ICS 35.040
L80

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX—XXXX

信息安全技术 安全电子签章密码技术规范

Information security technology-Secure electronic seal cryptography technical specification

（报批稿）

在提交反馈意见时，请将您知道的相关专利连同支持文件一并附上

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

本标准依据 GB/T 1.1—2009《标准化工作导则　第 1 部分：标准的结构和编写》给出的规则起草。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准起草单位：北京数字认证股份有限公司、中安网脉（北京）技术股份有限公司、兴唐通信科技有限公司、上海格尔软件股份有限公司、长春吉大正元信息技术股份有限公司、卫士通信息产业股份有限公司、北京海泰方圆科技股份有限公司、北京三未信安科技发展有限公司、上海市数字证书认证中心有限公司、上海颐东网络信息有限公司。

本标准主要起草人：傅大鹏、刘岩、谢峰、徐惠清、朱亚飞、王天顺、张金铭、陈中林、郑强、赵丽丽、罗俊、蒋红宇、高志权、许永欣、韩玮、夏东山、王文昌、张妍、陈景燕等。

信息安全技术 安全电子签章密码技术规范

1 范围

本标准规定了采用密码技术实现安全电子印章和安全电子签章的数据结构定义，以及相应的生成与验证流程。

本标准适用于电子印章系统的开发和使用，也可用于指导该类系统的检测。

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。

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 32905 信息安全技术 SM3密码杂凑算法

GB/T 32918 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 33560 信息安全技术 密码应用标识规范

GB/T 35276 信息安全技术 SM2密码算法使用规范

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 seal

一种由电子印章制作者数字签名的安全数据，包括电子印章所有者信息和图形化内容的数据，用于安全签署电子文件。

3.2

电子签章 electronic seal signature

一种通过图像处理在数据上加盖电子印章并进行数字签名技术形成的安全数据，实现与纸质文件盖章操作相同的可视效果，可保障数据来源的真实性、数据完整性以及签名人行为的不可否认性。

3.3

原文 original data

需要进行电子签章处理的原始文件。

3.4

电子签章数据 electronic seal signature data

电子签章过程产生的包含电子印章和数字签名等信息的数据。

3.5

电子印章系统 electronic seal system

电子印章系统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。

3.6

制章者 electronic seal maker

制章者即电子印章系统中具有电子印章制作和管理权限的机构。制章者证书应是该机构的单位证书，电子印章中的图像和相关信息应经制章者进行数字签名。

3.7

签章者 electronic seal signer

签章者即电子印章的所有者，是具备电子印章法定使用权限的实体。

3.8

SM2密码算法SM2 algorithm

由GB/T 32918定义的一种椭圆曲线密码算法。

3.9

SM3 算法 SM3 algorithm

由GB/T 32905定义的一种杂凑算法。

4 符号和缩略语

下列缩略语适用于本文件。

ASN.1：抽象语法记法（Abstract Syntax Notation One）

BMP：位图（Bitmap）

DER：非典型编码规则（Distinguished Encoding Rules）

GIF：图形交换格式（Graphics Interchange Format）

JPG：联合图像专家组的文件格式（Joint Photographic Experts Group）

OID：对象标识符（Object Identifier）

PKI：公钥基础设施（Public Key Infrastructure）

SVG：可缩放的矢量图形（Scalable Vector Graphics）

5 概述

安全电子签章是通过采用PKI公钥密码技术，将数字图像处理技术与电子签名技术进行结合，以电子形式对加盖印章图像数据的电子文档进行数字签名，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。通过数字签名，将印章图像数据与签章使用者等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，签章者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、完整性以及签章者行为的不可否认性。

6 电子印章

6.1 数据格式

电子印章的数据结构如图 1 所示：

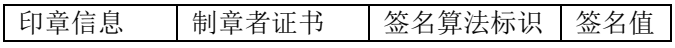

图 1 电子印章的数据结构示意图

电子印章数据的 ASN.1 定义为：

```
SESeal::=SEQUENCE{
    eSealInfo     SES_SealInfo,  --印章信息
    cert    OCTET STRING,          --制章者证书
    signAlgID    OBJECT IDENTIFIER,  --签名算法标识
    signedValue     BIT STRING    --制章者对印章信息域的签名值
    }
```

上述电子印章数据结构由 eSealInfo、cert、signAlgID、signedValue 四个域构成：

a）eSealInfo 是印章信息，是电子印章基本域。

b）cert 是制章者的 X.509 证书，建议按 DER 编码格式存放。

c）signAlgID 是制章者对 eSealInfo 域进行数字签名所使用的签名算法标识。

d）signedValue 域包含了制章者对 eSealInfo 域进行数字签名的结果。

6.1.1 印章信息

印章信息域 eSealInfo 结构如图 2 所示：

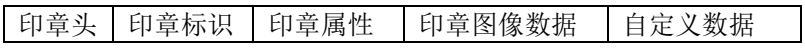

图 2 印章信息的数据结构示意图

印章信息 eSealInfo 的 ASN.1 定义如下：

```
SES_SealInfo::= SEQUENCE{
    header     SES_Header,                    --印章头
    esID       IA5String,                     --电子印章标识，电子印章的唯一标识编码
    property    SES_ESPropertyInfo,           --印章属性
```

```
    picture     SES_ESPictrueInfo,              --电子印章图像数据,机构的电子印章宜采用相关国
                                                家管理部门指定的印章印模
    extDatas    ExtensionDatas OPTIONAL         --自定义数据
}
```

eSealInfo 域是电子印章基本域，包含了印章头、印章标识、印章属性、电子印章图像数据、自定义数据等基本信息。

6.1.1.1 印章头

印章头的结构如图 3 所示：

标识	版本号	厂商 ID

图 3 电子印章头示意图

印章头的 ASN.1 定义为：

```
SES_Header::=SEQUENCE{
    ID  IA5String,      --电子印章标识
    version INTEGER,    --电子印章版本号标识
    Vid IA5String       --电子印章厂商 ID
}
```

其中：

ID ：固定值“ES”；

version ：电子印章数据结构版本号， 本标准设定数值为 3，代表当前版本为 4；

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；

6.1.1.2 印章标识

esID：区分电子印章的唯一标识编码，用于查找和索引其它信息。

6.1.1.3 印章属性

印章属性的结构如图 4 所示：

印章类型	印章名称	签章者证书列表类型	签章者证书列表数据	制作日期	有效起始日期	有效终止日期

图 4 印章属性的数据结构示意图

印章属性的 ASN.1 定义为：

```
SES_ESPropertyInfo::=SEQUENCE{
    type        INTEGER,            --印章类型
    name    UTF8String,             --印章名称
    certListType    INTEGER,        --签章者证书列表类型
    certList    SES_CertList,   --签章者证书列表数据,是签章者证书列表或签章者证书杂凑值列
    表
    createDate  GeneralizedTime,    --印章制作日期
```

```
    validStart   GeneralizedTime,   --印章有效起始日期
    validEnd     GeneralizedTime        --印章有效终止日期
}
```

其中：

type ：代表印章类型，可根据业务需要自定义；

name ：印章名称，如“XXXX 公司财务专用章”，对于在公安部门进行备案的印章，其印章名称与备案的名称保持一致；

certListType ：签章者证书列表类型，1-证书列表，2-证书杂凑值列表

certList ：签章者证书列表数据，签章者证书列表或签章者证书杂凑值列表；

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

```
SES_CertList::= CHOICE {
  certs CertInfoList,            -- 签章者证书
  certDigestList CertDigestList  --签章者证书杂凑
}

CertInfoList:: = SEQUENCE OF Cert
certDigestList = SEQUENCE OF CertDigestObj

Cert::= OCTET STRING
```

Cert 符合 GB/T 20518 中 Certificate 定义，建议按 DER 编码格式存放。

```
CertDigestObj ::= SEQUENCE {
  type ObjType,          --自定义类型
  value CertDigestValue  --证书杂凑值
}
ObjType ::= PrintableString
CertDigestValue::= OCTET STRING
```

6.1.1.4 印章图像数据

印章图像数据的结构如图 5 所示：

图像类型	图像数据	图像显示的宽度和高度

图 5 印章图像数据结构示意图

印章图像数据的 ASN.1 定义为：

```
SES_ESPictrueInfo::=SEQUENCE{
    type    IA5String,      --图像类型
    data    OCTET STRING,   --图像数据
    width   INTEGER,    --图像显示宽度
```

```
    height  INTEGER --图像显示高度
}
```

其中：

type ：代表印章图像类型，如 GIF、BMP、JPG、SVG 等

data ：印章图像数据

width ：图像显示宽度（单位为毫米 mm）

height ：图像显示高度（单位为毫米 mm）

6.1.1.5 自定义数据

自定义数据的ASN.1定义为：

```
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
}
```

6.1.2 制章者证书

cert ：代表对电子印章进行签名的制章者证书，符合 GB/T 20518 中 Certificate 定义，建议按 DER 编码格式存放。

6.1.3 签名算法标识

signAlID ：代表签名算法OID标识，遵循 GB/T 33560。

例如，基于SM2算法和SM3算法的签名OID为1.2.156.10197.1.501。

6.1.4 签名值

signedValue ：代表制章者对电子印章格式中印章信息域 SES_SealInfo，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GB/T 35276。

6.2 电子印章生成流程

电子印章生成流程如下：

a) 按 6.1.1 定义的数据格式，将印章头、印章标识、印章属性、印章图像、自定义数据等数据按 SEQUENCE 方式组成印章信息域；

b) 根据签名算法标识 signAlgID，对上述步骤 a)的印章信息域进行数字签名运算，形成印章的签名值；

c) 将上述步骤 a）和 b）的数据以及制章者证书、signAlgID 组包形成安全的电子印章。

6.3 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正确性

按照电子印章格式，解析电子印章，验证是否符合本标准 6.1 定义的电子印章格式。
如果电子印章数据格式不正确，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
根据印章信息域 eSealInfo、制章者证书、签名算法标识来验证电子印章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) 验证电子印章制章者证书的有效性
验证制章者证书的有效性，验证项至少包括：制章者证书信任链验证、制章者证书有效期验证、制章者证书是否被撤销、密钥用法是否正确。
如果制章者证书验证失败，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，则电子印章验证正确有效，可正常退出验证流程。

7 电子签章

7.1 数据格式

电子签章数据由、签章者证书、签名算法标识及签名值等组成。
电子签章的数据结构如图6所示：

待电子签章数据	签章者数字证书	签名算法标识	签名值	时间戳

图 6 电子签章的数据结构示意图

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
    cert    OCTET STRING,   --签章者数字证书
    signatureAlgID OBJECT IDENTIFIER,   --签名算法标识
    signature   BIT STRING,     --电子签章中签名值
    timeStamp [0] BIT STRING  OPTIONAL  --对签名值的时间戳
}
```

待电子签章的数据，由版本号、电子印章、签章时间、原文杂凑值、原文属性、自定义数据等组成，结构如图7所示：

版本号	电子印章	签章时间	原文杂凑值	原文属性	自定义数据

图 6 待电子签章的数据结构示意图

```
TBS_Sign::=SEQUENCE{
    version INTEGER,                --电子签章的版本，本标准设定数值为 3,代表当前版本为 4;
    eseal    SESeal,                    --电子印章
    timeInfo    GeneralizedTime,        --签章时间
    dataHash    BIT STRING,             --原文杂凑值
```

```
    propertyInfo    IA5String,                --原文数据的属性
    extDatas [0] ExtensionDatas OPTIONAL    --自定义数据
}
```

其中：

version	：签章数据格式版本号，该版本号与电子印章版本号保持一致；
eseal	：生成电子签章使用的电子印章；
timeInfo	：电子签章对应的时间，可以是GeneralizedTime时间；
dataHash	：待签名原文的杂凑值；
propertyInfo	：原文数据的属性，如文档 ID、日期、段落、原文内容的字节数、指示信息、签名保护范围等，此部分受签名保护，propertyInfo 的具体结构可自行定义，但至少应包含签名保护范围；
extDatas	：厂商自定义数据；
cert	：执行本次签章操作的签章者数字证书，符合 GB/T 20518,建议按 DER 编码格式存放；
signatureAlgID	：签名算法 OID，遵循 GB/T 33560； 例如，使用 SM2 签名的 OID 为 1.2.156.10197.1.501；
signature	：签章者对电子签章数据格式中版本号、电子印章、签章时间、原文杂凑值、原文属性、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 GB/T 35276；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 GB/T 32905。

timeStamp ：（可选）如果采用时间戳，应遵循 GB/T 20520，时间戳格式按 DER 编码存放。

7.2 电子签章生成流程

电子签章生成流程如下：

a) 为验证电子印章的正确性和有效性，准备电子印章，具体步骤如下：

1）选择拟进行电子签章的签章者证书，并验证签章者证书有效性。验证项至少包括：证书信任链、证书有效期验证、证书是否被撤销、密钥用法是否正确；

2）获取电子印章，按照 6.3 电子印章验证流程验证印章的正确性和有效性；

3）根据电子印章中的签章者证书列表类型，如果是证书列表，则比对证书；如果是杂凑，则比对杂凑。提取电子印章中的签章者证书列表，使用步骤 1）中的签章者证书逐一进行证书数据二进制比对，按下述方式确认签章者证书是否在签章者证书列表中：

- 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；
- 如果是因为签章者证书执行更新、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。

b) 对原文进行电子签章

1）按照 propertyInfo 中的签名保护范围来准备待签名原文；

2）将待签名原文数据进行杂凑运算，形成原文杂凑值；

3）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、签章时间、原文杂凑值、原文属性、自定义数据；

4）签章者对待签名数据进行数字签名，生成电子签章签名值；

5）如果电子签章需要加盖时间戳，则将前述电子签章签名值用来产生相应的时间戳；

6）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。

7.3 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正确性

1）根据 7.1 数据格式来解析电子签章数据；

2）按照 6.3 流程来验证上述电子签章中的电子印章的正确性；

3）如果电子签章或电子印章数据格式不正确，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

1）从电子签章数据格式提取待验证数据，待验证数据包括：版本号、电子印章、签章时间、原文杂凑值、原文属性、自定义数据等，验证电子签章签名值是否正确；

2）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) 验证签章者证书是否存在于签章者列表中

1）从电子签章数据中提取签章者数字证书和电子印章，并从中提取签章者证书列表类型、签章者证书列表数据；

2）根据上述签章者证书列表类型，如果是类型是证书列表，则比对证书。将电子印章中签章者证书列表与电子签章签章者数字证书逐一进行证书数据二进制比对,确认签章者证书是否存在于签章者证书列表中，若不存在，则验证失败并退出验证流程；

3）根据上述签章者证书列表类型，如果是杂凑，则比对杂凑。将电子签章中签章者数字证书进行杂凑，再与电子印章中签章者证书列表杂凑值逐一进行比对，确认签章者证书是否存在于签章者证书列表中，若不存在，则验证失败并退出验证流程。

d) 验证签章者数字证书有效性

1) 从电子签章数据获得签章者数字证书，验证签章者证书有效性，验证项至少包括：证书信任链验证、证书有效期验证、证书是否被撤销、密钥用法是否正确；

2) 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者证书有效性验证失败，则返回失败原因并退出验证流程；

3) 如果是由于证书有效期或证书状态已撤销导致的签章者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。

e) 验证签章的时间有效性

根据签章者数字证书有效期和电子签章中的签章时间进行比对，判断签章的时间有效性：

1）如果签章时间处于签章者数字证书有效期内，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者数字证书有效期内，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者数字证书有效期内，但是证书在签章之前已被撤销，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者数字证书有效期内，但是证书在签章之后被撤销，则需要继续后续步骤验证；

5）如果电子签章中包含时间戳，首先验证时间戳的有效性，并比对签章时间不能晚于时间戳中的时间。

f）验证原文杂凑

1）从电子签章数据中提取 propertyInfo 数据，从 propertyInfo 中提取签名保护范围提取待验证原文；

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）从电子签章数据中提取原文杂凑值，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。

g）验证电子印章的有效性

1）从电子签章数据中提取电子印章，按照 6.3 电子印章验证流程验证印章的有效性。再根据电子签章中的签章时间验证签章的有效性：

2）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。

h）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。