对证书内容加密的过程就如同签发 CA 把自己的“印章”盖在了证书上，这样，就解决了传递信任的问题。关于目录、公钥、异名等概念将在后几章中详细说明。

2. 信任理论

电子商务中的问题集中体现在“信任”二字上。在建立信任的方法中，理论上有许多模式。正是基于它们，现实中的 CA 体系结构得以实现和完善。目前，流行的 CA 结构有层次型和交叉型两种。它们到底是什么含义，下面的内容可以帮助你的理解。要说明一点，我们将要谈到的“信任”以及“信任模型”都是就电子商务而言的，更具体一点，都是在 PKI 范围之中的。

1) 信任关系

在说“信任”之前，这里先给出关于数字证书的国际标准 X.509 中对它的定义：“当

一个实体认为另一个实体的行为将是按照它（实体 1）所设想的那样时，我们说实体 1 信任实体 2。”

当然，实体 1 对实体 2 的设想应该局限于某一个范围之内，而我们所说的“信任”也是属于那样一个范围的。在这里，我们讨论的行为局限于在电子商务中散播和使用公共密钥。在这些过程中，不同的信任关系所能传递的信任类型是不一样的。基于公钥加密技术的信任关系是为了确保双方实体身份的真实性和约束双方履行自身的职责。

在日常生活中，信任的例子屡见不鲜。银行和储户，政府和公民，出版商和读者等等，他们之间的关系是如何建立起来的？条件是什么？这些问题已经超出了本书的讨论范围，我们权且把它们当作是数学论证中的公理。

在 PKI 领域中，建立信任关系所必须的一步就是：一个实体（A）从另一个实体（B）那儿获取一把公共密钥并用它来保证 A 和 B 之间的通信安全。得到公共密钥的实体称之为依赖方（Relying Party），之所以称为“依赖”，是因为它要依靠所得的密钥来实现之后的一切安全交流。另一方则被称为密钥持有者（Key Holder），因为它是拥有散发密钥权力的实体。当然，任何实体在这个关系中都可以是双向的，即一个实体可以同时具有“双重身份”，既为依赖方，又为密钥持有者。事实上，大多数情况下实体都具有“双重身份”，二者关系如图 1.3 所示。

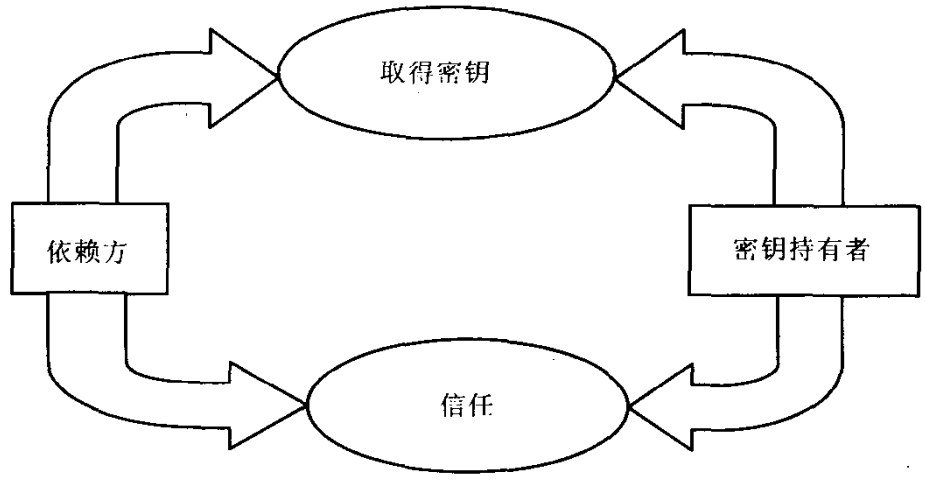


图 1.3　依赖方和密钥持有者

这其中的获取密钥过程必须以一种可以保证密钥的真实性和完整性的形式进行。也就是说，必须保证密钥安全地被接收到；途中没有被改动过；并且这把密钥是可信任的密钥持有者颁发的；在密钥的使用上，依赖方和密钥持有者的理解应该是一致的。这一系列的安全要求实际上是一个建立信任的过程。可以说，在这个过程建立之前，双方不存在信任关系。这样，我们好像是进入了一个循环：一方面依赖方要靠所得的密钥和密钥持有者建立信赖关系，密钥的用途是用来保证安全传输的，它实际上是传递信任的工具；另一方面，密钥获得的过程必须是安全的，也就是说，这个过程必须是在某种信任业已存在的基础之上实现的。如此看来，如果没有已存在的信任关系，似乎新的信任关系是无法“创建”的。的确，事实就是如此。业已存在的信任关系只可以被“检验”和“组合”以构成具有新特性的信任关系。我们在这里只不过是用已存在的信任关系

（如：银行和储户，政府和公民等）和公钥加密技术来建立一些有我们所需要的特点的信任关系。

下面给出PKI中最简单的一种建立信任的方式。它虽然十分简单，但它仍然是用已有的关系来建立新得信任，并且它保证了真实、完整和清晰的特性。

图1.4表现了这个简单过程中的数据流向。在这里，浅色的箭头表示的是在已有的信任关系下数据的传递；深色的箭头表示了第一次接触后的数据交换，它通常是自动完成的。前者我们视为完全可信，可靠的。而后者的可信度要根据前者的内容而定。通常，人们都是要在已有的信任关系下进行一番接触，之后才有在PKI意义上的交流。在现实生活中，我们申请信用卡是一个与之极其相似的例子。我们总是必须亲身走到银行去填写申请表格。银行和我们之间的信任关系是长久以来形成的。凭着这份关系，我们得到了一张信用卡，而信用卡的密码却可能是用一个密封的信封装着送到我们的手中。

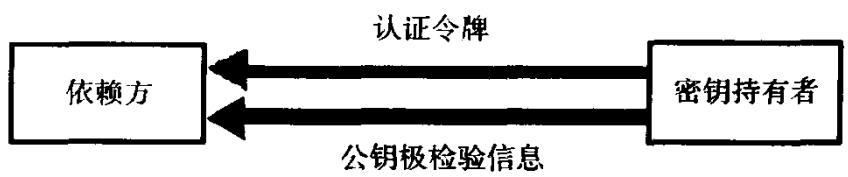


图1.4 简单地建立信任

在这个例子中，认证令牌可以用一种可读字符串的形式，使依赖方可以方便地在计算机上很容易地阅读和写入。或者它也可以是某种双方事先约定好的密文，当然这段密文是和公共密钥以及检验信息相关的。认证令牌的可靠传输要依靠现有的信任关系。之后，公共密钥和检验信息的真实性和完整性就依靠于认证令牌了。可以看出，认证令牌实际上起到公共密钥的“密码”的作用。那为什么不直接将公共密钥以传统的方式交给依赖方呢？原因主要是因为公共密钥的存在形式是一个数据结构，将其存放在计算机中要比将其固化成物理形式安全得多，不会损坏和遗失，也不易被人窃取。以传统方式取得认证令牌，再依靠它自动得到公共密钥，可以很简单地实现。

检验信息中最重要的一项就是密钥持有者的描述符。这个描述符可以是共享的或是惟一的。例如，它可以是密钥持有者的名字，或是几个共享名称的组合。在许多应用中，依赖方的最终目的是从密钥持有者那里得到某种特权。它也可以用密钥持有者的公钥来对其身份进行认证。但这只不过是授权的第一步而已。在其他情况下，检验信息可以直接提供对密钥持有者权力的证明。在那些内部服务和处理个人信息的应用中，也许只需要密钥持有者的身份描述符就足够了。具体选择哪一种策略没有一个固定不变的格式，它取决于所希望达到的安全级别、所采用的安全策略和周围的环境。

2) 信任与风险

根据X.509标准对“信任”的定义，被信任方的行为并不是必须像信任方那样所设想的。也就是说，信任不是“公平”的。存在这样的风险，密钥持有者的行为可能不会像依赖方所期望的那样。这种例子在PKI中有很多，诸如：