

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



电子工业出版社
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



电子工业出版社

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单位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入门教材。

未经许可, 不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有, 侵权必究。

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 zlt@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、软件开发、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

7.2	RSA 算法示例	123
7.2.1	密钥产生	123
7.2.2	加密解密	124

第三部分 PKI 之数字证书与私钥：网络身份证

第 8 章	公/私钥格式	126
8.1	RSA	126
8.2	SM2	128
第 9 章	数字证书格式	130
9.1	基本格式	130
9.1.1	证书域组成 (Certificate)	130
9.1.2	证书内容 (tbsCertificate)	130
9.2	标准扩展项	135
9.2.1	标准扩展项 (Standard Extensions)	135
9.2.2	专用互联网扩展项	145
9.3	国内扩展项	146
9.3.1	卫生系统专用扩展项	146
9.3.2	国内通用扩展项	147
第 10 章	数字证书分类	150
10.1	根据证书持有者分类	150
10.2	根据密钥分类	150
第 11 章	私钥与证书存储方式	152
11.1	证书保存形式	152
11.1.1	DER 文件形式	152
11.1.2	Base64 文件形式	154
11.1.3	PKCS#7 文件形式	154
11.1.4	Windows 证书库形式	155
11.2	私钥保存形式	157
11.2.1	PKCS#8 文件形式	158
11.2.2	PKCS#12 文件形式	158
11.2.3	Java Keystore 文件形式	160
11.2.4	密码设备形式	161
11.2.5	软件系统形式	162
第 12 章	私钥与证书访问方式	164
12.1	CryptoAPI	164

12.1.1	CryptoAPI 简介	164
12.1.2	使用证书	166
12.1.3	使用私钥	168
12.2	PKCS#11	172
12.2.1	PKCS#11 简介	172
12.2.2	使用证书	178
12.2.3	使用私钥	181
12.3	JCA/JCE	183
12.3.1	JCA/JCE 简介	183
12.3.2	使用证书	187
12.3.3	使用私钥	189
12.4	CNG	190
12.4.1	CNG 简介	190
12.4.2	使用证书	195
12.4.3	使用私钥	196
12.5	PC/SC	200
12.5.1	PC/SC 简介	200
12.5.2	使用证书	202
12.5.3	使用私钥	213
12.6	国密接口	213
12.6.1	国密接口简介	213
12.6.2	使用证书	215
12.6.3	使用私钥	217
第 13 章	实验二	222
13.1	RSA 公钥格式编码示例	222
13.1.1	ASN.1 描述与实例	222
13.1.2	DER 编码过程	222
13.2	数字证书格式编码示例	223
13.2.1	ASN.1 描述与实例	223
13.2.2	DER 编码过程	225
13.3	Windows 证书库操作示例	229
13.3.1	查看证书库内容	229
13.3.2	导入证书	230
13.3.3	导出证书	233

第四部分 PKI 之 CA 与 KMC: 管理网络身份证

第 14 章	系统结构	236
14.1	国际标准	236

14.2 国内标准	237
14.2.1 证书认证系统 CA	237
14.2.2 密钥管理系统 KMC	239
第 15 章 系统设计	241
15.1 证书认证系统 CA	241
15.1.1 用户注册管理系统 RA	241
15.1.2 证书/CRL 签发系统	242
15.1.3 证书/CRL 存储发布系统	243
15.1.4 证书/CRL 查询系统	244
15.1.5 证书管理系统	245
15.1.6 安全管理系统	245
15.2 密钥管理系统 KMC	246
15.3 企业级 CA 总体设计示例	248
15.3.1 技术路线选择	248
15.3.2 模块设计	250
15.3.3 数据库设计	251
15.3.4 双证书技术流程设计	253
第 16 章 对外在线服务	256
16.1 OCSP/SOCSP 服务	256
16.1.1 OCSP	256
16.1.2 SOCSP	258
16.2 CRL 服务	259
16.2.1 基本域组成 (CertificateList)	259
16.2.2 CRL 内容 (tbsCertList)	260
16.2.3 CRL 扩展项 crlExtensions	262
16.2.4 CRL 条目扩展项 crlEntryExtensions	265
16.3 LDAP 服务	267
16.3.1 发布数字证书到 LDAP	267
16.3.2 访问 LDAP 获取数字证书	268
第 17 章 网络部署结构	270
17.1 运营型 CA	270
17.2 企业级 CA	273
17.2.1 双层标准模式	273
17.2.2 双层简化模式	273
17.2.3 单层单机模式	274
17.2.4 纯硬件模式	274

17.3 按企业管理模式部署 CA	276
17.3.1 单机构	276
17.3.2 集团公司+集中部署+集中发证	276
17.3.3 集团公司+集中部署+分布发证	277
17.3.4 集团公司+两级部署+分布发证	278
第 18 章 实验三	280
18.1 OpenSSL CA 示例	280
18.1.1 简介	280
18.1.2 安装配置	280
18.1.3 申请证书	284
18.1.4 生成并下载 CRL	287
18.1.5 导入 CA 证书到 IE 可信任证书库	290
18.2 EJBCA 示例	291
18.2.1 简介	291
18.2.2 安装配置	292
18.2.3 申请证书	300
18.2.4 下载 CRL	303
第五部分 PKI 之应用：使用网络身份证	
第 19 章 基本应用	308
19.1 身份认证	308
19.2 保密性	310
19.3 完整性	311
19.4 抗抵赖性	312
19.5 证书有效性验证	314
第 20 章 通用应用技术	315
20.1 SSL/TLS (Secure Socket layer/Transport Layer Security)	315
20.1.1 概述	315
20.1.2 记录协议	315
20.1.3 握手协议	316
20.1.4 警告协议	317
20.1.5 改变密码约定协议	318
20.1.6 应用数据协议	318
20.2 IPSec	318
20.3 Kerberos	323
20.4 TSP	326

20.5	SET	331
20.6	3-D Secure	333
20.7	WAP	335
20.8	S/MIMI	338
第 21 章	常见应用	345
21.1	防止假网站与 Web 服务器证书	345
21.1.1	假网站	345
21.1.2	使用 Web 服务器证书预防假网站	346
21.2	防止假软件与代码签名证书	348
21.2.1	Web 技术的发展	348
21.2.2	插件技术与假网银软件	350
21.2.3	使用代码签名证书预防假网银软件	351
21.3	网上银行系统	352
21.3.1	简介	352
21.3.2	应用安全需求	353
21.3.3	应用安全总体架构	354
21.4	网上报税系统	355
21.4.1	简介	355
21.4.2	应用安全需求	356
21.4.3	应用安全总体架构	356
21.5	电子病历系统	357
21.5.1	简介	357
21.5.2	应用安全需求	357
21.5.3	应用安全总体架构	359
21.5.4	网络部署结构	359
21.6	公交 IC 卡在线充值系统	361
21.6.1	简介	361
21.6.2	应用安全需求	361
21.6.3	应用安全总体架构	362
21.6.4	充值交易流程	362
第 22 章	实验四	365
22.1	Windows IIS 服务器证书配置	365
22.1.1	下载并安装服务器证书	366
22.1.2	配置 SSL 策略	373
22.1.3	访问 Web Server	374
22.2	Apache 服务器证书配置	375
22.2.1	下载并安装服务器证书	375

22.2.2	配置 SSL 策略	379
22.2.3	访问 Web Server	381
22.3	Tomcat 服务器证书配置	381
22.3.1	下载并安装服务器证书	381
22.3.2	配置 SSL 策略	384
22.3.3	访问 Web Server	384

第六部分 PKI 之运营: CA 中心

第 23 章	机房建设	388
23.1	业务系统	388
23.1.1	证书认证中心	388
23.1.2	密钥管理中心	390
23.2	应用安全	391
23.3	数据备份	394
23.4	系统可靠性	394
23.5	物理安全	394
23.6	人事管理制度	396
第 24 章	运营文件	397
24.1	CPS	397
24.2	CP	398
24.3	RA 管理	399
第 25 章	业务管理	402
25.1	管理模式	402
25.1.1	总体框架	402
25.1.2	具体要求	404
25.1.3	管理模式示例	410
25.2	主要业务流程	412
25.2.1	证书申请类	412
25.2.2	证书作废类	417
25.2.3	证书查询类	418
25.3	客户服务	420
第 26 章	资质申请	422
26.1	电子认证服务使用密码许可证	422
26.1.1	政策法规要点	422
26.1.2	申请流程	423
26.2	电子认证服务许可证	424

26.2.1 政策法规要点	424
26.2.2 申请流程	425
26.3 电子政务电子认证服务管理	426
26.4 卫生系统电子认证服务管理	427
26.4.1 政策法规要点	427
26.4.2 接入流程	428

第七部分 PKI 之法规与标准

第 27 章 国内法规	432
27.1 电子签名法	432
27.2 电子认证服务管理办法	436
27.3 电子认证服务密码管理办法	440
27.4 电子政务电子认证服务管理办法	443
27.5 卫生系统电子认证服务管理办法	447
27.6 商用密码管理条例	449
27.7 商用密码科研管理规定	452
27.8 商用密码产品生产管理规定	454
27.9 商用密码产品销售管理规定	456
27.10 商用密码产品使用管理规定	458
27.11 境外组织和个人在华使用密码产品管理办法	459
第 28 章 国内标准	461
28.1 通用性标准	461
28.1.1 祖冲之序列密码算法 (GM/T 0001)	461
28.1.2 SM4 分组密码算法 (GM/T 0002)	461
28.1.3 SM2 椭圆曲线公钥密码算法 (GM/T 0003)	461
28.1.4 SM3 密码杂凑算法 (GM/T 0004)	462
28.1.5 SM2 密码算法使用规范 (GM/T 0009)	462
28.1.6 SM2 密码算法加密签名消息语法规则 (GM/T 0010)	463
28.1.7 数字证书认证系统密码协议规范 (GM/T 0014)	463
28.1.8 基于 SM2 密码算法的数字证书格式规范 (GM/T 0015)	464
28.1.9 通用密码服务接口规范 (GM/T 0019)	464
28.1.10 证书应用综合服务接口规范 (GM/T 0020)	467
28.1.11 IPSec VPN 技术规范 (GM/T 0022)	467
28.1.12 SSL VPN 技术规范 (GM/T 0024)	468
28.1.13 安全认证网关产品规范 (GM/T 0026)	468
28.1.14 签名验签服务器技术规范 (GM/T 0029)	469
28.1.15 安全电子签章密码技术规范 (GM/T 0031)	469

28.1.16	时间戳接口规范 (GM/T 0033)	470
28.1.17	基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范 (GM/T 0034)	470
28.1.18	证书认证系统检测规范 (GM/T 0037)	471
28.1.19	证书认证密钥管理系统检测规范 (GM/T 0038)	472
28.1.20	证书认证系统密码及其相关安全技术规范 (GB/T 25056)	473
28.1.21	电子认证服务机构运营管理规范 (GB/T 28447)	473
28.2	行业性标准	474
28.2.1	卫生系统电子认证服务规范	474
28.2.2	卫生系统数字证书应用集成规范	475
28.2.3	卫生系统数字证书格式规范	475
28.2.4	卫生系统数字证书介质技术规范	476
28.2.5	卫生系统数字证书服务管理平台接入规范	477
28.2.6	网上银行系统信息安全通用规范 (JR/T 0068)	477
第 29 章	国际标准	479
29.1	PKCS 系列	479
29.2	ISO 7816 系列	491
29.3	IETF RFC 系列	494
29.4	Microsoft 规范	502
29.5	Java 安全 API 规范	504
29.6	CCID 规范	506
附录	主要参考资料	507