ICS 35.240.30
L 76

中华人民共和国国家标准

GB/T 33481—2016

党政机关电子印章应用规范

Application specification for electronic seal of Party and government organs

2016-12-30 发布　　2017-07-01 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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　通用要求 …… 1
5　制章要求 …… 2
5.1　管理要求 …… 2
5.2　功能要求 …… 2
5.3　维护要求 …… 2
5.4　安全要求 …… 2
6　用章要求 …… 3
6.1　概述 …… 3
6.2　管理要求 …… 3
6.3　用章流程 …… 4
6.4　安全要求 …… 4
7　验章要求 …… 4
7.1　概述 …… 4
7.2　验证流程 …… 5
7.3　验证结果 …… 5
8　签章组件应用要求 …… 5
8.1　签章组件应用要求 …… 5
8.2　签章组件应用接口 …… 5
参考文献 …… 12

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。

本标准由中共中央办公厅、国务院办公厅提出。

本标准由国家电子文件管理部际联席会议办公室归口。

本标准起草单位：国家密码管理局、中办信息中心、中国电子技术标准化研究院、国家信息安全工程技术中心、北京电子科技学院、方正国际软件(北京)有限公司、航天福昕软件(北京)有限公司、北京数科网维技术有限责任公司、华迪计算机集团有限公司。

本标准主要起草人：高林、袁峰、李海波、张定华、胡艳晖、李平立、苗宗利、方春燕、丛培勇、陈亚军、谢永泉、冯辉、贾曙瑞、赵洪、刘贤刚、董建、王雷、王寒冰。

引　言

本标准基于《中华人民共和国电子签名法》的基本法理，定义了党政机关电子公文印章的应用要求以及申请、审批、制作和验证流程，在管理和使用流程方面参照实物公章的管理模式，加盖电子印章的电子公文与纸质公文具有同等效力。

党政机关电子印章应用规范

1 范围

本标准规定了党政机关电子公文中应用电子印章的通用要求，制章要求、用章要求、验章要求以及相关的安全要求；本标准还规定了签章组件的应用接口和相关约定。

本标准适用于非涉密的电子印章系统建设，电子印章的制作、管理、使用和验证。其他场景的电子印章系统建设可在满足行业相关要求的前提下参照执行。

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 15843.1—2008 信息技术 安全技术 实体鉴别 第1部分：概述

GB/T 16264.8—2005 信息技术开放系统互连 目录 第8部分：公钥和属性证书框架

3 术语和定义

GB/T 16264.8—2005、GB/T 15843.1—2008界定的以及下列术语和定义适用于本文件。

3.1

公钥基础设施 Public Key Infrastructure；PKI

支持公钥管理体制的基础设施，提供鉴别、加密、完整性和不可否认性服务。

[GB/T 16264.8—2005，3.3.45]

3.2

数字证书 digital certificate

用户的公钥连同其他信息，并由发布该证书的证书认证机构的私钥进行加密使其不可伪造。

3.3

数字签名 digital signature

附加在数据单元上的一些数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接受者确认数据单元的来源和完整性，并防止数据单元被人(例如接收者)伪造。

[GB/T 15843.1—2008，3.1.2]

3.4

电子印章 electronic seal

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。

3.5

电子印章系统 electronic seal system

支持电子印章制作、管理、使用和验证等过程的系统的统称。

4 通用要求

电子印章管理通用要求如下：

a) 加盖在电子公文上的电子印章应具有与实物印章一致的外观；
b) 电子印章的管理、使用方式参照实物印章管理的有关要求；
c) 电子印章的制作和验证过程应依托电子印章系统实现；
d) 电子印章系统应综合应用数字图像技术和密码技术，保证盖章后的电子公文在传递、使用过程中的真实性、完整性、不可抵赖性和可验证性；
e) 电子印章系统的运行应依托于公钥基础设施提供信任基础保障，应符合国家电子政务电子认证管理的相关要求；
f) 电子印章应存储于密钥对载体(智能密码钥匙 UKey 或系统)中，满足离线或在线用章需求；
g) 密钥对载体、电子印章和签章的数据格式应遵循国家密码局的相关规范。

5 制章要求

5.1 管理要求

制章管理应满足以下要求：
a) 电子印章的制作审批过程应参照实物印章；
b) 制章系统应参照实物印章管理方式，具有相对独立的运行环境和操作流程；
c) 制章过程中应记录申请、审批、制作、发布等信息。

5.2 功能要求

电子印章的制章功能宜包括申请、审批、制作、维护管理、状态发布 5 个部分，其中申请、审批可在电子印章系统内实现。

具体功能应满足以下要求：
a) 制章申请：制章申请信息应包括制章申请机构、电子印章内容、申请时间、电子印章使用范围、电子印章有效期、申请原因等内容。发起申请的操作员信息应同时记录。如该流程在电子印章系统内实现，应由操作员对上述信息进行数字签名；
b) 制章审批：由具有审批权限的操作员依据相关电子印章制作管理规范对制章申请信息进行审核，给出审核意见，并记录审批结果。如该过程由系统审批流程实现，应由审批员对上述信息进行数字签名；
c) 电子印章制作：由电子印章制章系统制作电子印章。电子印章由制章者私钥进行数字签名，被签名内容和电子印章结构按照国家密码局的相关要求。电子印章应存储在密钥对载体(智能密码钥匙，或是集中系统)中；
d) 电子印章发布：将电子印章及其状态信息进行公布，为验章和各种应用提供查询服务。电子印章发布内容应包括制章基础信息、电子印章状态信息和有效期，还可包括电子印章所属组织和使用范围等信息。

5.3 维护要求

电子印章维护包括查看、注销、停用、恢复和变更等功能操作，并将各种操作状态结果传递给电子印章发布系统；还包括电子印章制作的日志信息查看。集中存储时应将电子印章与部门或用户绑定。

5.4 安全要求

5.4.1 总体要求

制章安全总体要求如下：

a) 操作员进入系统时,应进行基于密码技术的身份识别和权限验证;
b) 应使用密码技术对系统中的制章数据进行防篡改保护。

5.4.2 申请要求

制章申请的安全要求如下:

a) 采用信息系统进行制章申请方式的,操作员应对申请信息做数字签名,由接收服务端进行验签;采用纸质单据进行制章申请方式的,应有操作员的签字;
b) 应记录申请信息明细。

5.4.3 审批要求

制章审批的安全要求如下:

a) 应通过密码技术确保审批信息与申请信息的一致性,其内容应与相关电子印章制作管理规范相符合;
b) 采用信息系统进行制章审批方式的,应对申请签名进行验证,对审批内容和审批意见做数字签名,由接收服务端进行验签;采用纸质单据进行制章审批方式的,应有审批者的审批意见和签字;
c) 应记录审批信息明细。

5.4.4 制作要求

电子印章制作的安全要求如下:

a) 应对电子印章审批信息进行签名验证;
b) 应对电子印章制作结果由制章服务做数字签名;
c) 制作完成的电子印章应存储在对应的密钥对载体中;
d) 应记录制作信息明细。

5.4.5 管理要求

电子印章管理的安全要求如下:

a) 对电子印章的状态信息变更结果,应由操作员进行数字签名;
b) 在发布环节中,应确保电子印章信息状态的完整性、真实性;
c) 应记录管理操作信息明细。

6 用章要求

6.1 概述

用章应包括用章申请、用章审批、用章操作;其中用章申请、用章审批可在电子印章系统内实现。

6.2 管理要求

用章管理要求如下:

a) 参照实物用章的保管和使用要求制定电子印章的用章管理办法;
b) 用章单位应指定专人保管保存电子印章的密钥对载体;
c) 应对用章申请、审批、用章过程进行记录;
d) 电子印章丢失或变更时,应及时到制章机构进行登记报备。

6.3 用章流程

用章流程应满足以下要求：

a) 用章申请：用章申请信息应包括申请人、隶属机构、申请时间、电子印章应用对象等内容。发起申请的操作员信息应同时记录。如果该过程是由用章系统申请流程实现的，应由操作员对上述信息进行数字签名，审核接收服务端进行验签；

b) 用章审核：由具有审核权限的操作员依据相关电子印章用章管理规范对电子印章申请内容进行审核，同时要核对电子印章自身的有效性，给出审核意见，应记录审核结果。如果该过程是由用章系统审核流程实现的，应由审核员对上述信息进行数字签名，由接收服务端进行验签；

c) 用章操作：审核通过后，使用用章软件和硬件对用章对象加盖电子印章。操作流程包括将电子印章放置到对象指定位置，用电子印章对应的私钥对已经含有电子印章内容的对象进行整体数字签名，并将签名结果放置到对象相应位置，形成完整的签章信息。用章时应记录用章对象、电子印章、操作者、操作者签名、用章时间等相关记录日志。

6.4 安全要求

6.4.1 用章申请安全

用章申请的安全要求如下：

a) 应对申请信息进行数字签名；

b) 应记录申请信息明细。

6.4.2 用章审批安全

用章审批的安全要求如下：

a) 应确保审批信息与申请信息的一致性；

b) 应对审批内容和审批意见进行数字签名；

c) 应记录审批信息明细。

6.4.3 公文用章安全

公文用章的安全要求如下：

a) 用章前应对已审批的电子印章、待使用的电子印章以及审批信息、待用章文件的一致性进行检查验证；

b) 应记录公文用章明细并做数字签名。

7 验章要求

7.1 概述

验章分为本地验证和在线验证两类：

a) 本地验证：用制章系统的证书验证电子印章的真实性，用电子印章的公钥验证公文文件的真实和完整性；

注：本地验证只能验证电子印章真实性，不能校验电子印章及数字证书的有效性。

b) 在线验证：在本地验证结果的基础上，通过网络查询制章发布系统，确定公文盖章时该电子印章及数字证书的有效性。

7.2 验证流程

验证流程应包括验证数字证书、电子印章真实性和有效性、验证公文真实性，并返回验证结果。

7.3 验证结果

验证结果的显示信息应包括验证方式(在线验证或本地验证)、文件的完整性、电子印章的真实性、数字证书的真实性；如果是在线验证，还应包括电子印章的有效性、数字证书的有效性。

8 签章组件应用要求

8.1 签章组件应用要求

8.1.1 函数返回值常量

函数返回值要求适用于除 8.2.13 以外的所有签章客户端接口。具体返回值定义如表 1 所示。

表 1 函数返回值说明

序号	含义	取值	备注
1	调用成功	0x00000000	常量名为 OES_OK
2	使用者主动取消	0x00000010	常量名为 OES_CANCEL
3	预留使用	0x00000000～0x00001111	错误码不得占用

8.1.2 印章图像常量

印章图像常量要求适用于 8.2.5 和 8.2.12。具体取值及含义如表 2 所示。

表 2 印章图像常量说明

序号	含义	取值	备注
1	用于显示	0x00000000	常量名为 OES_SEALIMAGE_FLAG_DISPLAY
2	用于打印	0x00000001	常量名为 OES_SEALIMAGE_FLAG_PRINT
3	用于打印预览	0x00000002	常量名为 OES_SEALIMAGE_FLAG_PREVIEW

8.1.3 接口参数约定

接口函数调用中有多个返回值的，在函数中使用字节数组和数组长度结合的方式定义，并标注[out]或[out/in]字样。当传入字节数组为空(NULL)时，由函数的实现者确定字节数组所需长度并通过数组长度返回，由函数调用者申请对应长度的空数组后再次调用获得返回值。

8.1.4 离线应用要求

带有电子签章文件的印章应随时可见，且在不联网的情况下可验章。

8.2 签章组件应用接口

8.2.1 返回组件提供者信息

功能说明：

返回签章组件提供者信息。

接口原型：

```
int OES_GetProviderInfo(unsigned char * puchName, int * piNameLen,
                unsigned char * puchCompany, int * piCompanyLen,
                unsigned char * puchVersion, int * piVersionLen,
                unsigned char * puchExtend, int * piExtendLen)
```

参数说明(8 个参数)：

参数 1:[out] puchName 名称(UTF-8 编码)；

参数 2:[out/in] piNameLen 名称长度；

参数 3:[out] puchCompany 公司名称(UTF-8 编码)；

参数 4:[out/in] piCompanyLen 公司名称长度；

参数 5:[out] puchVersion 版本(UTF-8 编码)；

参数 6:[out/in] piVersionLen 版本长度；

参数 7:[out] puchExtend 扩展信息(UTF-8 编码)；

参数 8:[out/in] piExtendLen 扩展信息长度。

返回值说明：

调用成功返回 OES_OK,否则是错误代码。

8.2.2 获取电子印章列表

功能说明：

获取电子印章列表,该函数用于进行印章名称到标识的转换。

接口原型：

```
int OES_GetSealList(unsigned char * puchSealListData,int * piSealListDataLen)
```

参数说明(2 个参数)：

参数 1:[out] puchSealListData 印章列表数据(UTF-8 编码)；

参数 2:[out/in] piSealListDataLen 印章列表数据长度。

返回值说明：

调用成功返回 OES_OK,否则是错误代码。

8.2.3 获取电子印章

功能说明：

获取指定标识的电子印章数据。

接口原型：

```
int OES_GetSeal(unsigned char * puchSealId,int iSealIdLen,
                unsigned char * puchSealData,int * piSealDataLen)
```

参数说明(3 个参数)：

参数 1:[in] puchSealId 印章标识或名称(字符串)；

参数 2:[in] iSealIdLen 印章标识或名称长度；

参数 3:[out] puchSealData 印章数据；

参数 4:[out/in] piSealDataLen 印章数据长度。

返回值说明：

调用成功返回 OES_OK,否则是错误代码。

8.2.4 获取电子印章信息

功能说明：

获取电子印章信息。

接口原型：

```
int OES_GetSealInfo(unsigned char * puchSealData,int iSealDataLen,
                    unsigned char * puchSealId,int * piSealIdLen,
                    unsigned char * puchVersion,int * piVersionLen,
                    unsigned char * puchVenderId,int * piVenderIdLen,
                    unsigned char * puchSealType,int * piSealTypeLen,
                    unsigned char * puchSealName,int * piSealNameLen,
                    unsigned char * puchCertInfo,int * piCertInfoLen,
                    unsigned char * puchValidStart,int * piValidStartLen,
                    unsigned char * puchValidEnd,int * piValidEndLen,
                    unsigned char * puchSignedDate,int * piSignedDateLen,
                    unsigned char * puchSignerName,int * piSignerNameLen,
                    unsigned char * puchSignMethod,int * piSignMethodLen)
```

参数说明(24 个参数)：

参数 1:[in] puchSealData 印章数据；

参数 2:[in] iSealDataLen 印章数据长度；

参数 3:[out] puchSealId 头信息-印章标识；

参数 4:[out/in] piSealIdLen 头信息-印章标识长度；

参数 5:[out] puchVersion 头信息-版本；

参数 6:[out/in] piVersionLen 头信息-版本长度；

参数 7:[out] puchVenderId 头信息-厂商标识；

参数 8:[out/in] piVenderIdLen 头信息-厂商标识长度；

参数 9:[out] puchSealType 印章信息-印章类型；

参数 10:[out/in] piSealTypeLen 印章信息-印章类型长度；

参数 11:[out] puchSealName 印章信息-印章名称；

参数 12:[out/in] piSealNameLen 印章信息-印章名称长度；

参数 13:[out] puchCertInfo 印章信息-证书列表信息；

参数 14:[out/in] piCertInfoLen 印章信息-证书列表信息长度；

参数 15:[out] puchValidStart 印章信息-有效起始时间；

参数 16:[out/in] piValidStartLen 印章信息-有效起始时间长度；

参数 17:[out] puchValidEnd 印章信息-有效结束时间；

参数 18:[out/in] piValidEndLen 印章信息-有效结束长度；

参数 19:[out] puchSignedDate 印章信息-制作日期；

参数 20:[out/in] piSignedDateLen 印章信息-制作日期长度；

参数 21:[out] puchSignerName 签名信息-制章人；

参数 22:[out/in] piSignerNameLen 签名信息-制章人长度；

参数 23:[out] puchSignMethod 签名信息-制章签名方法；

参数 24:[out/in] piSignMethodLen 签名信息-制章签名方法长度。

返回值说明：

调用成功返回 OES_OK,否则是错误代码。

8.2.5 获取电子印章图像

功能说明：

获取电子印章图像，该接口应在不插入智能密码钥匙时可用。

接口原型：

```
int OES_GetSealImage(unsigned char * puchSealData, int iSealDataLen,
                     int iRenderFlag,unsigned char * puchSealImage,int * piSealImageLen,
                     int * piSealWidth, int * piSealHeight)
```

参数说明(7 个参数)：

参数 1：[in] puchSealData 印章数据；

参数 2：[in] iSealDataLen 印章数据长度；

参数 3：[in] iRenderFlag 绘制用途标记；

参数 4：[out] puchSealImage 印章图像数据；

参数 5：[out/in] piSealImageLen 印章图像数据长度；

参数 6：[out/in] piSealWidth 印章宽度(单位 mm)；

参数 7：[out/in] piSealHeight 印章高度(单位 mm)。

返回值说明：

调用成功返回 OES_OK，否则是错误代码。

8.2.6 获取签名时间

功能说明：

获取签名时间(时间戳或明文形式)。

接口原型：

```
int OES_GetSignDateTime(unsigned char * puchSignDateTime,int * piSignDateTimeLen)
```

参数说明(2 个参数)：

参数 1：[out] puchSignDateTime 签名时间(字符时用 UTF-8 编码；时间戳时二进制值)；

参数 2：[out/in] piSignDateTimeLen 时间戳长度。

返回值说明：

调用成功返回 OES_OK，否则是错误代码。

8.2.7 获取签名算法标识

功能说明：

获取签名算法标识，该标识应遵循国家密码局的相关要求。

接口原型：

```
int OES_GetSignMethod(unsigned char * puchSignMethod,int * piSignMethodLen)
```

参数说明(2 个参数)：

参数 1：[out] puchSignMethod 签名算法(UTF-8 编码)；

参数 2：[out/in] piSignMethodLen 签名算法长度。

返回值说明：

调用成功返回 OES_OK，否则是错误代码。

8.2.8 获取摘要算法标识

功能说明：

获取摘要算法标识，该标识应遵循国家密码局的相关要求。

接口原型：

```
int OES_GetDigestMethod(unsigned char * puchDigestMethod,int * piDigestMethodLen)
```

参数说明(2 个参数)：

参数 1:[out] puchDigestMethod 摘要算法(UTF-8 编码)；

参数 2:[out/in] piDigestMethodLen 摘要算法长度。

返回值说明：

调用成功返回 OES_OK，否则是错误代码。

8.2.9 代理计算摘要

功能说明：

代理计算摘要。

接口原型：

```
int OES_Digest(unsigned char * puchData,int iDataLen,
               unsigned char * puchDigestMethod,int iDigestMethodLen,
               unsigned char * puchDigestValue,int * piDigestValueLen)
```

参数说明(6 个参数)：

参数 1:[in] puchData 待摘要的数据；

参数 2:[in] iDataLen 待摘要的数据长度；

参数 3:[in] puchDigestMethod 摘要算法；

参数 4:[in] iDigestMethodLen 摘要算法长度；

参数 5:[out] puchDigestValue 摘要值；

参数 6:[out/in] piDigestValueLen 摘要值长度。

返回值说明：

调用成功返回 OES_OK，否则是错误代码。

8.2.10 代理计算签名

功能说明：

代理计算签名，如果计算前需要输入密码，应由组件实现者需要提供输入界面。

接口原型：

```
int OES_Sign (unsigned char * puchSealId,int iSealIdLen,
              unsigned char * puchDocProperty,int iDocPropertyLen,
              unsigned char * puchDigestData,int iDigestDataLen,
              unsigned char * puchSignMethod,int iSignMethodLen,
              unsigned char * puchSignDateTime,int iSignDateTimeLen,
              unsigned char * puchSignValue,int * piSignValueLen)
```

参数说明(12 个参数)：

参数 1:[in] puchSealId 印章标识；

参数 2:[in] iSealIdLen 印章标识长度；

参数 3:[in] puchDocProperty 文档信息，一般为 Signature.xml 的绝对路径；

参数 4:[in] iDocPropertyLen 文档信息长度；

参数 5:[in] puchDigestData 摘要数据；

参数 6:[in] iDigestDataLen 摘要数据长度；

参数 7:[in] puchSignMethod 签名算法;
参数 8:[in] iSignMethodLen 签名算法长度;
参数 9:[in] puchSignDateTime 签名时间;
参数 10:[in] iSignDateTimeLen 签名时间长度;
参数 11:[out] puchSignValue 签名值;
参数 12:[out/in] piSignValueLen 签名值长度。

返回值说明:

调用成功返回 OES_OK,否则是错误代码。

8.2.11 代理验证签名

功能说明:

代理验证签名,离线验证时该接口应在不插入智能密码钥匙时可用。

接口原型:

```
int OES_Verify(unsigned char * puchSealData,int iSealDataLen,
               unsigned char * puchDocProperty,int iDocPropertyLen,
               unsigned char * puchDigestData,int iDigestDataLen,
               unsigned char * puchSignMethod,int iSignMethodLen,
               unsigned char * puchSignDateTime,int iSignDateTimeLen,
               unsigned char * puchSignValue,int iSignValueLen,
               int iOnline)
```

参数说明(11 个参数):

参数 1:[in] puchSealData 印章数据;
参数 2:[in] iSealDataLen 印章数据长度;
参数 3:[in] puchDocProperty 文档信息;
参数 4:[in] iDocPropertyLen 文档信息长度;
参数 5:[in] puchSignMethod 签名算法;
参数 6:[in] iSignMethodLen 签名算法长度;
参数 7:[in] puchSignDateTime 签名时间;
参数 8:[in] piSignDateTimeLen 签名时间长度;
参数 9:[in] puchSignValue 签名值;
参数 10:[in] iSignValueLen 签名值长度;
参数 11:[in] iOnline 是否在线验证。

返回值说明:

调用成功返回 OES_OK,否则是错误代码。

8.2.12 获取电子签章图像

功能说明:

获取电子签章数据中的图像及其他信息,该接口应在不插入智能密码钥匙时可用。

接口原型:

```
int OES_GetSignImage(unsigned char * puchSignedValueData,int iSignedValueLen,
               int iRenderFlag,
               unsigned char * puchSealImage, int * piSealImageLen,
               int * piSealWidth,int * piSealHeight)
```

参数说明(7 个参数):

参数 1:[in] puchSignedValueData 签章数据;

参数 2:[in] iSignedValueLen 签章数据长度;

参数 3:[in] iRenderFlag 绘制用途标记;

参数 4:[out] puchSealImage 印章图像数据;

参数 5:[out/in] piSealImageLen 印章图像数据长度;

参数 6:[out/in] piSealWidth 印章宽度(单位 mm);

参数 7:[out/in] piSealHeight 印章高度(单位 mm)。

返回值说明:

调用成功返回 OES_OK,否则是错误代码。

8.2.13 获取错误信息

功能说明:

获取错误信息。

接口原型:

```
int OES_GetErrMessage(unsigned long errCode,
                      unsigned char* puchErrMessage,int* piErrMessageLen)
```

参数说明(3 个参数):

参数 1:[in] errCode 错误代码;

参数 2:[out] puchErrMessage 错误信息(UTF-8 编码);

参数 3:[out/in] piErrMessageLen 错误信息长度。

返回值说明:

无。

参 考 文 献

[1] 中华人民共和国电子签名法