人力资源社会保障电子印章 印章技术规范（试行）

1 范围

本标准规定了人力资源社会保障电子印章的数据格式和电子印章的验证流程。

本标准适用于人力资源社会保障电子印章系统的建设、使用和各地区人力资源社会保障电子印章系统的接入。

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 32905 信息安全技术 SM3 密码杂凑算法

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 33481 党政机关电子印章应用规范

GB/T 33560 信息安全技术 密码应用标识规范

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 35276 信息安全技术 SM2 密码算法使用规范

GM/T 0015-2012 基于SM2 密码算法的数字证书格式规范

GB/T 38540-2020 信息安全技术 安全电子签章密码技术规范

ZWFW C 0119-2018 国家政务服务平台统一电子印章 签章技术要求

ZWFW C 0120-2018 国家政务服务平台统一电子印章 印章技术要求

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

一种以电子签名数据为表现形式的印章，可用于签署电子文件，其内容包括电子印章印文图像数据、印章信息和信任凭证。

3.2 电子印章系统 electronic seal system

支持电子印章制作、管理、使用、验证等过程的系统。

3.3 电子印章标识 electronic seal identification

由电子印章系统签发的用于识别电子印章的标识编码，是区分电子印章数据的唯一标识编码，用于查找和索引其它信息以及电子文档的数字签名、验签等。

3.4 电子印章所有者 electronic seal signer

具备电子印章法定使用权限的主体。

3.5 SM2 算法 SM2 cryptographic algorithm

由GB/T 32918(所有部分) 定义的一种算法。

3.6 SM3 算法 SM3 cryptographic algorithm

由GB/T 32905 定义的一种算法。

4 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 一种图像交换格式 (Graphics Interchange Format)

JPG 一种图像文件格式 (Joint Photographic Experts Group)

OID 对象标识符 (Object Identifier)

PKI 公钥基础设施 (Public Key Infrastructure)

PNG 便携式网络图像格式 (Portable Networks Graphics)

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

5 概述

人力资源社会保障电子印章系统的电子签章是采用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，以印章外观模拟方式对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，应定义一个安全的电子印章数据格式。通过数字签名，将印章图像数据与电子印章所有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，也可对电子印章进行安全性验证。

人力资源社会保障电子印章系统中数字签名算法为SM2，密码杂凑算法为SM3。

6 电子印章数据格式

6.1 数据结构

电子印章的数据结构见图1。

印章信息	制章系统证书	签名算法标识	签名值

图1 电子印章的数据结构

电子印章数据的ASN.1 定义为：

```
SESeal::=SEQUENCE{
    eSealInfo           SES_SealInfo,           -- 印章信息
```

```
    cert            OCTET STRING,          -- 制章系统证书
    signAlgID       OBJECT IDENTIFIER,     -- 签名算法标识
    signedValue     BIT STRING             -- 制章系统对印章信息域的签名值
}
```

其中：

eSealInfo：　印章信息，是电子印章基本域；

cert：　制章系统的X.509 证书，宜使用DER 编码格式；

signAlgID：　制章系统对eSealInfo 域进行数字签名所使用的签名算法标识；

signedValue　制章系统对eSealInfo 域进行数字签名的结果。

6.2　印章信息

6.2.1　印章信息域结构

印章信息域eSealInfo 是电子印章基本域，包含了印章头、电子印章标识、印章属性、印章图像数据、自定义数据等基本信息，eSealInfo 结构见图2 。

印章头	电子印章标识	印章属性	印章图像数据	自定义数据

图2　印章信息域结构

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国
                                               家有关管理部门指定的印章印模
    extDatas    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，由电子印章所有者的统一社会信用代码+3 位顺序号组成；例如，人力资源和社会保障部信息中心的第一个电子印章，esID 表示为‘‘12100000717825712K001’’，其中‘‘121000007178257l2K’’为人力资源和社会保障部信息中心的统一社会信用代码；‘001’’为顺序号。

6.2.2　印章头

印章头的结构见图3 。

标识	版本号	厂商ID

图3　印章头结构

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，由2 位序号组成，第1 位标识主版本号，第2 位标识次版本号，如‘41’’标识版本4.1，本规范中版本号统一表示为41；

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；宜用厂商域名表示。

6.2.3　印章属性

印章属性的数据结构见图 4 。

印章类型	印章名称	电子印章所有者证书列表类型	电子印章所有者证书列表数据	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

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,            -- 电子印章所有者证书列表类型
    certList        SES_CertList,       -- 电子印章所有者证书列表数据，是电子印章所有
                                           者证书列表或电子印章所有者证书杂凑值列表
    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，电子印章类型格式分为电子公章标识和电子名章标识两类，电子印章类型至少包括电子法定名称章(代码：01）、电子财务专用章(代码：02）、电子发票专用章(代码：03）、电子合同专用章（代码：04)、电子名章（代码：05 ）五类，当印章类型代码为01 、02 、03、04 时，称为电子公章标识；当印章类型代码为05 时，称为电子名章标识；

name：　　印章名称，如‘XXXX 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：　电子印章所有者证书列表类型，1- 证书列表，2- 证书杂凑值列表；

certList：　　电子印章所有者证书列表数据，电子印章所有者证书列表或电子印章所有者证书杂凑值列表，电子印章所有者数字证书即电子印章数字证书；

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。

注：电子印章含有印章有效期和电子印章所有者数字证书有效期，两者宜保持一致。

```
SES_CertList::= CHOICE {
    certs               CertInfoList,       -- 电子印章所有者证书列表
    certDigestList      CertDigestList      -- 电子印章所有者证书杂凑值列表
}
CertInfoList:: = SEQUENCE OF Cert
```

certDigestList:: = SEQUENCE OF CertDigestObj

Cert::= OCTET STRING

Cert 符合GB/T 20518 中Certificate 定义，宜使用DER 编码格式。该证书用电子印章根证书或其子证书对应的私钥签发，证书项目内容要求见附录A 。

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

6.2.4 印章图像数据

印章图像数据的结构见图 5 。

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

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、PNG 等；

data：印章图像数据，电子印章备案采用的印章图片格式为PNG8 格式，2 色，分辨率为600DPI；

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）。

6.2.5 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
}
```

自定义数据包括如下内容：

a) 印章制作单位信息

印章制作单位信息（sealMakingUnitInfo）用于标识电子印章的印章制作单位。该数据项应为字符型，长度不大于200 个字节，单位信息格式为‘‘统一社会信用代码+ 名称’’。其ASN.1 的结构如下：

Id-sealMakingUnitInfo OBJECT IDENTIFIER ::= {1.2.156.112600.7.1}

sealMakingUnitInfo::= OCTET STRING

b) 印章使用单位_ 单位少数民族文字名称

印章使用单位_ 单位少数民族文字名称（sealHoldingUnit_EthnicMinoritiesName）用于印章使用单位的单位少数名族名称。其ASN.1 的结构如下：

Id-sealHoldingUnitEthnicMinoritiesName OBJECT IDENTIFIER ::= {1.2.156.112600.7.2}

sealHoldingUnitEthnicMinoritiesName::= OCTET STRING

c) 印章使用单位_ 单位英文名称

印章使用单位_ 单位英文名称（sealHoldingUnit_EnglishName）用于印章使用单位的单位英文名称。其ASN.1 的结构如下：

Id-sealHoldingUnitEnglishName OBJECT IDENTIFIER ::= {1.2.156.112600.7.3}

sealHoldingUnitEnglishName::= OCTET STRING

6.3 制章系统证书

cert：对电子印章进行签名的制章系统证书，符合 GB/T 20518 中 Certificate 定义，宜按DER 编码格式存放。

6.4 签名算法标识

signAlgID：签名算法OID 标识，遵循 GB/T 33560，基于SM2 算法和SM3 算法的签名OID 为 1.2.156.10197.1.501 。

6.5 签名值

signedValue：代表制章系统对电子印章格式中印章信息SES_SealInfo 按SEQUENCE 方式组成的信息内容的数字签名。

签名算法使用SM2，遵循GB/T 35275 和GB/T 35276，杂凑算法使用SM3 算法，遵循GB/T 32905 。

7 电子印章生成流程

电子印章生成流程见图6 。

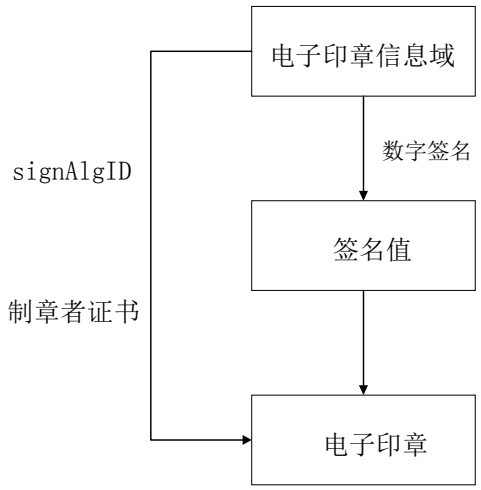

图6　电子印章生成流程

电子印章生成流程如下：

a) 人社行业内机构的电子印章以及需要跨行业互认互信的电子印章，在制作印章之前需向上级部门申请赋码；如果不需要跨行业互认互信的，可以不需要申请，赋码留空。

b) 按6.2 定义的电子印章数据格式，将电子印章头、电子印章标识、电子印章属性、电子印章图像数据、自定义数据等数据按SEQUENCE 方式组成电子印章信息域。

c) 根据签名算法标识signAlgID，对上述步骤b）的电子印章信息域进行数字签名运算，形成印章的签名值。

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

8　电子印章验证流程

电子印章验证流程见图7 。

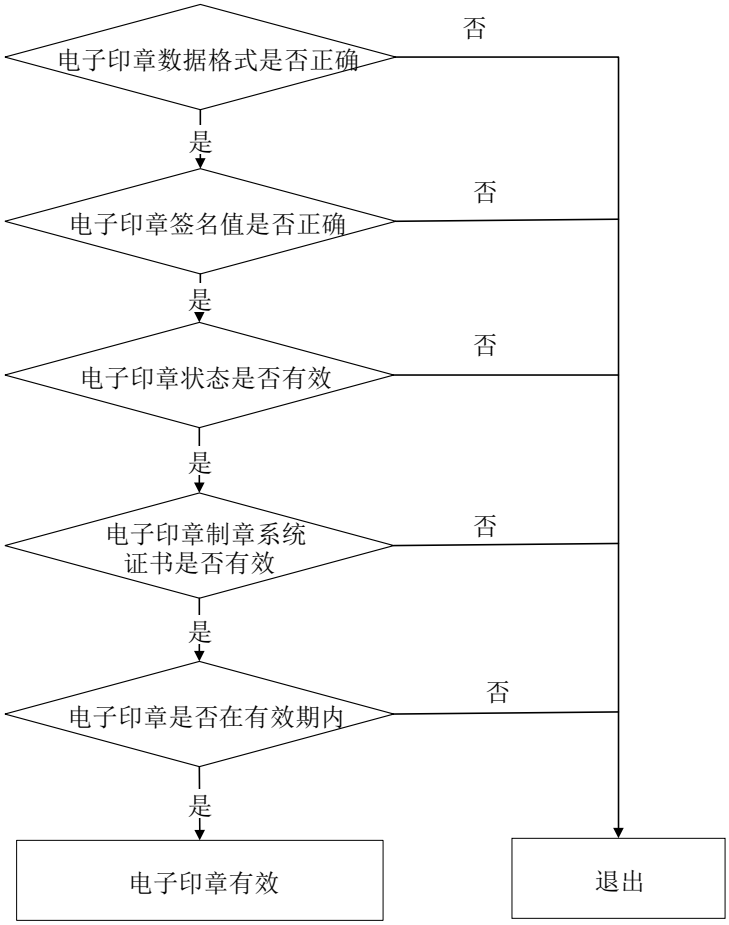

图7　电子印章验证流程

电子印章验证按如下步骤依次进行：

a) 验证电子印章数据格式是否正确。

按照电子印章数据格式，解析电子印章，验证是否符合第6 章定义的电子印章数据格式；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 、制章系统证书、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；如果电子印章签名值不正确，则验证失败，返回失败原因并退出验证流程。

c) 验证电子印章状态的有效性。

在联网条件下，可访问统一电子印章系统，在线查验电子印章的有效性；在没有联网条件下，也可通过电子印章吊销列表查询印章是否被吊销；如果电子印章无效，则验证失败，返回失败原因并退出验证流程。

d) 验证电子印章制章系统证书的有效性。

验证制章系统证书的有效性，验证项至少包括：制章系统证书信任链、制章系统证书有效期、密钥用法是否正确；如果制章系统证书验证失败，返回失败原因并退出验证流程。

e) 验证电子印章是否在有效期内。

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。

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。

附　录A
（规范性附录）
证书内容规范

A.1　电子印章根证书内容规范

表A.1 给出了电子印章业务系统中电子印章根证书的各项内容。

表A.1　电子印章根证书数据项

域	关键项标识	值	描述
Certificate			
Signature			
AlgorithmIdentifier			必须与 signatureAlgorithm 域匹配
algorithm		1.2.156.10197.1.501	SM3WithSM2Encryption
tbsCertificates			待签名内容
version		2	整数 2 用于版本 3
serialNumber		INTEGER	唯一正整数，由根 CA 设置
issuer			与根 CA 保持一致
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue			UTF8String
validity			
NotBefore			
Time			
utcTime		YYMMDDHHMMSSZ	用于2049 之前的年份（含2049）
generalTime		YYYYMMDDHHMMSSZ	用于 2049 之后的年份
NotAfter			
Time			
utcTime		YYMMDDHHMMSSZ	用于 2049 之前的年份（含2049）
generalTime		YYYYMMDDHHMMSSZ	用于 2049 之后的年份
subject			国家：CN
			组织：印章 CA 证书的持有机构对应的统一社会信用代码，18 个字节
			名称：印章 CA 证书的名称，不大于20 个字节
			x500UniqueIdentifier：电子政务电子认证服务机构编码+ 两个数字，电子政务电子认证服务机构编码为A001~A999 或

域	关键项标识	值	描述
			B001~B999，该编码之外的 CA 机构采用 G001~G999。两个数字为 01~99，该数字表示相同认证服务机构下不同根的编号，例如：A00101。该 object 对应 OID 为 2.5.4.45, 详见 RFC 2256 《A Summary of theX.500(96) User Schema for usewith LDAPv3》5.46 分节
Name			
RDNSequence			
relativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttrubuteValue			UTF8String
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			
algorithm		1.2.156.10197.1.301	SM2 椭圆曲线公钥密码算法
parameters		ecPublicKey	SM2 算法曲线的 OID（1.2.840.10045.2.1）
subjectPublicKey		BIT STRING	SM2 算法公钥长度至少为 256 位
必须的扩展项			
authorityKeyIdenitfier	FALSE		签发者密钥标识符
keyIdentifier		OCTET STRING	签发者公钥值的 SHA-1 摘要值
authorityCertSerialNumber		CertificateSerial Number::= INTEGER	颁发者证书序列号
subjectKeyIdenitfier	FALSE		主题密钥标识符用于证书路径查询
keyIdentifier			主题公钥值的 SHA-1 摘要值
basicConstraints	TRUE		
CA		TRUE	
pathLenConstraint			设置为 0，0 值表明在路径中只可以向终端实体签发证书
KeyUsage	TRUE		
KeyCertSign			
CRLSign			
CRLDistributionPoints			
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			

域	关键项标识	值	描述
GeneralNames			
GeneralName			
uniformResourceIdentifier			采用‘http://’形式
authorityInfoAccess	TRUE		
AccessDescription			
accessMethod		Id-ad-ocsp(1.3.6.1.5.5. 7.48.1)	
accessLocation			
GeneralName			
uniformResourceIdentifier			采用‘http://’形式

A.2 电子印章证书内容规范

表A.2 给出了电子印章业务系统中电子印章证书的各项内容

表A.2 电子印章证书数据项

域	关键项标识	值	描述
Certificate			
Signature			
AlgorithmIdentifier			必须与 signatureAlgorithm 域匹配
algorithm		1.2.156.10197.1.501	SM3WithSM2Encryption
parameters		NULL	当算法为 SM2 时，不需要此项
tbsCertificates			待签名内容
version		2	整数 2 用于版本 3
serialNumber		INTEGER	唯一正整数，由根 CA 设置
issuer			与根 CA 保持一致
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue			UTF8String
validity			
NotBefore			
Time			
utcTime		YYMMDDHHMMSSZ	用于 2049 之前的年份（含 2049）
generalTime		YYYYMMDDHHMMSSZ	用于 2049 之后的年份
NotAfter			
Time			

域	关键项标识	值	描述
utcTime		YYMMDDHHMMSSZ	用于 2049 之前的年份（含 2049）
generalTime		YYYYMMDDHHMMSSZ	用于 2049 之后的年份
subject			国家：CN
			组织：电子印章标识持有者对应的‘‘统一社会信用代码+ 单位名称’ 组成
			名称：省市区(6 个字节) + 印章赋码 (8 个字节)
Name			
RDNSequence			
relativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttrubuteValue			UTF8String
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			
algorithm		1.2.156.10197.1.301	SM2 椭圆曲线公钥密码算法
parameters		ecPublicKey	SM2 算法曲线的 OID (1.2.840.10045.2.1)
subjectPublicKey		BIT STRING	SM2 算法公钥长度至少为 256 位
必须的扩展项			
authorityKeyIdenitfier	FALSE		签发者密钥标识符
keyIdentifier		OCTET STRING	签发者公钥值的 SHA-1 摘要值
authorityCertSerialNumber		CertificateSerial Number::= INTEGER	颁发者证书序列号
subjectKeyIdenitfier	FALSE		主题密钥标识符用于证书路径查询
keyIdentifier		OCTET STRING	主题公钥值的 SHA-1 摘要值
KeyUsage	TRUE		
digitalSignature			
nonRepudiation			
CRLDistributionPoints			
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
uniformResourceIdentifier			采用‘http://’’形式

域	关键项标识	值	描述
authorityInfoAccess	FALSE		
AccessDescription			
accessMethod		Id-ad-ocsp(1.3.6.1.5.5. 7.48.1)	
accessLocation			
GeneralName			
uniformResourceIdentifier			采用‘http://’形式