宁宇鹏　陈　昕　等编著

PKI技术

国家信息化安全教育认证(ISEC)系列教材

械工业出版社
NA MACHINE PRESS


PKI技术

国家信息化安全教育认证(ISEC)系列教材

PKI 技 术

宁宇鹏 陈 昕 等编著

机 械 工 业 出 版 社

PKI(公钥基础设施)是一种利用密码技术为网上安全通信提供一整套安全服务的基础平台。如同其他基础设施(电力、水利基础设施)一样,公钥基础设施也一样能为各种不同安全需求的用户,提供各种不同的安全服务。本书分为四部分,共 10 章。第一部分为基础知识,主要介绍了 PKI 的概念、主要内容、理论基础;第二部分为 PKI 体系结构,主要介绍了 PKI 体系和服务功能,以及 PKI 建设使用中所遇到的问题;第三部分 PKI 技术标准,主要介绍了现有的 PKI 技术标准体系;第四部分为应用案例,主要介绍了现有利用 PKI 实现的安全协议,以及网上银行、网上证券及电子税务的 PKI 应用系统。

本书适用于准备参加"国家信息化安全教育认证(ISEC)"考试的人员,还适合信息产业相关管理部门人员、PKI 建设运营人员、IT 人员及有关业务人员学习和参考,也可作为大专院校有关专业的参考教材和电子政务、电子商务的培训教材。

图书在版编目(CIP)数据

PKI 技术/宁宇鹏等编著. —北京:机械工业出版社,2004.3
(国家信息化安全教育认证(ISEC)系列教材)
ISBN 7-111-14168-7

Ⅰ.P... Ⅱ.宁... Ⅲ.电子商务—安全技术—资格考核—教材
Ⅳ.F713.36

中国版本图书馆 CIP 数据核字(2004)第 019297 号

机械工业出版社 (北京市百万庄大街 22 号 邮政编码 100037)
责任编辑:孙 业
责任印制:洪汉军
三河市宏达印刷有限公司印刷·新华书店北京发行所发行
2004 年 4 月第 1 版·第 1 次印刷
787mm×1092mm 1/16 · 9.25 印张 · 219 千字
0 001—5 000 册
定价:17.00 元

国家信息化安全教育认证(ISEC)专家组

卿斯汉　中国科学院信息安全技术工程研究中心主任　研究员
曲成义　中国航天科技集团公司第710研究所总工　研究员
许榕生　中国科学院高能物理研究所计算中心研究员
贾颖禾　国务院信息化工作办公室网络与信息安全组研究员
曹元大　北京理工大学软件学院院长　博士生导师
杨义先　北京邮电大学信息安全中心主任　博士生导师
林　鹏　国家计算机网络应急技术处理协调中心广东分中心副主任
　　教授级高级工程师
祁　金　公安部公共网络信息安全监察局管理监察处副处长
井乾元　公安部公共网络信息安全监察局安全对策处副处长
万平国　国际信息战略研究中心理事　中网通讯网络有限公司董事长
刘宝旭　中国科学院高能物理研究所计算中心副研究员

教材编委会

主　任：宋　玲
副主任：赵小凡　张会生　欧阳满　蔡金荣　沈志工
成　员：洪京一　张宝泰　王　宏　孙论强　彭　澎　张晓伟
　　刘树安　刘　旸　马志谦　胡　铮　宁宇鹏　阎　慧
　　王　伟　薛静锋　辛　阳

出版说明

随着信息化在我国的不断深入和发展，信息技术和网络给社会的经济、科教、文化和管理等各个方面注入了新的活力。人们在感受它所带来的新体验、享受它为我们带来高效率的同时，也面临着日益突出的信息安全问题。党和国家领导人多次强调，必须充分认识到做好信息安全保障工作的重要性，大力搞好技术开发和人才培养。

对信息安全专业人才的需求是多层次的。从信息安全基础理论研究到新技术的开发利用，再到各级网络信息系统信息安全保障体系的建设、运行，需要根据不同要求有针对性的进行人才培养。

国家信息化安全教育认证(ISEC)项目是由信息产业部信息化推进司推出的信息安全领域的国家级认证体系。该项目由中国电子商务协会监督，由 ISEC 国家信息化安全教育认证管理中心统一管理与实施。ISEC 国家信息化安全教育认证管理中心以行业为基础、以技术为核心制定了一套面向应用的教育方案。根据工作性质的不同，教育对象被划分为规划决策层、管理运营层和操作层三个层次。认证体系的设计，课程内容及相应的教学考试大纲的编写和指定是针对三个层次人员对信息安全知识和技能的不同需求和理解程度的不同而制定的。确保不同层次，不同需求的各类人员从各自的角度充分掌握和理解信息安全的知识和技能。

本系列教材是在国家信息化安全教育认证(ISEC)专家组的指导下，由国家信息化安全教育认证(ISEC)教材编委会组织编写的。始终以 ISEC 国家信息化安全教育认证管理中心制订的各级考试大纲为依据，坚持面向行业用户的需求和侧重技术应用两个基本原则，全面地介绍了信息安全各种主流技术和管理规范，以帮助读者深入了解信息安全本质，并熟练掌握相应的技能，从而建立完备的信息安全观念。本系列教材包括：《网络安全基础》、《防火墙原理与技术》、《入侵检测技术》、《VPN 技术》、《PKI 技术》、《数据备份与灾难恢复》、《网络隔离与网闸》、《信息安全法规与标准》、《信息安全策略与机制》、《信息安全团队构建与管理》，共计 10 本。

在写作过程中，北京正阳天马信息技术有限公司为本系列教材的编写提供了很多宝贵的建议和支持。

前　言

在各种网络信息技术的应用中，保障用户的合法访问、保证数据在传输过程中的保密性以及确认发送者的合法身份是最基本的安全要求。越来越多的组织利用公开密钥基础设施(PKI)技术为用户提供信息安全服务。在我国，基于 PKI 技术的安全方案也从金融、电信等少数行业扩展到更多领域，出现在电子政务、电子商务等各类信息化应用中。

与众多广泛采用的成熟技术相比，PKI 技术还是一项新的技术，在算法、密钥管理等方面还在不断推陈出新。因此本书在写作过程中重点强调了对 PKI 技术的理解和应用，而对理论基础部分只做了简要介绍。本书以国家信息化安全教育认证(ISEC)考试大纲为依据，重点讲解了 PKI 的有关理论知识、技术标准和应用案例。全书包括 10 章内容，分别是：

➢ 第 1 章 绪论

本章介绍了 PKI 作为基础设施所必需具备的基本条件和要求，以及揭示了 PKI 的作用和功能，同时提出了 PKI 的理论基础和最新进展情况。

➢ 第 2 章 密码和密钥

本章介绍了密码学的基础知识，并详细介绍了常见的两种加密体制——“对称密码算法”和“非对称密码算法”。同时也介绍了散列算法和数字签名的基本概念和原理。最后介绍了密钥管理的有关知识。

➢ 第 3 章 数字证书和目录服务

本章介绍了数字证书的基本概念以及数字证书验证、存储等工作，同时也介绍了目录服务的基本概念以及目前常用的协议。

➢ 第 4 章 PKI 及其构件

本章在综述了 PKI 各个组成部分以后，详细介绍了各个部分的功能。

➢ 第 5 章 PKI 系统实际运作

PKI 系统在实际应用中经常会遇到很多问题，这些问题包括了信任域之间互不兼容，CPS，构建方式等等。本章针对这些问题进行了简要的描述和介绍。

➢ 第 6 章 PKI 涉及到的法律问题

PKI 的推广和正常运作一定需要有强有力的法律手段的支持。自从 20 世纪 90 年代以来，世界上各发达国家都纷纷推出了电子商务有关的法律法规，这些法律法规都或多或少地涉及了 PKI 的法律的问题。本章简要介绍了世界上主要国家的相关法律法规的情况，并对我国的 PKI 相关法律问题提出了建议和参考。

➢ 第 7 章 PKI 技术标准

PKI 自诞生至今，已经出现了很多技术标准。本章详细介绍了 PKI 的相关技术标准，如 ITU－T 系列、PKIX 系列、WPKI、SET 协议等等。

➢ 第 8 章 PKI 应用及案例

PKI 的技术非常复杂，但是在这些复杂技术的支撑下，PKI 的应用要尽量的简单、易用。

本章针对当今网络应用中的安全需求，讲述了 PKI 典型应用及案例。同时也简要介绍了国外成熟的 PKI 系统。

➢ 第 9 章 电子商务认证机构管理基础

在信息安全领域有着这样一种说法："三分技术，七分管理"，在保证信息的安全性方面管理扮演着异常重要的角色。本章介绍了中国电子商务认证机构管理中心对于我国电子商务认证机构所必需考虑的安全问题提出的具体要求。

➢ 第 10 章 电子商务认证机构可信评估

对于 CA 来说，作为一个非常复杂的信息系统，需要对其进行严格的评估，并在达到标准后才能运行。本章介绍了 CA 系统的安全风险的来源以及相关风险防范措施。

本书由宁宇鹏和陈昕等编写，其中前 7 章主要由宁宇鹏完成，后 3 章主要由陈昕完成，另外刘益良、李延昭、萨江雷、刘辛越、刘洁、杨涛海、杨广嘉、张帆也参与了本书的编写工作。本书在写作过程中得到了阎慧博士、王伟博士、薛静锋博士的热情帮助。

由于时间仓促，加之编者水平有限，书中难免存在不妥和错漏之处，恳请专家和广大读者批评指正。

编　者

目　录

第二部分 PKI 体系结构

第三部分 技 术 标 准

第四部分 应 用 案 例

第一部分　基 础 知 识

第1章　绪　　论

本章导读：

PKI——公钥基础设施，是一种运用公钥的概念与技术来实施并提供安全服务的具有普遍适用性的网络安全基础设施。本章介绍了 PKI 作为基础设施所必需具备的基本条件和要求，以及揭示了 PKI 的作用和功能，同时提出了 PKI 的理论基础和最新进展情况。

1.1　什么是 PKI

PKI 是 Public Key Infrastructure 的缩写，通常译作公钥基础设施。为什么说 PKI 是一种“基础设施”？原因很简单，因为它具备了基础设施的主要特征。让我们将 PKI 在网络信息空间的地位与电力基础设施在人们生活中的地位进行类比：电力系统通过延伸到用户端的标准插座为用户提供能源；PKI 通过延伸到用户本地的接口为各种应用提供安全服务，包括身份认证、识别、数字签名、加密等。一方面，作为基础设施，PKI 的主要目标是对应用提供支撑，它与使用 PKI 的应用系统是分离的，它所支撑的对象既包括“旧”的应用，也包括“新”的应用，因此具有“公用”的特性；另一方面，离开 PKI 应用系统，PKI 本身没有任何用处。类似地，电力系统基础设施离开电器设备就不能发挥作用，公路基础设施离开了汽车也毫无用处。正是这种基础设施的特征使得 PKI 系统设计和开发的效率大大提高，因为 PKI 系统的设计、开发、生产及管理都可以独立地进行，不需要考虑应用的特殊性。

有了 PKI，安全应用程序的开发者就不必再关心复杂的数学模型和运算，只需要直接按照标准使用一种接口即可，正如用户在使用电器时不必关心电力是如何发送的一样。

PKI 必须具有如下的性能要求：

- 透明性和易用性；
- 可扩展性；
- 互操作性；
- 多用性；
- 支持多平台。

1.2　为什么需要 PKI

一台独立的计算机是很有用的，但却具有一定的局限性。当用户想要在自己的计算机硬盘外查找信息，与外界进行信息交流时，就需要联网，而最广为人知的网络就是 Internet。

与单个的计算机不同，作为当今世界上最大的信息集散地，Internet 最大的特点是它的开

放性、广泛性和自发性，它向使用者提供了广泛的自由度和自治权力。Internet给整个人类社会带来的好处是显而易见的，Internet通过将数以亿计的计算机联为一体，使得任何组织和个人都可以利用联网的计算机不受时间和空间的限制传递信息，即使远隔万里，信息的发布者与接受者之间也可直接沟通，实现即时、双向的交流。同时，海量的信息在Internet上流转，人们可以方便地搜索到自己所需的信息，这仿佛是给人类装上了"千里眼"和"顺风耳"，使人类的能力得到了延伸。在Internet之上，网络通信、远程登录、文件传送、信息浏览与查询、现代远程教育、电子商务、休闲娱乐等应用大行其道，极大地扩展了计算机的功能，赋予了计算机全新的角色。

正如任何一件事物总有它的两面性一样，Internet在给我们带来了开放、自由的同时，也打开了"潘多拉之盒"。由于Internet从建立开始就缺乏安全的总体构想和设计，使得Internet与生俱来地带有其特有的痼疾——过分自由，缺乏约束，这给以数字形式在Internet上传输的大量信息，特别是用户的银行或信用卡账号、网络登录口令、电子邮箱密码、机密邮件等敏感信息带来了巨大的威胁。这些威胁既可以来自黑客、竞争对手，也可以来自内部人员。

对不同的人来说，网络中的安全威胁的含义是不一样的：

- 从个人、组织等用户的角度来说，他们希望涉及个人隐私或组织利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私，同时也避免其他用户的非授权访问和破坏。
- 从网络运行和管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现"陷门"、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。
- 对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，对国家造成巨大损失。
- 从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

根据网络中的安全威胁的种类，我们通常把网络安全归纳为物理安全和逻辑安全。物理安全指的是对网络系统中各通信、计算机设备及相关设施的物理保护，使这些基础设施免于受到破坏；逻辑安全则包含了信息的真实性、完整性、机密性和不可否认性等几个方面的内容。

Internet在催生了大批先进技术的同时也培养了一批以破坏计算机系统为乐的人。他们或通过互联网络未经许可便进入他人的计算机设施，破解他人的密码，使用他人的计算机资源；或通过网络向他人计算机系统散布计算机病毒，堵塞网络，破坏他人计算机和数据；或进行间谍活动，窃取、篡改或者删除国家机密和商业秘密；或盗窃银行中他人存款，非法转移资金；或湮没证据，对自己的所作所为百般抵赖，其结果只有一个：让受害者遭受损失。

近几年来，随着网络安全事件给互联网用户造成的损失的迅速上升，网络安全得到了广泛的关注，病毒的泛滥，黑客的肆虐，使得杀毒软件和防火墙成为了计算机系统中最基本的安全配置。然而，杀毒软件和防火墙只解决了网络安全中物理安全的一部分，而对于逻辑安全方面却没有丝毫的帮助。网络安全问题并不仅仅只有病毒和黑客，信任的缺失也是一个非常重要的方面。由于在互联网上人们无法鉴别与之交流的人或设备的身份，再加上信息极易被伪造，让人们对在互联网上公开传输的信息不免心存疑虑，也引发了人们对信息的真实性、完整性、

机密性和不可否认性的更高要求。

逻辑安全方面的威胁主要有：

- 假冒：指非法用户假冒合法用户身份获取敏感信息(参见图1-1)。
- 截取：指非法用户截获通信网络的数据(参见图1-2)。
- 篡改：指非法用户改动所截获的信息和数据(参见图1-3)。
- 否认：指通信的单方或多方事后否认曾经参与某次活动(参见图1-4)。

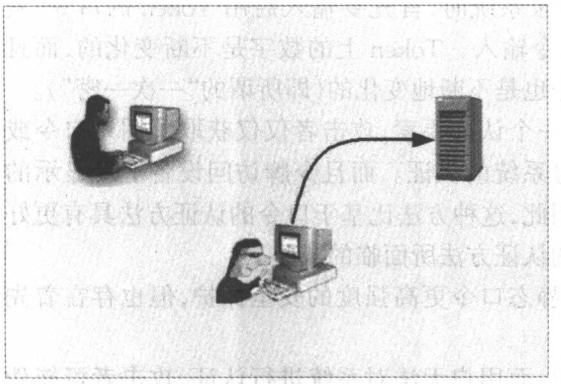

图1-1 假冒

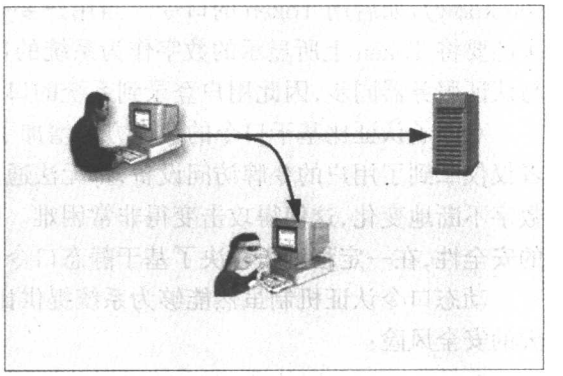

图1-2 截取

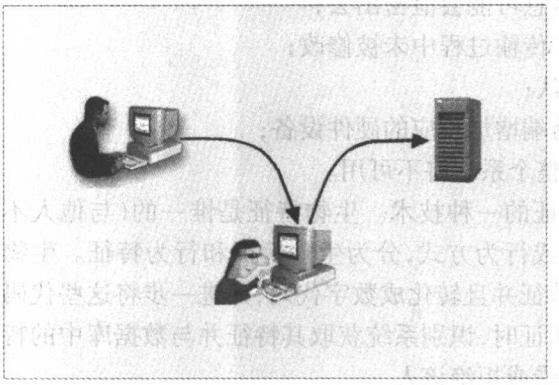

图1-3 篡改

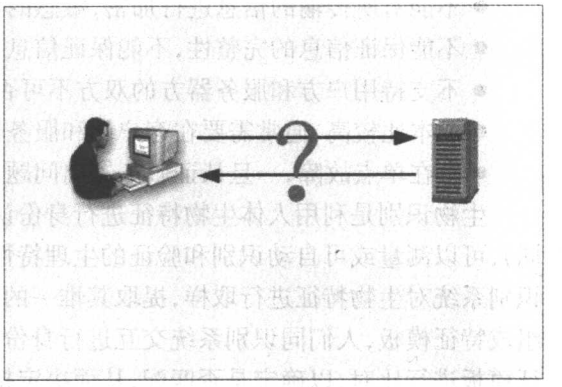

图1-4 否认

为了防范用户身份(包括人和设备)的假冒、数据的截取和篡改以及行为的否认等安全漏洞，互联网急需一种技术或体制来实现对用户身份的认证，建立可信的网络应用环境，并保证互联网上所传输数据的安全。

目前，能够实现用户身份认证的技术有很多，常见的有静态口令、动态口令、生物识别和PKI等。

“用户名+静态口令”是当今最基本、最常用的网络身份认证技术。静态口令认证机制可以分为两个阶段：第一个阶段是身份识别阶段，确认你是谁；第二阶段是身份验证阶段，获取身份信息并进行验证。一个简单的身份验证过程通常是弹出一个窗口，提示用户输入用户名及“只有用户自己知道”的静态口令，一旦用户名及静态口令都通过验证，用户即可拥有系统分配

的权限来执行相应的操作。

静态口令虽然具有用户使用方便,线路上传输的数据量最小,后台服务器数据调用量最小,速度最快,实现的成本最低等优点,但在口令强度、口令传输、口令验证、口令存储等许多环节上都存在着严重的安全隐患,可以说是最不安全的身份认证技术。

动态口令技术是对传统的静态口令技术的改进,它采用双因子认证的原理,即用户既要拥有一些东西(something you have),如系统颁发的Token(令牌),又要知道一些东西(something you know),如启用Token的口令。当用户要登录系统时,首先要输入启用Token的口令,其次还要将Token上所显示的数字作为系统的口令输入。Token上的数字是不断变化的,而且与认证服务器同步,因此用户登录到系统的口令也是不断地变化的(即所谓的"一次一密")。

双因子认证比基于口令的认证方法增加了一个认证要素,攻击者仅仅获取了用户口令或者仅仅拿到了用户的令牌访问设备,都无法通过系统的认证。而且令牌访问设备上所显示的数字不断地变化,这使得攻击变得非常困难。因此,这种方法比基于口令的认证方法具有更好的安全性,在一定程度上解决了基于静态口令的认证方法所面临的威胁。

动态口令认证机制虽然能够为系统提供比静态口令更高强度的安全保护,但也存在着先天的安全风险:

- 只能进行单向认证,即系统可以认证用户,而用户无法对系统进行认证,攻击者可能伪装成系统骗取用户的口令;
- 不能对所传输的信息进行加密,敏感的信息可能会泄密出去;
- 不能保证信息的完整性,不能保证信息在传输过程中未被修改;
- 不支持用户方和服务器方的双方不可否认;
- 成本比较高,通常需要在客户端和服务器端增加相应的硬件设备;
- 存在单点故障,一旦认证服务器出问题,整个系统将不可用。

生物识别是利用人体生物特征进行身份认证的一种技术。生物特征是惟一的(与他人不同),可以测量或可自动识别和验证的生理特性或行为方式,分为生理特征和行为特征。生物识别系统对生物特征进行取样,提取其惟一的特征并且转化成数字代码,并进一步将这些代码组成特征模板,人们同识别系统交互进行身份认证时,识别系统获取其特征并与数据库中的特征模板进行比对,以确定是否匹配,从而决定接受或拒绝该人。

用于生物识别的生物特征有指纹、手形、脸形、虹膜、视网膜、脉搏、耳廓等,行为特征有签字、声音、按键力度等。基于这些特征,人们已经发展了手形识别、指纹识别、面部识别、发音识别、虹膜识别、签名识别等多种生物识别技术。目前,指纹、虹膜等生物识别技术已经应用于网络上的用户身份认证。

生物识别较为方便,安全性也很高,它既不需要记住复杂的密码,也不需随身携带钥匙、智能卡之类的东西。但生物识别技术应用的成本较高,一件识别终端少则几百元,多则数千元,且不能保证所传输信息的完整性和机密性,认证信息在互联网中传输时还存在着被截取和仿冒的危险,因此,生物识别技术在互联网中的应用还有待完善。

PKI是为适应网络开放状态应运而生的一种技术,以前的信息安全技术(如防火墙、入侵检测、防病毒等)基本上都是解决网络安全某一方面的问题,而PKI则是比较完整的网络安全解决方案,能够全面保证信息的真实性、完整性、机密性和不可否认性。

PKI技术以公钥技术为基础,以数字证书为媒介,结合对称加密和非对称加密技术,将个人、组织、设备的标识信息与各自的公钥捆绑在一起,其主要目的是通过自动管理密钥和证书,为用户建立起一个安全、可信的网络运行环境,使用户可以在多种应用环境下方便地使用加密和数字签名技术,在互联网上验证用户的身份,从而保证了互联网上所传输信息的真实性、完整性、机密性和不可否认性。PKI是目前为止既能实现用户身份认证,又能保证互联网上所传输数据安全的惟一技术。

1.3 PKI的理论基础

PKI技术是随着公钥密码技术的发展而发展起来的,它的理论基础是公钥密码理论。

在传统密码体制(又称"对称密钥密码体制")中,用于加密的密钥和用于解密的密钥完全相同。这种体制所使用的加密算法比较简单,但高效快速,密钥简短,破译困难。然而密钥的传送和保管是一个问题。例如,您与朋友通信,用同一个密钥加密与解密。首先,将密钥分发出去是一个难题,在不安全的网络上分发密钥显然是不合适的;另外,如果您和您的朋友之间任何一人将密钥泄露,那么大家都要重新启用新的密钥。

1976年,为解决上述密钥管理的难题,美国的密码学专家Diffie和Hellman,在他们的里程碑式的巨著《密码学的新方向》一文中,提出了一种密钥交换协议,允许在不安全的媒体上双方交换信息,安全地获取相同的用于对称加密的密钥。

信任,惟有信任才能构筑安全的基石。人类社会关系的维系在于信任关系的建立、维护,人类的各种合作需要信任,人类生活离不开信任;同样的,对于人类活动空间延伸的网络而言,人们在网络上进行的各种合作也需要信任来维系。表1-1给出了信任在现实世界和网络世界的实现方式的对比。

表1-1 信任在现实世界和网络世界的实现方式对比

信任类型	现实世界	网络世界
身份认证	身份证、护照、信用卡、驾照	数字证书、数字签名
完整性	签名、支票、第三方证明	数字签名
保密性	保险箱、信封、警卫、密藏	加密
不可否认性	签名、挂号信、公证、邮戳	数字签名

1.4 PKI技术发展现状及趋势

自20世纪90年代初期以来,作为电子商务信息安全的关键和基础性技术的PKI逐步得到了许多国家的政府和企业的广泛重视,PKI技术由理论研究进入到商业化应用阶段。在这一时期,IETF、ISO等机构陆续颁布了X.509、PKIX、PKCS、S/MIME、SSL、SET、IPSec、LDAP等PKI应用相关标准,RSA、VeriSign、Entrust、Baltimore等企业纷纷推出了自己的PKI产品和服务。一些大的厂商,如Microsoft、Netscape、Novel、Sun等,都开始在自己的网络基础设施产品中增加PKI功能。加拿大、美国、欧盟等国家和地区也相继建立起了自己的PKI体系,银