



中华人民共和国密码行业标准

GM/T 0125.3—2022

JSON Web 密码应用语法规范 第 3 部分：数据加密

JavaScript Object Notation Web cryptographic application syntax
specification—Part 3: Data encryption

2022-11-20 发布

2023-06-01 实施

国家密码管理局 发布

目 次

前言 I

引言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 3

5 符号 3

6 JSON Web 数据加密(JWE) 3

 6.1 概述 3

 6.2 JOSE 头部 3

7 JWE 密钥加密密钥算法 6

 7.1 概述 6

 7.2 SM2 公钥加密算法 6

 7.3 SM9 加密算法 6

8 JWE 内容加密算法 6

 8.1 概述 6

 8.2 可鉴别的加密机制算法 6

 8.3 参数要求 7

9 JWE 加密和解密 7

 9.1 概述 7

 9.2 消息加密过程 7

 9.3 消息解密过程 8

10 字符串比较规则 9

11 密钥身份标识 9

12 序列化 9

 12.1 概述 9

 12.2 紧凑型序列化 9

 12.3 JSON 序列化 9

附录 A (资料性) JWE 示例 12

 A.1 综述 12

 A.2 基于“SGD_SM2_3”和“SGD_SM4_CCM”的 JWE 序列化示例 12

 A.3 基于“SGD_SM2_3”和“SGD_SM4_GCM”的 JWE 序列化示例 14

 A.4 基于“SGD_SM2_3”和“SGD_SM4_CCM”的 JWE 多个接收者示例 16

 A.5 基于“SGD_SM2_3”和“SGD_SM4_GCM”的 JWE 多个接收者示例 19

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 3 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、郑州迪维勒普科技有限公司、河南省鼎信信息安全等级测评有限公司、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、岳志军、陈宇、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 3 部分,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。

JSON Web 密码应用语法规范

第 3 部分:数据加密

1 范围

本文件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。

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 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 32907 信息安全技术 SM4 分组密码算法

GB/T 32915 信息安全技术 二元序列随机性检测方法

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

GB/T 36624 信息技术 安全技术 可鉴别的加密机制

GB/T 38635(所有部分) 信息安全技术 SM9 标识密码算法

GM/T 0080 SM9 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

带额外数据的可鉴别加密 **authenticated encryption with associated data; AEAD**

加密明文,可指定额外的可鉴别数据,并对密文和额外可鉴别数据提供完整性校验的加密。

注:使用该机制的算法也称 AEAD 算法,AEAD 算法接受两个输入,明文和额外可鉴别数据,并产生两个输出,分别是密文和鉴别标志。

3.2

额外可鉴别数据 **additional authenticated data; AAD**

AEAD 算法的输入,受完整性保护但未加密的数据。

3.3

鉴别标志 **authentication tag**

AEAD 算法的输出,用于确保密文和额外可鉴别数据的完整性。