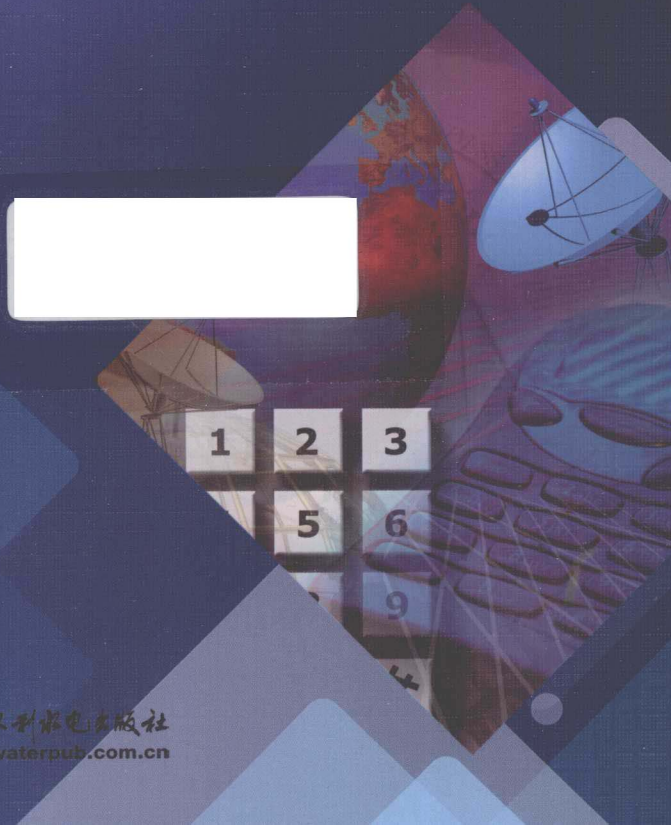
“十二五”职业教育国家规划教材（经全国职业教育教材审定委员会审定）
高等职业教育精品示范教材 信息安全系列

数字身份认证技术

主　编　梁雪梅　路　亚
副主编　周观民　罗　萱
主　审　武春岭

本书特色：

- 以就业为导向，以能力为本位
- 项目案例引导，任务需求驱动
- 生活实例链接知识点，案例增加趣味性
- 通用教学内容与特殊教学内容协调配置



中国水利水电出版社
www.waterpub.com.cn

“十二五”职业教育国家规划教材（经全国职业教育教材审定委员会审定）

高等职业教育精品示范教材（信息安全系列）

数字身份认证技术

主　编　梁雪梅　路　亚

副主编　周观民　罗　萱

主　审　武春岭

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

数字身份认证的目的是使通信双方建立信任关系，从而保证后续的网络活动正常进行。公钥基础设施能为各种不同安全需求的用户提供不同的网上安全服务，主要有身份识别与鉴别、数据保密、防止数据篡改、抗抵赖等，在国内外得到广泛应用。

本书共7章，每一章都精心设计了图文并茂的实训内容，便于学生学习和实践，内容安排合理、重点突出。本书可以作为普通高校、应用型本科、高职高专或成人教育计算机、信息安全等专业学生的PKI相关课程教材，也可作为电子商务、电子政务的参考书或培训教材。

本书配有电子教案，读者可以从中国水利水电出版社网站和万水书苑免费下载，网址为：http://www.waterpub.com.cn/softdown/和 http://www.wsbookshow.com。

图书在版编目（CIP）数据

数字身份认证技术 / 梁雪梅，路亚主编. -- 北京 : 中国水利水电出版社，2014.9

“十二五”职业教育国家规划教材. 高等职业教育精品示范教材. 信息安全系列

ISBN 978-7-5170-2581-8

Ⅰ. ①数… Ⅱ. ①梁… ②路… Ⅲ. ①计算机网络－身份认证－安全技术－高等职业教育－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2014)第228382号

策划编辑：祝智敏　责任编辑：李　炎　加工编辑：田新颖　封面设计：李　佳

书　名	“十二五”职业教育国家规划教材（经全国职业教育教材审定委员会审定） 高等职业教育精品示范教材（信息安全系列） **数字身份认证技术**
作　者	主　编　梁雪梅　路　亚　副主编　周观民　罗　萱 主　审　武春岭
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路1号D座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（发行部）、82562819（万水）
经　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643、68545874 全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	北京蓝空印刷厂
规　格	184mm×240mm　16开本　15印张　377千字
版　次	2014年9月第1版　2014年9月第1次印刷
印　数	0001—4000册
定　价	32.00元

高等职业教育精品示范教材（信息安全系列）

丛书编委会

序言

随着信息技术和社会经济的快速发展，信息和信息系统成为现代社会极为重要的基础性资源。信息技术给人们的生产、生活带来巨大便利的同时，计算机病毒、黑客攻击等信息安全事故层出不穷，社会对于高素质技能型计算机网络技术和信息安全人才的需求日益旺盛。党的十八大明确指出“高度关注海洋、太空、网络空间安全”，信息安全被提到前所未有的高度。加快建设国家信息安全保障体系，确保我国的信息安全，已经上升为我国的国家战略。

发展我国信息安全技术与产业，对确保我国信息安全有着极为重要的意义。信息安全领域的快速发展，亟需大量的高素质人才。但与之不相匹配的是，在高等职业教育层次信息安全技术专业的教学中，还更多地存在着沿用本科专业教学模式和教材的现象，对于学生的职业能力和职业素养缺乏有针对性的培养。因此，在现代职业教育体系的建立过程中，培养大量的技术技能型信息安全专业人才成为我国高等职业教育领域的重要任务。

信息安全是计算机、通信、数学、物理、法律、管理等学科的交叉学科，涉及计算机、通信、网络安全、电子商务、电子政务、金融等众多领域的知识和技能。因此，探索信息安全专业的培养模式、课程设置和教学内容就成为信息安全人才培养的首要问题。高等职业教育信息安全系列丛书编委会的众多专家、一线教师和企业技术人员，依据最新的专业教学目录和教学标准、结合就业实际需求，组织了以就业为导向的高等职业教育精品示范教材（信息安全系列）的编写工作。该系列教材由《网络安全产品调试与部署》、《网络安全系统集成》、《Web开发与安全防范》、《数字身份认证技术》、《计算机取证与司法鉴定》、《操作系统安全（Linux）》、《网络安全攻防技术实训》、《大型数据库应用与安全》、《信息安全工程与管理》、《信息安全法规与标准》、《信息安全等级保护与风险评估》等组成，在紧跟当代信息安全研究发展的同时，全面、系统、科学地培养信息安全类技术技能型人才。

本系列教材在组织规划的过程中，遵循以下几个基本原则：

（1）体现就业为导向、产学结合的发展道路。学科和专业同步加强，按企业需要、按岗位需求来对接培养内容。既能反映信息安全学科的发展趋势，又能结合信息安全专业教育的改革，且及时反映教学内容和教学体系的调整更新。

（2）采用项目驱动、案例引导的编写模式。打破传统的以学科体系设置课程体系、以知识点为核心的框架，更多地考虑学生所学知识与行业需求及相关岗位、岗位群的需求相一致，坚持“工作流程化”、“任务驱动式”，突出“走向职业化”的特点，努力培养学生的职业素养、职业能力，实现教学内容与实际工作的高仿真对接，真正以培养技术技能型人才为核心。

（3）专家和教师共建团队，优化编写队伍。由来自信息安全领域的行业专家、院校教师、企业技术人员组成编写队伍，跨区域、跨学校进行交叉研究、协调推进，把握行业发展和创新

教材发展方向，融入信息安全专业的课程设置与教材内容。

（4）开发课程教学资源，推进专业信息化建设。从充分关注人才培养目标、专业结构布局等入手，开发补充性、更新性和延伸性教辅资料，开发网络课程、虚拟仿真实训平台、工作过程模拟软件、通用主题素材库以及名师讲义等多种形式的数字化教学资源，建立动态、共享的课程教材信息化资源库，服务于系统培养技术技能型人才。

信息安全类教材建设是提高信息安全专业技术技能型人才培养质量的关键环节，是深化职业教育教学改革的有效途径。为了促进现代职业教育体系的建设，使教材建设全面对接教学改革、行业需求，更好地服务区域经济和社会发展，我们殷切希望各位职教专家和老师提出建议，并加入到我们的编写队伍中来，共同打造信息安全领域的系列精品教材！

丛书编委会

2014 年 6 月

前　言

近几年来，随着国内的网上银行、电子商务、电子政务的飞速发展，广大用户对提供网上交易普适性的安全服务，如网上身份认证，防止假冒；网上传输数据不被篡改；网上交易绝对保密；发生争端有相应的仲裁措施等的需求越来越迫切。经过近几年的应用与实践得出，数字证书是目前解决上述问题比较有效的措施，其相关知识和技术也成为信息安全技术专业学生必须掌握的核心知识和技术。

在教学实践中，我们发现目前适合高职信息安全技术专业教学使用的数字身份认证教材及参考书籍稀缺，不适应专业教学需要。因此为了更好地适应教学，满足学生未来的职业需求，我们共同开发了本教材。本教材主要针对高职学生学习需求和高职教育教学要求，采用项目案例引导、任务需求驱动的形式组织教材，精选最新社会案例，增加趣味性，将相对枯燥的基础知识贯穿于趣味盎然的故事中，激发学生学习兴趣，提高学习效率。

本书主要论述数字身份认证技术的广泛应用以及相关知识。全书共 7 章，第 1 章介绍和分析了公钥基础设施的概念、由来和典型应用；第 2 章讲述了 PKI 相关的密码学基础知识；第 3 章介绍了 PKI 的功能和结构；第 4 章具体介绍了 PKI 数字认证技术；第 5 章介绍了 Kerberos 数字认证技术；第 6 章介绍了微软数字认证技术；第 7 章介绍了 PKI 的常规应用。全书注重讲述技术实现和具体操作，减少纯理论性内容，以适应高职学生特点和高职教学需要。

本书可以作为普通高校、应用型本科、高职高专或成人教育计算机、信息安全等专业学生的 PKI 相关课程教材，也可作为学习 PKI 技术的参考书或培训教材。

本书由重庆电子工程职业学院梁雪梅、路亚担任主编，武春岭任主审，梁雪梅编写了全书大纲，并统稿。本书第 1 至 3 章由路亚编写，第 4 至 6 章由梁雪梅编写，第 7 章由重庆青年职业技术学院罗萱编写，周观民参与方案制定、大纲讨论和初稿的修改工作。本书在编写和出版过程中得到了中国水利水电出版社的大力支持和帮助，也得到了单位领导和同事的支持，在此一并表示感谢。

由于编者水平有限且时间仓促，尽管我们花了大量时间和精力校验，但书中疏漏之处仍在所难免，敬请各位读者批评指正，万分感谢。

编　者

2013 年 10 月

目　录

1 PKI 概述

本章导读：

本章主要介绍公钥基础设施（Public Key Infrastructure，PKI）的概念及发展过程，并简单分析 PKI 的各个组成部分的内容。由于公钥基础设施必须有信息安全作为基础，因此本章也介绍了信息安全基础的相关内容。

学习目标：

- 了解网络信息安全的基本概念
- 掌握公钥基础设施（PKI）的基本概念
- 掌握 PKI 的基本组成以及各组成部分的基本功能

引入案例

网易等 7 家互联网巨头启动网络安全教育活动

2013-08-26 15:41　来源：中国网

日前，网易联合阿里巴巴及支付宝、百度、腾讯、新浪、360 等联合启动名为“守护英雄”的网络安全教育主题活动，旨在通过在线科普网络安全知识，培养用户良好的网络安全使用习惯，增强用户对信息安全保障的信心。

这是继去年 7 月举办“反裸奔”网络安全教育活动后，我国互联网巨头再一次联动科普网络安全知识。

近年，随着互联网应用深入亿万民众的日常生活，围绕网络信息的安全威胁也日渐增加，

而一些网友的安全防范意识薄弱，放任电脑和账号“裸奔”，导致信息被盗等情况时有发生，严重的甚至危及用户资金安全。

为帮助网民防御网络安全威胁，共建互联网健康发展环境，去年6月，网易联合阿里巴巴集团及支付宝、微软、百度、腾讯、新浪、人人等互联网巨头共同组建了互联网企业安全工作组（ISWG.CN），通过用户教育和技术创新的方式，双管齐下为用户网络信息安全“保驾护航”。

而“守护英雄”活动，则是今年工作组利用安全教育提升用户安全意识和知识水平的重要举措。据悉，“守护英雄”活动由互联网企业安全工作组成员网易联手阿里巴巴集团及支付宝、新浪、百度、腾讯以及360七家互联网企业联合发起，作为去年“反裸奔”活动的延伸，发起方希望帮助用户树立正确的网络安全观。

“我们需要业内企业单位协同合作，给用户提供良好的网络安全防护习惯指引，网聚最广大网民的主动性，共同维护中国互联网用户安全。”网易安全专家表示。

事实上，随着互联网巨头联动协作日渐紧密，网络安全问题已得到很大的改善。据介绍，2013年上半年，互联网企业安全工作组共拦截2110万个钓鱼网站，处理不法信息达8700万条，拦截木马达到365万次，给用户网络信息安全提供了巨大的保障。再以拥有超过5.7亿邮箱用户的网易公司为例，其积极推广DMARC技术以支持安全工作组成员单位进行反钓鱼工作，已经取得了极大的成果。目前DMARC已保护了中国超过50%的邮箱用户，而且还有越来越多的企业正在部署DMARC。

业内人士认为，网易等互联网巨头对网络安全普及教育的持续推动，将深化网络安全防范行动的效果和影响，有助于帮助更多网民树立安全上网意识，提高安全防护技术，从而进一步净化网络环境。

知识模块

1.1 网络攻击与防范

计算机网络出现后，在世界范围内得到了迅猛的发展，网络用户数量每年都呈几何级数增长，中国互联网络信息中心（CNNIC）所做的《第 31 次中国互联网络发展状况统计报告》显示，截至 2012 年 12 月底，我国网民规模达 5.64 亿人，网络购物用户规模达到 2.42 亿人，团购用户数为 8327 万人。

在网络应用普及的背景下，网络上的信息安全问题越来越突出，网络攻击事件逐年增长，越来越受到人们的重视。CNNIC《2012 年中国网民信息安全状况研究报告》显示，84.8%的网民遇到过信息安全事件，总人数为 4.56 亿。安全事件中，垃圾短信和手机骚扰电话发生比例最高，分别有 68.3%和 56.5%的网民遇到过，其他事件比例分别为：欺诈诱骗信息（38.2%）、中病毒或木马（23.1%）、假冒网站（17.6%）、账号或密码被盗（13.8%）、手机恶意软件（10.6%）、个人信息泄露（7.1%）。

在电子商务和电子政务飞速发展的今天，网络信息安全问题更是成为关系所有上网用户切身利益的大问题。

1.1.1 常见的网络攻击方式

对常见的网络安全事件进行分析后，可以总结出基本的网络攻击形式有四种：中断、截获、篡改、伪造。

图 1-1（a）表示的是在没有攻击发生的正常情况下，信息从信源传向信宿的过程。

图 1-1（b）表示的是“中断”攻击，它是以可用性作为攻击目标，它毁坏系统资源，切断通信线路，或使文件系统变得不可用。拒绝服务攻击、制造并传播病毒等属于中断攻击。

图 1-1（c）表示的是“截获”攻击，它是以保密性作为攻击目标，非授权用户通过某种手段获得通信信息，如搭线窃听、非法拷贝、截获个人信息等，这种攻击会给通信带来很大的隐患，因为通信双方可能在不知道的情况下已经泄露了机密信息。

图 1-1（d）表示的是“篡改”攻击，它是以信息的完整性作为攻击目标，非授权用户不仅获得对系统资源的访问，而且对文件进行篡改，如改变文件中的数据或修改网上传输的信息等，可以用消息摘要的方式防范这种攻击。

图 1-1（e）表示的是“伪造”攻击，它是以信源的完整性作为攻击目标，非授权用户要么将伪造的数据插入到正常的系统中，要么发布欺诈诱骗信息、假冒网站，要么未经授权使用、获取系统资源和权限。

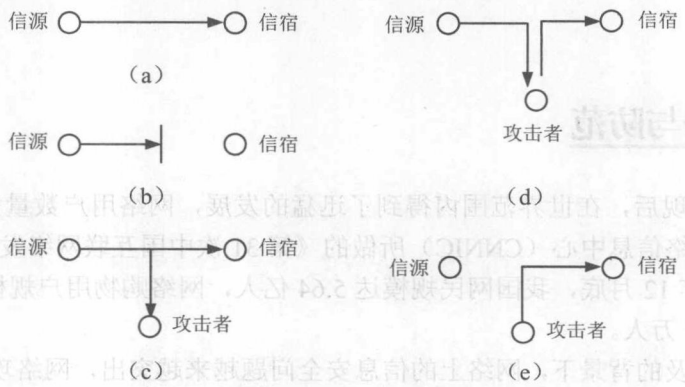


图 1-1　网络攻击的几种形式

1.1.2　网络信息安全的概念

网络信息安全是一个复杂领域，是涉及计算机科学、网络通信、密码学、应用数学、数论、信息论等多学科的综合学科。信息安全又与系统的硬件、软件、网络、数据等复杂系统有关，是与信息、人、组织、网络、环境有关的技术安全、结构安全和管理安全的总和，要求确保信息在存储、处理和传输过程中的可靠性、可用性、保密性、完整性、不可抵赖性和可控性。

（1）可靠性（Reliability）：指信息系统能够在规定条件下和规定时间内完成规定功能的特性。

（2）可用性（Availability）：指信息可被授权实体访问并按需求使用的特性，是系统面向用户的安全性能。

（3）保密性（Confidentiality）：指信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。

（4）完整性（Integrity）：指网络信息未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。

（5）不可抵赖性（Non-repudiation）：指在信息交互过程中，确信参与者的真实同一性，即所有参与者都不可否认或抵赖曾经完成的操作和承诺的特性。

（6）可控性（Controllability）：指对信息传播及内容具有控制能力的特性。

为了提供上述安全特性，ISO7498-2 建议的安全机制主要有：

（1）密码机制（Encipherment）：密码技术提供数据或信息交互的保密性，而且对其他安全机制也起着非常重要的基础作用。

（2）数字签名机制（Digital Signature Mechanisms）：应用公钥密码体制，使用私钥进行签名，公钥进行验证，防止否认、仿造、篡改和冒充等安全方面的问题。

（3）访问控制机制（Access Control Mechanisms）：访问控制机制是从计算机系统的处理

能力方面对信息提供保护。防止资源的非授权使用或越权使用。

（4）数据完整性机制（Data Integrity Mechanisms）：通常使用消息摘要加时间戳信息的形式判断消息是否被篡改或重发，消息摘要很多时候使用杂凑函数来产生。

此外还有验证交换机制、业务流填充机制、仲裁机制、可信功能等。

1.2 PKI 的基本概念

1.2.1 基础设施的概念和特点

在学习 PKI 的概念前，我们先了解下一般基础设施的概念。

基础设施一般是由政府提供给公众享用或使用的公共产品，所以经常称为“公共基础设施”。基础设施建设是经济发展的奠基石，在经济学上，是一种“社会先行资本”（Social Overhead Capital，SOC），例如各地的招商引资，在招商之前都要做大量的基础设施建设，以达到吸引资金的目的。基础设施建设也是保障和改善民生的需要，其建设水平直接影响和决定人民的生活水平和质量，影响民众的幸福指数。

基础设施出现在人们生活的方方面面，主要有：

（1）交通。包括：地面交通、航空、水道和港口、联合运输设施、公共交通。

（2）电力。包括：电力生产和电力传送设施，如水电站、煤、石油、天然气发电站、高压电传输线、变电站、电力分配系统和控制中心、服务和保护设施和核电站等。

（3）给水和污水处理设施。包括：给水供应设施，如给水和水处理厂、主要供水线、井、机械和电力设备；供水的构筑物，如大坝、临时性的支路、构筑物、水道和沟渠；污水处理设施，如污水管线、化粪池、污水处理厂。

（4）通信。包括电话网、电视网、无线和卫星网络、信息高速公路网络。

（5）垃圾处理。包括：垃圾填埋、处理厂、循环利用设施。

（6）煤气供应及管道设施。如煤气生产、管道、控制中心、储存柜、维护设施等。

（7）石油运输设施。如输油管道等。

（8）公共建筑设施。包括：学校、医院、政府办公楼、警察局、消防站、邮局、监狱、法庭、剧场、会议中心、展览中心、体育馆、电影院等。

（9）休闲设施。主要是指公园和广场。

分析上述基础设施，不难总结出基础设施的一些共同点：

（1）由可信机构（政府）兴建和管理。

（2）有统一的标准。如电力基础设施中，有统一的供电标准、统一的用电标准（市电 220V 等）、统一的接口规范（电源插座的设计规范等）。网络基础设施中，有统一的数据传输规范、统一的接口规范、统一的网络协议等。

（3）使用便捷（接入）。只要遵循相关设施的使用原则，不同的实体都可以方便地使用

基础设施提供的服务。

（4）根据环境的不同，实现方式可以略有不同。如在网络基础设施中，不同的物理层接口规范等。

（5）不同实现方式之间具有互操作性。如手机可以拨打座机，移动终端上网和台式 PC 上网可以互联等。

（6）支持新的应用扩展。如新的电器设备可以在旧的电力基础设施上应用等。

1.2.2 公钥基础设施的概念

公钥基础设施（Public Key Infrastructure，PKI）是利用公钥理论和技术建立的提供信息安全服务的基础设施，是生成、管理、存储、分发和吊销基于公钥密码学的公钥证书所需要的硬件、软件、人员、策略和规程的总和，提供身份鉴别和信息加密，保证消息的数据完整性和不可否认性。

PKI 是一种普遍适用的网络信息安全基础设施，最早是 20 世纪 80 年代由美国学者提出来的概念，实际上，授权管理基础设施、可信时间戳服务系统、安全保密管理系统、统一的安全电子政务平台等系统的构筑都离不开它的支持，是目前公认的保障网络信息安全的最佳体系。

PKI 包括权威认证机构 CA（如政府部门）、证书库、密钥备份及恢复系统、证书作废管理系统、PKI 应用接口系统等主要组成部分。各部分的主要功能如下：

（1）认证机构 CA，是证书的签发机构，它是 PKI 的核心，是 PKI 中权威的、可信任的、公正的第三方机构。

（2）证书库，数字证书的集中管理和存放地，提供公众查询。数字证书（Digital Certificate）就是标志网络用户身份信息的一系列数据，用来在网络通信中识别通信各方的身份，数字证书是一个经证书授权中心数字签名的包含公开密钥（简称公钥）拥有者信息以及公开密钥的文件。证书包含的信息：证书使用者的公钥值、使用者的标识信息、证书的有效期、颁发者的标识、颁发者的数字签名等。

（3）密钥备份及恢复系统，对用户的解密密钥进行备份，当丢失时进行恢复，而签名密钥不能备份和恢复。

（4）证书作废管理系统，当证书由于某种原因（密钥丢失、泄密、过期等）需要作废、终止使用时，将证书放入证书作废列表（CRL）进行管理、存放，提供公众查询。

（5）PKI 应用接口系统，为各种各样的应用提供安全、一致、可信任的接口与 PKI 系统进行交互，确保所建立起来的网络环境安全可信，并降低管理成本。

1.2.3 公钥基础设施的特点

PKI 作为一种信息安全基础设施，其目标就是要充分利用公钥密码学的理论基础，建立起一种普遍适用的基础设施，为各种网络应用提供全面的安全服务。公开密钥密码为我们提供了一种非对称性质，使得安全的数字签名和开放的签名验证成为可能，而这种优秀技术的使用却

面临着理解困难、实施难度大等问题。正如让每个人自己开发和维护发电厂有一定的难度一样，要让每一个开发者完全正确地理解和实施基于公开密钥密码的安全系统有一定的难度。PKI希望通过一种专业的基础设施的开发，让网络应用系统的开发人员从繁琐的密码技术中解脱出来同时享有完善的安全服务。

PKI作为基础设施，提供的服务必须简单易用，便于实现。将PKI在网络信息空间的地位与电力基础设施在工业生活中的地位进行类比可以更好地理解PKI。电力基础设施，通过延伸到用户的标准插座为用户提供能源，而PKI通过延伸到用户本地的接口，为各种应用提供安全的服务。有了PKI，安全应用程序的开发者可以不用再关心那些复杂的数学运算和模型，而直接按照标准使用一种插座（接口）。正如电冰箱的开发者不用关心发电机的原理和构造一样，只要开发出符合电力基础设施接口标准的应用设备，就可以享受基础设施提供的能源。

PKI与应用的分离也是PKI作为基础设施的重要特点。正如电力基础设施与电器的分离一样。网络应用与安全基础设施实现分离，有利于网络应用更快地发展，也有利于安全基础设施更好地建设。正是由于PKI与其他应用能够很好地分离，才使我们能够将其称为基础设施，PKI也才能从千差万别的安全应用中独立出来，有效地、独立地发展壮大。PKI与网络应用的分离，实际上就是网络社会的一次分工，有效促进各自独立发展，并在使用中实现无缝结合。

CA认证系统要在满足安全性、易用性、扩展性等需求的同时，从物理安全、环境安全、网络安全、CA产品安全以及密钥管理和操作运营管理等方面按严格标准制定相应的安全策略；要有专业化的技术支持力量和完善的服务系统，保证系统7×24小时高效、稳定运行。

1.3 PKI的功能

PKI可以解决绝大多数信息安全问题，并初步形成了一套完整的解决方案，它是基于公开密钥理论和技术建立起来的安全体系，是提供信息安全服务的具有普适性的安全基础设施。PKI体系为网上金融、网上银行、网上证券、电子商务、电子政务、网上交税、网上工商等多种网上办公、交易提供了完备的安全服务功能，这是PKI最基本、最核心的功能。

PKI提供的系统功能是指PKI的各个功能模块分别具有的功能，主要包括证书的审批和颁发、密钥的产生和分发、证书查询、证书撤销、密钥备份和恢复、证书撤销列表管理等，这些内容将在第3章详细介绍。

PKI体系提供的安全服务功能主要包括：身份认证、数据完整性、数据机密性、不可否认性、时间戳等。

1. 身份认证

认证的实质就是证实被认证对象是否属实和是否有效的过程，常常被用于通信双方相互确认身份，以保证通信的安全。其基本思想是通过验证被认证对象的某个专有属性，达到确认被认证对象是否真实、有效的目的。被认证对象的属性可以是口令、数字签名或者指纹、声音、视网膜这样的生理特征等。