ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20518—2018
代替 GB/T 20518—2006

信息安全技术　公钥基础设施 数字证书格式

Information security technology—Public key infrastructure—Digital certificate format

2018-06-07 发布　　2019-01-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准代替GB/T 20518—2006《信息安全技术　公钥基础设施　数字证书格式》，与GB/T 20518—2006相比主要技术变化如下：

——在附录E算法技术支持中增加了对SM2和SM3密码算法的支持；删除了MD5，SHA-1算法的介绍；

——增加了5.3证书撤销列表的基本结构以及数字证书格式中扩展项的内容；

——修订了5.2.4中一些OID的值。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：上海格尔软件股份有限公司、长春吉大正元信息技术股份有限公司、上海市数字证书认证中心有限公司、中国金融认证中心、北京海泰方圆科技有限公司、北京数字认证股份有限公司、无锡江南信息安全工程技术中心、成都卫士通信息产业股份有限公司、兴唐通信科技有限公司、山东得安信息技术有限公司、国家信息安全工程技术研究中心。

本标准主要起草人：刘平、郑强、杨文山、赵丽丽、韩玮、赵改侠、傅大鹏、蒋红宇、罗俊、徐明翼、王妮娜、孔凡玉、袁锋。

本标准所代替标准的历次版本发布情况为：

——GB/T 20518—2006。

信息安全技术　公钥基础设施
数字证书格式

1　范围

本标准规定了数字证书和证书撤销列表的基本结构、各数据项内容。

本标准适用于数字证书认证系统的研发、数字证书认证机构的运营以及基于数字证书的安全应用。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

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

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

GB/T 17969.1—2015　信息技术　开放系统互联 OSI 登记机构的操作规程　第1部分：一般规程

GB/T 35275　SM2 密码算法加密签名消息语法规范

GB/T 35276　SM2 密码算法使用规范

PKCS #7　密码消息语法(Cryptographic message syntax)

3　术语和定义

下列术语和定义适用于本文件。

3.1

公钥基础设施　public key infrastructure；PKI

支持公钥管理体制的基础设施，提供鉴别、加密、完整性和不可否认性服务。

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

证书撤销列表　certificate revocation list；CRL

一个已标识的列表，它指定了一套证书颁发者确认为无效的证书。除了普通 CRL 外，还定义了一些特殊的 CRL 类型用于覆盖特殊领域的 CRLs。

3.4

证书序列号　certificate serial number

在 CA 颁发的证书范围内为每个证书分配的一个整数值。此整数值对于该 CA 所颁发的每一张证书必须是唯一的。

3.5

证书认证机构　certification authority；CA

受用户信任，负责创建和分配证书的权威机构。证书认证机构也可以为用户创建密钥。