ICS 35.040
L 80
备案号:44632—2014

GM

中华人民共和国密码行业标准

GM/T 0031—2014

安全电子签章密码技术规范

Secure electronic seal cryptography technical specification

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　　发布

中华人民共和国密码
行业标准
安全电子签章密码技术规范
GM/T 0031—2014
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 0.75 字数 16 千字
2014年4月第一版 2014年4月第一次印刷
*
书号:155066·2-27012 定价 14.00 元

GM/T 0031-2014

目　　次

前言 …… Ⅰ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　电子签章的密码应用安全机制 …… 2
6　电子签章密码应用协议 …… 2
6.1　电子印章 …… 2
6.1.1　数据格式 …… 2
6.1.2　电子印章验证流程 …… 5
6.2　电子签章 …… 5
6.2.1　数据格式 …… 5
6.2.2　电子签章生成流程 …… 6
6.2.3　电子签章验证流程 …… 6

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由密码行业标准化技术委员会提出并归口。

本标准主要起草单位：北京数字认证股份有限公司、上海市数字证书认证中心有限公司、卫士通信息产业股份有限公司、兴唐通信科技股份有限公司、北京海泰方圆科技有限公司、上海格尔软件股份有限公司、吉大正元信息技术股份有限公司、上海颐东网络信息有限公司。

本标准主要起草人：刘平、马臣云、冯承勇、李述胜、程小茁、刘伟、傅大鹏、刘承、李元正、李玉峰、柳增寿、谭武征、李伟平、蒋健等。

安全电子签章密码技术规范

1 范围

本标准规定了电子印章和电子签章的数据结构、密码处理流程。

本标准适用于电子印章系统的开发和使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

GM/T 0003 SM3 密码杂凑算法

GM/T 0006 密码应用标识规范

GM/T 0009 SM2 密码算法使用规范

PKCS#1：RSA Cryptography Standard

3 术语和定义

下列术语和定义适用于本文件。

3.1

电子印章 electronic stamp

一种由制作者签名的包括持有者信息和图形化内容的数据，可用于签署电子文件。

3.2

电子签章 electronic seal

使用电子印章签署电子文件的过程。

3.3

电子签章数据 electronic seal data

电子签章过程产生的包含电子印章信息和签名信息的数据。

3.4

电子印章系统 electronic seal system

包含电子印章管理系统和电子签章软件，其中电子印章管理系统包括印章管理员管理、电子印章制作与管理、电子印章验证服务以及安全审计等功能。电子签章软件是使用电子印章对各类电子文档进行电子签章的软件。

3.5

制章人 electronic stamp maker

电子印章系统中具有签署和管理电子印章信息权限的管理员。管理员可以是单位证书或个人证书，电子印章中的图片和信息必须经制章人的数字证书进行数字签名。

3.6

签章人 electronic seal signer

电子印章系统中对文档进行签章操作的最终用户。

3.7

SM2 算法　SM2 algorithm

一种椭圆曲线公钥密码算法，其密钥长度为 256 比特。

3.8

SM3 算法　SM3 algorithm

一种密码杂凑算法，其输出为 256 比特。

4　缩略语

下列缩略语适用于本文件。

BMP　位图(Bitmap)

GIF　图像交换格式(Graphics Interchange Format)

JPG　联合图像专家组(Joint Photographic Experts Group)

OID　对象标识符(Object Identifier)

PKI　公钥基础设施(Public Key Infrastructure)

5　电子签章的密码应用安全机制

电子签章是将传统印章与电子签名技术进行结合，通过采用组件技术、PKI 技术、图像处理技术以及密码技术，按照公钥密码技术标准体系，以电子形式对电子文档进行数字签名及签章，以确保文档来源的真实性以及文档的完整性，防止对文档未经授权的篡改，并确保签章行为的不可否认性。

为了确保电子印章的完整性、不可伪造性，以及合法用户才能使用，需要定义一个安全的电子印章数据格式。可以通过数字签名，将印章图像数据与签章使用者以及印章属性进行安全绑定，形成安全电子印章，在使用印章过程中，也能够很方便地对电子印章进行安全性验证。

在使用电子印章对各种文档进行电子签章过程中，签章人通过数字签名对文档数据进行签章处理，从而达到与传统纸质文件盖章操作相同的可视化效果，同时又利用数字签名技术保障了文档数据的真实性、完整性以及签章人行为的不可否认性。

6　电子签章密码应用协议

6.1　电子印章

6.1.1　数据格式

电子印章数据的逻辑结构如图 1 所示。

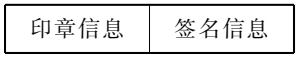

图 1　电子印章数据的逻辑结构

电子印章数据的 ASN.1 定义为：

```
SESeal::= SEQUENCE{
    esealInfo       SES_SealInfo,          --印章信息
    signInfo        SES_SignInfo           --制章人对印章签名的信息
}
```

6.1.1.1 印章信息

印章信息的结构如图 2 所示。

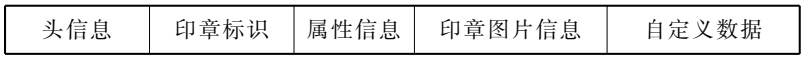

图 2 印章信息结构图

印章信息的 ASN.1 定义为：

```
SES_SealInfo::= SEQUENCE{
    header          SES_Header,             --头信息
    esID            IA5String,              --电子印章标识,电子印章数据的唯一标识编码
    property        SES_ESPropertyInfo,     --印章属性信息
    picture         SES_ESPictrueInfo,      --电子印章图片数据
    extDatas        EXPLICIT ExtensionDatas OPTIONAL    --自定义数据
}
```

其中：

esID：区分电子印章数据的唯一标识编码，用于查找和索引其他信息；

extDatas：用于厂商使用自定义数据。

```
ExtensionDatas ::= SEQUENCE SIZE (0..MAX) OF ExtData
ExtData ::= SEQUENCE {
    extnID OBJECT IDENTIFIER,           --自定义扩展字段标识
    critical BOOLEAN DEFAULT FALSE,     --自定义扩展字段是否关键
    extnValue OCTET STRING              --自定义扩展字段数据值
}
```

a) 印章头信息：

印章头信息的结构如图 3 所示。

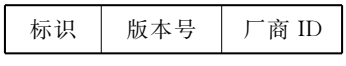

图 3 电子印章头信息

头信息的 ASN.1 定义为：

```
SES_Header::= SEQUENCE{
    ID          IA5String,          --电子印章数据标识
    version     INTEGER,            --电子印章数据版本号标识
    Vid         IA5String           --电子印章厂商 ID
}
```

其中：

ID：固定值“ES”；

Version：电子印章数据版本号，如“11”；

Vid：电子印章厂商 ID，在互联互通时，用于识别不同的软件厂商实现。

b) 印章属性信息：

印章属性信息的结构如图 4 所示。

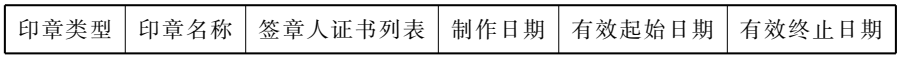

图 4 印章属性信息结构

印章属性信息的 ASN.1 定义为：

```
SES_ESPropertyInfo::= SEQUENCE{
    type              INTEGER,              --印章类型
    name              UTF8String,           --印章名称
    certList          SEQUENCE OF cert,     --签章人证书列表
    createDate        UTCTIME,              --印章制作日期
    validStart        UTCTIME ,             --印章有效起始日期
    validEnd          UTCTIME               --印章有效终止日期
}
certID::= IA5String
```

其中：

type：代表印章类型，如 1 为单位印章，2 为个人印章；

name：印章的助记名称，如个人章、公章、财务章；

certList：可使用印章进行签章的签章人证书列表；

createDate：印章制作日期；

validStart：印章有效期起始时间；

validEnd：印章有效期终止时间。

c) 印章图片信息：

印章图片信息的结构如图 5 所示。

图片类型	图片数据	图片显示的宽度和高度

图 5 印章图片信息结构

印章图片信息的 ASN.1 定义为：

```
SES_ESPictrueInfo::= SEQUENCE{
    type          IA5String,            --图片类型
    data          OCTET STRING,         --图片数据
    width         INTEGER,              --图片显示宽度
    height        INTEGER               --图片显示高度
}
```

其中：

type：代表印章图片类型，如 GIF、BMP、JPG；

data：印章图片数据；

width：图片显示宽度，单位为毫米(mm)；

height：图片显示高度，单位为毫米(mm)。

6.1.1.2 印章签名信息

印章签名信息的结构如图 6 所示。

制章人证书	签名算法标识	签名值

图 6 印章签名信息结构

印章签名信息的 ASN.1 定义为：

```
SES_SignInfo::= SEQUENCE{
    cert                    OCTET STRING,              --制章人签名证书
    signatureAlgorithm      OBJECT IDENTIFIER,         --签名算法标识
    signData                BIT STRING                 --制章人的签名值
```

}

其中：

cert：代表对电子印章数据进行签名的制章人证书；

signatureAlgorithm：代表签名算法 OID 标识，遵循 GM/T 0006。例如，使用 SM2 签名的 OID 为 1.2.156.10197.1.501；

signData：代表制章人对电子印章格式中印章信息 SES_SealInfo、制章人证书、签名算法标识按 SEQUENCE 方式组成的信息内容的数字签名。

如果签名算法使用 SM2，则遵循 GM/T 0009；如果签名算法使用 RSA，则遵循 PKCS#1。

6.1.2 电子印章验证流程

电子印章验证流程如下：

a) 验证电子印章数据格式的合规性：
   按照电子印章格式，解析电子印章，验证是否是符合规范的电子印章格式；
   如果电子印章数据格式不合规，则验证失败，返回失败原因并退出验证流程。

b) 验证电子印章签名值是否正确：
   根据印章信息数据、制章人证书、签名算法标识验证电子印章签名信息中的签名值是否正确；
   如果电子印章签名验证失败，返回失败原因并退出验证流程。

c) 验证电子印章制章人证书的有效性：
   验证制章人证书的有效性，验证项至少包括：制章人证书信任链验证、制章人证书有效期验证、制章人证书是否被吊销、密钥用法是否正确；
   如果制章人证书验证失败，返回失败原因并退出验证流程。

d) 验证电子印章的有效期：
   根据印章属性中的印章有效起始日期和有效终止日期，验证电子印章的是否过期；
   如果电子印章已过期，则验证失败，返回失败原因并退出验证流程；

e) 如果上述步骤都验证成功，则电子印章验证合规有效，可正常退出验证流程。

6.2 电子签章

6.2.1 数据格式

电子签章数据由版本号、电子印章、时间信息、原文杂凑值、原文属性信息、证书标识、签名算法标识及签名值等组成。

电子签章数据的逻辑结构如图 7 所示。

版本号	电子印章	时间信息	原文杂凑值	原文属性信息	签章人数字证书	签名算法标识	签名值

图 7 电子签章数据的逻辑结构

电子签章数据的 ASN.1 定义为：

```
SES_Signature::= SEQUENCE{
    toSign                  TBS_Sign,           --待电子签章数据
    signature               BIT STRING          --电子签章中签名值
}

TBS_Sign::= SEQUENCE{
    version                 INTEGER,            --版本信息
    eseal                   SESeal,             --电子印章
```

```
    timeInfo                TIME,               --签章时间信息
    dataHash                BIT STRING,         --原文杂凑值
    propertyInfo            IA5String,          --原文数据的属性信息
    cert                    OCTET STRING,       --签章人对应的签名证书
    signatureAlgorithm      OBJECT IDENTIFIER   --签名算法标识
}
```

其中：

version：代表签章数据结构版本号；

eseal：代表生成电子签章使用的电子印章数据；

timeInfo：代表电子签章对应的时间信息，可以是时间戳，也可以是 UTCTIME 时间；

dataHash：代表待签名原文的杂凑值；

propertyInfo：代表原文数据的属性信息，如文档 ID、日期、段落、原文内容的字节数、指示信息、签章保护范围等，此部分受签名保护，propertyInfo 的具体含义可自行定义；

cert：代表执行本次签章操作的签章人数字证书；

signatureAlgorithm：代表签名算法 OID，遵循 GM/T 0006。例如，使用 SM2 签名的 OID 为 1.2.156.10197.1.501；

signature：代表签章人对电子签章数据格式中版本号、电子印章、时间信息、原文杂凑值、原文属性信息、证书、签名算法标识组成的待签章数据 TBS_Sign 进行数字签名。

如果签名算法使用 SM2，则遵循 GM/T 0009；如果签名算法使用 RSA，则遵循 PKCS＃1。

原文杂凑值所采用的杂凑算法应与电子签章签名算法保持一致，如果签名算法是 SM2，则杂凑算法应采用 SM3 算法，遵循 GM/T 0003；如果签名算法是 RSA，则杂凑算法应采用 SHA1 或 SHA256 算法，具体参见相应的国际标准。

6.2.2 电子签章生成流程

电子签章生成流程如下：

a) 选择拟进行电子签章的签章人证书，并验证签章人证书有效性：
   验证签章人证书有效性，验证项至少包括：证书信任链验证、证书有效期验证、证书是否被吊销、密钥用法是否正确。如果签章人证书验证失败，返回失败原因并退出生成流程。

b) 获取电子印章，按照 6.1.2 验证印章的合规性和有效性。

c) 获取电子印章中的签章人证书列表，使用步骤 a)中的签章人证书逐一进行证书数据二进制比对，确认签章人证书是否在签章人证书列表中。
   如果比对失败或证书不在列表当中，返回失败原因并退出生成流程。
   如果是因为签章人证书执行更新、重签发等操作而导致证书比对失败，此时需要重新制作印章，再重新进行签章生成流程。

d) 按照 propertyInfo 信息中的签名保护范围获取待签名原文。

e) 将待签名原文数据进行杂凑运算，形成原文杂凑值。

f) 按照电子签章数据格式组装待签名数据：
   待签名数据包括：版本号、电子印章、时间信息、原文杂凑值、原文属性信息、签章人证书、签名算法标识。

g) 签章人对待签名数据进行数字签名，生成电子签章签名值。

h) 按照电子签章数据格式，把以上数据打包形成电子签章数据。

6.2.3 电子签章验证流程

电子签章验证流程如下：

a) 验证电子签章数据格式的合规性：

根据电子签章格式规范解析电子签章数据。如果电子签章或电子印章数据格式不合规，则验证失败并退出验证流程。

b) 验证电子签章签名值是否正确：

从电子签章数据格式获取待验证数据，待验证数据包括：版本号、电子印章、时间信息、原文杂凑值、原文属性信息、签章人证书、签名算法标识，验证电子签章签名值的是否正确。

如果签名值验证不正确则验证失败，并将失败原因返回上层应用并退出验证流程。

c) 验证签章人数字证书有效性：

从电子签章数据获得签章人数字证书，验证签章人证书有效性，验证项至少包括：证书信任链验证、证书有效期验证、证书是否被吊销、密钥用法是否正确。

如果是由于证书信任链验证或密钥用法不正确导致的签章人证书有效性验证失败，则返回失败原因并退出验证流程。

如果是由于证书有效期或证书状态已吊销导致的签章人证书有效性验证失败，则还需要进一步结合签章时间进行综合判定。

d) 验证签章的时间有效性：

根据签章人数字证书有效期和电子签章中的时间信息进行比对，判断签章的时间有效性：

1) 如果签章时间处于签章人数字证书有效期内，并且证书有效，则需要继续进一步验证。
2) 如果签章时间不在签章人数字证书有效期内，则签章无效，验证失败，返回失败原因并退出验证流程。
3) 如果签章时间处于签章人数字证书有效期内，但是证书在签章之前已被吊销，则签章视为无效，验证失败，返回失败原因并退出验证流程。
4) 如果签章时间处于签章人数字证书有效期内，但是证书在签章之后被吊销，则需要继续进一步验证。

e) 验证原文杂凑：

1) 按照 propertyInfo 信息中的签名保护范围获取待验证原文；
2) 将待验证原文数据进行杂凑运算，形成待验证原文杂凑值；
3) 获取电子签章数据中的原文杂凑值，与待验证原文杂凑值进行二进制比对，如果比对失败，则电子签章验证失败，返回失败原因并退出验证流程。

f) 验证电子印章的有效性：

首先，获取电子印章，按照 6.1.2 验证印章的有效性。再根据电子签章中的时间信息验证签章的有效性。

如果签章时间不处于印章有效期内，则签章无效，验证失败，返回失败原因并退出验证流程。

g) 如果上述各步骤验证均有效，那么电子签章验证结果为有效，可正常退出验证流程。