第六部分　PKI 之运营：CA 中心

第七部分 PKI 之法规与标准

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。