ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20519—2006

信息安全技术　公钥基础设施 特定权限管理中心技术规范

Information security technology—Public key infrastructures—Privilege management center technical specification

2006-08-30 发布　　2007-02-01 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

本标准的附录 A、附录 B 和附录 C 为资料性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准主要起草单位：国家信息安全工程技术研究中心。

本标准主要起草人：袁峰。

引　言

本标准依据 GB/T 20518—2006 要求，结合我国关于属性证书的实际应用经验，规范了权限管理系统的技术框架，是与 GB/T 20518—2006 属性证书格式标准相配套的技术标准。

特定权限管理基础设施 PMI(Privilege Management Infrastructure)是信息安全支撑平台的一个重要组成部分。PMI 中的特定权限管理中心是属性证书管理机构、策略管理机构、权限管理机构、计算机软硬件以及应用系统的集合，它为网络信任体系的访问控制系统提供权限管理和角色认证服务。本标准与 GB/T 16264.8—2005 配合构成完整的权限管理系统标准。

在本标准实施过程中，涉及到密码技术的具体应用时，按照国家密码管理局的有关规定和相关规范执行。

信息安全技术　公钥基础设施
特定权限管理中心技术规范

1　范围

本标准规定了一套作为特定权限管理基础设施(PMI)的特定权限管理中心技术框架,并规定了相关服务的要求。

本标准适用于特定权限管理中心基础设施的设计、建设和检测;对于特殊需求的应用系统,可根据具体的业务需求和情况进行灵活配置。

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 20518—2006　信息安全技术　公钥基础设施　数字证书格式

GB/T 16262.1—2006　信息技术　抽象语法记法一(ASN.1)　第1部分:基本记法规范(ISO/IEC 8824-1:2002,IDT)

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)

GB/T 16975.1—2000　信息技术　远程操作　第1部分:概念、模型和记法(idt ISO/IEC 13712-1:1995)

GB/T 1988　信息技术　信息交换用七位编码字符集(GB/T 1988—1998,eqv ISO/IEC 646:1991)

国家密码管理局《证书认证系统密码及其相关安全技术规范》

国家密码管理局《CA密码设备应用程序接口规范》

3　术语和定义

下列术语定义适用于本标准。

3.1

属性证书　attribute certificate

属性授权机构进行数字签名的数据结构,把持有者的身份信息与一些属性值绑定。

3.2

属性授权机构　attribute authority

通过发布属性证书来分配权限的认证机构,也称属性管理机构。

3.3

属性证书撤消列表　attribute certificate revocation list

标识由发布机构已发布的、不再有效的属性证书的索引表。