ICS 35.040
L 80

中华人民共和国国家标准

GB/T 38540—2020

信息安全技术　安全电子签章密码技术规范

Information security technology—Technical specification secure electronic seal signature cryptography

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:北京数字认证股份有限公司、中安网脉(北京)技术股份有限公司、兴唐通信科技有限公司、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、成都卫士通信息产业股份有限公司、国家密码管理局商用密码检测中心、北京海泰方圆科技股份有限公司、北京三未信安科技发展有限公司、上海市数字证书认证中心有限公司、上海颐东网络信息有限公司、中国电子技术标准化研究院。

本标准主要起草人:傅大鹏、刘岩、谢峰、徐惠清、朱亚飞、王天顺、张金铭、郑强、李述胜、田敏求、吕春梅、赵丽丽、罗俊、陈中林、蒋红宇、高志权、许永欣、韩玮、夏东山、陈亚军、王文昌、邵淼、陈景燕、张妍、李敏、刘中。

信息安全技术　安全电子签章密码技术规范

1　范围

本标准规定了采用密码技术实现电子印章和电子签章的数据结构定义，以及相应的生成与验证流程。

本标准适用于电子印章系统的开发和使用，也可用于指导该类系统的检测。

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 20520　信息安全技术　公钥基础设施　时间戳规范

GB/T 32905　信息安全技术　SM3 密码杂凑算法

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 33560　信息安全技术　密码应用标识规范

GB/T 35276　信息安全技术　SM2 密码算法使用规范

3　术语和定义

下列术语和定义适用于本文件。

3.1

电子印章　electronic seal

一种由电子印章制章者数字签名的安全数据。

注：包括电子印章所有者信息和图形化内容的数据，用于安全签署电子文件。

3.2

电子签章　electronic seal signature

使用电子印章签署电子文件的过程。

注：电子签章可实现与纸质文件盖章操作相似的可视效果，可保障数据来源的真实性、数据完整性以及签名人行为的不可否认性。

3.3

原文　original data

需要进行电子签章或数字签名处理的电子文件。

3.4

电子签章数据　electronic seal signature data

电子签章过程产生的包含电子印章、原文信息和数字签名等信息的数据。

3.5

电子印章系统　electronic seal system

电子印章管理系统和电子签章软件的统称。