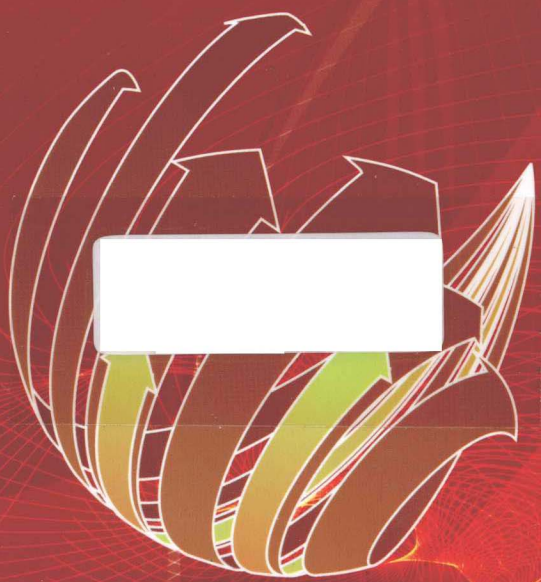
PKI/CA与数字证书技术大全

张明德　刘　伟　编著



中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

PKI/CA 与数字证书技术大全

张明德　刘　伟　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

数字证书技术，又称作 PKI 技术或 CA 技术，不仅涉及的技术领域广泛、标准规范庞杂，而且还涉及运营管理和法律法规。本书是国内第一部全面介绍数字证书技术的书籍，涵盖技术、标准、运营、法规等内容。为方便读者快速理解 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，本书主要从七个方面来全面介绍数字证书技术，主要内容包括：如何理解 PKI、PKI 技术基础、PKI 之数字证书与私钥（网络身份证）、PKI 之 CA 与 KMC （管理网络身份证）、PKI 之应用（使用网络身份证）、PKI 之运营（CA 中心）、PKI 之法规与标准。

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。可以作为从事信息安全领域（如系统设计、软件研发、项目实施、系统运维、技术管理等）的技术人员的技术参考手册，也可以作为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的学习资料，同时还可以作为信息安全、密码学、计算机等专业的本科高年级学生和研究生的入门教材。

图书在版编目（CIP）数据

PKI/CA 与数字证书技术大全/张明德，刘伟编著. —北京：电子工业出版社，2015.6
ISBN 978-7-121-26106-0

Ⅰ. ①P… Ⅱ. ①张… ②刘… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2015）第 105944 号

策划编辑：赵 平
责任编辑：周宏敏
印 刷：北京京科印刷有限公司
装 订：北京京科印刷有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×1 092 1/16印张：33 字数：888 千字
版 次：2015 年 6 月第 1 版
印 次：2015 年 6 月第 1 次印刷
印 数：3000 册 定价：98.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

（一）

四十年前，世界上还没有公钥密码算法。1976 年，公钥密码算法的思想被提出，1978 年，第一个公钥密码算法 RSA 诞生了，标志着密码学进入了一个全新时代，使密码技术的应用从单纯的保密通信扩展到了身份认证。

三十年前，世界上还没有数字证书。1988 年，第一个数字证书标准 X.509 v1 诞生了（作为 ITU X.500 的一部分），标志着密码学应用开始进入 PKI 时代。

二十年前，中国还没有数字证书。1997 年，第一个基于数字证书的电子交易规范 SET 诞生了，当年便正式走进中国。由于受电子商务泡沫经济和对 PKI 前景过于追捧的影响，自 1998 年开始形成一种盲目的 CA 中心建设热潮，各部委及各省份（直辖市）均开始积极投资建设 CA 中心。

十年以前，大家都不知道数字证书（俗称 U 盾）为何物，就连专门从事数字证书服务的 CA 中心也不知道路在何方。截至 2004 年底，一半以上省份（直辖市）建立了区域 CA 中心，部分部委建立了行业 CA 中心，CA 中心总数已经超过 60 家，形成了一种乱序竞争的态势。尽管累计投入已超数亿元，但数字证书发放量不过几百万，业务收入不足几千万。随着电子商务泡沫的破灭，全球经济进入低谷，CA 中心也陷入困境。

五年以前，很多人依然不知道数字证书为何物，但已经有发烧友开始炫耀如何在家里就可实现网上银行汇款转账，也已经有企业员工开始享受在办公室就可完成报税、报关、报检等业务。2005 年 4 月 1 日开始生效的《电子签名法》，让数字证书有了法律的武装，也给 CA 中心带来了崭新的生机，CA 中心正式进入规范管理和有序发展的轨道，数字证书也逐步在报税、报关、报检、网上银行等领域得到广泛应用。截至 2010 年底，获得行政许可资质的 CA 中心约 30 家。

到了今天，还有几个人不知道数字证书为何物呢？没有数字证书，你还对淘宝网店的资金账户放心吗？你还敢开通网上银行的汇款转账功能吗？你还能忍受去报税或社保大厅去排队办理业务吗？已经有调皮者开始抱怨手里的 U 盾太多！哎，只能怪他银行账户太多。截至 2013 年底，获得行政许可资质的 CA 中心约 33 家，有效数字证书已达 2.6 亿张。CA 中心的发展进入黄金时期，数字证书进一步向社保缴纳、公积金管理、第三方支付、电子病历、移动办公、企业管理、电子保单、网上招投标等领域渗透。

也许五年以后，“一证通”时代就会来到。一个 U 盾就可访问所有银行的网上银行，一张数字证书就能访问政府的所有公共业务，我们拭目以待！

（二）

那么数字证书到底为何物？PKI 和 CA 又是什么？数字证书与公钥密码算法有什么关

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，负责管理并运营 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 PKI（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属于 PKI 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

第二部分　PKI 技术基础

第三部分 PKI 之数字证书与私钥：网络身份证

第五部分　PKI 之应用：使用网络身份证

第六部分　PKI 之运营：CA 中心

第七部分 PKI 之法规与标准