ICS 35.030
CCS L 80

GM

# 中华人民共和国密码行业标准

GM/T 0112—2021

# PDF 格式文档的密码应用技术要求

**Technical requirements of cryptography application in portable document format**

2021-10-19 发布　　2022-05-01 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。

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：北京数字认证股份有限公司、数安时代科技股份有限公司、福建福昕软件开发股份有限公司、兴唐通信科技股份有限公司、北京信安世纪科技股份有限公司、三未信安科技股份有限公司、北京江南天安科技有限公司、上海市数字证书认证中心有限公司、中国科学院数据与通信保护研究教育中心、暨南大学。

本文件主要起草人：林雪焰、夏鲁宁、傅大鹏、王文昌、张永强、汪宗斌、梁俊义、高能、朱亚飞、刘岩、李元、谢峰、黄利繁、马晓艳、冯辉、韩玮、钱文飞、谭武征、王胜男、李向锋、赵松、张妍、李红、赵子轩、张超、王银平、李敏、刘中、王新华、邓钊汉。

# PDF 格式文档的密码应用技术要求

## 1 范围

本文件规定了采用密码算法对 PDF 格式文档进行数字签名、电子签章以及加解密应用的技术要求。

本文件适用于指导基于 PDF 格式文档的密码应用相关产品和系统的研发和检测。

## 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 32010.1—2015 文献管理 可移植文档格式 第 1 部分：PDF1.7

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

GB/T 38540 信息安全技术 安全电子签章密码技术规范

GM/T 0091 基于口令的密钥派生规范

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

**PDF 格式文档 portable document format**

一种由 GB/T 32010.1 定义的可移植文档格式(PDF)的文件格式。

3.2

**SM2 算法 SM2 algorithm**

由 GB/T 32918 定义的一种椭圆曲线密码算法。

3.3

**SM3 算法 SM3 algorithm**

由 GB/T 32905 定义的一种密码杂凑算法。

3.4

**SM4 算法 SM4 algorithm**

由 GB/T 32907 定义的一种分组密码算法。