

ICS 35.030
CCS L 80

GM

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

GM/T 0125.2-2022

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

JSON Web 密码应用语法规范 第2部分：数字签名
(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
JOSE header	4
JWS payload	5
JWS signature	6
Header parameter	7
JWS protected header	8
JWS unprotected header	9
JWS compact serialization	10
JWS JSON serialization	11
Abbreviations	12
Symbols	13
Overview	14
General	15
Extended header parameter names	16
User-defined header parameter names	17
Overview	18
SM2 Digital Signature Algorithm	19
Overview	20
Message Authentication Algorithm Based on SM3 Algorithm	21
Overview	22
Generation Process	23
Verification Process	24
Character String Comparison Rule	25
Key Identification	26

1 Scope

This document describes the syntax specification of digital signature or message authentication code based on JSON data structure to protect message content and gives the corresponding generation and verification processes.

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 15852.2 Cybersecurity Technology - Message Authentication Codes (MACs) - Part 2.

Mechanisms Using a Dedicated Hash-function 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 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 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 JOSE header

A JSON object describing cryptographic operations and parameters and consisting of a set of parameters.

3.2 JWS payload

Protected byte string message data, which refers to the data to be signed or message-authenticated by JWS.

3.3 JWS signature

A digital signature or message authentication code that provides integrity protection for the payload and protected header.

3.4 Header parameter

The "parameter name / value" pair in the JOSE header.

3.5 JWS protected header

A header parameter subject to integrity protection by the JWS digital signature or message authentication code, which is a JSON object. If it is compact serialization, the protected header is equivalent to the JOSE header.

3.6 JWS unprotected header

A JSON object that is not subject to integrity protection by the JWS digital signature or message authentication code. It only exists in the JSON serialization format.

3.7 JWS compact serialization

The serialization represented by a compact URL-safe character string used by JWS.

3.8 JWS JSON serialization

The serialization represented by a JSON-structured character string used by JWS. Unlike JWS compact serialization, JSON serialization can support unprotected header and multiple digital signatures or message authentication codes.

4 Abbreviations

The following abbreviations are applicable to this document.

DER. Distinguished Encoding Rules JOSE. JSON Object Signing and Encryption JSON.
JavaScript Object Notation JWS. JSON Web Signature PEM. Privacy Enhanced Mail URI.
Uniform Resource Identifier

5 Symbols

The following symbols apply to this document.

ASCII(X). ASCII encoding of data X base64url(X). base64url encoding of data X UTF8(X).
UTF-8 encoding of data X x||y. concatenation of x and y; x and y are bit strings or byte
strings

6.1 Overview

JWS is a data structure that uses the mode of JSON to represent the digital signature or message authentication code of message data.

JWS consists of three parts. JOSE header, JWS payload and JWS signature. JWS

signature is divided into two serialization formats. compact serialization and JSON serialization. JSON serialization may include unprotected header, and it may also represent more than one signature.

6.2.1 General

The JOSE header is a JSON object. Each parameter of the JSON object describes the header parameter of JWS. The header parameter name in the JOSE header shall be unique. The JOSE header of JWS consists of the JWS protected header and the JWS unprotected header. The DER encoding rules used in this document shall comply with GB/T 16263.1.

There are three types of JWS header parameter names. defined parameter names, extended header parameter names and user-defined header parameter names.

6.2.2.6 "x5u" (certificate URL) header parameter the "x5u" header parameter is used to identify the signature certificate URL corresponding to the private key that digitally signs the JWS. Its value is a character string in the form of URI.

The resource shall provide a representation of the certificate or certificate chain in the form of PEM encoding, with each certificate separated by the following delimiters.

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----the first certificate shall be the signature certificate of the JWS. This header parameter is optional and shall be set as the protected header parameter.

6.2.2.7 "x5c" (certificate chain) header parameter the "x5c" header parameter is used to identify the signature certificate or certificate chain that digitally signs the JWS. Its value is a JSON character string array. The elements in the array are base64 encoded character strings of the digital certificate DER encoding. The first element of the array shall be the certificate used to digitally sign the JWS, and the following elements are successively the certificates held by the CA that issues the certificate of the previous element.

This header parameter is optional.

6.2.2.8 "x5t#sm3" (certificate SM3 hash value) header parameter the "x5t#sm3" header parameter is a character string used to identify the SM3 fingerprint of the digital signature certificate, which can be used to match the key. The value generation process. use the DER encoding of the digital certificate to perform SM3 hashing, and then, base64url encoding. The calculation method and steps of the SM3 algorithm shall comply with GB/T 32905. This header parameter is optional.

6.2.2.9 "typ" (type) header parameter the "typ" header parameter is a character string that is used to identify the media type of the entire JWS. This header parameter is optional.

6.2.2.10 "cty" (content type) header parameter the "cty" header parameter is a character