ICS 35.100.70
L 79

中华人民共和国国家标准

GB/T 20518—2006

信息安全技术　公钥基础设施 数字证书格式

Information security techniques—Public key infrastructure—Digital certificate format

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

本标准主要根据 IETF(互联网工程任务组) RFC 245 9 文件制定,并结合我国数字证书应用的特点进行相应的扩充和调整。

本标准凡涉及密码算法相关内容,按国家有关法规实施。

本标准的附录 A、附录 B、附录 C、附录 D 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(TC 260)归口。

本标准起草单位:吉大正元信息技术股份有限公司、中国电子技术标准化研究所、联想控股有限公司、国瑞数码安全系统有限公司、北京嘉学网络技术研究所。

本标准主要起草人:何立波、姜玉琳、袁文恭、张宝欣。

信息安全技术　公钥基础设施
数字证书格式

1　范围

本标准规定了中国数字证书的基本结构，并对数字证书中的各数据项内容进行了描述。本标准规定了一些标准的证书扩展域，并对每个扩展域的结构进行了定义，特别是增加了一些专门面向国内应用的扩充项。本标准同时还列举了一些证书中所支持的算法。

本标准适用于国内数字证书认证机构、数字证书认证系统的开发商以及基于数字证书的安全应用开发商。

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 16262.1—2006　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 16262.2—2006　抽象语法记法一(ASN.1)　第2部分：客体信息规范(ISO/IEC 8824-2：2002，IDT)

GB/T 16262.3—2006　抽象语法记法一(ASN.1)　第3部分：约束规范(ISO/IEC 8824-3：2002，IDT)

GB/T 16262.4—2006　抽象语法记法一(ASN.1)　第4部分：ASN.1规范的参数化(ISO/IEC 8824-4：2002，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 16284.4—1996　信息技术　文本通信　面向信报的文本交换系统　第4部分：抽象服务定义和规程(idt ISO/IEC 10021-4：1990)

GB/T 17969.1—2000　信息技术　开放系统互连　OSI登记机构的操作规程　第1部分：一般规程(eqv ISO/IEC 9834-1：1993)

ISO/IEC 9594-2：2001　信息技术　开放系统互连　目录　第2部分：模型

RFC 2313 PKCS #1：RSA加密版本1.5

RFC 822　Internet文本邮件的标准消息格式

RFC 1034　域名：概念和设备

RFC 1630　互联网中的通用资源标识(URL)

RFC 1738　统一资源定位器(URL)

RFC 791　互联网协议

3　术语和定义

下列术语和定义适用于本标准。