

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

## 第一部分

# 如何理解 PKI



# 第1章 为什么会出现 PKI 技术

## 1.1 保密通信催生了密码技术

从古到今，军队历来是使用密码技术最频繁的地方，因为保护己方秘密并洞悉敌方秘密是克敌制胜的重要条件。正如《孙子兵法》中所说：“知己知彼，百战不殆；不知彼而知己，一胜一负；不知彼不知己，每战必败。”

### 1.1.1 古代中国军队的保密通信方法

明末清初著名的军事理论家揭暄所著《兵经百言》系统阐述了中国古代军队的通信方法：军队分开行动后，如相互之间不能通信，就要打败仗；如果能通信但不保密，则也要被敌人暗算。所以除了用锣鼓、旌旗、骑马送信、燃火、烽烟等联系外，两军相遇，还要对暗号。当军队分开有千里之远时，宜用机密信进行通信。机密信分为三种：改变字的通常书写或阅读方式；隐写术；不是把书信写在常用的纸上，而是写在特殊的、不引人注意的载体上。这些通信方式连送信的使者都不知道信中的内容，但收信人却可以接收到信息。

#### 1.1.1.1 阴符和阴书

公元前 1000 多年前，西周开国功臣姜子牙所著《六韬》中，讲述了战争中君主与在外将领保密通信的两种方法：阴符和阴书。

阴符共有八种：一种长一尺，表示大获全胜，摧毁敌人；一种长九寸，表示攻破敌军，杀敌主将；一种长八寸，表示守城的敌人已投降，我军已占领该城；一种长七寸，表示敌军已败退，远传捷报；一种长六寸，表示我军将誓死坚守城邑；一种长五寸，表示请拨运军粮，增派援军；一种长四寸，表示军队战败，主将阵亡；一种长三寸，表示战事失利，全军伤亡惨重。如奉命传递阴符的使者延误传递，则处死；如阴符的秘密被泄露，则无论无意泄露者或有意传告者也处死。只有国君和主将知道这八种阴符的秘密。这就是不会泄露朝廷和军队之间相互联系内容的秘密通信语言。

阴书是一种特殊书信，用于君主和主将之间军机大事的秘密联络。阴书都要拆分成三部分，并分派三人发出，每人拿一部分。只有这三部分合在一起才能读懂信的内容。

#### 1.1.1.2 虎符、信牌和字验

古代中国的君王常以虎符作为调用军队的凭证。虎符一般由铜、银等金属制成，背面刻有铭文，以示级别、身份、调用军队的对象和范围等；虎符分为两半，一半放在朝廷，另一半由在外的将帅保管。朝廷派来的使者，需携虎符验合，才可调兵遣将。春秋战国时期，魏信陵君使如姬窃取魏王的虎符，并以此夺取大将晋鄙的兵权，然后率兵大破秦军，解了赵国之围。