ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0092—2020

基于 SM2 算法的证书申请语法规范

Specification of certificate request syntax based on SM2 cryptographic algorithm

2020-12-28 发布　　2021-07-01 实施

国家密码管理局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：北京信安世纪科技股份有限公司、格尔软件股份有限公司、北京数字认证股份有限公司、长春吉大正元信息技术股份有限公司、兴唐通信科技有限公司、卫士通信息产业股份有限公司、国家信息安全工程技术研究中心、山东得安信息技术有限公司、北京创原天地科技有限公司。

本文件主要起草人：汪宗斌、刘婷、郑强、傅大鹏、赵丽丽、王妮娜、赵闪、罗俊、张旭、周淑静、张庆勇、焦靖伟、史晓峰、马洪富。

引　言

本文件的内容参照证书请求语法规范(RFC2986 PKCS#10),按照我国相关密码政策和规范,结合我国实际应用需求及产品生产厂商的实践经验,定义了基于SM2算法的证书申请和证书申请信息语法格式,增添了证书申请信息的扩展属性和证书响应格式。

证书申请,由证书申请信息、数字签名算法和对证书申请信息的数字签名三部分组成。其中,证书申请信息又包括可区分的主体名称、主体公钥信息、一组可选属性集。

证书申请发送到证书认证机构之后,证书认证机构将该申请转换为数字证书。

基于SM2算法的证书申请语法规范

1 范围

本文件定义了使用SM2密码算法的证书申请语法、证书申请信息的扩展属性和证书响应格式。

本文件适用于数字证书认证系统的研制，数字证书应用系统使用SM2密码算法进行证书申请操作时，对证书申请语法的标准化封装。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 31503—2015 信息安全技术 电子文档加密与签名消息语法

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 33560—2017 信息安全技术 密码应用标识规范

GB/T 35275—2017 信息安全技术 SM2密码算法加密签名消息语法规范

GB/T 35276—2017 信息安全技术 SM2密码算法使用规范

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

证书 certificate

由国家认可的，具有权威性、可信性和公正性的第三方证书认证机构进行数字签名的一个可信的数字化文件。

3.2

签名 signature

由GB/T 32905定义的一种算法。由一个应用程序通过密码算法用私钥运算所产生的值，具有完整性，消息鉴别和/或签名者鉴别的特性。

3.3

属性 attributes

由对象的属性和一个相关属性值组成的集合。

4 缩略语

下列缩略语适用于本文件。

ASN.1：抽象语法标记(Abstract Syntax Notation One)

BER：基本编码规则(Basic Encoding Rule)