ICS 35.040
L 80

中华人民共和国国家标准

GB/T 38541—2020

信息安全技术　电子文件密码应用指南

**Information security technology—
Guidance of cryptographic application for electronic records**

2020-03-06 发布　　2020-10-01 实施

国家市场监督管理总局
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。

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:中安网脉(北京)技术股份有限公司、北京电子科技学院、北京国脉信安科技有限公司、国家密码管理局商用密码检测中心、北京海泰方圆科技有限公司、北京书生电子技术有限公司、中国软件与技术服务有限公司。

本标准主要起草人:童新海、吴科科、冯雁、刘歆、谢四江、王佳宁、王天顺、袁峰、吕春梅、蒋红宇、郝立臣、郑志梅、李强。

信息安全技术　电子文件密码应用指南

1　范围

本标准提出了电子文件的密码应用技术框架和安全目标，描述了对电子文件进行密码操作的方法和电子文件应用系统使用密码技术的方法。

本标准适用于电子文件应用系统的开发和使用。

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 20518　信息安全技术　公钥基础设施　数字证书格式

GB/T 25069—2010　信息安全技术　术语

GB/T 31913—2015　文书类电子文件形成办理系统通用功能要求

GB/T 32905　信息安全技术　SM3 密码杂凑算法

GB/T 32907　信息安全技术　SM4 分组密码算法

GB/T 32918(所有部分)　信息安全技术　SM2 椭圆曲线公钥密码算法

GB/T 35275　信息安全技术　SM2 密码算法加密签名消息语法规范

GM/T 0019　通用密码服务接口规范

GM/T 0031　安全电子签章密码应用技术规范

GM/T 0033　时间戳接口规范

GM/T 0054　信息系统密码应用基本要求

GM/T 0055—2018　电子文件密码应用技术规范

3　术语和定义

GB/T 31913—2015、GB/T 25069—2010、GM/T 0055—2018 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了 GM/T 0055—2018 中的某些术语和定义。

3.1

电子文件　electronic records

在数字设备及环境中形成，以数码形式存储于磁带、磁盘、光盘、智能密码钥匙等载体，依赖计算机等数字设备阅读、处理，并可在通信网络上传送的文字、图表、音频、视频等不同形式的文件，由文件内容和文件属性组成。

注：改写 GB/T 31913—2015，定义 3.1。

3.2

文书类电子文件　administrative electronic records

反映党务、政务、生产经营管理等各项管理活动的电子文件。

3.3

标签　label

和电子文件绑定的一段数字实体，用于标识文件的属性和状态，定义文件的操作对象、操作行为及