

ICS 35.040  
L 80  
备案号：38313—2013



# 中华人民共和国密码行业标准

GM/T 0015—2012

---

## 基于 SM2 密码算法的数字证书格式规范

Digital certificate format based on SM2 algorithm

2012-11-22 发布

2012-11-22 实施

---

国家密码管理局 发布

## 目 次

前言 .....	III
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 缩略语 .....	1
5 数字证书与 CRL .....	2
5.1 概述 .....	2
5.2 数字证书格式 .....	2
5.3 CRL 格式 .....	21
附录 A (规范性附录) 证书的结构 .....	27
A.1 证书构成(见表 A.1) .....	27
A.2 基本证书域(见表 A.2) .....	27
A.3 标准的扩展域(见表 A.3) .....	27
附录 B (规范性附录) 证书的结构实例 .....	29
B.1 用户证书的结构实例(见表 B.1) .....	29
B.2 服务器证书的结构实例(见表 B.2) .....	29
附录 C (规范性附录) 证书内容表 .....	31
C.1 自签名 CA 证书内容表(见表 C.1) .....	31
C.2 下级 CA 证书内容表(见表 C.2) .....	34
C.3 终端实体签名证书内容表(见表 C.3) .....	38
C.4 终端实体加密证书内容表(见表 C.4) .....	42
C.5 证书撤销列表内容表(见表 C.5) .....	46
附录 D (资料性附录) 数字证书编码举例 .....	50
D.1 RSA 数字证书编码 .....	50
D.2 SM2 数字证书编码 .....	54

## 前 言

本标准依据 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

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

本标准由国家密码管理局提出并归口。

本标准起草单位：上海格尔软件股份有限公司、北京市数字认证股份有限公司、北京海泰方圆科技有限公司、无锡江南信息安全工程技术中心、上海市数字证书认证中心有限公司、长春吉大正元信息技术股份有限公司、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、北京华大智宝电子系统有限公司、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、国家密码管理局商用密码检测中心。

本标准起草人：刘平、谭武征、李述胜、柳增寿、徐强、刘承、赵丽丽、李元正、王妮娜、陈跃、孔凡玉、袁峰、李志伟。

本标准涉及的密码算法按照国家密码管理部门的要求使用。

# 基于 SM2 密码算法的数字证书格式规范

## 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,并对数字证书和证书撤销列表中的各数据项内容进行了描述。

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 16264.8 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

GM/T 0006 密码应用标识规范

GM/T 0009 SM2 密码算法使用规范

GM/T 0010 SM2 密码算法加密签名消息语法规范

PKCS #7 Cryptographic Message Syntax Standard

RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**数字证书 digital 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(CA)进行数字签名的一个可信的数字化文件。

### 3.2

**证书撤销列表 certificate revocation list;CRL**

CA 对撤销的证书而签发的一个列表文件。

### 3.3

**CA 证书 CA certificate**

颁发给数字证书认证机构的证书。

### 3.4

**终端实体证书 entity certificate**

终端实体也称为用户证书,是由数字证书认证机构签发的个人证书、机构证书、设备证书等。

## 4 缩略语

下列缩略语适用于本文件。