

ICS 38.040
CCS L 80

GM

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

GM/T 0081-2020

**SM9 cryptographic algorithm encryption and signature
message syntax specification**

SM9密码算法加密签名消息语法规范

(English Translation)

Issued on: December 28, 2020

Implemented on: July 1, 2021

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative References	2
Terms and Definitions	3
Algorithm identifier	4
SM9 algorithm	5
Signature master key	6
Encryption master key	7
Signature key	8
Encryption key	9
Identity trust chain	10
Abbreviations	11

1 Scope

This Document defines the encryption and signature message syntax using the SM9 cryptographic algorithm.

This Document is applicable to the standardized encapsulation of operation results when the SM9 algorithm is used for encryption and signature operations.

2 Normative References

The following documents are essential to the application of 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 33560 Information Security Technology - Cryptographic Application Identifier Criterion Specification
 GB/T 38635 (all parts) Information Security Technology - Identity-Based Cryptographic Algorithms
 SM9 GM/T 0080 SM9 Cryptographic Algorithm Application Specification
 GM/Z 4001-2013 Cryptographic Terms

3 Terms and Definitions

For the purposes of this Document, the terms given in GB/T 38635 (all parts) and GM/Z 4001-2013 and the following apply.

3.1 Algorithm identifier

Digitized information that is used to indicate algorithmic mechanisms.

3.2 SM9 algorithm

A cryptographic algorithm of national commercial bilinear pair elliptic curve public key.

3.3 Signature master key

The root signature key pair of the key management infrastructure, including the signature master private key and signature master public key, which is used for digital signature, verification and generating user signature key for the users.

3.4 Encryption master key

The root encryption key pair of the key management infrastructure, including the encryption master private key and the encryption master public key, which is used for digital encryption, decryption, and generating user encryption key for users.

3.5 Signature key

Thereof, the private key is generated by the key management infrastructure and distributed to users. This type of key includes user signature private key and signature public key, which are used for digital signature and signature verification.

3.6 Encryption key

Thereof, the private key is generated by the key management infrastructure and distributed to users. This type of key includes user encryption private key and encryption public key, which are used for encryption, decryption and key agreement.

3.7 Identity trust chain

A hierarchical ordered collection of identity application attribute information, in which stores the identity application attribute information from the user terminal to the root KGC.

4 Abbreviations

The following abbreviations are applicable to this Document.

IBC: Identity-Based Cryptography.

IRIs: Internationalized Resource Identifiers.

IRL: Identifier Revocation List.

KGC: Key Generation Centre.

OID: Object Identifier.

Where:

The version item (version) determines the version of the IBCSysParams format. The format mentioned in this document shall be set to 2.

The name item (districtName) is an IA5 string that shall be encoded with URI or IRI.

districtSerial represents an integer that can be set by the only available IBC public parameter (for URI or IRI defined by districtName). If a new parameter is announced for districtName, the value of districtSerial shall be greater than the value of districtSerial used before.

The validity period item (validity) determines the life of a specific IBCSysParams example and is determined according to the following:

The values of notBefore and notAfter must be expressed in Greenwich Mean Time and include seconds (for example, the time is expressed as YYYYMMDDHHMMSSZ).

Even if the number of seconds is zero, it must be expressed as the nearest number of seconds. The customer must confirm that the date of the IBC public parameter it uses is between the notBefore time and the notAfter time of the IBC public parameter. At the same time, if the date is not in this interval, the parameter used for IBC encryption operation cannot be used.

When the value of IbcPublicParameters, IbcIdentityType or IbcParamExtensions changes an area, the IBC public parameters shall be regenerated and announced. The customer shall retrieve the IBC public parameters within the application configuration interval to ensure the version of the parameters is latest.

The IBCPublicParameters public parameter item is a structure that contains public parameters (corresponding to the IBC algorithm formula supported by PKG). It is defined as follows:

Where:

ibcAlgorithm OID determines the IBC algorithm formula. Two IBC algorithmic OIDs and their publicParameterData structures.

publicParameterData is a DER encoding structure of SM9PublicParameterData, which contains the real encrypted parameters. Its specific structure is as follows: