

Translated English of Chinese Standard: GM/T0010-2023

www.ChineseStandard.net → Buy True-PDF → Auto-delivery.

Sales@ChineseStandard.net

GM

CRYPTOGRAPHIC INDUSTRY STANDARD
OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

GM/T 0010-2023

Replacing GM/T 0010-2012

SM2 Cryptography Message Syntax Specification

SM2 密码算法加密签名消息语法规范

Issued on: December 4, 2023

Implemented on: June 1, 2024

Issued by: State Cryptography Administration

Table of Contents

Foreword	3
1 Scope	5
2 Normative References	5
3 Terms and Definitions	5
4 Abbreviated Terms	6
5 OID Definitions	6
6 Definitions of Basic Types	6
6.1 CertificateRevocationLists	6
6.2 ContentEncryptionAlgorithmIdentifier	6
6.3 DigestAlgorithmIdentifier	7
6.4 DigestEncryptionAlgorithmIdentifier	7
6.5 Certificate	7
6.6 IssuerAndSerialNumber	7
6.7 KeyEncryptionAlgorithmIdentifier	7
6.8 Version	7
6.9 ContentInfo	8
7 Data (a Data Type)	8
8 SignedData (a Signed Data Type)	8
8.1 signData type	8
8.2 signerInfo type	9
9 EnvelopedData (a Digital Enveloped Data Type)	10
9.1 envelopedData type	10
9.2 recipientInfo type	11
10 SignedAndEnvelopedData (a Signed and Enveloped Data Type)	12
11 EncryptedData (an Encrypted Data Type)	13
12 KeyAgreementInfo (a Key Agreement Type)	14
Appendix A (Informative) Example	15
Appendix B (Normative) SM2 Implicit Certificate Cryptographic Signature Message Syntax	27
Appendix C (Normative) SM2 Key Format	32

Foreword

This Document was drafted as per the rules specified in GB/T 1.1-2020 *Directives for Standardization – Part 1: Rules for the Structure and Drafting of Standardizing Documents*.

This Document replaced GM/T 0010-2012 *SM2 Cryptography Message Syntax Specification*. Compared with GM/T 0010-2012, the major technical changes of this Document are as follows besides the structural adjustments and editorial modifications:

- a) Add normative references GB/T 25069, GM/T 0015 and GM/Z 4001 (see Clause 3, 6.5); and delete the reference to PKCS# 6 (see 6.5 of the 2012 Edition);
- b) Delete the terms "algorithm identifier" and "SM2 cryptographic algorithm" (see 3.1 and 3.2 of the 2012 Edition); and add the term "implicit certificate" (see 3.1 of this Edition);
- c) Add 3 OIDs related to implicit certificates (see Clause 5 of this Edition);
- d) Delete the description of extended certificate types (see 6.5 of the 2012 Edition);
- e) Change "contentInfo SM2Signature" (see Clause 8 of this Edition; Clause 8 of the 2012 Edition);
- f) Change userCertificate (see Clause 12 of this Edition; Clause 12 of the 2012 Edition; Chapter);
- g) Add normative Appendix B (see Appendix B of this Edition).

Please note some contents of this Document may involve patents. The issuing agency of this Document shall not assume the responsibility to identify these patents.

This Document was proposed by and under the jurisdiction of Cryptography Standardization Technical Committee.

Drafting organizations of this Document: Koal Software Co., Ltd.; Beijing Haitai Fangyuan High Technology Co., Ltd.; Beijing Certificate Authority Co., Ltd.; Guangdong Electronic Certification Authority Co., Ltd.; Wuxi Jiangnan Information Security Engineering Technology Center; CETC Cyberspace Security Technology Co., Ltd.; Beijing Infosec Technologies Co., Ltd.; Beijing Guomai Xinan Technology Co., Ltd.; Shanghai Electronic Certificate Authority Center Co., Ltd.; Xingtang Communication Technology Co., Ltd.; Shandong De'an Information Technology Co., Ltd.; Shandong University; Shenzhen Aolian Information Security Technology Co., Ltd.; SmartPunch (Shanghai) Testing Technology Co., Ltd.; Shanghai Yidong Network Information Co., Ltd.; and National Research Center for Information Technology Security.

Chief drafting staffs of this Document: Liu Ping, Zheng Qiang, Tang Wuzheng, Liu Zengshou, Li Shusheng, Zhao Yongsheng, Zhao Min, Liang Ningning, Wang Zongbin, Yuan Feng, Kong

SM2 Cryptography Message Syntax Specification

1 Scope

This Document specifies the syntax of encrypted and signed messages using the SM2 cryptographic algorithm.

This Document is applicable to the standardized encapsulation of the results of encryption and signing operations using the SM2 cryptographic algorithm.

2 Normative References

The provisions in following documents become the essential provisions of this Document through reference in this Document. For the dated documents, only the versions with the dates indicated are applicable to this Document; for the undated documents, only the latest version (including all the amendments) is applicable to this Document.

GB/T 25069 Information security techniques - Terminology

GM/T 0006 Cryptographic application identifier criterion specification

GM/T 0009 SM2 cryptography algorithm application specification

GM/T 0015 Digital certificate format

GM/Z 4001 Cryptology terminology

3 Terms and Definitions

For the purposes of this Document, the terms and definitions given in GB/T 25069 and GM/Z 4001 apply.

3.1 Implicit certificate

A digital certificate that contains user identification, public key recovery data, and issuer identification information but does not explicitly contain a digital signature from a certification authority (CA).

NOTE: The actual public key associated with the user is calculated from the elliptic curve system parameters, the CA's public key, and the associated user information and public key recovery data in the implicit certificate.

4 Abbreviated Terms

The following abbreviated terms are applicable to this Document.

CA: certification authority

OID: object identity

5 OID Definitions

This Document defines the identifiers for 9 objects, such as data, signedData, envelopedData, signedAndEnvelopedData, encryptedData, keyAgreementInfo, imcSignedData, imcEnvelopedData, and imcSignedAndEnvelopedData; see Table 1 in detail.

6 Definitions of Basic Types

6.1 CertificateRevocationLists

The CertificateRevocationLists type identifies a set of certificate revocation lists.

CertificateRevocationLists ::= SET OF CertificateRevocationList

6.2 ContentEncryptionAlgorithmIdentifier

The ContentEncryptionAlgorithmIdentifier type identifies a data encryption algorithm. Its OID shall comply with GM/T 0006.

ContentEncryptionAlgorithmIdentifier ::= AlgorithmIdentifier

6.3 DigestAlgorithmIdentifier

The DigestAlgorithmIdentifier type indicates a message digest algorithm. This Document is the SM3 cryptographic algorithm; and its OID shall comply with GM/T 0006.

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

6.4 DigestEncryptionAlgorithmIdentifier

The DigestEncryptionAlgorithmIdentifier type indicates a signature algorithm. This Document is the SM2 signature algorithm; and its OID shall comply with GM/T 0006.

DigestEncryptionAlgorithmIdentifier ::= AlgorithmIdentifier

6.5 Certificate

The Certificate type specifies a certificate that conforms to the format in GM/T 0015. It represents a set sufficient to contain the certificate chain from a recognized "root" or "top CA" to all signers.

Certificates ::= SET OF Certificate

6.6 IssuerAndSerialNumber

The IssuerAndSerialNumber type specifies a certificate issuer's distinguished name and the certificate serial number determined by the issuer, which can be used to identify a certificate and the entity and public key corresponding to the certificate.

```
IssuerAndSerialNumber ::= SEQUENCE {  
    issuer Name,  
    serialNumber CertificateSerialNumber  
}
```

6.7 KeyEncryptionAlgorithmIdentifier

The KeyEncryptionAlgorithmIdentifier type identifies the encryption algorithm used to encrypt a symmetric key.

KeyEncryptionAlgorithmIdentifier ::= AlgorithmIdentifier

6.8 Version

The Version type indicates the syntax version number.

Version ::= INTEGER(1)

6.9 ContentInfo

The ContentInfo type indicates the general syntax structure of content exchange. The general syntax structure of content exchange is defined as follows:

```
ContentInfo ::= SEQUENCE {  
    contentType ContentType,  
    content[0] EXPLICIT ANY DEFINED BY contentType OPTIONAL  
}
```

ContentType ::= OBJECT IDENTIFIER

Thereof:

ContentType is an object identifier, as defined in Clause 5.

content is optional.

7 Data (a Data Type)

The Data structure of data type is defined as follows:

Data ::= OCTET STRING

The Data of data type represents an arbitrary byte string.

8 SignedData (a Signed Data Type)

8.1 signData type

The data type of signedData consists of data of any type and a signature value of at least one signer. Data of any type can be signed by any number of signers at the same time. For an example of the signature data type, see A.1 in Appendix A. The signed data type in an implicit certificate shall comply with B.1 in Appendix B.

The data type structure of the signedData is defined as follows:

```
SignedData ::= SEQUENCE {  
    version Version,  
    digestAlgorithms DigestAlgorithmIdentifiers,  
    contentInfo ContentInfo,
```

This is an excerpt of the PDF (Some pages are marked off intentionally)

Full-copy PDF can be purchased from 1 of 2 websites:

1. <https://www.ChineseStandard.us>

- SEARCH the standard ID, such as GB 4943.1-2022.
- Select your country (currency), for example: USA (USD); Germany (Euro).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Tax invoice can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with download links).

2. <https://www.ChineseStandard.net>

- SEARCH the standard ID, such as GB 4943.1-2022.
- Add to cart. Only accept USD (other currencies - <https://www.ChineseStandard.us>).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with PDFs attached, invoice and download links).

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

About Us (Goodwill, Policies, Fair Trading...): <https://www.chinesestandard.net/AboutUs.aspx>

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: <https://www.linkedin.com/in/waynezhengwenrui/>

----- The End -----