**电子保函电子签名（签章）**

**签名与验证规则**

**2023年7月**

**一、目标读者**

电子签名（签章）开发人员。

**二、签名节点格式**

主要目录结构顺序为：

/Root /AcroForm /Fields /Annot为Annot节点；

/Root /AcroForm /Fields /Annot/Sig为盖章信息节点，/Sig节点为引用节点；

/Root /AcroForm /Fields /Annot/Sig/Contents为关键的签名值节点，/Sig/EP\_M存在且为1时采用国密V4；

**三、PDF验签**

**3.1、国密V4结构验签**

电子签章数据的ASN.1结构的数据内容保存在/Root /AcroForm /Fields /Annot /Sig /Contents 节点中。

签名数据保护范围保存在/Root /AcroForm /Fields /Annot /Sig /ByteRange节点中。

格式按照《[GB/T 38540-2020 信息安全技术 安全电子签章密码 技术规范](http://www.banshujiang.cn/e_books/2366)》。



**3.2、验签步骤**

1. 首先从pdf中把签章结构获取到，签章结构在

/Root /AcroForm /Fields /Annot/Sig/Contents节点中，如下所示。

|  |
| --- |
| /Root: -> Dictionary of type: /Catalog  /AcroForm:Dictionary  /Fields:Array  /Annot  /Sig  /Contents: |

签章结构需要按照V4结构解析。V4结构的描述请参考《[GB/T 38540-2020 信息安全技术安全电子签章密码 技术规范](http://www.banshujiang.cn/e_books/2366)》

**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)若解析失败，则返回错误代码并退出验证流程。

3)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。

4)如果电子签章或电子印章数据格式不正确，则返回错误代码并退出验证流程。

b)验证电子签章签名值是否正确

1)根据步骤a)解析所得的签章信息、签章者证书和签名算法标识，验证电子签章签名值。

2)如果签名值验证失败，则返回错误代码并退出验证流程。

c)验证签章者证书与电子印章的匹配性

1)提取电子印章中的签章者证书信息类型与签章者证书信息列表。

2)如果上述签章者证书信息类型值为1,则需要比对数字证书。将步骤a)解析所得的签章者证书与电子印章中签章者证书信息列表内的证书逐一作二进制比对，若均比对失败，则返回错误代码并退出验证流程。

3)如果上述签章者证书信息类型值为2,则需要比对证书的杂凑值。先计算步骤a)解析所得的签章者证书的杂凑值，再与电子印章中签章者证书信息列表内的杂凑值逐一作比对，若均比对失败，则返回错误代码并退出验证流程。

d)验证电子印章的有效性

1)从签章信息中提取电子印章，按照6.3电子印章验证流程验证印章的有效性，若验证失败，需结合签章信息中的签章时间综合判断。

2)若电子印章失效因制章者证书失效导致，且在签章时间点上制章者证书也是无效的，则应记录为提示信息。

3)若电子印章失效因过期或被撤销所导致，且在签章时间不在电子印章有效期内，或当时电子印章不在正常状态，则返回错误代码并退出验证流程。

4)验证签章时刻，电子印章是否处于正常状态，如不处于正常状态，则返回错误代码并退出验证流程。

e)验证签章者证书有效性

1)从电子签章数据获得签章者证书，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)若签章者证书有效性验证失败且是由于证书信任链验证或密钥用法不正确导致的，则返回错误代码并退出验证流程。

3)若签章者证书有效性验证失败且是由于证书过期或证书状态已撤销导致的，则按步骤f)进一步判断。

f)验证签章时间的有效性

1)比对签章者证书有效期和签章时间，如果签章时间不在签章者证书有效期内，则签章无效，验证失败，返回错误代码并退出验证流程。

2)如果签章时间处于签章者证书有效期内，则检查对应的撤销列表，如果证书在签章时间处于失效状态，则签章无效，验证失败，返回错误代码并退出验证流程。

g)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，与上述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，返回错误代码并退出验证流程。

h)验证时间戳的有效性

1)如果电子签章数据中包含时间戳，则应进行时间戳的有效性验证。

2)若时间戳验证不通过，则签章无效，返回错误代码并退出验证流程。

3)比对时间戳中的时间与签章时间，若签章时间晚于时间戳中的时间，则签章无效，返回错误代码并退出验证流程。

4)按照步骤f)验证时间戳中时间的有效性，若不通过，返回错误代码并退出验证流程。

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。

**四、特殊说明**

1. 约定电子签章数据的签名数据保护范围是PDF原文（支持无序合并）。

**五、附录**

