ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0125.4—2022

JSON Web 密码应用语法规范 第 4 部分:密钥

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

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4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、广东邮电职业技术学院、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、黎明、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 4 部分，定义了密钥的 JSON 数据结构表示方法。

JSON Web密码应用语法规范
第4部分:密钥

1 范围

本文件定义了密钥的JSON数据结构表示方法。

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

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

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

JWK集合 JWK set

表示一组JWK的JSON对象。

3.2

base64url编码 base64url encode

base64url编码是URL和文件名安全的编码。base64url编码是先按照base64编码规则进行不填充编码,然后将base64编码结果中的'+'符号替换为'-'符号、将'/'符号替换为'_'符号。

4 缩略语

下列缩略语适用于本文件。

DER:可辨别编码规则(Distinguished Encoding Rules)

JSON:JavaScript对象标记(JavaScript Object Notation)

JWK:JSON Web密钥(JSON Web Key)

PEM:隐私增强邮件(Privacy Enhanced Mail)

5 JSON Web 密钥格式

5.1 通则

JSON Web 密钥(JWK)是表示密钥信息的 JSON 对象。该对象的参数用来描述密钥的属性。本文件定义了通用参数及与密钥类型相关的参数,使用的 DER 编码规则,应符合 GB/T 16263.1。JWK 示例见附录 A。

JWK 中的参数名称应唯一,JWK 解析器应拒绝包含重复参数名称的 JWK,各参数定义见表 1。

表 1 JWK 密钥参数

参数值	类型	说明	要求
kty	字符串	密钥类型	必选
use	字符串	公钥用法	可选
key_ops	数组	密钥操作	可选
alg	字符串	算法	可选
kid	字符串	密钥 ID	可选
x5u	字符串	证书 URL	可选
x5c	数组	证书链	可选
x5t#sm3	字符串	证书 SM3 杂凑值	可选

5.2 “kty”(密钥类型)参数

5.2.1 总体说明

“kty”参数用于标识密钥的类型,用区分大小写的字符串形式表示,该参数必选。

本文件定义了两种“kty”参数值。见表 2。

表 2 kty 参数

“kty”参数值	说明
EC	ECC 密钥
oct	对称密钥或者字节串

5.2.2 SM2 密钥

5.2.2.1 总体说明

本文件描述了 SM2 密钥相关的参数,用于标识用户签名或加密的密钥信息,SM2 密钥参数见表 3。

表 3　SM2 密钥参数

参数	类型	说明
kty	字符串	密钥类型，应为 EC
crv	字符串	算法曲线，应为 sm2p256v1
x	字符串	SM2 公钥 x 坐标，具体见 5.2.2.2
y	字符串	SM2 公钥 y 坐标，具体见 5.2.2.3

5.2.2.2　SM2 的“x”

对于 SM2 算法，“x”表示椭圆曲线点的 x 坐标。其值用 x 坐标八位字节串的 base64url 编码表示。

5.2.2.3　SM2 的“y”

对于 SM2 算法，“y”表示椭圆曲线点的 y 坐标，其值用 y 坐标八位字节串的 base64url 编码表示。

5.2.3　SM9 密钥

5.2.3.1　总体说明

本文件描述了 SM9 密钥相关的参数，用于标识用户签名或加密的公钥信息，SM9 密钥由以下参数组成，见表 4。

表 4　SM9 密钥参数

参数	类型	说明
kty	字符串	密钥类型，应为 EC
crv	字符串	算法曲线，应为 sm9curve
id	字符串	用户标识，具体见 5.2.3.2
hid	整数	签名或加密私钥生成函数识别符，具体见 5.2.3.3
x_pub	字符串	签名或加密主公钥的 x 坐标，具体见 5.2.3.4
y_pub	字符串	签名或加密主公钥的 y 坐标，具体见 5.2.3.5

5.2.3.2　SM9 的“id”

“id”表示用户标识。其值用八位字节串的 base64url 编码表示。

5.2.3.3　SM9 的“hid”

“hid”表示私钥生成函数识别符，长度为一个字节，其值用无符号整数表示。如果公钥用途为数字签名，对应为签名私钥生成函数识别符；如果公钥用途为加密，对应为加密私钥生成函数识别符。

5.2.3.4　SM9 的“x_pub”

“x_pub”表示主公钥的 x 坐标。如果公钥用途为数字签名，对应为签名主公钥 x 坐标；如果公钥用

途为加密，对应为加密主公钥 x 坐标。其值用八位字节串的 base64url 编码表示。

5.2.3.5 SM9 的“y_pub”

“y_pub”表示主公钥的 y 坐标。如果公钥用途为数字签名，对应为签名主公钥的 y 坐标。如果公钥用途为加密，对应为加密主公钥 y 坐标。其值用八位字节串的 base64url 编码表示。

5.2.4 对称密钥

5.2.4.1 总体说明

本文件描述了对称密钥的参数，用于标识对称密钥的信息。其中对称密钥的算法需要结合“alg”参数才能区分。对称密钥由以下参数组成，见表 5。

表 5 对称密钥参数

参数	类型	说明
k	字符串	对称密钥

5.2.4.2 对称密钥的“k”

“k”表示对称密钥或其他密钥字节串，其值用八位字节串的 base64url 编码表示。

5.3 “use”（公钥用法）参数

“use”参数用于标识公钥的预期用途。其值是区分大小写的字符串，此参数可选，该参数定义的值为：

——“sig”（签名）；

——“enc”（加密）。

5.4 “key_ops”（密钥操作）参数

“key_ops”参数用于标识密钥操作类型。它的值是一组密钥操作值的字符串数组。该参数取值可包括：

——“sign”（计算数字签名或消息鉴别码）；

——“verify”（验证数字签名或消息鉴别码）；

——“encrypt”（加密内容）；

——“decrypt”（解密内容并验证解密，如果适用）；

——“wrapKey”（密钥封装）；

——“unwrapKey”（解密密钥封装并验证解密，如果适用）；

——“deriveKey”（派生密钥）；

——“deriveBits”（派生不用作密钥的位）。

所有密钥操作值是区分大小写的字符串，重复的密钥操作值不能出现在数组中。“key_ops”参数是可选的。

不应为密钥指定多个不相关的密钥操作，可使用 “sign”与“verify”，“encrypt”与“decrypt”，和“wrapKey”与“unwrapKey”的组合。

“use”和“key_ops”参数不宜一起使用，如果两者都被使用，它们表示的信息应一致，应用程序应明确指定使用哪些参数。

5.5 “alg”(算法)参数

“alg”参数用于标识密钥相关的算法。其取值是区分大小写的字符串。该参数可选,取值应符合GM/T 0125.1。

5.6 “kid”(密钥 ID)参数

“kid”参数用于匹配特定密钥。其值是区分大小写的字符串,此参数可选。

当在JWK集合中使用“kid”值时,JWK集合中的不同密钥应使用不同的“kid”值。当与JWS或JWE一起使用时,“kid”值可用于匹配JWS或JWE“kid”参数值。

5.7 “x5u”(证书 URL)参数

“x5u”参数用于标识数字证书或证书链的资源,其值是一个URI形式的字符串。该资源应提供符合PEM编码形式的证书或证书链,每个证书使用以下分隔符隔开:

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

-----END CERTIFICATE-----

第一个证书中的密钥应匹配JWK其他参数所代表的公钥。此参数可选。

5.8 “x5c”(证书链)参数

“x5c”参数用于标识密钥相关的数字证书或证书链,其值是一个JSON字符串数组。数组中的元素是数字证书DER编码的base64编码字符串。数组第一个元素应是匹配密钥的数字证书,后面的元素依次是向前一个元素的颁发证书的CA所持有的证书。此参数可选。

与“x5u”参数一样,当使用“x5c”参数时,可能存在提供密钥用法、算法或其他信息的可选JWK参数。如果存在其他参数,则这些参数的内容应在语义上与第一张证书中的相关字段一致。

5.9 “x5t#sm3”(证书 SM3 杂凑值)参数

“x5t#sm3”参数是一个字符串,用于标识数字证书的SM3指纹,可用来匹配密钥。该值生成过程:先计算数字证书DER编码进行SM3杂凑后再进行base64url编码。SM3算法的计算方法和步骤应符合GB/T 39205。此参数可选。

6 JWK 集合格式

6.1 总体说明

JWK集合是一个JSON对象,表示一组JWK。JSON对象应存在一个“keys”参数,其值是一个JWK数组。此JSON对象可包含空格、“/”和换行符。

JWK集合中的参数名称应唯一,JWK集合解析器应拒绝包含重复参数名称的JWK集合,JWK集合示例见附录A。

6.2 “keys”参数

“keys”参数的值是JWK值的数组。默认情况下,数组中JWK值的顺序并不意味着它们之间的优先顺序,JWK集合的应用程序可根据需要为顺序指定含义。

7 字符串比较规则

处理JWK时，应将已知字符串与JSON对象中的头部参数名称和头部参数值进行比较并严格区分大小写，该比较规则适用于一般情况下对所有JSON字符串的比较。当头部参数的定义明确指出要为该头部参数值使用其他比较规则时，应遵循头部参数的具体定义。

附 录 A
（资料性）
JWK 示例

A.1 综述

本附录中，明文采用 UTF-8 编码。

本附录展示了 SM2 数字签名的用户公钥信息、SM2 加密时的用户公钥信息、SM9 加密时的用户标识信息、用户持有的 SM2 证书信息、对称密钥信息和 JWK 集合的示例。

A.2 SM2 签名公钥

该示例展示使用 SM2 数字签名的用户公钥信息，用于标识用户和验证数字签名。

```
{
    "kty":"EC",
    "crv":"sm2p256v1",
    "use":"sig",
    "x":"TnSVmMedma1KTK20gMTimZGylhJf2JgI8LsYpHosAEg",
    "y":"V0Bn7fBeiPlA66Nzde08dx9culLLjds76HdlaIwvygU"
}
```

A.3 SM2 加密公钥

该示例展示使用 SM2 加密时的用户公钥信息，用于标识用户和匹配对应的解密私钥。

```
{
    "kty":"EC",
    "crv":"sm2p256v1",
    "use":"enc",
    "x":"yJxuyluqb24nw_VpAMFMP0ZtryQexPUwYhKt79oe0Jw",
    "y":"dEK3Qy1crFnVjlNlac-Tx_CnkJoXhyBB8Y1Jm-FzKKE"
}
```

A.4 SM9 加密用户标识

该示例展示使用 SM9 加密时的用户标识信息，用于标识用户和匹配对应的解密私钥，其中 id 是用户名称 Alice 的 base64url 编码。

```
{
    "kty":"EC",
    "crv":"sm9curve",
    "use":"enc",
    "id":"QWxpY2U"
}
```

A.5 SM2 证书

该示例展示用户持有的 SM2 证书信息，证书被用于标识用户和验证数字签名。

```
{
    "kty":"EC",
    "crv":"sm2p256v1",
    "use":"sig",
    "x5c":
    ["MIIBqzCCAU+gAwIBAgIUfuH5LnZVH2mvK2Qr8MXNJHc7sv0wDAYIKoEcz1UBg3U
    FADAlMQswCQYDVQQGEwJDTjEWMBQGA1UEAwwNU20yX1Jvb3RfVGVzdDAeFw0y
    MDAyMjUwMzQwMDdaFw0zNTAyMjUwMzQwMDdaMCAxCzAJBgNVBAYTAkNOMR
    EwDwYDVQQDDAhTTTIgU2lnbjBZMBMGByqGSM49AgEGCCqBHM9VAYItA0IABE50l
    ZjHnZmtSkyttIDE4pmRspYSX9iYCPC7GKR6LABIV0Bn7fBeiPlA66Nzde08dx9culLLjds76
    HdlaIwvygWjYDBeMB8GA1UdIwQYMBaAFKoL1nBIYnHh5BMWrD84Tx0tJ3r5MB0GA1
    UdDgQWBBQcPQghGArysGLq7AXU6WE6VyqG+DAMBgNVHRMBAf8EAjAAMA4GA1
    UdDwEB/wQEAwIGwDAMBggqgRzPVQGDdQUAA0gAMEUCIQC3Joxo7p5nfP4oa6Gsl4
    BPlWu9sPD8Lv/xxHtHrikfnAIgVb55YLDbzIMkf1TCaGIewUMDLeIsGVHHBudnXOWrl
    zw="]
}
```


A.6 对称密钥

该示例展示在使用基于 SM3 的消息鉴别算法时相关对称密钥的信息。


```
{
    "kty":"oct",
    "alg":"SGD_SM3_HMAC",
    "k":"MzEzMjMzMzQzNTM2MzczODMxMzIzMzM0MzUzNjM3MzgzMTMyMzMzNDM1Mz
    YzNzM4MzEzMjMzMzQzNTM2MzczOA"
}
```


A.7 JWK 集合

该示例展示包含对称密钥和 SM2 密钥的多个 JWK 的集合，不同的 JWK 使用不同的 kid 来标识。


```
{
"keys":
[
  {
    "kty":"oct",
    "alg":"SGD_SM3_HMAC",
    "k":"MzEzMjMzMzQzNTM2MzczODMxMzIzMzM0MzUzNjM3MzgzMTMyMzMzNDM1Mz
    YzNzM4MzEzMjMzMzQzNTM2MzczOA",
    "kid":"C95EA6AE-2ECF-423F-9AA6-102EE5B9D73A"
  },
  {
    "kty":"EC",
    "crv":"sm2p256v1",
```

```
    "use":"sig",
    "x":"TnSVmMedma1KTK20gMTimZGylhJf2JgI8LsYpHosAEg",
    "y":"V0Bn7fBeiPlA66Nzde08dx9culLLjds76HdlaIwvygU",
    "kid":"E5841F06-CF2A-4E8C-9654-2B9542E60FA5"
  }
]
}
```