人力资源社会保障电子印章 签章技术规范（试行）

1. 范围

本标准规定了人力资源社会保障电子签章的数据格式、生成流程和验证流程。

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 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(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 33476.3-2016 党政机关电子公文格式规范 第3 部分：实施指南

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

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 电子印章签章 stamp with electronic seal

使用电子印章签署电子文件的过程，也称为电子签章或电子印章盖章。

3.3 电子印章验章 verify stamp of electronic seal

对电子印章签章结果进行验证的过程，也称为电子签章验证。

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信息和签名信息的数据。

3.5 电子印章所有者 owner of electronic seal

具备电子印章法定使用权限的主体。

3.6 SM2 算法 SM2 cryptographic algorithm

由GB/T 32918(所有部分)定义的一种算法。

3.7 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）
DER　非典型编码规则（Distinguished Encoding Rules）
OID　对象标识符（Object Identifier）
PKI　公钥基础设施（Public Key Infrastructure）

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。

在使用电子印章对各种文档进行电子签章过程中，电子印章所有者通过电子印章对文档数据进行签章处理，可视化效果与传统纸质盖章方式相同，同时用数字签名保障了文档数据的真实性、完整性以及电子印章所有者行为的不可否认性。

人力资源社会保障电子印章系统中数字签名算法为SM2，杂凑算法为SM3。

6. 电子签章数据格式

电子签章数据由待电子签章数据、电子印章所有者数字证书、签名算法标识、签名值和时间戳(可选)组成，其数据结构见图1。

待电子签章数据	电子印章所有者数字证书	签名算法标识	签名值	时间戳

图1　电子签章数据结构

```
SES_Signature::=SEQUENCE{
    toSign                  TBS_Sign,               -- 待电子签章数据
    cert                    OCTET STRING,           -- 电子印章所有者数字证书
    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
}
```

其中：

toSign：　需要进行签章的电子印章原文相关数据；

cert：　执行本次签章操作的电子印章所有者数字证书，宜使用DER 编码格式；

signatureAlgID：　签名算法OID，遵循GB/T 33560；SM2 算法对应的OID 为1.2.156.10197.1.501；

signature：　电子印章所有者对“待签章数据（toSign）”进行数字签名其中签名算法使用SM2，遵循GB/T 35276；原文杂凑值所采用的杂凑算法为SM3 算法，遵循GB/T 32905；

timeStamp ：　（可选）对 “签名值（signature）”计算的时间戳，遵循GB/T 20520，使用DER 编码格式。

待电子签章数据由版本号、电子印章、签章时间、原文杂凑值、原文属性和自定义数据组成，其数据结构见图2 。

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2　待电子签章数据结构

待电子签章数据的ASN.1 定义为：

```
TBS_Sign::=SEQUENCE{
    version         INTEGER，                       -- 电子签章的版本
    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：　电子印章数据版本号，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 ；

eseal：　生成电子签章使用的电子印章；

timeInfo：　电子签章对应的时间，类型为GeneralizedTime ；

dataHash：　待签章原文的杂凑值；

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。

7. 电子印章签章流程

电子印章签章流程见图3 。

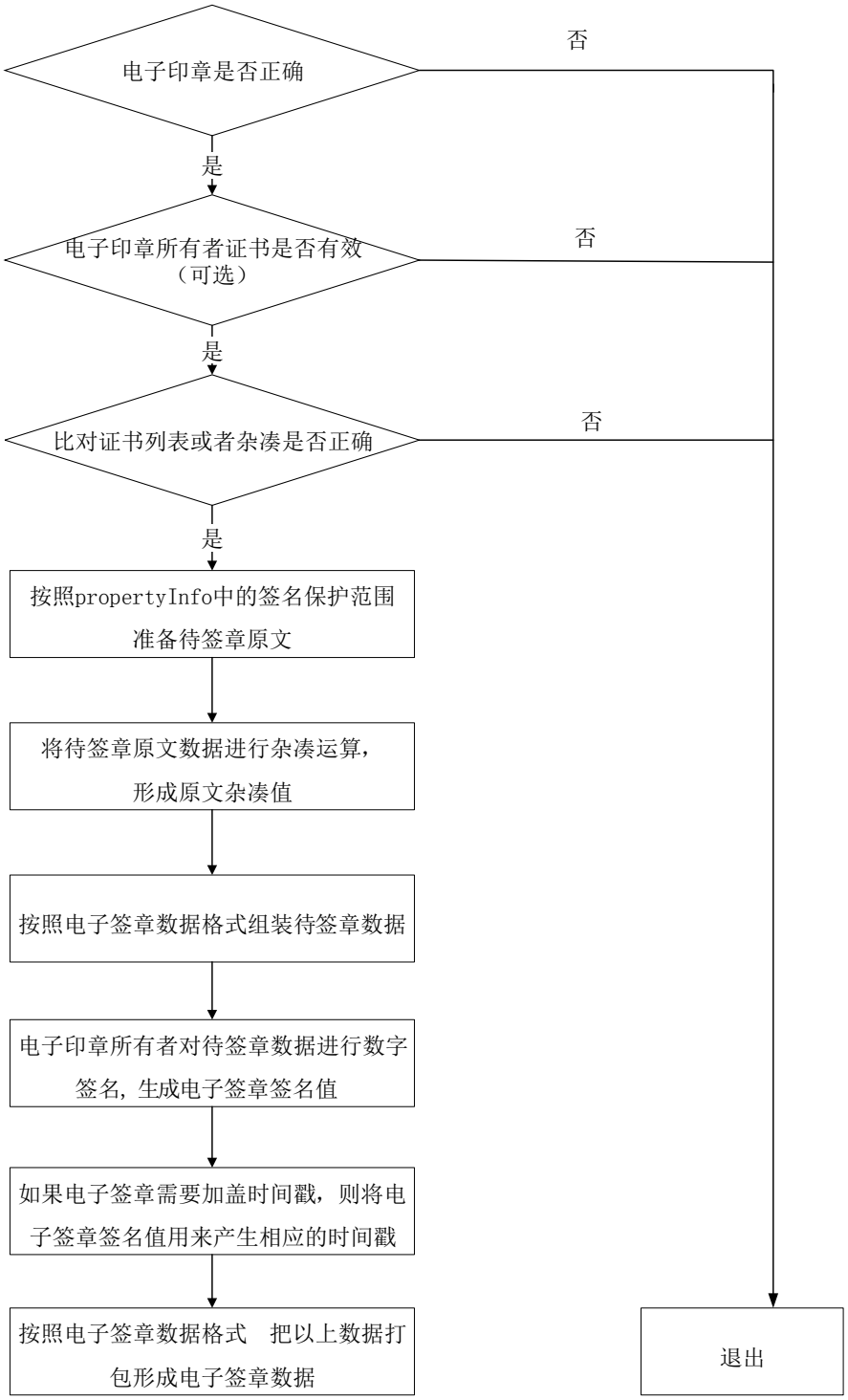

图3　电子印章签章流程

电子印章签章流程如下：

a） 准备电子印章，验证电子印章的正确性和有效性。

1） 选择拟进行电子签章的电子印章，按照《印章技术规范》中电子印章验证流程验证印章的正确性和有效性；

2) 选择拟进行电子签章的电子印章所有者证书，可验证电子印章所有者证书有效性。验证项至少包括：证书信任链、证书有效期、密钥用法是否正确；

3) 根据电子印章中的电子印章所有者证书列表类型，如果是证书列表，则比对证书；如果是证书杂凑值列表，则比对证书杂凑值。提取电子印章中的电子印章所有者证书列表，使用步骤b ）中的电子印章所有者证书逐一进行证书数据二进制比对，确认电子印章所有者证书是否在电子印章所有者证书列表中。

——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；

——如果是因为电子印章所有者证书执行更新、重签发等操作而导致证书比对失败，则需要重新制作印章，再重新进行签章生成流程。

b) 对原文进行电子签章

1) 按propertyInfo 中的签名保护范围准备待签章原文；

2) 对待签章原文进行杂凑运算，形成原文杂凑值；

3) 按照电子签章数据格式组装待签章数据。待签章数据包括：版本号、电子印章、签章时间、原文杂凑值、原文属性、电子印章所有者数字证书、签名算法标识；

4) 电子印章所有者对待签章数据进行数字签名，生成电子签章签名值；

5) 如果电子签章需要加盖时间戳，则利用前述电子签章签名值计算产生相应的时间戳；

6) 按电子签章数据格式，把以上数据组装为电子签章数据。

签章数据在OFD 版式文件中的使用见GB/T 33476.3-2016 。

8. 电子印章验章流程

电子印章验章流程见图4 。

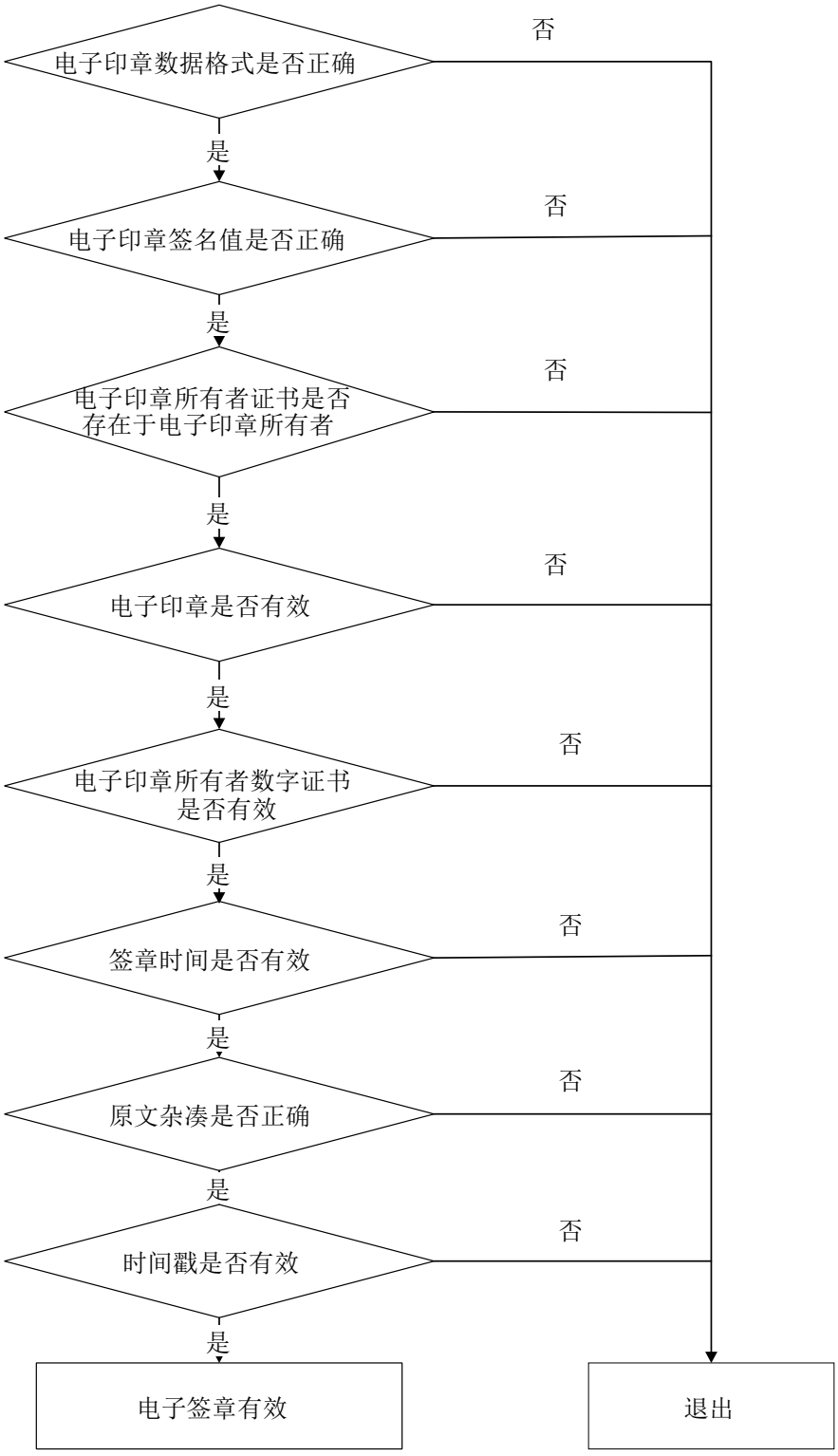
电子印章数据格式是否正确
否
是
电子印章签名值是否正确
否
是
电子印章所有者证书是否
存在于电子印章所有者
否
是
电子印章是否有效
否
是
电子印章所有者数字证书
是否有效
否
是
签章时间是否有效
否
是
原文杂凑是否正确
否
是
时间戳是否有效
否
是
电子签章有效
退出

图4　电子印章验章流程

电子印章验章流程如下：

a) 验证电子签章数据格式的正确性

1) 根据第6 章电子签章数据格式解析电子签章数据；

2) 按照《印章技术规范》第6 章电子印章数据格式解析上述电子签章中的电子印章数据；

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、电子印章所有者数字证书、签名算法标识，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，返回失败原因并退出验证流程。

c) 验证电子印章所有者证书是否存在于电子印章所有者列表中

1) 从电子签章数据中提取电子印章所有者数字证书和电子印章，并从电子印章中提取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；

2) 根据上述电子印章所有者证书列表类型，如果类型是证书列表，则比对证书。将电子印章中电子印章所有者证书列表与电子签章中电子印章所有者数字证书逐一进行证书数据二进制比对，确认电子印章所有者证书是否存在于电子印章所有者证书列表中，若不存在，则验证失败，返回失败原因并退出验证流程；

3) 根据上述电子印章所有者证书列表类型，如果类型是证书杂凑值列表，则比对杂凑值。将电子签章中电子印章所有者数字证书进行杂凑，再与电子印章中电子印章所有者证书杂凑值列表逐一进行比对，确认电子印章所有者证书是否存在于电子印章所有者证书列表中，若不存在，则验证失败，返回失败原因并退出验证流程。

d) 验证电子印章的有效性

1) 从电子签章数据中提取电子印章，按照《印章技术规范》第 8 章中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时间标记验证签章的有效性；

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。

e) 验证电子印章所有者数字证书有效性

1) 从电子签章数据获得电子印章所有者数字证书，验证电子印章所有者证书有效性，验证项至少包括：证书信任链、证书有效期、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电子印章所有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导致的电子印章所有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。

f) 验证签章时间有效性

1) 根据电子印章所有者数字证书有效期和电子签章中的时间标记进行比对，判断签章时间有性；

2) 如果签章时间处于电子印章所有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；

3) 如果签章时间不在电子印章所有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；

4) 如果签章时间处于电子印章所有者数字证书有效期内，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；

5) 如果签章时间处于电子印章所有者数字证书有效期内，但是证书在签章之后被吊销，则需要继续后续步骤验证；

6) 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。

g）验证原文杂凑

1 ）从电子签章数据中提取propertyInfo 数据，按照propertyInfo 提取签名保护范围内的待验证原文；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。 **h）验证时间戳有效性**

如果存在时间戳，则需要对时间戳有效性和时间戳时间的有效性进行验证。

1) 首先，调用时间戳服务进行时间戳有效性验证，如果验证失败，返回失败原因并退出验证流程；

2) 如果验证通过，则解析时间戳获取签发时间，对签发时间的有效性进行验证，具体的验证流程同步骤f)。

i）如果上述各步骤验证均有效，那么电子印章验章结果为有效，可正常退出验证流程。