

<<PKI原理与技术>>

图书基本信息

书名：<<PKI原理与技术>>

13位ISBN编号：9787302076407

10位ISBN编号：7302076405

出版时间：2004-1

出版时间：清华大学出版社

作者：谢冬青

页数：368

字数：483000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<PKI原理与技术>>

内容概要

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。

。

<<PKI原理与技术>>

书籍目录

第1章 PKI基础设施 1.1 基础设施 1.2 安全基础设施的概念 1.3 公钥基础设施 习题第2章 核心PKI服务 2.1 PKI服务 2.2 PKI服务的内容 2.3 PKI服务的操作性 习题第3章 证书和证书注销列表 3.1 ASN.1 3.2 证书 3.3 证书策略 3.4 密钥和策略信息扩展 3.5 主题和签发者信息扩展 3.6 证书路径约束扩展 3.7 认证机构和注册机构 3.8 证书注销列表 3.9 属性证书和漫游证书 习题第4章 信任模型 4.1 信任相关的概念 4.2 信任关系 4.3 信任模型 4.4 交叉认证 4.5 实体命名 4.6 证书路径处理 4.7 信任计算 习题第5章 公开密钥密码体制标准 5.1 信息对象类 5.2 RSA密码体系标准 5.3 Diffid-Hellman密钥约定标准 5.4 基于口令的加密标准 5.5 扩展证书语法标准 5.6 密码信封封装标准 5.7 私钥信息语法标准 5.8 可选择的对象类和属性类型 5.9 证书请求语法描述标准 5.10 密码组件接口标准 5.11 个人信息交换语法 习题第6章 认证中心标准 6.1 简单认证标准 6.2 强认证标准 6.3 证书管理标准 6.4 PKI运作方式 习题第7章 安全协议 7.1 SSL协议及其应用 7.2 安全电子交易系统 7.3 S/MIME 习题第8章 安全应用概述 8.1 X.509标准与PKIX标准的差异 8.2 电子商务 8.3 电子政务概述 习题第9章 实施PKI的问题和措施 9.1 CPCA设计 9.2 CA系统结构和功能描述 9.3 CA数据和业务流程 9.4 CPCA系统安全性设计 习题附录A 技术标准和规范附录B 应用编程接口参考文献

<<PKI原理与技术>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>