


系？既然有了数字证书，为什么还需要私钥？既然数字证书是公开的，还需要U盾干什么？很多人对此都困惑不解。由于数字证书涉及的技术领域非常广泛，而且技术专业性比较强，如果没有相当的专业功底，指望在短期内快速搞清楚相关概念和基本原理是十分困难的。

通俗地讲，数字证书可想象成一个“网络版的身份证”。数字证书里包含姓名、性别等身份信息，更重要的是也包含一个公钥。每个用户都拥有一个数字证书和一个私钥（与数字证书中的公钥配对），数字证书可以公开，但私钥必须保密。基于数字证书和私钥，素昧平生的交易双方无需见面，在网上就可确认对方的真实身份（客户需出示自己的数字证书，商家首先从客户数字证书中获得其身份信息，然后商家远程验证客户是否拥有对应的私钥；如果验证通过，则说明客户的身份真实有效，可以继续交易，否则应拒绝交易）。由于私钥的安全性至关重要，为防止私钥泄露，必须采用硬件设备加以安全保护，对于个人私钥，目前均采用 USB Key 方式，俗称为 U 盾。

专门负责颁发数字证书的系统称为 CA 系统，负责管CA 系统的机构称作 CA 中心。所有与数字证书相关的各种概念和技术，统称为Public Key Infrastructure），其中数字证书格式、CA 以及如何使用数字证书等内容均在其范畴。PKI 的主要功能是绑定证书持有者的身份和相关的密钥对（通过为公钥及相关的用户身份信息签发数字证书），为用户提供方便的证书申请、证书作废、证书获取、证书状态查询的途径，并利用数字证书及相关的各种服务（证书发布、黑名单发布、时间戳服务等）实现通信中各实体的身份认证、完整性、抗抵赖性和保密性。

但在日常沟通交流中，也将 PKI 技术称为 CA 技术、数字证书技术。

### （三）

数字证书技术并不仅仅只解决身份认证问题，事实上，它已经成为当前解决身份认证、数据保密与完整、行为抗抵赖等问题的最佳技术。尽管数字证书如此重要、如此普及，但这方面的书籍并不多，要么过于简单内容不全面，要么偏重理论缺乏实用性，对行业内从事技术管理、系统设计、软件研发、项目实施、系统运维等人员的指导性不足。

本书作者具有近二十年的应用安全工作经验和近十年的企业信息化工作经验，见证了中国 CA 行业从无到有的发展历程，有丰富的 PKI 领域研究、开发、工程及标准等相关经验。为方便业界人士快速理解 PKI、快速把握数字证书技术，并能快速运用到具体的工作当中，作者将多年的实践经验进行总结和提炼，经过长达近两年的辛苦编写终于完成本书的全部内容，希望能得到业内同行们的指教，以促进 CA 行业的健康发展。本书是国内第一部全面介绍 PKI 技术的书籍，涵盖技术、标准、运营、法规等内容。

本书内容共分为 7 部分，由 29 章内容组成：

第一部分：“如何理解 PKI”。由 3 章内容组成，包括为什么会出现 PKI 技术、PKI 包括哪些内容、其他非对称密钥管理体系等。

第二部分：“PKI 技术基础”。由 4 章内容组成，包括 ASN.1 及其编码规则、密码技术、LDAP 技术、实验一（DER 编码示例和 RSA 算法示例）等。

第三部分：“PKI 之数字证书与私钥：网络身份证”。由 6 章内容组成，包括公/私钥格式、数字证书格式、数字证书分类、私钥与证书存储方式、私钥与证书访问方式、实验二（RSA 公钥格式编码示例、数字证书格式编码示例和 Windows 证书库操作示例）等。

第四部分：“PKI 之 CA 与 KMC：管理网络身份证”。由 5 章内容组成，包括系统结构、系统设计、对外在线服务、网络部署结构、实验三（OpenSSL CA 和 EJBCA 示例）等。

第五部分：“PKI 之应用：使用网络身份证”。由 4 章内容组成，包括基本应用、通用应用技术、常见应用、实验四（Windows IIS、Apache、Tomcat 等服务器证书配置）等。

第六部分：“PKI 之运营：CA 中心”。由 4 章内容组成，包括机房建设、运营文件、业务管理、资质申请等。

第七部分：“PKI 之法规与标准”。由 3 章内容组成，包括国内法规、国内标准、国际标准等。

本书精心选材、内容翔实、重点突出、特点鲜明，既有原理介绍，又有实验案例，具有很强的实用性。本书非常适合以下读者：

1. 从事信息安全领域（如系统设计、软件研发、项目实施、系统运维、技术管理等）的技术人员。

2. 希望了解数字证书技术的各类企事业技术人员或管理人员。

3. 信息安全、密码学、计算机等专业的本科高年级学生和研究生。

本书由张明德担任主编，刘伟等多人参与了本书部分内容的编写。其中，张明德负责内容策划、提纲拟定、统筹协调、内容审核和大部分内容的编写；刘伟负责第 6 章、第 12 章、第 18 章、第 19 章、第 22 章、第 24 章、第 29 章等内容的编写；张迪、刘文涛、胡安勇、李伟斌、王秋凤等参与部分内容的资料整理。本书在写作过程中得到了很多朋友的支持和关心，在此非常感谢所有关心、支持和帮助过作者的朋友们。

由于 PKI 是一门专业性很强的技术，涉及知识面很广，况且作者的能力及水平有限，出书时间又十分紧张，本书的缺点或错误在所难免，如蒙指正不胜感激。热忱欢迎广大读者的批评指导。

作者联系方式：zmdbook@163.com。

张明德

2014 年 9 月于北京

# 目 录

## 第一部分 如何理解 PKI

第 1 章 为什么会出现 PKI 技术 .....	2
1.1 保密通信催生了密码技术 .....	2
1.1.1 古代中国军队的保密通信方法 .....	2
1.1.2 传统密码学与古代西方保密通信方法 .....	3
1.1.3 两次世界大战的密码斗法 .....	6
1.1.4 现代密码学与信息时代 .....	7
1.2 密码技术普及推动了密钥管理技术的发展 .....	9
1.2.1 密钥管理 .....	9
1.2.2 对称密钥管理技术 .....	11
1.2.3 非对称密码技术简化了密钥管理 .....	12
1.3 PKI 本质是把非对称密钥管理标准化 .....	14
1.4 私钥专有权使人联想到手写签名 .....	15
1.5 电子签名法赋予电子签名与认证法律地位 .....	16
第 2 章 PKI 包括哪些内容 .....	18
2.1 PKI 体系框架 .....	18
2.2 PKI/数字证书与私钥 .....	20
2.3 PKI/CA 与 KMC .....	22
2.4 PKI/应用 .....	25
2.5 PKI/运营 .....	27
2.6 PKI/法规与标准 .....	29
2.6.1 国内法规 .....	29
2.6.2 国内标准 .....	30
2.6.3 国际标准 .....	31
2.7 PKI/信任模型 .....	36
2.7.1 根 CA 信任模型 .....	37
2.7.2 交叉认证信任模型 .....	38
2.7.3 桥 CA 信任模型 .....	39
2.7.4 信任列表信任模型 .....	39



第 3 章 其他非对称密钥管理体系 .....	41
3.1 PGP .....	41
3.2 EMV .....	42

## 第二部分 PKI 技术基础

第 4 章 ASN.1 及其编码规则 .....	48
4.1 ASN.1 (抽象文法描述语言) .....	48
4.2 BER (基本编码规则) 与 DER (定长编码规则) .....	50
4.2.1 数据类型标识 .....	50
4.2.2 BER 基本编码规则 .....	52
4.2.3 DER 定长编码规则 .....	54
第 5 章 密码技术 .....	56
5.1 密码算法 .....	56
5.1.1 算法分类 .....	56
5.1.2 对称密码算法 .....	56
5.1.3 非对称密码算法 .....	60
5.1.4 摘要算法 .....	62
5.2 运算模式 (工作模式) .....	64
5.2.1 ECB .....	64
5.2.2 CBC .....	64
5.2.3 CFB .....	64
5.2.4 OFB .....	65
5.3 扩展机制 .....	65
5.3.1 MAC 与 HMAC .....	65
5.3.2 OTP .....	67
5.3.3 数字签名 .....	68
5.3.4 数字信封 .....	69
5.4 密码应用实践 .....	70
5.4.1 软件加密与硬件加密 .....	70
5.4.2 网络层加密与应用层加密 .....	72
5.4.3 密钥管理的基本原则 .....	72
5.4.4 密码设备的自身安全性 .....	73
5.5 密码算法 ASN.1 描述 .....	74
5.5.1 密码算法格式 .....	74
5.5.2 密码算法 OID .....	75
5.6 密码消息 ASN.1 描述 .....	75
5.6.1 通用内容消息 ContentInfo .....	75
5.6.2 明文数据消息 Data .....	75

5.6.3	数字签名消息 SignedData	76
5.6.4	数字信封消息 EnvelopedData	77
5.6.5	数字签名及信封消息 SignedAndEnvelopedData	78
5.6.6	摘要消息 DigestedData	78
5.6.7	加密数据消息 EncryptedData	79
5.6.8	密钥协商消息 KeyAgreementInfo	79
5.6.9	密码消息类型 OID	79
5.7	Base64 编码	80
第 6 章	LDAP 技术	82
6.1	目录服务与 LDAP 概述	82
6.1.1	目录服务简介	82
6.1.2	X.500 协议简介	83
6.1.3	LDAP 协议简介	84
6.1.4	LDAP 模型简介	85
6.1.5	LDAP Schema	88
6.1.6	LDAP 认证方式	91
6.1.7	LDIF 数据交换文件	94
6.2	常见 LDAP 产品介绍	97
6.2.1	IBM TDS	97
6.2.2	Sun Java 系统目录服务器	97
6.2.3	Novell eDirectory	98
6.2.4	GBase 8d	98
6.2.5	OpenLDAP	99
6.2.6	Microsoft Active Directory	99
6.3	LDAP 部署与优化	100
6.3.1	复制介绍	100
6.3.2	引用机制介绍	101
6.3.3	复制机制的部署	102
6.3.4	引用机制的部署	104
6.3.5	LDAP 优化	105
6.4	面向 LDAP 的系统设计与开发	106
6.4.1	LDAP 管理工具	106
6.4.2	应用接口编程与实例	109
6.4.3	LDAP 应用案例	119
第 7 章	实验一	120
7.1	DER 编码示例: X.501 Name 类型	120
7.1.1	ASN.1 描述与实例	120
7.1.2	DER 编码过程	121