ICS 35.100.70
L 79

中华人民共和国国家标准

GB/T 19714—2005

信息技术　安全技术　公钥基础设施　证书管理协议

Information technology—Security technology—Internet public key infrastructure—Certificate management protocol

2005-04-19 发布　　2005-10-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准是依据 IETF RFC 2510 制定的。

本标准凡涉及密码算法相关内容，按国家有关法规实施。

本标准中引用的 RSA、SHA1、DH 密码算法均为举例性说明，具体使用时均须采用国家商用密码管理委员会批准的相应算法。

本标准的附录 B、附录 C、附录 F 为规范性附录，附录 A、附录 D、附录 E、附录 G 为资料性附录。

本标准由中华人民共和国信息产业部提出。

本标准由全国信息安全标准化技术委员会(TC260)归口。

本标准主要起草单位：北京创原天地科技有限公司、中国电子技术标准化研究所。

本标准主要起草人：林雪焰、吴志刚、王炳艳、陈震琦、张科研、李 丹、罗锋盈、陈 星。

引　言

本标准描述了公钥基础设施(PKI)证书管理协议,定义了与证书产生和管理相关的各方面所需要的协议消息,主要包括:申请证书、撤销证书、密钥更新、密钥恢复、交叉认证等等。

公钥基础设施中总共有四类实体:CA、RA、终端实体、证书/CRL 库,如何保证四实体之间的通信安全、在证书业务中如何对四类实体进行管理,这些问题是本标准解决的主要问题。

信息技术　安全技术　公钥基础设施 证书管理协议

1　范围

本标准描述了公钥基础设施(PKI)中的证书管理协议,定义了与证书产生和管理相关的各方面所需要的协议消息,这些消息主要包括申请证书、撤销证书、密钥更新、密钥恢复、交叉认证等。

本标准主要适用于在安全或不安全环境中实施 PKI 组件并实施管理,可作为 PKI 运营机构、PKI 组件开发者的参考指南。

2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB/T 16264.8—2005　信息技术　开放系统互连　目录　第 8 部分:公钥和属性证书框架(ISO/IEC 9594-8:2001,IDT)

RFC2511 因特网 X.509 公开密钥基础设施证书消息格式

3　术语和定义

下列术语和定义适用于本标准。

3.1

抽象语法记法一(ASN.1)　Abstract Syntax Notation 1(ASN.1)

用来组织复杂数据对象的表示法。

3.2

公钥证书　public key certificate

用户的公钥连同其他信息,并由发布该证书的证书认证机构的私钥进行加密使其不可伪造。

3.3

证书持有者　certificate holder

有效证书的主体对应的实体。

3.4

证书用户　certificate user

需要确切地知道另一实体的公开密钥的某一实体。

3.5

证书认证机构(CA)　Certificate Authority(CA)

负责创建和分配证书,受用户信任的权威机构。用户可以选择该机构为其创建密钥。

3.6

证书认证路径　certification path

一个 DIT 中对象证书的有序序列,通过处理该有序序列及其起始对象的公钥可以获得该路径的末端对象的公钥。