

ICS 35.030
CCS L 80

GM

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

GM/T 0112-2021

**Technical requirements of cryptography application in portable
document format**

PDF格式文档的密码应用技术要求
(English Translation)

Issued on: October 18, 2021

Implemented on: May 1, 2022

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative references	2
Requirements for cryptography applications	3
Overview	4
Signature field object	5
Digital signature generation	6
Digital signature verification	7
Timestamp	8
Overview	9
Electronic signature verification	10
Timestamp	11
Encryption mechanism	12

1 Scope

This document specifies the technical requirements for digitally signing, electronically stamping, and encrypting and decrypting PDF documents using cryptographic algorithms.

This document is intended to guide the development and testing of cryptographic application-related products and systems based on PDF format documents.

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 32010.1-2015, Document management -- Portable document format -- Part 1.

PDF 1.7

GB/T 32905, Information security techniques -- SM3 cryptographic hash algorithm
 GB/T 32907, Information security technology -- SM4 block cipher algorithm
 GB/T 32918 (all parts), Information security technology -- public key cryptographic algorithm SM2 base on elliptic curves
 GB/T 35275, Information security technology -- SM2 cryptographic algorithm

encrypted signature message syntax specification GB/T 38540, Information security technology -- Technical specification secure electronic seal signature cryptography GM/T 0091, Cryptography-based key derivation specification the cross-reference table contains information that allows random access to indirect objects in the file. It is not necessary to read the entire file to find a specific object.

d) Trailer

Trailer of the document enables conforming readers to quickly locate cross-reference tables and certain special objects.

The trailer shall include a trailer dictionary. Encryption-related attribute information is stored in the Encrypt item of the trailer dictionary.

5.2 Requirements for cryptography applications

The security goal of cryptography application for PDF format documents is to ensure their authenticity, integrity, confidentiality and non-repudiation.

The signature/signer of a PDF document uses his/her private signature key to digitally sign/electronically sign the PDF document to achieve document protection. The recipient verifies the signed PDF document, including the digital signature/electronic signature and digital certificate, to confirm the authenticity of the document source and the integrity of the document. At the same time, the signature/signer cannot deny the signing of the PDF document.

PDF format documents are protected by using a cryptography mechanism to encrypt the PDF document content that needs confidentiality protection, using cryptography-based encryption or digital certificate public key-based encryption to achieve document confidentiality requirements.

When both encryption and signing are applied to the same PDF document, encryption must be performed first and then signing.

6.1 Overview

PDF digital signatures are used to verify the authenticity of the PDF document signer's identity, ensure the integrity of the document content, and ensure the non-repudiation of document signing behavior.

PDF digital signature uses the private key of the document signer to sign the PDF document. The signature operation is implemented by calling the PDF signature handler.

The signature appearance is the visual representation of a PDF digital signature, which is described by the Appearance (AP) object. The Appearance AP defines the appearance of the signature on the PDF page, where the Rect key defines the position and size of the signature on the PDF page. The height and width of the invisible signature Rect shall be

0. PDF readers that conform to this document shall treat such signatures as invisible.

6.2.1 Signature field object

To adapt the personalized user interface processing effects of SM2 digital signatures to different PDF readers, this document describes two PDF SM2 signature implementation methods.

- a) Form signature field object. Implement PDF SM2 digital signature by setting an interactive AcroForm signature field that supports SM2 signature.
- b) Annotation signature field object. Implement PDF SM2 digital signature by setting the annotation object that supports SM2 signature.

NOTE: Any annotated signature field objects defined in the document shall not be referenced by interactive forms.

During the application implementation process, developers can choose one of the two implementation methods based on their needs.

During the application implementation process, developers can choose one of the two implementation methods based on their needs. You can create a form signature field object or annotate a signature object and associate it with a signature dictionary to set PDF signature-related property information, thereby achieving a digital signature.

The form signature field object is used to implement the SM2 digital signature. The definition of the object dictionary is shown in Table 1.

6.5 Digital signature generation

The process of generating a digital signature for a PDF document is as follows.

- a) Prepare PDF documents for signing.
 - 1) Determine the signing method. Set the PDF signature field object.
 - If the form signature field method is used, set the signature field object according to Table 1;
 - If the signature field is marked, set the signature field object according to Table 2.
 - 2) For digital signatures with signature appearance, place the appearance image in the area specified by the Rect key of the PDF AP appearance. It is up to the application to ensure that the source of the appearance image is authentic.
- b) Determine the PDF digital signature protection range. Set the ByteRange value in the signature dictionary in Table 3.

c) According to the signature processing mode of Filter or SubFilter in the signature dictionary definition in Table 3 and the original text established by the PDF digital signature protection range specified by ByteRange, the hash value is calculated for the original text according to the hash algorithm in GB/T 32905.

d) Call the operator's signature private key to digitally sign the hash value of the signature information.

- Call the operator's signature private key to digitally sign the hash value of step

c). Pack it according to the original signedData signature format in GB/T 35275;

- If a timestamp is also required, create the timestamp data according to 6.7 of this document to form the final signature data type signedData format. After DER encoding, put it into the Contents field of Table 3 as a hexadecimal string.

e) According to the PDF document format, a signed PDF document is generated.

In addition, in multi-signature application scenarios such as official document circulation and multi-person approval, if there is already a digital signature in the document, when signing again, a new signature shall be added or one of the multiple signatures shall be deleted by incremental PDF update, but the validity of the remaining original signatures must not be changed.

6.6 Digital signature verification

The PDF digital signature verification process is as follows.

a) Select a signed PDF document. Based on the signature field object, signature dictionary and other information in the document, parse and obtain the relevant information required to verify the signature.

b) Perform signature verification based on the Filter or SubFilter signature processing method. Parse the Contents to be in the signature data format in GB/T 35275. Verify the validity of the signature according to the signedData format in GB/T 35275. If a timestamp is included, verify the timestamp.

c) Verify the validity of digital certificates, including certificate chain, certificate validity period, certificate status, etc.

d) The PDF reader displays the signature verification effect based on the verification result.

6.7 Timestamp

PDF documents can contain timestamps. Timestamps can prove that the digital signature of a PDF document existed before a certain time.

For PDF digital signatures with timestamps, the calculation source of the timestamp is the