ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0112—2021

PDF 格式文档的密码应用技术要求

Technical requirements of cryptography application in portable document format

2021-10-19 发布　　2022-05-01 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：北京数字认证股份有限公司、数安时代科技股份有限公司、福建福昕软件开发股份有限公司、兴唐通信科技股份有限公司、北京信安世纪科技股份有限公司、三未信安科技股份有限公司、北京江南天安科技有限公司、上海市数字证书认证中心有限公司、中国科学院数据与通信保护研究教育中心、暨南大学。

本文件主要起草人：林雪焰、夏鲁宁、傅大鹏、王文昌、张永强、汪宗斌、梁俊义、高能、朱亚飞、刘岩、李元、谢峰、黄利繁、马晓艳、冯辉、韩玮、钱文飞、谭武征、王胜男、李向锋、赵松、张妍、李红、赵子轩、张超、王银平、李敏、刘中、王新华、邓钊汉。

PDF 格式文档的密码应用技术要求

1 范围

本文件规定了采用密码算法对 PDF 格式文档进行数字签名、电子签章以及加解密应用的技术要求。

本文件适用于指导基于 PDF 格式文档的密码应用相关产品和系统的研发和检测。

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 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 20520 信息安全技术 公钥基础设施 时间戳规范

GB/T 32010.1—2015 文献管理 可移植文档格式 第 1 部分：PDF1.7

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32918(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

GB/T 38540 信息安全技术 安全电子签章密码技术规范

GM/T 0091 基于口令的密钥派生规范

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

PDF 格式文档 portable document format

一种由 GB/T 32010.1 定义的可移植文档格式(PDF)的文件格式。

3.2

SM2 算法 SM2 algorithm

由 GB/T 32918 定义的一种椭圆曲线密码算法。

3.3

SM3 算法 SM3 algorithm

由 GB/T 32905 定义的一种密码杂凑算法。

3.4

SM4 算法 SM4 algorithm

由 GB/T 32907 定义的一种分组密码算法。

4 缩略语

下列缩略语适用于本文件。

CBC:密文分组链接(Cipher Block Chaining)

CMS:加密签名消息语法(Cryptographic Message Syntax)

CRL:证书撤销列表(Certificate Revocation List)

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

ISO:国际标准化组织(International Organization for Standardization)

PDF:可移植文档格式(Portable Document Format)

PKI:公钥基础设施(Public Key Infrastructure)

5 PDF 密码应用需求

5.1 PDF 格式文档结构概述

PDF 文件通常由以下 4 个元素构成(见图 1):

——文件头(header),标识文件所符合的 PDF 规范版本;

——正文(body),包含组成文件中所含文档的对象;

——交叉引用表(cross-reference table),包含关于文件中间接对象的信息;

——文件尾注(trailer),提供交叉引用表和文件正文内某些特殊对象的位置。

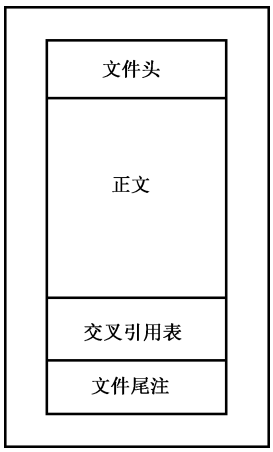

图 1 PDF 文件结构示意图

a) 文件头

PDF 文件的第一行应为文件头,%PDF-1.N 表示 PDF 版本号,其中 N 是 0～7 之间的数字,目前 PDF 最新版本为%PDF-1.7。

b) 正文

正文包含 PDF 文档的各种数据对象,包括文字、图形、字典对象、流对象等间接对象,正文至少包含一个间接对象序列,表示文档的内容。PDF 的数字签名的签名域对象、签名字典及结果、电子签章签章域对象、签章字典及结果、加密结果通常都以对象形式存放在正文中相应位置。

c) 交叉引用表

交叉引用表包含的信息允许对文件中的间接对象进行随机访问，不需要读取整个文件来查找具体对象。

d) 文件尾注

文件尾注使符合本文件的阅读器可以快速找到交叉引用表和某些特殊对象。

文件尾注应包括尾注字典。加密相关属性信息存储在文件尾注字典的加密(Encrypt)项中。

5.2 密码应用需求

PDF 格式文档的密码应用安全目标是保证其真实性、完整性、机密性和不可否认性。

PDF 格式文档的签名者/签章者通过其签名私钥对 PDF 文档进行数字签名/电子签章实现文档保护，接收者通过对已签 PDF 文档进行验证，包括对数字签名/电子签章和数字证书进行验证，确认文档来源的真实性，验证文档的完整性，同时也实现了签名者/签章者对 PDF 文档签署行为的不可否认。

PDF 格式文档通过使用密码机制对需要机密性保护的 PDF 文档内容进行加密保护，使用基于口令的加密或基于数字证书公钥的加密，从而实现文档的机密性要求。

在对同一个 PDF 文档加密、签名都应用的场景中，需要先加密处理后，再进行签名。

6 PDF 数字签名

6.1 概述

PDF 数字签名用于验证 PDF 文档签名者身份的真实性、保障文档内容的完整性、文档签名行为的不可否认性。

PDF 数字签名采用文档签名者私钥对 PDF 文档进行签名运算，签名运算是通过调用 PDF 的签名处理程序(signature handler)来实现。

签名外观是用于 PDF 数字签名的可视化展现，是由外观(AP)对象来描述。外观 AP 定义了签名呈现在 PDF 页面上的外观，其中 Rect 键定义了签名在 PDF 页面中的位置与大小。不可见的签名 Rect 的高度和宽度应为 0，符合本文件的 PDF 阅读器应将这种签名作为不可见处理。

6.2 PDF 签名结构

6.2.1 签名域对象

为了适应不同 PDF 阅读器对 SM2 数字签名的个性化用户界面处理效果，本文件描述了两种 PDF 的 SM2 签名实现方式。

a) 表单签名域对象。通过设置支持 SM2 签名的交互式表单签名域(AcroForm signature field)来实现 PDF SM2 数字签名。

b) 标注签名域对象。通过设置支持 SM2 签名的 annotation 对象来实现 PDF SM2 数字签名。

注：在文档中定义的任何一个标注签名域对象，不应被交互式表单索引。

在应用实现过程中，开发者根据需求自行选择两种实现方式之一。可通过创建表单签名域对象或者标注签名对象，并与签名字典(signature dictionary)关联，来设置 PDF 签名相关属性信息，从而实现数字签名。

采用表单签名域对象实现 SM2 数字签名，该对象字典的定义见表 1。

表 1　用于 SM2 数字签名的表单签名域字典的部分条目

键	值类型	值
Type	name	Annot
Subtype	name	Widget
Rect	rectangle	[left,bottom,right,top],left 与 bottom 构成签名外观的左下角坐标,right 与 top 构成签名外观的右上角坐标,这四个值为 float 类型,单位为 pt
F	integer	Flag 设置标注各种特性的标志,见 GB/T 32010.1—2015 的 12.5.3
AP	dictionary	签名外观字典的定义,指定应如何在页面上显示标注的外观字典,见 GB/T 32010.1—2015 的 12.5.5
T	String	表明 annot 的标题,由厂商自己定义,需要保证在该文档中唯一性
FT	String	Sig
V	Dictionary	(自定义字段),签名字典,见表 3

在表 1 中,域类型(FT)为 Sig,域值(V)为签名字典,签名字典的定义见表 3。

采用标注签名域对象实现 SM2 数字签名,该对象字典的定义见表 2。

表 2　用于 SM2 数字签名的标注签名域字典的部分条目

键	值类型	值
Type	name	Annot
Subtype	name	SigAnnot
Rect	rectangle	[left,bottom,right,top],left 与 bottom 构成签名外观的左下角坐标,right 与 top 构成签名外观的右上角坐标,这四个值为 float 类型,单位为 pt
F	integer	Flag 设置标注各种特性的标志,见 GB/T 32010.1—2015 的 12.5.3
AP	dictionary	签名外观字典的定义,指定应如何在页面上显示标注的外观字典,见 GB/T 32010.1—2015 的 12.5.5
T	String	表明 annot 的标题,由厂商自己定义,需要保证在该文档中唯一性
FT	String	Sig
V	Dictionary	(自定义字段),签名字典,见表 3

在表 2 中,标注签名域字典的 Type 值应为 Annot,子类型 Subtype 值为 SigAnnot,域类型 FT 值应为 Sig,V 值应为签名字典,签名字典的定义见表 3。

6.2.2　签名字典

PDF 签名信息是通过签名字典(signature dictionary)来定义,签名值包含在签名字典中,签名字典的定义见表 3。

表 3　签名字典的部分条目

键	类型	值
Type	name	签名字典类型值应为 Sig
Filter	name	指定了用于数字签名的首选处理程序，一些签名处理程序示例，如 Adobe.PPKLite、Entrust.PPKEF、CICI.SignIt、VeriSign.PPKVS。采用 SM2 算法进行数字签名，签名处理程序名称由厂商自行定义，命名规则宜按“厂商名称.GMPkiLite”
SubFilter	name	子过滤器，是 PDF 数字签名的具体处理方式。SM2 算法的数字签名，采用子过滤器 GM. sm2cms. detached，用于处理符合 GB/T 35275 签名数据类型 signedData 格式，该数据是不带原文的格式
Contents	byte string	Contents 用于存放数字签名值，通常是一个 DER 编码十六进制数据对象，并以字符串形式存放在 PDF 文档中，数字签名值为 GB/T 35275 签名数据类型 signedData 格式，调用子过滤器 GM.sm2cms.detached 进行处理
ByteRange	array	描述 PDF 签名过程中杂凑计算的确切字节范围，是一个包含四个整数的数组。 数组的元素 0 和 2 表示从文件头开始的字节偏移量，1 和 3 表示长度。 当前签名的原文是从 ByteRange[0]位置开始，读取 ByteRange[1]长度的字节数；然后跳转到 ByteRange[2]位置，再读取 ByteRange[3]长度的字节数。把这两次读取的数据连接成一个数据，这就是 PDF 签名的原文。 ByteRange 取值范围是除签名值本身(Contents 条目)之外的整个文件，包括签名字典。 即一个签名完成的 PDF 文档中，除了原文，就是签名值本身；对 PDF 文档的任何一个字节的变动都会造成签名验证失败

签名字典中其他条目定义，见 GB/T 32010.1—2015 中 12.8 的表 250。

6.3　签名算法要求

PDF 格式文档的签名算法要求：

a)　使用的签名算法应当符合密码国家标准、行业标准的相关要求；

b)　使用 SM2 签名算法应遵循 GB/T 32918，使用 SM3 杂凑算法应遵循 GB/T 32905。

6.4　数字证书要求

用于 PDF 数字签名的数字证书，应符合 GB/T 20518。

6.5　数字签名的生成

PDF 文档数字签名的生成流程如下。

a)　准备待签名的 PDF 文档。

1)　确定签名方式，设置 PDF 签名域对象：

——采用表单签名域方式，则按表 1 设置签名域对象；

——采用标注签名域方式，则按表 2 设置签名域对象。

2)　对于带签名外观的数字签名，通过在 PDF 的 AP 外观的 Rect 键指定区域放置外观图片，并由应用来保证外观图片来源的真实可靠。

b)　确定 PDF 数字签名保护范围，设置表 3 签名字典中的 ByteRange 值。

c) 根据表3签名字典定义中Filter或SubFilter签名处理方式，以及ByteRange指定的PDF数字签名保护范围确立的原文，按照GB/T 32905杂凑算法对原文计算杂凑值。

d) 调用操作人签名私钥对签名信息的杂凑值进行数字签名：

——调用操作人签名私钥对步骤c)的杂凑值进行数字签名，并按GB/T 35275中的无原文signedData签名格式进行组包；

——如果还需要时间戳，则按本文件的6.7创建时间戳数据，形成最终的签名数据类型signedData格式，并经过DER编码，按十六进制字符串，放入表3的Contents字段。

e) 根据PDF文档格式，形成签名后的PDF文档。

此外，在公文流转、多人审批等多重签名应用场景中，如果文档中已有数字签名，再进行签名处理的情况下，应以PDF增量更新方式添加新签名或删除多个签名其中之一，但不得改变其余原有签名的有效性。

6.6 数字签名的验证

PDF数字签名验证流程如下：

a) 选择已签名的PDF文档，根据文档中的签名域对象、签名字典等信息，解析得到验证签名所需相关信息。

b) 根据Filter或SubFilter签名处理方式，进行签名验证。解析Contents是GB/T 35275签名数据格式，按GB/T 35275的signedData格式验证签名的有效性；如果含有时间戳，则对时间戳进行验证。

c) 验证数字证书的有效性，包括证书链、证书有效期、证书状态等。

d) PDF阅读器根据验证结果显示签名验证效果。

6.7 时间戳

PDF文档可包含时间戳，时间戳可以证明PDF文档数字签名是在某个时间之前就已经存在。

带时间戳的PDF数字签名，时间戳的计算原文是GB/T 35275签名数据格式signedData中SM2Signature值，时间戳结果放置在GB/T 35275签名数据格式signedData定义的unauthenticatedAttributes字段中。

PDF时间戳数据格式按GB/T 20520的规定。

7 PDF电子签章

7.1 概述

PDF电子签章用于验证PDF文档签章者身份的真实性、保障文档内容的完整性、文档签章行为的不可否认性。

PDF电子签章采用文档签章者私钥对PDF文档进行签章运算，签章运算是通过调用PDF的签章处理程序来实现。

签章外观是用于PDF电子签章的可视化展现，是由外观(AP)对象来描述。外观AP定义了签章呈现在PDF页面上的外观，其中Rect定义了签章在PDF页面中的位置与大小。不可见的签章的Rect高度和宽度应为0，符合本文件的PDF阅读器应将这种签章作为外观不可见处理。

7.2 PDF签章结构

7.2.1 签章域对象

为了适应不同PDF阅读器对安全电子签章的个性化用户界面处理效果，本文件描述了两种PDF

的 SM2 电子签章实现方式。

a) 表单签章域对象。通过设置支持安全电子签章的交互式表单签名域(AcroForm signature field)来实现 PDF SM2 电子签章。

b) 标注签章域对象。通过设置支持安全电子签章的 annotation 对象来实现 PDF SM2 电子签章。

注：在文档中定义的任何一个标注签章域对象，不应被交互式表单索引。

在应用实现过程中，开发者根据需求自行选择两种实现方式之一。

PDF 电子签章可通过创建表单签章域对象或者标注签章域对象，并与签章字典关联，来设置 PDF 电子签章相关信息，从而实现安全电子签章。

采用表单签章域对象实现 SM2 电子签章，该对象字典的定义见表 4。

表 4 用于 SM2 电子签章的表单签章域字典的部分条目

键	值类型	值
Type	name	Annot
Subtype	name	Widget
Rect	rectangle	[left,bottom,right,top]，left 与 bottom 构成签章外观的左下角坐标，right 与 top 构成签章外观的右上角坐标，这四个值为 float 类型，单位为 pt
F	integer	Flag 设置标注各种特性的标志，见 GB/T 32010.1—2015 的 12.5.3
AP	dictionary	签章外观字典的定义，应指定如何在页面上显示标注的外观字典，见 GB/T 32010.1—2015 的 12.5.5
T	String	表明 annot 的标题，由厂商自己定义，需要保证在该文档中唯一性
FT	String	Sig
V	Dictionary	(自定义字段)，签章字典，见表 6

在表 4 中，域类型(FT)为 Sig，域值(V)为签章字典，签章字典的定义见表 6。

采用标注签章域对象实现 SM2 电子签章，该对象字典的定义见表 5。

表 5 用于 SM2 电子签章的标注签章域字典的部分条目

键	值类型	值
Type	name	Annot
Subtype	name	SigAnnot
Rect	rectangle	[left,bottom,right,top]，left 与 bottom 构成签章外观的左下角坐标，right 与 top 构成签章外观的右上角坐标，这四个值为 float 类型，单位为 pt
F	integer	Flag 设置标注各种特性的标志，见 GB/T 32010.1—2015 的 12.5.3
AP	dictionary	签章外观字典的定义，应指定如何在页面上显示标注的外观字典，见 GB/T 32010.1—2015 的 12.5.5
T	String	表明 annot 的标题，由厂商自己定义，需要保证在该文档中唯一性
FT	String	Sig
V	Dictionary	(自定义字段)，签章字典，见表 6

在表5中，标注签名对象字典的Type值应为Annot，子类型Subtype值为SigAnnot，域类型FT值应为Sig，V值应为签章字典，签章字典的定义见表6。

7.2.2 签章字典

PDF签章信息是通过签章字典来定义，电子签章值包含在签章字典中，签章字典的定义见表6。

表6 签章字典的部分条目

键	类型	值
Type	name	签章字典类型值应为Sig
Filter	name	指定了用于电子签章的首选处理程序。SM2电子签章处理程序名称由厂商自行定义，命名规则宜按“厂商名称.GMPkiLite”
SubFilter	name	子过滤器，是PDF电子签章的具体处理方式。SM2电子签章子过滤器为GM.sm2seal，用于处理符合GB/T 38540格式签章数据
Contents	byte string	Contents用于存放电子签章值，通常是一个DER编码十六进制数据对象，并以字符串形式存放在PDF文档中，签章值是GB/T 38540签章格式，调用子过滤器GM.sm2seal进行处理
ByteRange	array	描述PDF签章过程中杂凑计算的确切字节范围，是一个包含四个整数的数组。数组的元素0和2表示从文件头开始的字节偏移量，1和3表示长度。 签章保护原文是从ByteRange[0]位置开始，读取ByteRange[1]长度的字节数；然后跳转到ByteRange[2]位置，再读取ByteRange[3]长度的字节数。把这两次读取的数据连接成一个数据，这就是PDF签名的原文。 ByteRange取值范围是除电子签章值本身(Contents条目)之外的整个文件，包括签章字典。即一个已签章的PDF文档中，除了原文，就是电子签章值本身；对PDF文档的任何一个字节的变动都会造成签章验证失败

签章字典中其他条目定义，可参见GB/T 32010.1—2015中12.8的表250。

7.3 签名算法要求

PDF格式文档的签名算法要求：

a) 使用的签名算法应当符合密码国家标准、行业标准的相关要求；

b) 使用SM2签名算法应遵循GB/T 32918，使用SM3杂凑算法应遵循GB/T 32905。

7.4 数字证书要求

用于PDF电子签章的数字证书，应符合GB/T 20518。

7.5 电子签章的生成

PDF文档电子签章的生成流程如下。

a) 准备待签章的PDF文档。

1) 确定PDF安全电子签章方式，设置PDF签章属性对象：

——采用标准签章域方式，则按表4设置签章属性对象；

——采用标注签章域方式，则按表5设置签章属性对象。

2) 设置PDF电子签章的签章外观。通过在PDF的AP外观的Rect键指定区域放置印章图

片，印章图片应从符合 GB/T 38540 的电子印章中获取，PDF 中应存放印章图片的原始尺寸数据，不得更改。GB/T 38540 中指定了印章图片的物理尺寸，但是印章图片在 PDF 中的展示大小在实际应用中可以根据需要进行调节；

b) 确定 PDF 电子签章保护范围，设置表 6 签章字典中的 ByteRange 值。

c) 根据表 6 签章字典定义中 Filter 或 SubFilter 签名处理方式，以及根据 ByteRange 指定的 PDF 电子签章保护范围来确定原文，调用 GB/T 32905 杂凑算法计算杂凑值，并将杂凑结果放入 GB/T 38540 电子签章结构中的原文杂凑值 dataHash 字段。

d) 调用操作人签名私钥进行电子签章。根据签章格式计算签章值，签章具体过程遵照 GB/T 38540 描述。如果还需要时间戳，则按本文件的 6.7 创建时间戳数据，附在电子签章尾部，并经过 DER 编码，以十六进制字符串，放入表 6 的 Contents 字段。

e) 根据 PDF 文档格式，形成已签章的 PDF 文档。

此外，在公文流转、多人审批等多重签章应用场景中，如果文档中已有电子签章，再进行签章处理的情况下，应以 PDF 增量更新方式添加新签章或删除原有多个签章之一，但不得改变其余原有签章的有效性。

7.6 电子签章的验证

PDF 电子签章验证流程如下：

a) 选择已签章 PDF 文档，根据文档中的签章域对象、签章字典等信息，解析得到验证签章所需相关信息。

b) 根据 Filter 或 SubFilter 签名处理方式，进行签章验证。除按照 GB/T 38540 电子签章验证流程来验证签章有效性之外，应用可根据需求对 PDF 签名外观中的印章图片与电子签章数据中的印章原图片进行一致性验证。

c) 验证数字证书的有效性，包括证书链、证书有效期、证书状态等。

d) PDF 阅读器根据验证结果显示签章验证效果。

7.7 时间戳

PDF 文档可包含时间戳，时间戳可以证明 PDF 文档电子签章是在某个时间之前就已经存在。

带时间戳的 PDF 电子签章，时间戳计算的原文和存放符合 GB/T 38540，时间戳原文是电子签章结构中的签名值，时间戳结果附在电子签章尾部。

PDF 时间戳数据格式按 GB/T 20520 的规定。

8 PDF 加解密

8.1 加密机制

可以对 PDF 文档加密以保护其内容免受未经授权的访问。

加密应用于文档的 PDF 文件中的所有字符串和流，以下内容除外：

a) 尾注(trailer)中 ID 条目的值；

b) 加密字典中的任何字符串；

c) 内容流和压缩对象流等流内部的任何字符串，它们本身已加密。

加密信息被存储在文件尾注字典的加密(Encrypt)项中。与加密相关的属性信息是通过定义加密字典(Encrypt Directory)来描述。

PDF 的加解密处理主要有基于口令的加密、基于数字证书的加密两种加密方式，由相应的安全处理程序(security handler)进行处理。

8.2 基于口令的 PDF 加密

8.2.1 概述

基于口令的 PDF 加密可为文档设置两类口令：一个文档所有者口令(owner password)和一个用户口令(user password)。PDF 文档加密与否取决于创建文档的用户是否设置了相应口令或访问限制。

具体见 GB/T 32010.1—2015 的 7.6。

8.2.2 口令加密字典

PDF 口令加密方式的加密字典主要条目定义见表 7。

表 7 基于口令加密的加密字典的部分条目

键	类型	值
Filter	name	Filter 条目定义了 PDF 文档进行基于口令加解密操作的安全处理程序名称。如果 SubFilter 不存在，在打开文档时仅应使用此安全处理程序。如果 SubFilter 存在，可以使用实现了 SubFilter 指定的安全处理程序
SubFilter	name	SubFilter 条目定义了 PDF 文档可以使用 Filter 条目定义以外的安全处理程序来进行基于口令的加解密。如果 SubFilter 存在，则使用实现了 SubFilter 指定的安全处理程序
V	number	该值指定在加密和解密文档过程中使用的算法，考虑到 1～5 在 PDF 标准中已被使用，使用 SM4 密码算法时，该 V 值为 90，使用 CF、StmF、StrF 条目指定规则
CF	dictionary	指向 Crypt 过滤器字典
StmF	name	对 PDF 文档中 stream 流数据处理时所使用的 Crypt 过滤器的名称
StrF	name	对 PDF 文档中字符串数据处理时所使用的 Crypt 过滤器的名称
R	number	一个数字，指定应使用安全处理程序的哪个修订版来解释此字典。 使用 SM4 算法时 R 值为 90

其他条目定义见 GB/T 32010.1—2015 的 7.6 中表 20 和表 21 的定义。

支持 SM4 密码算法的加密处理程序由开发者定义。

8.2.3 基于口令的加解密过程

基于口令的 PDF 加密方法，见 GM/T 0091 中基于口令的密钥派生方法。

加密算法使用 SM4 密码算法 CBC 模式，算法过程符合 GB/T 32907。

具体过程见 GB/T 32010.1—2015 的 7.6.3。

8.3 基于数字证书的 PDF 加密

8.3.1 概述

PDF 文档可以使用公钥加密技术来加密文档中的字符串和流。通过指定一个或多个接收者列表，每个列表具有自己的唯一访问权限，只有指定的接收者才可以打开加密的文档或内容。

基于数字证书的 PDF 加密机制是通过调用公钥安全处理程序(Public-Key Security Handlers)实现，使用支持 SM2 密码算法的 GB/T 35275 中数字信封消息语法来编码接收者列表、加密密钥和访问

权限信息。

8.3.2 公钥加密字典

公钥安全处理程序定义的公钥加密字典见表8。

表8 公钥安全处理程序的加密字典部分条目

键	类型	值
Filter	name	Filter条目应是公钥安全处理程序的名称。 如果SubFilter不存在,在打开文档时仅应使用此安全处理程序。如果SubFilter存在,可以使用实现了SubFilter指定的安全处理程序
SubFilter	name	SubFilter条目定义了PDF文档可以使用Filter条目定义以外的安全处理程序来加解密。如果SubFilter存在,则使用实现了SubFilter指定的安全处理程序
P	integer	一个标志集,指定在打开文档时允许用户执行哪些用户操作。位2设置为1,具体含义见GB/T 32010.1—2015中7.6的表24

其他条目定义见GB/T 32010.1—2015中7.6的表20和表23的定义。

支持SM2数字证书的PDF加密,由开发者自行定义公钥安全处理程序,Filter名称宜为GM.PubSec。如果采用SubFilter并使用Crypt过滤器,则SubFilter名称宜为GM.sm2cms.s5,可以包含CF、stmF和StrF条目,接收者列表与访问权限在Crypt过滤器中指定,Crypt过滤器字典定义见GB/T 32010.1—2015的7.6.5。

8.3.3 公钥加解密过程

利用证书加解密PDF文档的处理流程,采用数字信封方式。

对需保护的PDF文档数据内容用对称密钥(即数据加密密钥)加密,加密算法采用SM4算法CBC模式。同时,对该数据加密密钥用接收者的证书进行保护。形成的数字信封,格式符合GB/T 35275的数字信封envelopedData类型语法规范。

每个接收者的证书,格式应符合GB/T 20518。

加解密过程见GB/T 32010.1—2015的7.6.4。