

## <<公开密钥基础设施>>

### 图书基本信息

书名：<<公开密钥基础设施>>

13位ISBN编号：9787115090249

10位ISBN编号：7115090246

出版时间：2001-1

出版时间：人民邮电出版社 (2001年1月1日)

作者：CarlisleAdams

页数：198

字数：333000

译者：冯登国

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>

## <<公开密钥基础设施>>

### 内容概要

本书分为三部分。

第一部分提供了基本的背景信息，这些信息有利于更好地理解PKI的概念和原理。

第二部分讲述与PKI相关的标准和活动。

书的这一部分有两个基本目的。

第一，提供了PKI包括的主要标准的概述，并讨论了每组的侧重点。

第二，展示了该领域的相对稳定性和成熟性，突

## <<公开密钥基础设施>>

### 作者简介

Carlisle Adams从事各种公开密钥基础设施的设地、规范和标准化工作已有多年，他为这些领域所作出的贡献已得到国际公认。

他积极地加入到IETF的公开密钥基础设施-X.509 (PKIX) 和通用认证技术 (CAT) 工作小组中，同时他编著和和他人合著了许多标准索引和报告规范，其中包括：RFCs2025 (SPKM)、2144 (CAST-128)、2479 (IDUP-GSS-API)、2510 (CMP)、2511 (CRMF)、2560 (OCSP) 和2612 (CAST-256)。他在其他PKI标准化的工作中也作出了贡献。

这些工作包括：ISO/SC2、ISO/TC68、ANSI X9.1和U.S.FPKI TWG。

Adams获得了计算机专业的学士和硕士学位以及电子工程专业的博士学位。

现在是信托技术标准程序委员会的高级密码学者和管理者。

他研究和所从事的领域包括对称分组密码的结构设计和分析以及Internet的安全协议的设计、分析和标准化。

## &lt;&lt;公开密钥基础设施&gt;&gt;

## 书籍目录

第一部分 概念 第1章 概述 第2章 公钥密码学 2.1 对称和非对称密码 2.2 公钥和私钥对 2.3 公钥密码的服务 2.4 算法 2.5 小结 参考文献 第3章 基础设施的概念 3.1 普适性基础 ( Pervasive Substrate ) 3.2 应用支撑 3.3 商业驱动 3.4 公开密钥基础设施的定义 3.5 小结 第4章 核心PKI服务：认证、完整性和机密性 4.1 定义 4.2 机制 4.3 可操作性的考虑 4.4 小结 参考文献 第5章 PKI支撑的服务 5.1 安全通信 5.2 安全时间戳 5.3 公证 5.4 不可否认 5.5 特权管理 5.6 创建PKI支撑的服务所需要的机制 5.7 可操作性的考虑 5.8 "综合PKI"和当前现实 5.9 小结 参考文献 第6章 证书和认证 6.1 证书 6.2 证书策略 6.3 认证机构 6.4 注册机构 6.5 小结 参考文献 第7章 密钥和证书管理 7.1 密钥/证书生命周期管理 7.2 小结 参考文献 第8章 证书撤消 8.1 周期发布机制 8.2 其他撤消选择 8.3 性能、扩展性和合时性 8.4 小结 参考文献 第9章 信任模型 9.1 认证机构的严格层次结构 9.2 分布式信任结构 9.3 Web模型 9.4 以用户为中心的信任 9.5 交叉认证 9.6 实体命名 9.7 证书路径处理 9.8 小结 参考文献 第10章 单实体多证书..... 第11章 PKI信息的分发：资料库与其他技术 第12章 PKI的运作考虑 第13章 法律框架 第14章 结论与进一步阅读的材料 第二部分 标准 第15章 概述 第16章 主要的标准化活动 第17章 标准化现状和发展 第18章 标准：必要但尚不足 第19章 结论与进一步阅读的材料 第21章 实施PKI的益处及成本 第22章 PKI实施中的问题与决策 第23章 PKI实施中的障碍 第24章 典型的商务模型 第25章 结论与进一步阅读的材料

## <<公开密钥基础设施>>

### 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>