

ICS 35.030
CCS L 80

GM

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GM/T 0125.3-2022

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

JSON Web 密码应用语法规范 第3部分：数据加密

(English Translation)

Issued on: November 20, 2022

Implemented on: November 20, 2022

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative References	2
Terms and Definitions	3
Authenticated encryption with associated data; AEAD	4
Additional authenticated data; AAD	5
Authentication tag	6
Content encryption key; CEK	7
JWE encrypted key	8
JWE initialization vector	9
JWE AAD	10
JWE ciphertext	11
JWE authentication tag	12
JWE protected header	13
JWE shared unprotected header	14
JWE per-recipient unprotected header	15
JWE compact serialization	16
JWE JSON serialization	17
Key encryption	18
Abbreviations	19
Symbols	20
Overview	21
User-defined header parameters	22
Overview	23
SM2 Public Key Encryption Algorithm	24
SM9 Encryption Algorithm	25
Message Decryption Process	26
String Comparison Rules	27
Key Identifiers	28
Overview	29
Compact Serialization	30

1 Scope

This document describes the technical requirements for using identity authentication and encryption to ensure data confidentiality and integrity.

This document is applicable to the research and development and testing of JSON Web cryptographic application products. It can be used as a reference for other security products that use the JSON data exchange format.

2 Normative References

The contents of the following documents constitute indispensable clauses of this document through the normative references in the text. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GB/T 16263.1 Information Technology - ASN.1 Encoding Rules - Part 1: Specification Of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) GB/T 32905 Information Security Techniques - SM3 Cryptographic Hash Algorithm GB/T 32907 Information Security Technology - SM4 Block Cipher Algorithm GB/T 32915 Information Security Technology - Randomness Test Methods for Binary Sequence GB/T 32918 (all parts) Information Security Technology - Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves GB/T 35276 Information Security Technology - SM2 Cryptographic Algorithm Usage Specification GB/T 36624 Information Technology - Security Techniques - Authenticated Encryption GB/T 38635 (all parts) Information Security Technology - Identity-based Cryptographic Algorithms SM9 GM/T 0080 SM9 Cryptographic Algorithm Application Specification GM/T 0125.1 JavaScript Object Notation Web Cryptographic Application Syntax Specification - Part 1: Algorithm Identifier GM/T 0125.4 JavaScript Object Notation Web Cryptographic Application Syntax Specification - Part 4: Key

3 Terms and Definitions

The following terms and definitions are applicable to this document.

3.1 Authenticated encryption with associated data; AEAD

Encryption of plaintext, which can specify additional authenticated data and provide integrity verification for ciphertext and additional authenticated data.

NOTE: the algorithm using this mechanism is also called AEAD algorithm. AEAD algorithm accepts two inputs, plaintext and additional authenticated data, and produces two outputs, which are respectively ciphertext and authentication tag.

3.2 Additional authenticated data; AAD

Input of AEAD algorithm, which is data that is integrity protected but not encrypted.

3.3 Authentication tag

Output of AEAD algorithm, which is used to ensure the integrity of ciphertext and additional authenticated data.

3.4 Content encryption key; CEK

Symmetric key of AEAD algorithm, which is used to encrypt plaintext to produce ciphertext and authentication tag.

3.5 JWE encrypted key

The ciphertext value obtained after encrypting CEK using key-encrypted key algorithm.

3.6 JWE initialization vector

The initialization vector value used by the encryption algorithm.

3.7 JWE AAD

Additional authenticated data of the JWE data structure, which only exists in JSON serialization.

3.8 JWE ciphertext

The ciphertext part of the output of the content encryption algorithm.

3.9 JWE authentication tag

The tag part of the output of the content encryption algorithm, which is used to ensure the integrity of the JWE ciphertext and JWE additional authenticated data.

3.10 JWE protected header

JSON object, which contains integrity-protected header parameters. The integrity of these header parameters is protected by authenticating encryption operations.

NOTE: these parameters apply to all recipients of the JWE. For JWE compact serialization, it contains the entire JOSE header. For JWE JSON serialization, it is part of the JOSE header.

3.11 JWE shared unprotected header

JSON object, which contains header parameters that are not integrity protected.

NOTE: these parameters apply to all recipients of JWE and are not integrity protected. They exist when using JWE JSON serialization.

3.12 JWE per-recipient unprotected header

JSON object, which contains header parameters that are not integrity protected. They are unique parameters to each recipient of JWE.

NOTE: these header parameter values are not integrity protected. They exist when using JWE JSON serialization.

3.13 JWE compact serialization

Serialization represented by JWE using a compact URL-safe character string form.

3.14 JWE JSON serialization

Serialization represented by JWE using a JSON structure.

NOTE: unlike JWE compact serialization, JSON serialization can support multiple recipients.

3.15 Key encryption

The process of encrypting a key.

NOTE: the key here generally refers to the content encryption key CEK.

4 Abbreviations

The following abbreviations are applicable to this document.

CA. Certification Authority CCM. Counter with Cipher Block Chaining-Message Authentication Code DER. Distinguished Encoding Rules GCM. Galois/Counter Mode IV. Initialization Vector JOSE. JSON Object Signing and Encryption JSON. JavaScript Object Notation JWE. JSON Web Encryption PEM. Privacy Enhanced Mail URL. Uniform Resource Locator

5 Symbols

The following symbols are applicable to this document.

ASCII(X). ASCII encoding of data X base64url(X). base64url encoding of data X IV. initialization vector T. authentication tag UTF8(X). UTF-8 encoding of data X ||. string concatenation symbol