PKI 相关标准

PKI 的标准可分为两个部分：一类用于定义 PKI，而另一类用于 PKI 的应用，下面主要介绍定义 PKI 的标准。

ASN．1 基本编码规则的规范——X．209(1988)

ASN．1 是描述在网络上传输信息格式的标准方法。它有两部分：第一部分(ISO 8824/ITU X．208)描述信息内的数据、数据类型及序列格式-也就是数据的语法；第二部分(ISO8825/ITU X．209)描述如何将各部分数据组成消息．也就是数据的基本编码规则。这两个协议除了在 PKI 体系中被应用外，还被广泛应用于通信和计算机的其他领域。

目录服务系统标准——X．500(1993)

X．500 是一套已经被国际标准化组织(ISO)接受的目录服务系统标准，它定义了一个机构如何在全局范围内共享其名字和与之相关的对象。X．500 是层次性的．其中的管理域(机构、分支、部门和工作组)可以提供这些域内的用户和资源信息。在 PKI 体系中，X．500 被用来唯一标识一个实体．该实体可以是机构、组织、个人或一台服务器。X.500 被认为是实现目录服务的最佳途径，但 X.500 的实现需要较大的投资，并且比其他方式速度慢；但其优势是具有信息模型、多功能和开放性。

IDAP 轻量级目录访问协议— IDAP V3

LDAP 规范(RFCl487)简化了笨重的 X．500 目录访问协议，并且在功能性、数据表示、编码和传输方面部进行了相应的修改，1997 年．LDAP 第 3 版本成为

互联网标准。目前 ,IDAP V3 已经在 PKI 体系中被广泛应用于证书信息发布、CRI。信息发布、CA 政策以及与信息发布相关的各个方面。

数字证书标准 X．509(1 993)

X．5(19 是南国际电信联盟(ITU—T)制定的数字证书标准、在 X．500 确保用户名称唯一性的基础上．X．509 为 X．500 用户名称提供了通信实体的鉴别机制并规定了实体鉴别过程中广泛适用的证书语法和数据接口。X．509 的最初版本公布于 l 988 年，由用户公开密钥和用户标识符组成此外还包括版本号、证书序列号、CA 标识符、签名算法标识、签发者名称、证书有效期等信息。这一标准的最新版本是 X．509 V3，该版数字证书提供了一个扩展信息字段．用来提供更多的灵活性及特殊应用环境下所需的信息传送。

OCSP 在线证二拉状态协议

OCSP(OnIine Certificate Status Protocol)是 IETF 颁布的用于检查数字证书在某一交易时刻是否仍然有效的标准。该标准提供给 PKI 用户一条方便快捷的数字证书状态查询通道．使 PKI 体系能够更有效、更安全地在各个领域中被广泛应用。

PKCS 系列标准

PKCS 是南美 RSA 数据安全公司及其合作伙伴制定的一组公钥密码学标准，其中包括证书申请、证书更新、证书作废表发布、扩展证书内容以及数字签名、数字信封的格式等方面的一系列相关协议。