

ICS 35.040
CCS L 80

GM

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

GM/T 0099-2020

**Cryptography application technical specification of open fixed
layout documents**

开放式版式文档密码应用技术规范

(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
Fixed layout	4
Electronic seal	5
Electronic seal signature	6
Abbreviations	7
Cryptography application mechanism	8
Cryptography application requirements	9
Overview	10
Protocol description	11
Data format requirements	12
Cryptography algorithm requirements	13
Digital certificate requirements	14
Timestamp requirements	15
Signature process	16
Signature verification process	17
Cryptography algorithm requirements	18
Decryption process	19
Generation process	20
Verification process	21
Overview	22
Protocol description	23
Data format requirements	24
Cryptography algorithm requirements	25
Digital certificate requirements	26
Timestamp requirements	27
Signature process	28
Signature verification process	29
Cryptography algorithm requirements	30
Decryption process	31
Generation process	32

1 Scope

This Standard regulates the use of cryptographic technology to sign, encrypt and protect the integrity of open format documents.

This Standard is applicable to guiding the development, use and testing of products and systems related to open-format document encryption applications.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 20518, Information security technology - Public key infrastructure -Digital certificate format
GB/T 20520, Information security technology - Public key infrastructure -Time stamp specification
GB/T 32905, Information security technology SM3 cryptographic hash algorithm

3 Terms and definitions

For the purposes of this document, the terms and definitions defined in GB/T 33190-2016, GB/T 38540-2020 as well as the followings apply.

3.1 Fixed layout

A format in which text, graphics, images and other digital content objects are solidified and presented on the layout according to certain rules.

3.3 Electronic seal

A type of secure data that is digitally signed by the creator of the electronic seal.

3.4 Electronic seal signature

The process of signing an electronic document with an electronic seal.

4 Abbreviations

The following abbreviations apply to this document.

5 Cryptography application mechanism

OFD is an electronic document format in which various digital content objects such as text, graphics, and images are solidified and presented in accordance with certain rules. It is an open format standard formulated by China. It is also one of the basic file formats for national electronic file management.

6 Cryptography application requirements

The goal of OFD's cryptographic application is to ensure the confidentiality, integrity, authenticity and non-repudiation of documents.

7.1 Overview

The security of OFD is jointly guaranteed by the three protocols of signature, encryption and integrity protection. Separately protect the authenticity and non-repudiation, confidentiality and integrity of documents.

7.2.1 Protocol description

The OFD signature protocol is used to ensure the authenticity of OFD documents and the undeniable signature of the signer. After the signature operation, a new signature file and signature value data will be formed in the OFD file. At the same time, the newly formed signature file record is added to the signature list.

7.2.2 Data format requirements

The signature file and signature list generated by OFD signature operation shall meet the requirements of Chapter 18 in GB/T 33190-2016. To support multiple signature types and custom parameters, the signature file shall be expanded as shown in Annex B.

7.2.3 Cryptography algorithm requirements

The requirements of OFD signature to cryptography algorithm are as follows.

7.2.4 Digital certificate requirements

The digital certificate requirements for OFD signature are as follows.

7.2.5 Timestamp requirements

The requirements of OFD signature for timestamp are as follows.

7.2.6 Signature process

The OFD digital signature process requirements are as follows.

7.2.7 Signature verification process

The signature verification process is as follows.

7.3.3 Cryptography algorithm requirements

The algorithm requirements for OFD encryption are as follows.

7.3.5 Decryption process

Decrypt the file according to the encryption scheme. The process is as follows.

a) Obtain the packaging key for symmetric encryption of the file from the encryption information of the key description file according to the identity of the electronic file visitor;

7.4.5 Generation process

The OFD integrity protection signature process is as follows.

7.4.6 Verification process

The OFD integrity protection verification signature process is as follows.

Annex A

(normative)

Cryptography protection scheme identification and protection method A.1 Cryptography protection scheme identification the identification of the cryptography protection scheme required by OFD cryptography application is shown in Table A.1.

GM/T 0099-2020

CRYPTOGRAPHIC INDUSTRY STANDARD ICS 35.040 CCS L 80 Cryptography application technical specification of open fixed layout documents Issued on. DECEMBER 28, 2020 Implemented on. JULY 01, 2021 Issued by. National Cryptography Administration

Table of Contents

Foreword... 3

1 Scope... 4

2 Normative references... 4

3 Terms and definitions... 5