Chinastandards.org

ICS 35.030
CCS L 80

GM

GM/T 0125.4-2022

JavaScript Object Notation Web cryptographic application syntax specification-Part 4:Key

JSON Web 密码应用语法规范 第4部分：密钥

(English Translation)

Issued on: November 20, 2022 **Implemented on: June 1, 2023**

Issued by: State Administration of Cryptography

Preview: page 1 of 5 shown, 13 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0125-4-2022

Chinastandards.org

Table of Contents

Foreword 1
Scope 2
Normative References 3
Terms and Definitions 4
JWK set 5
Base64url encoding 6
General Description 7

Foreword

This document was drafted in accordance with the rules provided in GB/T 1.1-2020 Directives for Standardization - Part 1: Rules for the Structure and Drafting of Standardizing Documents.

This document is Part 4 of GM/T 0125 JavaScript Object Notation Web Cryptographic Application Syntax Specification. GM/T 0125 has issued the following parts.

---Part 1: Algorithm Identifier;

---Part 2: Signature;

---Part 3: Data Encryption;

---Part 4: Key.

Please be noted that certain content of this document may involve patents. The institution issuing this document does not undertake the responsibility of identifying these patents.

This document was proposed by and shall be under the jurisdiction of Cryptography Standardization Technical Committee.

1 Scope

This document defines the JSON data structure representation method for keys.

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.

Preview: page 2 of 5 shown, 13 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0125-4-2022

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) GM/T 0125.1 JavaScript Object Notation Web Cryptographic Application Syntax Specification - Part 1: Algorithm Identifier GM/Z 4001 Cryptology Terminology

3 Terms and Definitions

The terms and definitions defined in GM/Z 4001 and the following are applicable to this document.

3.1 JWK set

A JSON object representing a set of JWKs.

3.2 Base64url encoding

Base64url encoding is a safe encoding for URLs and file names. base64url encoding is first performed without padding in accordance with the base64 encoding rules, and then, the '+' symbol in the base64 encoding result is replaced with a '-' symbol, and the '/' symbol is replaced with a '_' symbol.

sensitive character string. This parameter is optional. The values defined by this parameter are.

---"sig" (signature);

---"enc" (encryption).

5.4 "key_ops" (key operation) Parameter the "key_ops" parameter is used to identify the key operation type. Its value is a string array of key operation values. The values of this parameter may include.

---"sign" (calculate digital signature or message authentication code);

---"verify" (verify digital signature or message authentication code);

---"encrypt" (encrypt content);

Preview: page 3 of 5 shown, 13 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0125-4-2022

---"decrypt" (decrypt content and verify decryption, if applicable);

---"wrapKey" (key wrapping);

---"unwrapKey" (decrypt key wrapping and verify decryption, if applicable);

---"deriveKey" (derive key);

---"deriveBits" (derive bits not used as keys).

All key operation values are case-sensitive character strings, and repeated key operation values cannot appear in the array. The "key_ops" parameter is optional.

Multiple unrelated key operations shall not be specified for a key. A combination of "sign" and "verify", "encrypt" and "decrypt", and "wrapKey" and "unwrapKey" can be used.

The "use" and "key_ops" parameters should not be used together. If both are used, the information they represent shall be consistent, and the application program shall explicitly specify which parameters to use.

5.5 "alg" (algorithm) Parameter the "alg" parameter is used to identify the algorithm related to the key. Its value is a case-sensitive character string. This parameter is optional, and its value shall comply with GM/T 0125.1.

5.6 "kid" (key ID) Parameter the "kid" parameter is used to match a specific key. Its value is a case-sensitive character string, and this parameter is optional.

When the "kid" value is used in a JWK set, different keys in the JWK set shall use different "kid" values. When used with JWS or JWE, the "kid" value can be used to match the JWS or JWE "kid" parameter value.

5.7 "x5u" (certificate URL) Parameter the "x5u" parameter is used to identify the resource of a digital certificate or certificate chain, and its value is a character string in the form of URI. This resource shall provide a certificate or certificate chain in PEM-encoded form, with each certificate separated by the following delimiters.

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

-----END CERTIFICATE-----the key in the first certificate shall match the public key represented by the other parameters of JWK. This parameter is optional.

5.8 "x5c" (certificate chain) Parameter the "x5c" parameter is used to identify the digital certificate or certificate chain related to the key. Its value is a JSON array of strings. Each element in the array is a base64-encoded string of the DER-encoded digital certificate. The first element in the array shall be the digital certificate that matches the key, and the subsequent elements are successively the certificates held by the CA that issues the certificate of the previous element. This parameter is optional.

As with the "x5u" parameter, when the "x5c" parameter is used, optional JWK parameters

Preview: page 4 of 5 shown, 13 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0125-4-2022

may be present to provide key usage, algorithm, or other information. If other parameters are present, then, their content shall be semantically consistent with the relevant fields in the first certificate.

5.9 "x5t#sm3" (certificate SM3 hash value) Parameter the "x5t#sm3" parameter is a character string used to identify the SM3 fingerprint of the digital certificate, which can be used to match the key. The value is generated by first calculating the digital certificate DER code, performing SM3 hashing, and then, performing base64url encoding. The calculation method and steps of the SM3 algorithm shall comply with GB/T 39205.This parameter is optional.

6.1 General Description

A JWK set is a JSON object that represents a set of JWKs. The JSON object shall have a "keys" parameter, whose value is a JWK array. This JSON object may contain spaces, "/" and newlines.

The parameter names in the JWK set shall be unique, and the JWK set parser shall reject JWK sets containing duplicate parameter names. For examples of the JWK set, see Appendix A.

Preview: page 5 of 5 shown, 13 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0125-4-2022