ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0099—2020

开放式版式文档密码应用技术规范

Cryptography application technical specification of open fixed layout documents

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：中安网脉（北京）技术有限公司、北京数字认证股份有限公司、中国电子技术标准化研究院、北京电子科技学院、数安时代科技股份有限公司、北京数科网维技术有限责任公司、航天福昕软件（北京）有限公司、吉大正元信息技术股份有限公司、兴唐通信科技有限公司、成都卫士通信息产业股份有限公司。

本文件主要起草人：刘歆、王佳宁、王天顺、林雪焰、李海波、陈亚军、张永强、张立廷、田景成、朱亚飞、王少康、冯辉。

开放式版式文档密码应用技术规范

1 范围

本文件规范了采用密码技术对开放式版式文档进行签名、加密及完整性保护等相关内容。

本文件适用于指导开放式版式文档密码应用相关产品和系统的研发、使用和检测。

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 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 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 33190—2016 电子文件存储与交换格式 版式文档

GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GB/T 38540—2020 信息安全技术 安全电子签章密码技术规范

3 术语和定义

GB/T 33190—2016、GB/T 38540—2020 界定的以及下列术语和定义适用于本文件。

3.1

版式 fixed layout

将文字、图形、图像等多种数字内容对象按照一定规则进行版面固化呈现的一种格式。

[来源：GB/T 33190—2016，3.1]

3.2

开放式版式文档 open fixed layout document

独立于软件、硬件、操作系统、输出设备的版式文档格式。

[来源：GB/T 33190—2016，3.2]

3.3

电子印章 electronic seal

一种由电子印章制作者数字签名的安全数据。

[来源：GB/T 38540—2020，3.1]

3.4

电子签章 electronic seal signature

使用电子印章签署电子文件的过程。

[来源：GB/T 38540—2020，3.2]