ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0125.2—2022

JSON Web密码应用语法规范 第2部分:数字签名

JavaScript Object Notation Web cryptographic application syntax specification—Part 2:Signature

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2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、广东南方通信建设有限公司、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、傅鹏、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 2 部分，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。

JSON Web密码应用语法规范
第2部分:数字签名

1 范围

本文件描述了基于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。

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。

GB/T 15852.2 信息技术 安全技术 消息鉴别码 第2部分:采用专用杂凑函数的机制

GB/T 16263.1 信息技术 ASN.1编码规则 第1部分:基本编码规则(BER)、正则编码规则(CER)和非典型编码规则(DER)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 35276 信息安全技术 SM2密码算法使用规范

GM/T 0125.1 JSON Web密码应用语法规范 第1部分:算法标识

GM/T 0125.4 JSON Web密码应用语法规范 第4部分:密钥

3 术语和定义

下列术语和定义适用于本文件。

3.1

JOSE头部 JOSE header

描述密码运算和参数的JSON对象,由一组参数组成。

3.2

JWS有效载荷 JWS payload

受保护的字节串消息数据,指JWS待签名或消息鉴别的数据。

3.3

JWS签名 JWS signature

对有效载荷和保护头部提供完整性保护的数字签名或消息鉴别码。

3.4

头部参数 header parameter

JOSE头部里面的“参数名称/值”对。