高·等·院·校·信·息·安·全·专·业·系·列·教·材

中国计算机学会教育专业委员会与清华大学出版社联合组织编写

名誉主编：何德全　编委会主任：肖国镇

PKI Principle and Technology

PKI原理与技术

谢冬青　冷健　编著

清华大学出版社

高·等·院·校·信·息·安·全·专·业·系·列·教·材

PKI Principle and Technology

PKI原理与技术

谢冬青 冷健 编著

清华大学出版社
北京

内 容 简 介

本书系统全面地介绍了 PKI 原理与技术的主要内容，包括 PKI 基础设施的地位和作用，核心 PKI 服务的内容，认证中心构建，PKI 中的各种信任模型，PKI 工程所遵循的标准、协议和编码方式，并讨论了电子商务、电子政务的安全需求，给出了 PKI 解决方案的主要技术框架。

本书从工程化实用角度来讨论 PKI 原理与技术，适合作为信息安全、计算机科学与技术、软件工程、电子工程与通信工程等专业本科生、硕士生的教材，也可供从事相关专业的教学、科研和工程人员参考。

图书在版编目(CIP)数据

PKI 原理与技术/谢冬青，冷健编著. —北京：清华大学出版社，2003.12

(高等院校信息安全专业系列教材)

ISBN 7-302-07640-5

Ⅰ. P… Ⅱ. ①谢… ②冷… Ⅲ. 电子商务－安全技术－高等学校－教材 Ⅳ. F713.36

中国版本图书馆 CIP 数据核字(2003)第 106637 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦

http://www.tup.com.cn　　**邮　　编**：100084

社 总 机：010-62770175　　**客户服务**：010-62776969

组稿编辑：张　民

文稿编辑：王冰飞

印 刷 者：北京市清华园胶印厂

装 订 者：三河市李旗庄少明装订厂

发 行 者：新华书店总店北京发行所

开　　本：185×230　**印张**：24.25　**字数**：483 千字

版　　次：2004 年 1 月第 1 版　2004 年 6 月第2 次印刷

书　　号：ISBN 7-302-07640-5/TP·5602

印　　数：5001～8000

定　　价：32.00 元

高等院校信息安全专业系列教材

编审委员会

序

在社会信息化的进程中，信息已成为社会发展的重要资源，信息安全也成为21世纪国际竞争的重要战场。为了保护国家的政治利益和经济利益，各国政府都非常重视信息和网络安全，信息安全已成为一个世纪性、全球性的研究课题。

我国的信息安全事业正在蓬勃发展，国家领导高度重视，各部门通力合作、统筹规划，大大加快了我国信息安全产业发展的步伐。随着信息安全产业的快速发展，社会对信息安全人才的需求在不断增加，在高等教育领域大力推进信息安全的专业化教育，将是国家在信息安全领域掌握自主权、占领先机的重要举措。

目前，许多大学和科研院所已创办了信息安全专业或是开设了相关课程。很高兴中国计算机学会教育专业委员会和清华大学出版社在近期联合组织了一系列信息安全专业的研讨活动。他们以严谨负责的态度，认真组织全国各高校和科研院所的专家、学者，共同研讨信息安全专业的教育方法和课程体系，并在进行大量前瞻性研究工作的基础上，启动了“高等院校信息安全专业系列教材”的编写工作。这套教材将是我国信息安全专业的第一套完整、权威的教材，相信可以对全国的高等院校信息安全专业的建设起到很好的促进作用。

希望中国计算机学会教育专业委员会和清华大学出版社能够将这个研究课题一直做下去，也希望这套教材能够取得成功并不断完善，以促进各高等院校培养出更多、更好的信息安全专门人才，为我国的信息安全事业做出更大的贡献。

何德全

中国工程院院士

高等院校信息安全专业系列教材编审委员会名誉主编

2003年7月于北京

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，国家对信息安全人才的需求量不断增加，但目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信工程、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家何德全院士担任名誉主编，著名学者肖国镇教授担任编委会主任，共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了编写教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣，又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整，结构合理，内容先进。

② 适应面广，能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套，除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

我们的 E-mail 地址是：zhangm@tup.tsinghua.edu.cn；联系人：张民。

中国计算机学会教育专业委员会

清华大学出版社

2003 年 7 月

前言

网络和信息系统是现代社会最重要的信息基础设施，已经渗透到社会的各个领域。保障网络和信息系统的安全关系到国家的存亡、经济的发展、社会的稳定、优秀民族文化的继承和发扬。公开密钥基础设施(Public Key Infrastructure，PKI)是保障大型开放式网络环境下网络和信息系统安全的最可行、最有效的措施。

PKI是一个采用非对称密码算法原理和技术来实现并提供安全服务的、具有通用性的安全基础设施，它采用证书管理公钥，通过可信第三方机构，把用户的公钥和用户的其他标识信息绑定在一起，实现用户在Internet上的身份认证，从而提供安全可靠的信息处理。PKI所提供的安全服务以一种对用户完全透明的方式完成所有与安全相关的工作，极大地简化了终端用户使用设备和应用程序的方式，而且简化了设备和应用程序的管理工作，保证了他们遵循同样级别的安全策略。

PKI技术实现了人们长期追求的梦想：随时随地方便地同任何人秘密通信。它是开放、快速变化的社会信息交换的必然要求，是电子商务、电子政务广泛推行的基础，是诸多新业务、新产品开展的基本保证。

PKI技术是公开密钥密码学(Public Key Cryptography)完整的、标准化的、成熟的工程框架。它基于并且不断吸收公开密钥密码学丰硕的研究成果，按照软件工程的方法，采用成熟的各种算法和协议，遵循国际标准和RFC文档，如PKCS、SSL、X.509、LDAP，完整地提供网络和信息系统安全的解决方案。它摒弃了繁琐细致的理论证明和形式化描述，直接为广大的信息技术人员和管理工作者提供简便的服务。

本书是在作者长期从事PKI原理与技术教学、科研、开发工作的基础上总结而成的，旨在系统全面地介绍基于开放的、国际标准公认的安全基础设施构建技术。全书共9章。第1章简要地介绍了PKI基础设施的地位和概念；第2章介绍了核心PKI服务的内容；第3章是证书中心构建；第4章讨论了信任模型；第5章至第7章是PKI遵循的协议、标准、编码方式介绍；

第 8 章讨论了电子商务、电子政务的安全需求；第 9 章给出了实施 PKI 的主要问题和解决措施。

全书由谢冬青、冷健共同完成，其中第 1、2、5、6、8 章由谢冬青执笔，第 3、4、7、9 章由冷健编写。周洲仪、陈华勇、柳春雷、黄岩渠同志提供了帮助。中国科学院研究生院信息安全国家重点实验室主任冯登国教授对编写工作提出了很多指导性意见和有益的建议，并审阅了全书。谨向他们表示诚挚的感谢。

将发展迅速的现代化技术内容编写成教材是一件具有挑战性的工作。教材应注重系统全面、简明易学、逻辑性强、基本内容固定、适应性广，而 PKI 技术内容庞杂、发展迅速，要求实际开发能力和工程经验，本书试图在二者之间找到一个切入点，以“学以致用”为目标，不迁就国内发展水平不一的网络安全市场，直接采用国外流行的主流技术。囿于作者的学识和精力，书中一定存在不少问题和疏漏之处，诚恳地欢迎广大读者批评指正，我们的 E-mail 地址是 dqxie@hnu.cn。

作　者

2003 年 7 月

目录

第 1 章　PKI 基础设施 …… 1

1.1　基础设施 …… 1

1.1.1　基础设施的地位 …… 1

1.1.2　网络基础设施 …… 1

1.2　安全基础设施的概念 …… 2

1.2.1　安全基础设施的内容 …… 2

1.2.2　安全基础设施在信息基础设施中的地位 …… 6

1.3　公钥基础设施 …… 8

1.3.1　认证机构 …… 10

1.3.2　证书签发 …… 12

1.3.3　证书撤销 …… 12

1.3.4　密钥生成、备份和恢复 …… 13

1.3.5　证书注销列表处理 …… 15

1.3.6　信息发布 …… 15

习题 …… 16

第 2 章　核心 PKI 服务 …… 17

2.1　PKI 服务 …… 17

2.1.1　PKI 服务的概念 …… 17

2.1.2　PKI 服务的作用 …… 19

2.1.3　PKI 服务的意义 …… 20

2.2　PKI 服务的内容 …… 21

2.2.1　PKI 服务的认证性 …… 21

2.2.2　PKI 服务的保密性 …… 21

2.2.3　PKI 服务的不可否认性 …… 21

2.3 PKI 服务的操作性 …… 23
2.3.1 实施 PKI 服务的实体 …… 23
2.3.2 认证中心 …… 27
2.3.3 注册中心 …… 30
习题 …… 36

第 3 章 证书和证书注销列表 …… 37
3.1 ASN.1 …… 37
3.1.1 ASN.1 概述 …… 37
3.1.2 ASN.1 数据类型 …… 39
3.1.3 BER 编码和 DER 编码 …… 41
3.2 证书 …… 49
3.2.1 X.509 证书 …… 50
3.2.2 基本证书结构和语义 …… 53
3.2.3 tbsCertificate …… 57
3.2.4 证书扩展项 …… 64
3.3 证书策略 …… 70
3.3.1 交叉认证 …… 71
3.3.2 策略映射 …… 72
3.3.3 认证路径处理 …… 72
3.3.4 自签证书 …… 73
3.4 密钥和策略信息扩展 …… 73
3.4.1 需求 …… 73
3.4.2 公钥证书和 CRL 扩展字段 …… 74
3.5 主题和签发者信息扩展 …… 81
3.5.1 需求 …… 81
3.5.2 证书和 CRL 扩展字段 …… 81
3.6 证书路径约束扩展 …… 84
3.6.1 需求 …… 84
3.6.2 证书扩展字段 …… 85
3.7 认证机构和注册机构 …… 89
3.7.1 CA 信任链 …… 89
3.7.2 注册机构 …… 99

3.8 证书注销列表 …… 100
3.8.1 证书注销列表的概念 …… 100
3.8.2 证书注销列表的内容 …… 104
3.8.3 增量 CRL 和 CRL 发布点 …… 105
3.8.4 在线证书状态协议 …… 108
3.9 属性证书和漫游证书 …… 118
3.9.1 属性证书 …… 118
3.9.2 漫游证书 …… 119
习题 …… 119

第 4 章 信任模型 …… 121
4.1 信任相关的概念 …… 121
4.1.1 信任 …… 121
4.1.2 信任域 …… 122
4.1.3 信任锚 …… 123
4.2 信任关系 …… 124
4.3 信任模型 …… 125
4.3.1 严格层次结构 …… 125
4.3.2 分布式信任结构 …… 126
4.3.3 Web 模型 …… 127
4.3.4 以用户为中心的信任 …… 129
4.4 交叉认证 …… 130
4.5 实体命名 …… 131
4.6 证书路径处理 …… 132
4.6.1 路径构造 …… 133
4.6.2 路径确认 …… 134
4.6.3 信任锚的考虑 …… 134
4.7 信任计算 …… 134
4.7.1 可信性和信任的形式定义 …… 135
4.7.2 信任产生机制 …… 138
4.7.3 在线社团的信誉报告机制 …… 139
习题 …… 141

第 5 章　公开密钥密码体制标准 …… 142
5.1　信息对象类 …… 142
5.2　RSA 密码体系标准 …… 146
5.2.1　RSA 标准用到的符号 …… 146
5.2.2　密钥类型 …… 148
5.2.3　数据转换原语与密码原语 …… 149
5.2.4　加解密方案 …… 151
5.2.5　带附属的签名方案 …… 154
5.2.6　RSA 方案的 ASN.1 表述 …… 156
5.3　Diffie-Hellman 密钥约定标准 …… 158
5.3.1　定义和注记 …… 158
5.3.2　D-H 方案 …… 159
5.3.3　对象描述符 …… 160
5.4　基于口令的加密标准 …… 160
5.4.1　加解密过程 …… 161
5.4.2　对象描述符 …… 162
5.5　扩展证书语法标准 …… 162
5.6　密码信封封装标准 …… 164
5.6.1　密码信封封装标准概述 …… 164
5.6.2　通用语法 …… 166
5.6.3　内容类型 …… 166
5.7　私钥信息语法标准 …… 173
5.7.1　私钥信息语法 …… 173
5.7.2　加密私钥信息语法 …… 174
5.8　可选择的对象类和属性类型 …… 174
5.8.1　辅助对象类 …… 175
5.8.2　可选择类型 …… 176
5.9　证书请求语法描述标准 …… 180
5.9.1　证书请求步骤 …… 180
5.9.2　证书请求语法 …… 181
5.10　密码组件接口标准 …… 183
5.10.1　PKCS#11 中用到的数据类型 …… 183
5.10.2　应用编程接口 …… 184

5.11 个人信息交换语法 …… 189
5.11.1 PKCS#12 保密模式和完整模式 …… 189
5.11.2 PFX PDU 数据格式 …… 190
5.11.3 PFX PDUS 的产生与使用 …… 192
习题 …… 193

第 6 章 认证中心标准 …… 196
6.1 简单认证标准 …… 196
6.1.1 引言 …… 196
6.1.2 验证数据的明文传送 …… 197
6.1.3 利用单向散列函数传送随机或时间数据 …… 197
6.1.4 二次散列与对称加密传送 …… 199
6.2 强认证标准 …… 200
6.2.1 引言 …… 200
6.2.2 获取使用者会话公钥 …… 201
6.2.3 强认证的认证方式 …… 202
6.2.4 密钥的保存与令牌控制 …… 204
6.2.5 生物识别与三因素认证 …… 205
6.3 证书管理标准 …… 206
6.3.1 证书管理协议 …… 207
6.3.2 证书请求消息格式 …… 221
6.4 PKI 运作方式 …… 228
6.4.1 认证惯例框架 …… 228
6.4.2 证书策略和认证惯例陈述 …… 230
6.4.3 规定集的内容 …… 234
习题 …… 237

第 7 章 安全协议 …… 239
7.1 SSL 协议及其应用 …… 239
7.1.1 引言 …… 239
7.1.2 SSL 协议概述 …… 240
7.1.3 记录层协议 …… 244

7.1.4 change_cipher_spec 协议 …… 248
7.1.5 警告协议 …… 248
7.1.6 握手层协议 …… 250
7.1.7 密钥管理 …… 260
7.1.8 SSL 安全性 …… 261
7.1.9 SSL 应用 …… 265
7.2 安全电子交易系统 …… 266
7.2.1 SET 概述 …… 266
7.2.2 SET 的基本概念 …… 267
7.2.3 支付处理流程 …… 271
7.2.4 SET 安全性分析 …… 280
7.3 S/MIME …… 282
习题 …… 283

第 8 章 安全应用概述 …… 285
8.1 X.509 标准与 PKIX 标准的差异 …… 285
8.2 电子商务 …… 287
8.2.1 业务分类 …… 288
8.2.2 支付网关 …… 289
8.2.3 业务系统 …… 289
8.2.4 用户及终端 …… 289
8.2.5 用户接入 …… 290
8.2.6 电子商务支付体系功能 …… 291
8.2.7 SET 支付体系 …… 296
8.2.8 电子商务业务系统 …… 298
8.3 电子政务概述 …… 300
8.3.1 电子政务 …… 300
8.3.2 电子政务总体技术框架 …… 302
习题 …… 309

第 9 章 实施 PKI 的问题和措施 …… 311
9.1 CPCA 设计 …… 311

9.1.1 CPCA 的体系结构 …… 311
9.1.2 系统设计目标 …… 313
9.1.3 CPCA 系统软件结构 …… 314
9.1.4 软件功能模块概述 …… 317
9.1.5 证书分类和证书格式 …… 318
9.1.6 CPCA 交叉认证 …… 319
9.2 CA 系统结构和功能描述 …… 320
9.2.1 CPCA 网络总体结构 …… 320
9.2.2 CPCA 全国中心 …… 321
9.2.3 审核受理中心 …… 324
9.2.4 业务受理网点 …… 325
9.2.5 CPCA 系统主要子系统及其功能 …… 326
9.2.6 密钥管理 …… 331
9.2.7 证书管理 …… 334
9.3 CA 数据和业务流程 …… 335
9.3.1 CA 系统数据流程 …… 335
9.3.2 CA 系统业务流程 …… 338
9.3.3 证书作废状态查询 …… 342
9.3.4 证书的归档 …… 342
9.3.5 业务管理 …… 343
9.3.6 RA 管理系统 …… 344
9.4 CPCA 系统安全性设计 …… 349
9.4.1 网络安全性设计 …… 349
9.4.2 防火墙系统的功能介绍 …… 350
9.4.3 密码模块安全性 …… 351
9.4.4 数据库安全性 …… 352
9.4.5 程序中间数据的安全性 …… 355
9.4.6 身份认证安全性 …… 355
9.4.7 系统管理的安全性 …… 358
9.4.8 系统操作的可监控性 …… 358
9.4.9 灾难恢复设计 …… 359
习题 …… 360

附录 A　技术标准和规范 …… 362

附录 B　应用编程接口 …… 364

参考文献 …… 367