ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0125.1—2022

JSON Web 密码应用语法规范 第 1 部分:算法标识

JavaScript Object Notation Web cryptographic application syntax specification—Part 1:Algorithm identifier

2022-11-20 发布　　2023-06-01 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。

本文件是GM/T 0125《JSON Web密码应用语法规范》的第1部分。GM/T 0125已经发布了以下部分：

——第1部分：算法标识；

——第2部分：数字签名；

——第3部分：数据加密；

——第4部分：密钥。

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：广东省电子商务认证有限公司、智巡密码(上海)检测技术有限公司、格尔软件股份有限公司、北京信安世纪科技股份有限公司、北京数字认证股份有限公司、北京国脉信安科技有限公司、中国科学院信息工程研究所、广东邮电职业技术学院、上海市数字证书认证中心有限公司。

本文件主要起草人：陈树乐、韩玮、郑强、张永强、袁峰、高能、张庆勇、赵敏、刘义、黄志伟、林少柳、梁宁宁、梁家声、傅大鹏、黎明、王维初。

引　言

《JSON Web 密码应用语法规范》旨在以国产商用密码算法为核心，来保证数据机密性和完整性，适用于 JSON Web 密码应用产品的研发与检测，其他使用 JSON 数据交换格式的安全产品，可参考使用。《JSON Web 密码应用语法规范》由四个部分构成。

——第 1 部分：算法标识。定义了 JSON Web 密码应用的算法标识。

——第 2 部分：数字签名。描述了基于 JSON 数据结构来保护消息内容的数字签名或消息鉴别码的语法规范，并给出了相应的生成和验证流程。

——第 3 部分：数据加密。描述了使用身份鉴别和加密来确保数据的机密性和完整性的技术要求。

——第 4 部分：密钥。定义了密钥的 JSON 数据结构表示方法。

本文件为《JSON Web 密码应用语法规范》的第 1 部分，定义了 JSON Web 密码应用的算法标识，是其他各部分的基础。

JSON Web 密码应用语法规范
第 1 部分:算法标识

1 范围

本文件定义了 JSON Web 密码应用的算法标识。

本文件适用于 JSON Web 密码应用产品的研发与检测,其他使用 JSON 数据交换格式的安全产品,可参考使用。

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。

GM/T 0006 密码应用标识规范

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

JSON Javascript Object Notation

JavaScript 对象标记,一种轻量级、基于文本的、语言独立的数据交换格式。

4 缩略语

下列缩略语适用于本文件。

CCM:带有密文分组链接消息鉴别码的计数器模式(Counter with Cipher Block Chaining-Message Authentication Code)

GCM:伽罗瓦/计数器模式(Galois/Counter Mode)

5 算法标识定义规则

5.1 概述

本文件定义了数字签名算法、消息鉴别算法、密钥加密密钥算法和内容加密算法的标识命名规则。

5.2 定义规则

本文件的算法标识定义遵循 GM/T 0006 对算法标识的标签定义。

6 数字签名算法标识

6.1 概述

数字签名算法标识用于标识对消息数据进行数字签名的算法。

6.2 算法标识

本文件定义了数字签名算法的标识，见表1。

表1 数字签名算法标识

标识	说明
SGD_SM3_SM2	基于SM3和SM2的数字签名算法

7 消息鉴别算法标识

7.1 概述

消息鉴别算法标识用于标识对消息数据进行完整性保护的算法。

7.2 算法标识

本文件定义了消息鉴别算法的标识，见表2。

表2 消息鉴别算法标识

标识	说明
SGD_SM3_HMAC	基于SM3算法的消息鉴别算法

8 密钥加密密钥算法标识

8.1 概述

密钥加密密钥算法标识用来标识对密钥进行加密的算法。

8.2 算法标识

本文件定义了两种密钥加密密钥算法标识，见表3。

表3 密钥加密密钥算法标识

标识	说明
SGD_SM2_3	SM2公钥加密算法
SGD_SM9_3	SM9加密算法

9 内容加密算法标识

9.1 概述

内容加密算法标识用来标识对消息数据和额外数据进行可鉴别的加密算法。

9.2 算法标识

本文件定义了两种内容加密算法标识，见表4。

表4 内容加密算法标识

标识	说明
SGD_SM4_CCM	基于SM4算法的CCM加密算法
SGD_SM4_GCM	基于SM4算法的GCM加密算法