

LD

中华人民共和国劳动和劳动安全行业标准

LD/T 01.4—2022

人力资源社会保障电子印章体系 第4部分 系统接口规范

Human Resources and Social Security Electronic Seal System
Part 4: System Interface Specification

2022 - 03 - 23 发布

2022 - 06 - 01 实施

中华人民共和国人力资源和社会保障部 发布

目 次

前 言	II
引 言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	1
5 接口规范	1
5.1 接入接口规范	1
5.2 服务接口规范	2
5.3 签章应用规范	17
附录 A （资料性） 电子印章系统接入和服务接口示例	33
参 考 文 献	55

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规范》的规则起草。

LD/T 01—2022《人力资源社会保障电子印章体系》分为4个部分：

- 第1部分：总体技术架构
- 第2部分：印章技术规范
- 第3部分：签章技术规范
- 第4部分：系统接口规范

本文件是LD/T 01—2022《人力资源社会保障电子印章体系》第4部分。

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。

本文件由中华人民共和国人力资源和社会保障部信息中心提出并归口。

本文件起草单位：人力资源和社会保障部信息中心、山东省人力资源和社会保障厅网信办、江苏省人力资源和社会保障信息中心、北京信安世纪科技股份有限公司、同智伟业软件股份有限公司、江西金格科技股份有限公司、南京壹证通信息科技有限公司。

本文件主要起草人：马丹蕾、张嵩、耿建军、唐淑静、韩晓颖、王岩、叶鹏、高永昌、李德强、周海涛、秦玮、王珂、赵旺、张循。

引 言

LD/T 01—2022 《人力资源社会保障电子印章体系》分为4个部分。第4部分作为系统接口规范，规定了人力资源社会保障电子印章体系系统接口、接入接口、服务接口、签章应用规范等内容。其余部分为具体总体技术架构、印章规范、签章规范。一方面规范行业电子印章应用，并依据国务院电子政务办公室颁布的ZFW C 0118—2019、ZFW C 0119—2018、ZFW C 0120—2018、ZFW C 0121—2018和ZFW C 0122—2018标准，将行业电子印章系统接入国家政务服务平台统一电子印章平台，另一方面可为补充新标准内容预留空间，有利于对各个部分的灵活制定或修订。

人力资源社会保障电子印章体系

第4部分 系统接口规范

1 范围

本文件规定了人力资源社会保障电子印章系统相关应用服务接口。
本文件适用于人力资源社会保障电子印章系统集成设计、开发、测试及应用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GM/T 0016—2012 智能密码钥匙密码应用接口规范
GM/Z 0001—2013 密码术语
ZFW C 0122—2018 国家政务服务平台统一电子印章系统接口

3 术语和定义

GM/Z 0001—2013界定的以及下列术语和定义适用于本文件。

3.1

应用程序接口 application programming interface

应用程序接口，简称“接口”。是软件系统不同组成部分衔接的约定。

3.2

3.2 字符集 character set

多个字符的集合，字符集种类较多，每个字符集包含的字符个数不同，常见字符集名称包括ASCII字符集、GB2312字符集、BIG5字符集、GB18030字符集、Unicode字符集等。

4 缩略语

下列符号和缩略语适用于本文件。

API:应用程序编程接口 (Application Programming Interface)
ASCII:美国信息交换标准代码 (American Standard Code for Information Interchange)
BASE64:将十六进制数据转换为可见字符的编码规则
GUID:全局唯一标识符 (Globally Unique Identifier)
HTTP:超文本传输协议 (HyperText Transfer Protocol)
JSON:JavaScript对象标记或轻量级的数据交换格式 (JavaScript Object Notation)
REST:表述性状态传递 (Representational State Transfer)
URL:统一资源定位符 (Uniform Resource Locator)
USBKEY:智能密码钥匙,具有USB接口的硬件密码设备 (USB Key)

5 接口规范

5.1 接入接口规范

接入接口规范明确各省人社厅通过人社部政务服务平台电子印章系统的转发接口与国家政务服务平台电子印章系统交互完成印章备案、赋码申请、状态同步等功能的接口信息，完成基于国家政务服务平台电子印章系统规范标准的省级接入。

- a) 业务报文格式为 JSON 报文格式，其中包含 message_header 的报文体中携带相关身份识别信息
- b) 各省人社厅与其下级人社部门的接口标准，参考本文档实现，本文档未涉及的接口可自行定义。
- c) 字符集编码说明：接口中的字段全部采用 UTF-8 编码。
- d) 根据 taskCode 区分不同的业务请求。

5.2 服务接口规范

5.2.1 前置条件

接入应用需在应用安全支持平台获取到平台分配的syscode和authcode以及电子认证系统的数字证书，并且获得由电子认证系统签发的数字证书，获取到授权后才能调用电子印章服务管理系统相关电子签章接口服务，并通过电子认证系统的数字证书对收到的业务报文中签名值进行有效性验证。

5.2.2 message_header 报文参数

所有业务在进行业务接口调用时，需要在JSON报文中的message_header的报文体中携带相关身份识别信息，其参数说明如表1。报文示例见附录A中示例1。

表1 message_header 报文参数

参数名称	类型	是否必须	描述
syscode	String	是	由应用安全支持平台分配给接入应用的应用代码。
authcode	String	是	由应用安全支持平台分配给接入应用的授权码，根据策略定期更改。
businesstype	String	是	业务操作类型标识，具体详见各个接口业务标识说明。
sign	String	是	对业务报文message_content内容采用各个业务系统从应用安全支持平台获取的身份证书进行SM3WithSM2签名，签名算法oid字符串，1.2.156.10197.1.501，待签原文参数顺序根据参数名称的ASCII码表的顺序排序。如：foo=1, bar=2, foo_bar=3, foobar=4排序后的顺序是bar=2, foo=1, foo_bar=3, foobar=4。
version	String	是	版本号默认为1.0，后续升级后小版本号增加1。
ctime	String	是	应用系统的时间戳，格式为毫秒数。
random	String	是	应用系统生成的随机数信息，采用UUID去除“-”后得到的32位字符串。
hmac	String	是	根据与服务器协商的密钥，计算时间戳 随机数 系统应用代码的hmac值，密钥采用应用安全支持系统分配，算法采用sm3Hmac，字符串为Base64编码，密钥值syscode。

注：syscode为电子印章服务管理系统分配给接入应用的应用代码（即接入应用的唯一标识）、authcode是电子印章服务管理系统分配给接入应用的授权码（即应用访问电子印章接口服务的授权标识），syscode和authcode均统一由电子印章服务管理系统分配，应用在接入前应先向主管单位申请。

5.2.3 电子印章制作单位信息推送接口

5.2.3.1 功能描述

国家政务服务平台电子印章系统推送制作单位信息时需验证人社部政务服务平台身份，具体的身份认证流程见ZWF C 0122—2018中附录A，其中客户端为国家政务服务平台电子印章系统，服务端为人社部政务服务平台电子印章系统。

注：根据具体应用环境决定是否实现该接口。

5.2.3.2 前置条件

参见“5.2.1 前置条件”内容。

5.2.3.3 业务请求参数说明见表2，报文示例见附录A中示例2。

表2 业务请求参数说明

参数名称	类型	是否必须	描述
message_header			
businessstype	String	是	onlinePush: 印章单位推送。
message_content			
mspUnitNameCn	String	是	单位中文名称。
mspUnitNameEn	String	是	单位英文名称。
mspUnitNameFew	String	是	单位少数民族名称。
keyPlus	String	是	制作单位证书, 为 BASE64 编码后的证书文件。
mspSn	String	是	制作单位编号, 从 1 开始到 99999。
Operator	String	是	经办人。
operatorIdcard	String	是	经办人身份证。
mspUnitCode	String	是	制作单位统一社会信用代码。
mspUnitProvice	String	是	单位省。
mspUnitCity	String	是	单位市。
mspUnitDistrict	String	是	单位县(区)。
mspUnitAddress	String	是	单位详细地址。
mspUnitPhone	String	是	单位固定电话。
mspUnitZipcode	String	是	单位邮编。
approveUnitName	String	是	制作资格授权单位名称。
approveUnitCode	String	是	制作资格授权单位统一社会信用代码。
applyDate	String	是	申请日期。
lastCheckDate	String	是	证书失效日期。

5.2.3.4 业务返回参数说明见表 3, 报文示例见附录 A 中示例 2。

表3 业务返回参数说明

参数名称	类型	是否必须	描述
message_header			
businessstype	String	是	OnlinePush: 印章单位推送。
errorCode	String	是	错误码, 1 代表成功, 0 表示错误。
errorInfo	String	是	错误说明。
message_content			
参数名称	类型	是否必须	描述。
.....

5.2.4 电子印章信息备案获取随机数接口

5.2.4.1 功能描述

地方人社部门电子印章系统从人社部政务服务平台电子印章接入系统获取随机数信息, 并上传客户端随机数用于防重放攻击。

5.2.4.2 前置条件

服务接口安全接入条件, 地方人社部门电子印章制作系统已经向人社部政务服务平台电子印章管理系统完成注册。

5.2.4.3 业务请求参数说明见表 4, 报文示例见附录 A 中示例 3。

表4 业务请求参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	getRandom: 获取随机数。
message_content			
参数名称	类型	是否必须	描述
taskCode	String	是	命令编码 applyRandom。
version	String	是	版本号 1.0。
randomA	String	是	人社部政务服务平台电子印章制作系统产生的随机数，长度为 16 个字节。

5.2.4.4 业务返回参数说明见表 5，报文示例见附录 A 中示例 3。

表5 业务返回参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	getRandom: 获取随机数。
errorCode	String	是	错误码，1 代表成功，0 表示错误。
errorInfo	String	是	错误说明。
message_content			
参数名称	类型	是否必须	描述
randomB	String	是	国家政务服务平台电子印章系统产生随机数，长度为 16 个字节。

5.2.5 电子印章上传备案信息接口

5.2.5.1 功能描述

人社部政务服务平台电子印章系统将印章备案到国家政务服务平台电子印章系统，并上传备案信息。

5.2.5.2 前置条件

服务接口安全接入条件，人社部政务服务平台电子印章系统已经完成从国家政务服务平台电子印章系统获取随机数。

5.2.5.3 业务请求参数说明见表 6，报文示例见附录 A 中示例 4。

表6 业务请求参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businesstype	-	String	是	uploadRecordInfos: 上传备案信息。
message_content				
taskCode	-	String	是	命令编码 uploadRecordInfos。
version	-	String	是	版本号 1.0。
tokenInfo	-	String	是	客户端随机数 (randomA) 与服务端随机数 (randomB) 字符串拼接，中间无分割符号。
taskTypeCode	-	String	是	业务类型编码，0 表示备案业务，1 表示保护密钥更新业务，2 表示印章撤销，3 表示申请电子印章唯一赋码业务。
Data	sealEncCert	String	是	BASE64 编码的电子印章加密证书。
Data	sealSignCert	String	是	BASE64 编码的电子印章签名证书。
Data	sealData	String	是	电子印章的备案数据，备案的数据内容见《C0122—2018 国家政务服务平台统一电子印章 系统接口要求》附录 B.1。
Data	districtCode	String	是	行政区划代码。

表6 业务请求参数说明（续）

参数名称	参数子项	类型	是否必须	描述
signInfo (签名信息)	signAlgorithm	String	是	签名算法 oid 字符串, 1.2.156.10197.1.501。
signInfo (签名信息)	signValue	String	是	BASE64 编码的签名值, 编码前的签名值长度为 64 字节, 其中 r 和 s 分别为 32 字节。该签名值是人社部电子印章制作系统签名生成的, 各地方无需填充此参数。

5.2.5.4 业务返回参数说明见表 7, 报文示例见附录 A 中示例 4。

表7 业务返回参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businessType	-	String	是	uploadRecordInfos: 上传备案。
errorCode	-	String	是	错误码, 1 代表成功, 0 代表错误。
errorInfo	-	String	是	错误说明。
message_content				
taskTypeCode	-	String	是	业务类型编码, 0 表示备案业务, 1 表示保护密钥更新业务, 2 表示印章撤销, 3 表示申请电子印章唯一赋码业务。
data	taskId	String	是	国家政务服务平台电子印章系统返回的任务编号, 用于人社部政务服务平台电子印章系统查询任务结果时使用。
signInfo(签名信息)	signAlgorithm	String	是	签名算法 oid 字符串, 1.2.156.10197.1.501。
signInfo(签名信息)	signValue	String	是	BASE64 编码的签名值, 编码前的签名值长度为 64 字节, 其中 r 和 s 分别为 32 字节。该签名值是由国家政务服务平台电子印章系统的签名私钥进行签名生成的。

5.2.6 业务查询、下载公安部门下发数据接口

5.2.6.1 功能描述

各地人社部门电子印章系统查询并下载公安部门下发数据接口。

5.2.6.2 前置条件

参见“5.2.1 前置条件”内容。

5.2.6.3 业务请求参数说明见表 8, 报文示例见附录 A 中示例 5。

表8 业务请求参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businessType	-	String	是	checkResult: 业务查询。
message_content				
taskCode	-	String	是	命令编码 checkResult。
version	-	String	是	版本号 1.0。
taskTypeCode	-	String	是	业务类型编码, 0 表示备案业务, 1 表示保护密钥更新业务, 2 表示印章撤销, 3 表示申请电子印章唯一赋码业务。
data	taskId	String	是	国家政务服务平台电子印章系统返回的任务编号, 用于人社部政务服务平台电子印章系统查询任务结果时使用。
signInfo(签名信息)	signAlgorithm	String	是	签名算法 oid 字符串, 1.2.156.10197.1.501。
signInfo(签名信息)	signValue	String	是	BASE64 编码的签名值, 编码前的签名值长度为 64 字节, 其中 r 和 s 分别为 32 字节。该签名值是人社部电子印章制作系统签名生成的, 各地方无需填充此参数。

5.2.6.4 业务返回参数说明见表9，报文示例见附录A中示例5。

表9 业务返回参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businessType	-	String	是	checkResult: 业务查询。
errorCode	-	String	是	错误码, 1 代表成功, 0 代表错误。
errorInfo	-	String	是	错误说明。
message_content				
taskTypeCode	-	String	是	业务类型编码, 0 表示备案业务, 1 表示保护密钥更新业务, 2 表示印章撤销, 3 表示申请电子印章唯一赋码业务。
data	errorCode	String	是	每个申请包处理的返回结果, 0 是成功, 其他表示错误。
data	package	String	是	公安部门下发的数据信息。
signInfo(签名信息)	signAlgorithm	String	是	签名算法 oid 字符串, 1.2.156.10197.1.501。
signInfo(签名信息)	signValue	String	是	BASE64 编码的签名值, 编码前的签名值长度为 64 字节, 其中 r 和 s 分别为 32 字节。该签名值是由国家政务服务平台电子印章系统的签名私钥进行签名生成的。

5.2.6.5 公安部门下发数据信息见表10。

表10 公安部门下发数据信息表

编号	内容	数据项编码	类型说明	备注
1	印章编码	yzbm	String	备案信息中上传的印章编码, 为 14 个字节。
2	加密文件	encFile	String	公安部门下发的加密文件, 该文件采用 base64 编码, 使用对称加密算法模式为 sm4_ecb, 填充方式为 pkcs7, 加密文件的格式内容见《C0122—2018 国家政务服务平台统一电子印章系统接口要求》附录 B.3, 最大不大于 40K。
3	应用维护对称密钥密文	appSymKeyEnc	String	BASE64 编码的应用维护对称密钥密文, 编码前内容遵循 GM/T 0018—2012 中 ecc 加密数据结构定义, 最大为 256 字节。
4	数据加密对称密钥密文	dataSymKeyEnc	String	BASE64 编码的数据加密对称密钥密文, 编码前内容遵循 GM/T 0018—2012 中 ecc 加密数据结构定义, 最大为 256 字节。

5.2.6.6 公安部门下发加密文件数据格式

公安部门下发的加密文件数据加密前按照ASN.1格式拼接, 具体定义为:

```
GAData ::= SEQUENCE {
    deviceCode      IA5String      --设备编码
    yzmc            UTF8String    --印章名称
    yzbm            IA5String      --印章编码
    yzzzdwbm       IA5String      --印章制作单位编码
    yzlxdm          IA5String      --印章类型代码
    jbr_xm          UTF8String    --经办人姓名
    jbr_zjlx       IA5String      --经办人证件类型
    jbr_zjhm       IA5String      --经办人证件号码
    zzrq           IA5String      --制作日期
    yzsydw_dwmc    UTF8String    --印章使用单位_单位名称
    yzsydw_dwssmzwzmc UTF8String --印章使用单位_单位少数民族文字名称
    yzsydw_dwywmc  UTF8String    --印章使用单位_单位英文名称
    yzzzdwbm       UTF8String    --印章制作单位_单位名称
    yzzzdwbm       UTF8String    --印章制作单位_单位少数民族文字名称
}
```

```

        yzzzd_dwymc      UTF8String      --印章制作单位_单位英文名称
        yzsydw_tyshxydm  UTF8String      --印章使用单位_统一社会信用代码
    }

```

5.2.7 上传保护密钥更新信息接口

5.2.7.1 功能描述

当电子印章的证书更新时，人社部政务服务平台电子印章系统提交保护密钥更新信息给国家政务服务平台电子印章系统，并从国家政务服务平台电子印章系统获取任务编码，该编码用于查询更新结果并获取公安部门下发的数据。

5.2.7.2 前置条件

服务接口安全接入条件，人社部政务服务平台电子印章系统已经完成电子印章备案。

5.2.7.3 业务请求参数说明见表 11，报文示例见附录 A 中示例 6。

表11 业务请求参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businessstype	-	String	是	updateProtectKey: 保护密钥更新。
message_content				
taskCode	-	String	是	命令编码 updateProtectKey。
version	-	String	是	版本号 1.0。
tokenInfo	-	String	是	客户端随机数 (randomA) 与服务端随机数 (randomB) 字符串拼接，中间无分割符号。
taskTypeCode	-	String	是	业务类型编码，0 表示备案业务，1 表示保护密钥更新业务，2 表示印章撤销，3 表示申请电子印章唯一赋码业务。
data	yzbm	String	是	印章编码。
data	sealEncCert	String	是	BASE64 编码的电子印章加密证书。
data	sealSignCert	String	是	BASE64 编码的电子印章签名证书。
data	deviceCode	String	是	设备编码。
data	encDeviceCode	String	是	BASE64 编码的设备编码密文。
signInfo(签名信息)	signAlgorithm	String	是	签名算法 oid 字符串，1.2.156.10197.1.501。
signInfo(签名信息)	signValue	String	是	BASE64 编码的签名值，编码前的签名值长度为 64 字节，其中 r 和 s 分别为 32 字节。该签名值是人社部电子印章制作系统签名生成的，各地方无需填充此参数。

5.2.7.4 业务返回参数说明见表 12，报文示例见附录 A 中示例 6。

表12 业务返回参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businessstype	-	String	是	updateProtectKey: 保护密钥更新。
errorCode	-	String	是	错误码，1 代表成功，0 代表错误。
errorInfo	-	String	是	错误说明。
message_content				
taskCode	-	String	是	命令编码 updateProtectKey。
version	-	String	是	版本号 1.0。
resultCode	-	String	是	返回值，1 表示成功，其他表示错误。
resultCodeMsg	-	String	是	返回信息描述。
taskTypeCode	-	String	是	业务类型编码，0 表示备案业务，1 表示保护密钥更新业务，2 表示印章撤销，3 表示申请电子印章唯一赋码业务。

表12 业务返回参数说明（续）

参数名称	参数子项	类型	是否必须	描述
data	taskId	String	是	国家政务服务平台电子印章系统返回的任务编号，用于人社部政务服务平台电子印章系统查询任务结果时使用。
signInfo(签名信息)	signAlgorithm	String	是	签名算法 oid 字符串，1.2.156.10197.1.501。
signInfo(签名信息)	signValue	String	是	BASE64 编码的签名值，编码前的签名值长度为 64 字节，其中 r 和 s 分别为 32 字节。该签名值是由国家政务服务平台电子印章系统的签名私钥进行签名生成的。

5.2.8 上传电子印章撤销接口

5.2.8.1 功能描述

当电子印章撤销时，人社部政务服务平台电子印章系统提交印章撤销信息给国家政务服务平台电子印章系统，并从国家政务服务平台电子印章系统获取任务编码，该编码用于查询撤销结果并获取公安部门下发的数据。

5.2.8.2 前置条件

服务接口安全接入条件，人社部政务服务平台电子印章系统已经完成电子印章备案。

5.2.8.3 业务请求参数说明见表 13，报文示例见附录 A 中示例 7。

表13 业务请求参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businesstype	-	String	是	revocationSealInfo: 印章撤销。
errorCode	-	String	是	错误码，1 代表成功，0 代表错误。
errorInfo	-	String	是	错误说明。
message_content				
taskId	-	String	是	命令编码 revocationSealInfo。
version	-	String	是	版本号 1.0。
resultCode	-	String	是	返回值，0 表示成功，其他表示错误。
resultCodeMsg	-	String	是	返回信息描述。
taskTypeCode	-	String	是	业务类型编码，0 表示备案业务，1 表示保护密钥更新业务，2 表示印章撤销，3 表示申请电子印章唯一赋码业务。
taskId	-	String	是	国家政务服务平台电子印章系统返回的任务编号，用于人社部政务服务平台电子印章系统查询任务结果时使用。
signAlgorithm	-	String	是	签名算法 oid 字符串，1.2.156.10197.1.501。
signValue	-	String	是	BASE64 编码的签名值，编码前的签名值长度为 64 字节，其中 r 和 s 分别为 32 字节。该签名值是由国家政务服务平台电子印章系统的签名私钥进行签名生成的。
data	taskId	String	是	国家政务服务平台电子印章系统返回的任务编号，用于人社部政务服务平台电子印章系统查询任务结果时使用。
signInfo(签名信息)	signAlgorithm	String	是	签名算法 oid 字符串，1.2.156.10197.1.501。
signInfo(签名信息)	signValue	String	是	BASE64 编码的签名值，编码前的签名值长度为 64 字节，其中 r 和 s 分别为 32 字节。该签名值是由国家政务服务平台电子印章系统的签名私钥进行签名生成的。

5.2.8.4 业务返回参数说明见表 14，报文示例见附录 A 中示例 7。

表14 业务返回参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businesstype	-	String	是	revocationSealInfo: 印章撤销。
errorCode	-	String	是	错误码, 1 代表成功, 0 代表错误。
errorInfo	-	String	是	错误说明。
message_content				
taskCode	-	String	是	命令编码 revocationSealInfo。
version	-	String	是	版本号 1.0。
resultCode	-	String	是	返回值, 0 表示成功, 其他表示错误。
resultCodeMsg	-	String	是	返回信息描述。
taskTypeCode	-	String	是	业务类型编码, 0 表示备案业务, 1 表示保护密钥更新业务, 2 表示印章撤销, 3 表示申请电子印章唯一赋码业务。
data	taskId	String	是	国家政务服务平台电子印章系统返回的任务编号, 用于人社部政务服务平台电子印章系统查询任务结果时使用。
signInfo(签名信息)	signAlgorithm	String	是	签名算法 oid 字符串, 1.2.156.10197.1.501。
signInfo(签名信息)	signValue	String	是	BASE64 编码的签名值, 编码前的签名值长度为 64 字节, 其中 r 和 s 分别为 32 字节。该签名值是由国家政务服务平台电子印章系统的签名私钥进行签名生成的。signValue 的待签名数据, 参数详情及参数顺序见表 8 待签名业务参数说明。

5.2.9 申请电子印章唯一赋码接口

5.2.9.1 功能描述

人社部政务服务平台电子印章系统向国家政务服务平台电子印章系统提交获取电子印章唯一赋码的申请, 并从国家政务服务平台电子印章系统获取印章唯一赋码。

5.2.9.2 前置条件

服务接口安全接入条件, 人社部政务服务平台电子印章系统完成向国家政务服务平台电子印章系统的注册。

5.2.9.3 业务请求参数说明见表 15, 报文示例见附录 A 中示例 8。

表15 业务请求参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businesstype	-	String	是	applySealCode: 申请印章唯一赋码。
message_content				
taskCode	-	String	是	命令编码 revocationSealInfo。
version	-	String	是	版本号 1.0。
tokenInfo	-	String	是	客户端随机数 (randomA) 与服务端随机数 (randomB) 字符串拼接, 中间无分割符号。
taskTypeCode	-	String	是	业务类型编码, 0 表示备案业务, 1 表示保护密钥更新业务, 2 表示印章撤销, 3 表示申请电子印章唯一赋码业务。
data	areaNumber	String	是	行政区划代码, 长度为 3 字节。
signInfo(签名信息)	signAlgorithm	String	是	签名算法 oid 字符串, 1.2.156.10197.1.501。
signInfo(签名信息)	signValue	String	是	BASE64 编码的签名值, 编码前的签名值长度为 64 字节, 其中 r 和 s 分别为 32 字节。该签名值是人社部电子印章制作系统签名生成的, 各地方无需填充此参数。

5.2.9.4 业务返回参数说明见表 16，报文示例见附录 A 中示例 8。

表16 业务返回参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businesstype	-	String	是	applySealCode: 申请电子印章唯一赋码。
errorCode	-	String	是	错误码, 1 代表成功, 0 代表错误。
errorInfo	-	String	是	错误说明。
message_content				
taskCode	-	String	是	命令编码 applySealCode。
version	-	String	是	版本号 1.0。
resultCode	-	String	是	返回值, 1 表示成功, 0 表示错误。
resultCodeMsg	-	String	是	返回信息描述。
taskTypeCode	-	String	是	业务类型编码, 0 表示备案业务, 1 表示保护密钥更新业务, 2 表示印章撤销, 3 表示申请电子印章唯一赋码业务。
data	sealCode	String	是	电子印章唯一赋码。
signInfo(签名信息)	signAlgorithm	String	是	签名算法 oid 字符串, 1.2.156.10197.1.501。
signInfo(签名信息)	signValue	String	是	BASE64 编码的签名值, 编码前的签名值长度为 64 字节, 其中 r 和 s 分别为 32 字节。该签名值是由公安部门印章管理系统的签名私钥进行签名生成的。

5.2.10 确认回执接口

5.2.10.1 功能描述

当人社部政务服务平台电子印章系统将公安部门下发数据成功写入电子印章的安全载体后, 需要发送确认回执给国家政务服务平台电子印章系统。

5.2.10.2 前置条件

服务接口安全接入条件, 人社部政务服务平台电子印章系统已经将公安部门下发的数据成功写入电子印章的安全载体。

5.2.10.3 业务请求参数说明见表 17，报文示例见附录 A 中示例 9。

表17 业务请求参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businesstype	-	String	是	confirmReceipt: 确认回执。
message_content				
taskCode	-	String	是	命令编码 confirmReceipt。
version	-	String	是	版本号 1.0。
tokenInfo	-	String	是	客户端随机数 (randomA) 与服务端随机数 (randomB) 字符串拼接, 中间无分割符号。
taskTypeCode	-	String	是	业务类型编码, 0 表示备案业务, 1 表示保护密钥更新业务, 2 表示印章撤销, 3 表示申请电子印章唯一赋码业务。
data	taskId	String	是	在一项业务处理中, 国家政务服务平台电子印章系统返回的业务编号, 用于串联上下文。
data	yzbm	String	是	印章编码。
data	deviceCode	String	是	设备编码, 公安部门下发数据的数据密钥解密获得。
data	encDeviceCode	String	是	BASE64 编码的设备编码密文, 公安部门下发数据的数据密钥加密获得。
signInfo(签名信息)	signAlgorithm	String	是	签名算法 oid 字符串, 1.2.156.10197.1.501。

5.2.10.4

表17 业务请求参数说明（续）

参数名称	参数子项	类型	是否必须	描述
signInfo(签名信息)	signValue	String	是	BASE64 编码的签名值, 编码前的签名值长度为 64 字节, 其中 r 和 s 分别为 32 字节。该签名值是人社部电子印章制作系统签名生成的, 各地方无需填充此参数。

5.2.10.5 业务返回参数说明见表 18, 报文示例见附录 A 中示例 9。

表18 业务返回参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businesstype	-	String	是	confirmReceipt: 确认回执。
errorCode	-	String	是	错误码, 1 代表成功, 0 代表错误。
errorInfo	-	String	是	错误说明。
message_content				
taskCode	-	String	是	命令编码 confirmReceipt。
version	-	String	是	版本号 1.0
resultCode	-	String	是	返回值, 1 表示成功, 0 表示错误。
resultCodeMsg	-	String	是	返回信息描述。
taskTypeCode	-	String	是	业务类型编码, 0 表示备案业务, 1 表示保护密钥更新业务, 2 表示印章撤销, 3 表示申请电子印章唯一赋码业务。
data	errorCode	String	是	每个申请包处理的返回结果, 0 是成功, 其他表示错误。
data	yzbm	String	是	印章编码。
signInfo(签名信息)	signAlgorithm	String	是	签名算法 oid 字符串, 1.2.156.10197.1.501。
signInfo(签名信息)	signValue	String	是	BASE64 编码的签名值, 编码前的签名值长度为 64 字节, 其中 r 和 s 分别为 32 字节。该签名值是由国家政务服务平台电子印章系统的签名私钥进行签名生成的。

5.2.11 身份认证接口

5.2.11.1 功能描述

人社部政务服务平台电子印章系统推送状态信息时需验证平台身份, 具体的身份认证流程见 ZFWF C 0122—2018 国家政务服务平台统一电子印章系统接口要求 附录A, 其中客户端为人社部政务服务平台电子印章状态发布系统, 服务端为国家政务服务平台电子印章状态发布系统。

5.2.11.2 前置条件

服务接口安全接入条件, 人社部政务服务平台电子印章系统已经将公安部门下发的数据成功写入电子印章的安全载体。

5.2.11.3 业务请求参数说明见表 19, 报文示例见附录 A 中示例 10。

表19 业务请求参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	recvAuthServer: 身份认证
message_content			
idA	String	是	人社部电子印章状态发布系统的 Base64 编码格式的系统证书。各地市无需填充此参数。
randomA	String	是	人社部政务服务平台电子印章状态发布系统生成的 16 位随机数, 用于确定该次请求

5.2.11.4 业务返回参数说明见表 20, 报文示例见附录 A 中示例 10。

表20 业务返回参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	recvAuthServer: 身份认证。
errorCode	String	是	错误码, 1 代表成功, 0 代表错误。
errorInfo	String	是	错误说明。
message_content			
result	String	是	获取随机数成功为“0”。
msg	String	是	返回的描述信息。
token	String	是	随机数, 签名值, 国家政务服务平台电子印章系统状态发布系统数字证书拼接的字符串 idB randomB randomA signValue idB 是国家政务服务平台电子印章系统状态发布系统数字证书 randomB 是国家政务服务平台电子印章系统状态发布系统生成的 16 位字符串 randomA 是国家政务服务平台电子印章系统状态发布系统请求的 16 位随机数 signValue 是国家政务服务平台电子印章系统状态发布系统的内部签名。签名明文为 idB randomB randomA。

5.2.12 数据传输接口

5.2.12.1 功能描述

用于传输身份认证参数与业务参数。

5.2.12.2 前置条件

参见“5.2.1 前置条件”内容。

5.2.12.3 业务请求参数说明见表 21, 报文示例见附录 A 中示例 11。

表21 业务请求参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	msgCenterDoubleServer: 数据传输。
message_content			
data	String	是	由人社部电子印章系统状态发布系统数字证书 idA、16 位返回的随机数、业务数据 text、签名值拼接而成, 格式为: idA+ +randomB+ +text+ +signValue, 其中 signValue 是对 idA+ +randomB+ +text 做的 SM2 签名。

注: 拼接顺序不能换, 否则会请求验证失败。

电子印章状态信息发布的 text 格式:

```
{
  "taskCode": "",
  "taskData": "",
  "taskSignature": ""
}
```

其中“taskCode”必须为207, “taskData”是将印章对象转为json格式, “taskSignature”是对明文做的sm2签名。其参数内容见表22。

表22 参数

参数名称	类型	最大长度	是否必须	描述
provincePubSysId	String	1500	是	人社部电子印章系统状态发布系统数字证书。
sealCode	String	32	是	印章编码。
sealName	String	150	是	印章名称。
useUnitCode	String	32	是	社会信用代码。
sealZone	String	32	是	印章所属区域。
validStartTime	String	30	是	印章有效起始时间。
validEndTime	String	30	是	印章有效截至时间。
parentSealCode	String	32	是	印章上级编码。
createTime	String	30	是	印章创建时间。
creator	String	64	是	制作单位名称。
legalType	String	10	是	法人类型。
signature	String	200	是	印章签名值。
certStartTime	String	30	是	证书有效起始时间。
certEndTime	String	30	是	证书有效截至时间。
signCert	String	1500	是	印章证书。
requestParam	String	1500	是	印章参数转为 json 格式。

电子印章撤销、挂失、吊销的格式

```
{
  "taskCode": "",
  "taskData": "",
  "taskSignature": ""
}
```

其中“taskCode”必须为209，“taskData”是将印章对象转为json格式，“taskSignature”是对明文做的sm2签名。其参数内容见表23。

表23 参数

参数名称	类型	最大长度	是否必须	描述
provincePubSysId	String	1500	是	人社部发布系统证书。
sealName	String	150	是	印章名称。
cancelReason	String	2	是	挂失或吊销或撤销原因。0：因密钥泄露撤销；1：因信息变更撤销；2：因业务终止撤销；3：因印章丢失挂失；4：因其他原因撤销；5：因虚假注册吊销；6：因超范围经营吊销；7：无故不开业或停业吊销；8：因单位逾期不办理年检手续吊销；9：因其他原因吊销。
cancelDescribe	String	150	是	挂失或吊销或撤销原因描述。
applyDate	String	30	是	挂失或吊销或撤销申请时间。
signature	String	200	是	印章签名值。
invalidType	String	2	是	类型：0：吊销，1：撤销，2：挂失。
invalidEffectTime	String	30	是	挂失或吊销或撤销生效时间。

5.2.12.4 业务返回参数说明见表 24，报文示例见附录 A 中示例 11。

表24 业务返回参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	msgCenterDoubleServer：数据传输。
errorCode	String	是	错误码，1 代表成功，0 代表错误。

表24 业务返回参数说明（续）

参数名称	类型	是否必须	描述
errorInfo	String	是	错误说明。
message_content			
success	Boolean	是	调用内部接口是否成功 true-成功 false-不成功。

5.2.13 获取 Token 接口

5.2.13.1 功能描述

人社部政务服务平台电子印章应用服务系统在国家政务服务平台统一电子印章系统注册成为开发者后，可获得appkey、appsecret及用户盐值。用户通过该接口获取token，用于印章状态查询和印章吊销查询接口的访问。

5.2.13.2 前置条件

参见“5.2.1 前置条件”内容。

5.2.13.3 业务请求参数说明见表 25，报文示例见附录 A 中示例 12。

表25 业务请求参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	DB. oauth. token: 获取 Token。
message_content			
method	String	是	接口名称。
username	String	是	用户账户名。
password	String	是	用户密码，用户密码+用户盐值拼接后进行 SM3 算法散列。
client_id	String	是	用户注册并通过审核后返回的 appkey。
client_secret	String	是	用户注册并通过审核后返回的 appsecret。
grant_type	String	是	授权模式，固定为 password。
version	String	是	版本，目前为 1.0。
timestamp	String	是	时间戳，格式为 yyyyMMddHHmmss。

5.2.13.4 业务返回参数说明见表 26，报文示例见附录 A 中示例 12。

表26 业务返回参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businesstype	-	String	是	DB. oauth. token: 获取 Token。
message_content				
method	-	String	是	接口名称。
requestId	-	String	是	请求 ID。
code	-	String	是	请求结果代码。
data	scope	String	是	授权范围。
data	access_token	String	是	生成的 token。
data	token_type	String	是	token 类型。
data	expires_in	String	是	有效时间。
message	-	String	是	请求结果说明。

5.2.14 注册用户印章状态查询接口

5.2.14.1 功能描述

根据印章名称，查询指定时间下的印章状态。该接口提供注册用户调用方式。

5.2.14.2 前置条件

参见“5.2.1 前置条件”内容。

5.2.14.3 业务请求参数说明见表 27，报文示例见附录 A 中示例 13。

表27 业务请求参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	DB.seal.status.query: 印章状态查询。
message_content			
method	String	是	接口名称。
appKey	String	是	给用户颁发的 appkey。
sign	String	是	请求签名，用于安全控制，以参数名 ascii 码排序后签名。
username	String	否	用户账户名。
token	String	是	token 用于调用接口前授权检查。
timestamp	String	是	时间戳，格式 yyyyMMddHHmmss。
format	String	是	响应格式，默认为 json 格式，可选值：json。
version	String	是	API 协议版本，当前版本号 1.0。
type	String	是	请求类型，默认 sync。
sealName	String	是	印章名称。
sealCode	String	是	印章编码。
queryTime	String	是	查询时间，格式 yyyy-MM-dd HH:mm:ss。

5.2.14.4 业务返回参数说明见表 28，报文示例见附录 A 中示例 13。

表28 业务返回参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businesstype	-	String	是	DB.seal.status.query: 印章状态查询。
errorCode	-	String	是	错误码，1 代表成功，0 代表错误。
errorInfo	-	String	是	错误说明。
message_content				
method	-	String	是	接口名称。
requestId	-	String	是	请求 ID。
code	-	String	是	请求结果代码。
data	sealName	String	是	印章名称。
data	queryTime	String	是	查询时间，格式 yyyy-MM-dd HH:mm:ss。
data	sealStatus	String	是	印章状态，1 代表有效，0 代表无效。
message	-	String	是	请求结果说明。

5.2.15 非注册用户印章状态查询接口

5.2.15.1 功能描述

根据印章名称，查询指定时间下的印章状态。该接口提供非注册用户调用方式。

5.2.15.2 前置条件

参见“5.2.1 前置条件”内容。

5.2.15.3 业务请求参数说明见表 29，报文示例见附录 A 中示例 14。

表29 业务请求参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	DB.seal.status.query: 印章状态查询
message_content			
method	String	是	接口名称
sign	String	是	请求签名, 用于安全控制, 以参数名 ascii 码排序后签名
timestamp	String	是	时间戳, 格式 yyyyMMddHHmmss
format	String	否	响应格式, 默认为 json 格式, 可选值: json
version	String	是	API 协议版本, 当前版本号 1.0
type	String	否	请求类型, 默认 sync
sealName	String	是	印章名称
sealCode	String	是	印章编码
queryTime	String	是	查询时间, 格式 yyyy-MM-dd HH:mm:ss

5.2.15.4 业务返回参数说明见表 30, 报文示例见附录 A 中示例 14。

表30 业务返回参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businesstype	-	String	是	DB.seal.status.query: 印章状态查询。
errorCode	-	String	是	错误码, 1 代表成功, 0 代表错误。
errorInfo	-	String	是	错误说明。
message_content				
method	-	String	是	接口名称。
requestId	-	String	是	请求 ID。
code	-	String	是	请求结果代码。
data	sealName	String	是	印章名称。
data	queryTime	String	是	查询时间, 格式 yyyy-MM-dd HH:mm:ss。
data	sealStatus	String	是	印章状态, "1"-有效, "0"-无效。
message		String	是	请求结果说明。

5.2.16 印章吊销查询接口

5.2.16.1 功能描述

通过该接口获取印章吊销列表。

5.2.16.2 前置条件

参见“5.2.1 前置条件”内容。

5.2.16.3 业务请求参数说明见表 31, 报文示例见附录 A 中示例 15。

表31 业务请求参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	DB.seal.deactive.list.query: 印章吊销查询。
message_content			
method	String	是	接口名称。
appKey	String	是	给用户颁发的 appkey。

5.2.16.4

表31 业务请求参数说明（续）

参数名称	类型	是否必须	描述
sign	String	是	请求签名，用于安全控制，以参数名 ascii 码排序后签名。
username	String	否	用户账户名。
token	String	是	token 用于调用接口前授权检查。
timestamp	String	是	时间戳，格式为 yyyyMMddHHmmss。
format	String	否	响应格式。默认为 json 格式，可选值：json。
version	String	是	API 协议版本，当前版本号 1.0。
type	String	否	请求类型，默认 sync。
queryStartTime	String	是	查询起始时间格式 yyyy-MM-dd HH:mm:ss。
queryEndTime	String	是	查询截止时间格式 yyyy-MM-dd HH:mm:ss。
pageSize	String	是	吊销列表每页数据量。
pageNow	String	是	吊销列表当前页数。

5.2.16.5 业务返回参数说明见表 32，报文示例见附录 A 中示例 15。

表32 业务返回参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businesstype	-	String	是	DB.seal.deactive.list.query：印章吊销查询。
errorCode	-	String	是	错误码，1 代表成功，0 代表错误。
errorInfo	-	String	是	错误说明。
message_content				
method	-	String	是	接口名称。
requestId	-	String	是	请求 ID。
code	-	String	是	请求结果代码。
data	version	String	是	版本号。
data	invalidEffectTime	String	是	本次查询生效时间，格式 yyyy-MM-dd HH:mm:ss。
data	nextUpdateTime	String	是	下一次更新时间，建议更新时间一般为 1 个月，格式 yyyy-MM-dd HH:mm:ss。
data	signature	String	是	签名值。
data	signAlgorithm	String	是	签名算法。
data	signHashAlgorithm	String	是	签名摘要算法。
data	secretKey	String	是	签名公钥。
data	awardCompany	String	是	颁发机构名称。
data	revocationList	String	是	印章吊销列表。
data	sealCode	String	是	印章编码。
data	sealName	String	是	印章唯一编码。
data	revocationTime	String	是	印章无效生效时间。
message		String	是	请求结果说明。

5.3 签章应用规范

5.3.1 集中式签章

5.3.1.1 印章注册接口

5.3.1.1.1 功能描述

用于为业务接口提供印章注册接口功能。

5.3.1.1.2 前置条件

参见“5.2.1 前置条件”内容。

5.3.1.1.3 业务请求参数说明见表 33，报文示例见附录 A 中示例 16。

表33 业务请求参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	applySeal: 印章注册。
message_content			
sealName	String	是	印章名称。
templateName	String	是	印章模板名称。
photoData	String	是	图片数据。
certDN	String	是	证书 DN 值。

5.3.1.1.4 业务返回参数说明见表 34，报文示例见附录 A 中示例 16。

表34 业务返回参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	applySeal: 印章注册。
errorCode	String	是	错误码，1 代表成功，0 代表错误。
errorInfo	String	是	错误说明。
message_content			
.....

5.3.1.2 印章获取接口

5.3.1.2.1 功能描述

用于为业务接口提供印章获取接口功能。

5.3.1.2.2 前置条件

参见“5.2.1 前置条件”内容。

5.3.1.2.3 业务请求参数说明见表 35，报文示例见附录 A 中示例 17。

表35 业务请求参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	getSeal 获取印章。
message_content			
certDN	String	是	证书 DN 值。

5.3.1.2.4 业务返回参数说明见表 36，报文示例见附录 A 中示例 17。

表36 业务返回参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	getSealStatus 获取印章。
message_content			
Seal	String	否	印章信息 base64 编码。

5.3.1.3 印章状态查询接口

5.3.1.3.1 功能描述

用于为业务接口提供印章获取状态接口功能。

5.3.1.3.2 前置条件

参见“5.2.1 前置条件”内容。

5.3.1.3.3 业务请求参数说明见表 37，报文示例见附录 A 中示例 18。

表37 业务请求参数说明

参数名称	类型	是否必须	描述
message_header			
businessstype	String	是	getSealStatus 获取印章状态。
message_content			
certDN	String	是	证书 DN 值。

5.3.1.3.4 业务返回参数说明见表 38，报文示例见附录 A 中示例 18。

表38 业务返回参数说明

参数名称	类型	是否必须	描述
message_header			
businessstype	String	是	getSealStatus 获取印章状态。
message_content			
SealStatus	String	否	0-不可用 1-可用。

5.3.1.4 签章验证接口

5.3.1.4.1 功能描述

用于为业务接口提供PDF、OFD签章验证接口功能。

5.3.1.4.2 前置条件

参见“5.2.1 前置条件”内容。

5.3.1.4.3 业务请求参数说明见表 39，报文示例见附录 A 中示例 19。

表39 业务请求参数说明

参数名称	类型	是否必须	描述
message_header			
businessstype	String	是	verifyFile 印章验证。
errorCode	String	是	错误码，1 代表成功，0 代表错误。
errorInfo	String	是	错误说明。
message_content			
data	String	是	PDF、OFD 文件数据 base64 编码。

5.3.1.4.4 业务返回参数说明见表 40，报文示例见附录 A 中示例 19。

表40 业务返回参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businessstype	-	String	是	verifyFile: 签章验证。
errorCode	-	String	是	错误码，1 代表成功，0 代表错误。
errorInfo	-	String	是	错误说明。

表40 业务返回参数说明（续）

参数名称	参数子项	类型	是否必须	描述
message_content				
verifySealResults	status	String	是	签章验证验证结果，true 表示验证成功。
verifySealResults	info	String	是	签章验证验证结果描述。
verifySealResults	certDN	String	是	签章证书 DN 项。
verifySealResults	sealId	String	是	印章唯一标识。
verifySealResults	sealName	String	是	印章名称。

5.3.1.5 位置签章接口

5.3.1.5.1 功能描述

用于为业务接口提供PDF、OFD位置盖章接口功能。

5.3.1.5.2 前置条件

参见“5.2.1 前置条件”内容。

5.3.1.5.3 业务请求参数说明见表 41，报文示例见附录 A 中示例 20。

表41 业务请求参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businesstype		String	是	positionSealSign 位置签章。
message_content				
data		String	是	待签文件数据 base64 编码。
signList	pageNum	String	是	页号 整数。
signList	zx	String	是	左上坐标 X。
signList	zy	String	是	左上坐标 Y。
signList	sealId	String	是	传入该页文档所使用的印章 ID。
signList	certDN	String	否	签名服务器公钥证书 DN 项，根据具体服务器填写，可为空。
signList	secretKey	String	否	签名服务器密钥索引，根据具体服务器填写，可为空。
signList	keyPin	String	否	签名服务器密钥索引保护 PIN，根据具体服务填写，可为空。
BIZNUM		String	是	业务编号，为空时系统自动生成，整个文档业务编号唯一。

5.3.1.5.4 业务返回参数说明见表 42，报文示例见附录 A 中示例 20。

表42 业务返回参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	positionSealSign 位置签章。
errorCode	String	是	错误码，1 代表成功，0 代表错误。
errorInfo	String	是	错误说明。
message_content			
signedData	String	是	签章后的文件，按 base64 编码。

5.3.1.6 关键字签章接口

5.3.1.6.1 功能描述

用于为业务接口提供PDF、OFD关键字盖章接口功能。

5.3.1.6.2 前置条件

参见“5.2.1 前置条件”内容。

5.3.1.6.3 业务请求参数说明见表 43，报文示例见附录 A 中示例 21。

表43 业务请求参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businesstype	-	String	是	keyWordSealSign 关键字签章。
message_content				
data	-	String	是	待签文件数据 base64 编码。
signList	keyword	String	是	盖章关键字。
signList	keywordModel	String	是	关键字类型(1:首个,0:末个,-1:全部,-:区间,,:自定义页号)。
signList	sealId	String	是	传入该页文档所使用的印章 ID。
signList	certDN	String	否	签名服务器公钥证书 DN 项, 根据具体服务器填写, 可为空。
signList	secretKey	String	否	签名服务器密钥索引, 根据具体服务器填写, 可为空。
signList	keyPin	String	否	签名服务器密钥索引保护 PIN, 根据具体服务填写, 可为空。
BIZNUM	-	String	是	业务编号, 为空时系统自动生成, 整个文档业务编号唯一。

5.3.1.6.4 业务返回参数说明见表 44，报文示例见附录 A 中示例 21。

表44 业务返回参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	keyWordSealSign 关键字签章。
errorCode	String	是	错误码, 1 代表成功, 0 代表错误。
errorInfo	String	是	错误说明。
message_content			
signedData	String	是	签章后的文件, 按 base64 编码。

5.3.1.7 骑缝章接口

5.3.1.7.1 功能描述

用于为业务接口提供PDF、OFD签骑缝章接口功能。

5.3.1.7.2 前置条件

参见“5.2.1 前置条件”内容。

5.3.1.7.3 业务请求参数说明见表 45，报文示例见附录 A 中示例 22。

表45 业务请求参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businesstype	-	String	是	pagingSealSign 骑缝章签章。
message_content				
data	-	String	是	待签文件数据 base64 编码。
signList	sealId	String	是	传入该页文档所使用的印章 ID。
signList	page	String	是	骑缝页数。
signList	y	String	是	骑缝章 Y 坐标。
signList	certDN	String	否	签名服务器公钥证书 DN 项, 根据具体服务器填写, 可为空。

表45 业务请求参数说明（续）

参数名称	参数子项	类型	是否必须	描述
signList	secretKey	String	否	签名服务器秘钥索引，根据具体服务器填写，可为空。
signList	keyPin	String	否	签名服务器秘钥索引保护 PIN，根据具体服务填写，可为空。
BIZNUM	-	String	是	业务编号，为空时系统自动生成，整个文档业务编号唯一。

5.3.1.7.4 业务返回参数说明见表 46，报文示例见附录 A 中示例 22。

表46 业务返回参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	pagingSealSign 骑缝章签章
errorCode	String	是	错误码，1 代表成功，0 代表错误
errorInfo	String	是	错误说明
message_content			
signedData	String	是	签章后的文件，按 base64 编码

5.3.1.8 电子证照锁定签名接口

5.3.1.8.1 功能描述

用于为业务接口提供 OFD 电子证照锁定签名接口功能。

5.3.1.8.2 前置条件

参见“5.2.1 前置条件”内容。

5.3.1.8.3 业务请求参数说明见表 47，报文示例见附录 A 中示例 23。

表47 业务请求参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	lockSign 添加锁定签名。
message_content			
data	String	是	待签文件数据 base64 编码。
certDN	String	否	签名服务器公钥证书 DN 项，根据具体服务器填写，可为空。
secretKey	String	否	签名服务器秘钥索引，根据具体服务器填写，可为空。
keyPin	String	否	签名服务器秘钥索引保护 PIN，根据具体服务填写，可为空。
BIZNUM	String	是	业务编号，为空时系统自动生成，整个文档业务编号唯一。

5.3.1.8.4 业务返回参数说明见表 48，报文示例见附录 A 中示例 23。

表48 业务返回参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	lockSign 添加锁定签名。
errorCode	String	是	错误码，1 代表成功，0 代表错误。
errorInfo	String	是	错误说明。

表48 业务返回参数说明（续）

参数名称	类型	是否必须	描述
message_content			
signedData	String	是	签名后的文件，按 base64 编码。

5.3.1.9 电子证照删除锁定签名接口

5.3.1.9.1 功能描述

用于为业务接口提供OFD电子证照删除锁定签名接口功能。

5.3.1.9.2 前置条件

参见“5.2.1 前置条件”内容。

5.3.1.9.3 业务请求参数说明见表 49，报文示例见附录 A 中示例 24。

表49 业务请求参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	delLockSign 删除锁定签名。
message_content			
data	String	是	待操作文件数据 base64 编码。
BIZNUM	String	是	业务编号，为空时系统自动生成，整个文档业务编号唯一。

5.3.1.9.4 业务返回参数说明见表 50，报文示例见附录 A 中示例 24。

表50 业务返回参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	delLockSign 删除锁定签名。
errorCode	String	是	错误码，1 代表成功，0 代表错误。
errorInfo	String	是	错误说明。
message_content			
signedData	String	是	删除锁定签名后的文件，按 base64 编码。

5.3.1.10 电子证照签章并锁定签名接口

5.3.1.10.1 功能描述

用于为业务接口提供OFD电子证照签章并锁定签名接口功能。

5.3.1.10.2 前置条件

参见“5.2.1 前置条件”内容。

5.3.1.10.3 业务请求参数说明见表 51，报文示例见附录 A 中示例 25。

表51 业务请求参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businesstype		String	是	signAndLockSign 签章并锁定签名。
message_content				
data		String	是	待签文件数据 base64 编码。

表51 业务请求参数说明（续）

参数名称	参数子项	类型	是否必须	描述
signList	sealId	String	是	传入该页文档所使用的印章 ID。
signList	page	String	是	页数。
signList	x	String	是	签章章 x 坐标。
signList	y	String	是	签章章 Y 坐标。
signList	certDN	String	否	签名服务器公钥证书 DN 项，根据具体服务器填写，可为空。
signList	secretKey	String	否	签名服务器密钥索引，根据具体服务器填写，可为空。
signList	keyPin	String	否	签名服务器密钥索引保护 PIN，根据具体服务填写，可为空。
signList	ismain	String	否	是否作为锁定签名证书，1 是，0 否；没有 1 则默认最后一个作为锁定签名证书。
BIZNUM		String	是	业务编号，为空时系统自动生成，整个文档业务编号唯一。

5.3.1.10.4 业务返回参数说明见表 52，报文示例见附录 A 中示例 25。

表52 业务返回参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	signAndLockSign 签章并锁定签名。
errorCode	String	是	错误码，1 代表成功，0 代表错误。
errorInfo	String	是	错误说明。
message_content			
signedData	String	是	签章及锁定签名后的 OFD 文件，按 base64 编码。

5.3.1.11 电子证照验签接口

5.3.1.11.1 功能描述

用于为业务接口提供 OFD 电子证照验签接口功能，电子印章和锁定签名全部验证通过后返回验签成功，否则返回验签失败。

5.3.1.11.2 前置条件

参见“5.2.1 前置条件”内容。

5.3.1.11.3 业务请求参数说明见表 53，报文示例见附录 A 中示例 26。

表53 业务请求参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	verifyEleSign 电子证照验签。
message_content			
data	String	是	待签文件数据 base64 编码。
isSingle	String	是	是否只返回第一个校验不通过的签章校验信息，false 则验证所有。
BIZNUM	String	是	业务编号，为空时系统自动生成，整个文档业务编号唯一。

5.3.1.11.4 业务返回参数说明见表 54，报文示例见附录 A 中示例 26。

表54 业务返回参数说明

参数名称	参数子项	类型	是否必须	描述
message_header				
businesstype	-	String	是	verifyEleSign 电子证照验签。
errorCode	-	String	是	错误码, 1 代表成功, 0 代表错误。
errorInfo	-	String	是	错误说明。
message_content				
verifySealResults	status	String	是	签章验证验证结果, true 表示验证成功。
verifySealResults	info	String	是	签章验证验证结果描述。
verifySealResults	certDN	String	是	签章证书 DN 项。
verifySealResults	sealId	String	是	印章唯一标识。

5.3.1.12 电子证照加注并锁定签名接口

5.3.1.12.1 功能描述

用于为业务接口提供OFD电子证照加注并锁定签名接口功能。

5.3.1.12.2 前置条件

参见“5.2.1 前置条件”内容。

5.3.1.12.3 业务请求参数说明见表 55, 报文示例见附录 A 中示例 27。

表55 业务请求参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	watermarkAndLockSign 加注并锁定签名。
message_content			
data	String	是	待加注文件数据 base64 编码。
certDN	String	否	签名服务器公钥证书 DN 项, 根据具体服务器填写, 可为空。
secretKey	String	否	签名服务器密钥索引, 根据具体服务器填写, 可为空。
keyPin	String	否	签名服务器密钥索引保护 PIN, 根据具体服务填写, 可为空。
copyCreator	String	是	加注件作者。
copyCause	String	是	加注内容。
year	Int	是	加注有效年限从当前日期开始。
BIZNUM	String	是	业务编号, 为空时系统自动生成, 整个文档业务编号唯一。

5.3.1.12.4 业务返回参数说明见表 56, 报文示例见附录 A 中示例 27。

表56 业务返回参数说明

参数名称	类型	是否必须	描述
message_header			
businesstype	String	是	watermarkAndLockSign 加注并锁定签名。
errorCode	String	是	错误码, 1 代表成功, 0 代表错误。
errorInfo	String	是	错误说明。
message_content			
signedData	String	是	加注及锁定签名后的 OFD 文件, 按 base64 编码。

5.3.2 分散式签章

5.3.2.1 分散式签章接口规范

5.3.2.1.1 HRSSOpenFile 接口

原型: short HRSSOpenFile();
功能: 弹出打开文件对话框, 选择一个电子文件并打开
参数: 无
返回值: 成功返回1, 错误返回0

5.3.2.1.2 HRSSOpenFileByPath 接口

原型: short HRSSOpenFileByPath (LPCTSTR szFilePath, SHORT iType);
功能: 通过路径打开电子文件
参数:
szFilePath 电子文件路径, 本地路径或网络路径, 支持HTTP和FTP
iType 0标识为本地路径, 1标识为网络路径
返回值: 成功返回1, 错误返回0

5.3.2.1.3 HRSSCloseFile 接口

原型: short HRSSCloseFile();
功能: 关闭当前打开的文件
参数: 无
返回值: 成功返回1, 错误返回0

5.3.2.1.4 HRSSFileSaveAs 接口

原型: short HRSSFileSaveAs();
功能: 另存当前打开的电子文档
参数: 无
返回值: 成功返回1, 错误返回0

5.3.2.1.5 HRSSPrintFile 接口

原型: short HRSSPrintFile ();
功能: 打印当前打开的文件
参数: 无
返回值: 成功返回1, 错误返回0

5.3.2.1.6 HRSSFileZoomLarge 接口

原型: short HRSSFileZoomLarge ();
功能: 放大
参数: 无
返回值: 成功返回1, 错误返回0

5.3.2.1.7 HRSSFileZoomSmall 接口

原型: short HRSSFileZoomSmall ();
功能: 缩小
参数: 无
返回值: 成功返回1, 错误返回0

5.3.2.1.8 HRSSFileRotateLeft 接口

原型: short HRSSFileRotateLeft ();
功能: 左旋90度
参数: 无

返回值：成功返回1，错误返回0

5.3.2.1.9 HRSSFileRotateRight 接口

原型：short HRSSFileRotateRight ();

功能：右旋90度

参数：无

返回值：成功返回1，错误返回0

5.3.2.1.10 HRSSGoToNextPage 接口

原型：void HRSSGoToNextPage ();

功能：跳转到下一页

参数：无

返回值：无

5.3.2.1.11 HRSSGoToPrevPage 接口

原型：void HRSSGoToPrevPage ();

功能：跳转到上一页

参数：无

返回值：VOID

5.3.2.1.12 HRSSGoToFirstPage 接口

原型：void HRSSGoToFirstPage ();

功能：跳转到首页

参数：无

返回值：无

5.3.2.1.13 HRSSGoToLastPage 接口

原型：void HRSSGoToLastPage ();

功能：跳转到尾页

参数：无

返回值：无

5.3.2.1.14 HRSSGoToPage 接口

原型：short HRSSGoToPage (SHORT pageNo);

功能：跳转到指定页

参数：

SHORT pageNo 页码

返回值：成功返回1，错误返回0

5.3.2.1.15 HRSSShowToolBarButton 接口

原型：void HRSSShowToolBarButton (SHORT nIndex, VARIANT_BOOL bShow);

功能：控制工具栏按钮显示/隐藏

参数：

SHORT nIndex 按钮的索引

1 关闭

2 另存

3 放大

4 缩小

5 右旋

6 左旋

- 7 首页
- 8 上一页
- 9 下一页
- 10 尾页
- 11 书签
- 12 查找
- 13 关于
- 21 单页签章
- 22 骑缝签章
- 23 手写签名
- 24 批量验证
- 25 文档打印
- 26 参数设置
- 99 全部按钮

VARIANT_BOOL bShow TRUE显示, FALSE隐藏
返回值: VOID

5.3.2.1.16 HRSSInsertESeal 接口

原型: short HRSSInsertESeal ();

功能: 插入电子签章密码钥匙, 点击工具条插入签章, 当鼠标光标变成所盖印章时, 将印章光标移动到合适的位置, 单击鼠标左键进行盖章; 单击鼠标右键取消本次签章。

参数: 无

返回值: 成功返回1, 错误返回0

5.3.2.1.17 HRSSInsertPagingESeal 接口

原型: short HRSSInsertPagingESeal ();

功能: 插入电子签章密码钥匙, 点击工具条插入骑缝章, 当鼠标光标变成所盖印章时, 将印章光标移动到合适的位置, 骑缝章的位置和印章光标在文档中的Y坐标位置相同, 单击鼠标左键且文档大于2页时在文档上盖骑缝章, 默认情况下, 文档每10页加盖一个骑缝章, 剩余页加盖一个骑缝章; 单击鼠标右键取消本次盖骑缝章。

参数: 无

返回值: 成功返回1, 错误返回0

5.3.2.1.18 HRSSBatchVerify 接口

原型: short HRSSBatchVerify ();

功能: 显示文档中所有印章验证结果信息。

参数: 无

返回值: 成功返回1, 错误返回0

5.3.2.1.19 HRSSSysSet 接口

原型: short HRSSSysSet ();

功能: 配置所用USBKEY厂商信息等。

参数: 无

返回值: 成功返回1, 错误返回0

5.3.2.1.20 HRSSCheckKey 接口

原型: SHORT HRSSCheckKey ();

功能: 检测USBKEY是否存在

参数: 无

返回值: 成功返回1, 错误返回0。

5.3.2.1.21 HRSSGetKeyID 接口

原型: BSTR HRSSGetKeyID ();

功能: 获取USBKEY的硬件标识

参数: 无

返回值: 存在USBKEY返回USBKEY的硬件标识, 否则返回空串。

5.3.2.1.22 HRSSGetESealId 接口

原型: BSTR HRSSGetESealId ();

功能: 获取USBKEY中印章的唯一标识

参数: 无

返回值: 存在印章返回印章的唯一标识, 否则返回空串。

5.3.2.1.23 HRSSIsFileSigned 接口

原型: SHORT HRSSIsFileSigned ();

功能: 判断电子文件是否签章

参数: 无

返回值: 返回文档中印章数量。

5.3.2.1.24 HRSSIsPagingSigned 接口

原型: SHORT HRSSIsPagingSigned ();

功能: 判断电子文件是否签骑缝章

参数: 无

返回值: 返回文档中骑缝章数量。

5.3.2.1.25 HRSSGetCurrentSignatureCount 接口

原型: SHORT HRSSGetCurrentSignatureCount ();

功能: 获取当前文档签章数量

参数: 无

返回值: 返回文档中签章数量。

5.3.2.1.26 HRSSGetCurrentPageNum 接口

原型: SHORT HRSSGetCurrentPageNum ();

功能: 获取文档当前页面

参数: 无

返回值: 返回文档当前页面。

5.3.2.1.27 HRSSGetSignInfo 接口

原型: SHORT HRSSGetSignInfo ();

功能: 获取文档签章相关信息

参数: 无

返回值: 返回文档签章相关信息。

5.3.2.1.28 HRSSGotoBookMarkByBookMarkName 接口

原型: SHORT HRSSGotoBookMarkByBookMarkName (BSTR strBookMarkName);

功能: 跳转到书签所在页

参数:

BSTR strBookMarkName 书签名称

返回值: 成功返回1, 书签不存在返回0。

5.3.2.1.29 HRSSGotoPageByKeyWord 接口

原型: SHORT HRSSGotoPageByKeyWord (BSTR KeyWord);

功能: 跳转到关键字所在页

参数:

BSTR KeyWord 关键字

返回值: 成功返回1, 关键字不存在返回0。

5.3.2.1.30 HRSSHttpInit 接口

原型: VARIANT_BOOL HRSSHttpInit();

功能: 模拟HTTP实现初始化

参数: 无

返回值: 成功返回TRUE, 否则错误。

5.3.2.1.31 HRSSHttpAddPostString 接口

原型: VARIANT_BOOL HRSSHttpAddPostString(LPCTSTR FileName, LPCTSTR FieldValue)

功能: 模拟HTTP实现添加字段

参数:

FileName 字段名称

FieldValue 字段值

返回值: 成功返回TRUE, 否则错误。

5.3.2.1.32 HRSSHttpAddPostFile 接口

原型: VARIANT_BOOL HRSSHttpAddPostFile (LPCTSTR FileName, LPCTSTR FileName)

功能: 模拟HTTP实现添加文件

参数:

FileName 字段名称

FileName 文件路径

返回值: 成功返回TRUE, 否则错误。

5.3.2.1.33 HRSSHttpAddPostCurrFile 接口

原型: VARIANT_BOOL HttpAddPostCurrFile2(LPCTSTR FileName, LPCTSTR Reserved);

功能: 模拟HTTP实现添加当前文档

参数:

FileName 文件字段名称

Reserved 保留, 未使用

返回值: 成功返回TRUE, 否则错误。

5.3.2.1.34 HRSSHttpPost 接口

原型: VARIANT_BOOL HRSSHttpPost(BSTR url, BSTR cookie)

功能: 模拟HTTP提交数据到URL

参数:

BSTR url HTTP提交地址

BSTR cookie cookie信息

返回值: 成功返回TRUE, 否则错误。

5.3.2.1.35 HRSSSignByKeyword 接口

原型: SHORT HRSSSignByKeyword (BSTR szKeyWord, BSTR szPages, BSTR szIndexes)

功能: 关键字签章, 支持页数及次数关联签章; 如: 页数为2-5, 次数为2, 3: 给文件中第二页至第五页的关键字出现的第二次和第三次的关键字盖章。

参数:

BSTR szKeyWord 签章关键字

BSTR szPages 指定的页数，格式如 0;2-10;2, 5
 BSTR szIndexes 关键字出现的次数，格式如 0;2-10;2, 5
 返回值：成功返回1，错误返回0。

5.3.2.1.36 HRSSSignByPos 接口

原型：SHORT HRSSSignByPos (BSTR szPages, LONG xCenter, LONG yCenter)

功能：固定的页数的指定坐标签章；如：0：给文件的所有界面的指定坐标签章；1：给第一页的指定坐标签章；2-10：给第二页到第十页的指定坐标签章；2,5：给第二页和第五页的指定坐标签章。

参数：

BSTR szPages 指定的页数，格式如 0;2-10;2, 5
 LONG xCenter 签章位置坐标中心点X坐标位置
 LONG yCenter 签章位置坐标中心点Y坐标位置
 返回值：成功返回1，错误返回0。

5.3.2.1.37 HRSOfdLockSign 接口

原型：short HRSOfdLockSign(BSTR disc);

功能：ofd加注件锁定签章

参数：

disc 为json格式的签章描述，其结构为：

```
{
  "certificateCopyMetaData":{
    "certificateCopyCreatioinTime":"yy年mm月dd日 hh:mm:ss", //
    "certificateCopyCreator":"xxx",
    "certificateCopyCause":"xxx",
    "certificateCopyCpiringTime":" yy年mm月dd日"
  },
  "watermarkInfomation":{
    "watermarkType":"pic或text或为空",
    "watermarkPicture":"base64格式编码后的图片文件",
    "watermarkText":"水印文字",
    "watermarkFont":"字体名称",
    "watermarkFontSize":"字号（毫米）",
    "watermarkTextColor":"R, G, B",
    "watermarkCTM":"a, b, c, d, e, f",
    "watermarkBoundary":"x0 y0 w h",
    "watermarkPatternNode":"base64编码后的CT_Pattern节点数据"
  }
}
```

返回值：成功返回1，失败返回错误码。

json串中，各个键值对均为可选的，若因某键值对的值为空或该键值对不存在，而导致无法确定水印显示效果，则返回错误码。若disc参数为空，表明不添加注释信息。

其中：

- watermarkType 的值为 pic 或 text 或空字符串，空字符串表示不使用水印；
- watermarkPicture 为 base64 编码后的图片文件，图片文件的类型可为 bmp 或 png 或 jpg/jpeg；
- watermarkTextColor 为文字颜色的 RGB 描述，如红色 255, 0, 0；
- watermarkCTM 为文字或图片所使用的变形矩阵，变形矩阵的使用参 gb33190；
- watermarkBoundary 为文字或图片的区域，以毫秒为单位，描述图片或文字所占区域的左、顶、宽、高；

- f) watermarkPatternNode: 该节点在当上述参数不能满足要求时使用,如使用专有字体或定制水印文字的翻转等,该节点的值为一个完整的 CT_Pattern 节点的 base64 编码,注意,该 CT_Pattern 节点的所有 id 值均使用固定的"\$id\$"代替,在实际使用时,再"\$id\$"替换为真实的 id 值。另外,当该键值对存在且有效(不为空)时,若于其他键值对存在冲突,一切以本键值对为准。

5.3.2.1.38 HRSOfdDeleteLockSign 接口

原型: short HRSOfdDeleteLockSign();

功能: 删除锁定签名

参数: 无

返回值: 成功返回1,失败返回错误码。

5.3.2.1.39 HRSGetLastError 接口

原型: BSTR HRSGetLastError(short errno);

功能: 根据参数给定的错误号,返回具体的错误描述信息。

参数:

error 调用其他函数返回的错误号

返回值: 无

5.3.2.2 USBKEY 接口要求

USBKEY接口依据GM/T 0016—2012 智能密码钥匙密码应用接口规范执行。

5.3.2.3 印章数据要求

公安部门下发的加密文件、应用维护对称密钥密文、数据加密对称密钥密文、电子印章在进行写入USBKEY时,写入到固定目录下,并用固定名称进行命名。

公安部门下发的加密文件存储于USBKEY中枚举到的第一个应用中,以GA_ENCFILE命名。

应用维护对称密钥密文、数据加密对称密钥密文存储于USBKEY中枚举到的第一个应用中的第一个容器内。

电子印章存储于USBKEY中枚举到的第一个应用中,以HRSS_ESEAL命名,电子印章数据要求遵循《人力资源社会保障电子印章体系 第2部分 印章技术规范》。

5.3.2.4 签章集成要求

业务系统在调用集中式签章、分散式签章时,需要将业务系统设计成通过配置文件进行设置签章应用的模式,具体实现如下:

集中式签章:可通过配置文件,对集中式签章调用地址、端口进行配置,在调用集中式签章接口时动态进行加载。

分散式签章:可通过配置文件,对分散式签章控件的classId进行配置,打开相应页面时,通过读取配置文件动态加载。

附录 A
(资料性)
电子印章系统接入和服务接口示例

示例1: message_header 报文组装示例

```

"message_header":{
"syscode":"HBECS",
"authcode":"hjhjkja666sdfuuaUyydsa77654Ja",
"businesstype":"onlinePush",
"sign":"1333D3DFAFSDFASDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
"version":"1.0",
"ctime":"1498627266000",
"random":"550e8400e29b41d4a716446655440000",
"hmac":"Ubpyb0Gxk5JKTs8A5Sf18BOR/LRLe61W099NQHZUew4="}

```

示例2: 电子印章制作单位信息推送接口示例

请求URL示例

请求方法: POST

请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:

```

{
"message_header":{
"syscode":"HBECS",
"authcode":"hjhjkja666sdfuuaUyydsa77654Ja",
"businesstype":" onlinePush ",
"sign":"1333D3DFAFSDFASDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
"version":"1.0",
"ctime":"1498627266000",
"random":550e8400e29b41d4a716446655440000",
"hmac":"Ubpyb0Gxk5JKTs8A5Sf18BOR/LRLe61W099NQHZUew4="
},
"message_content":{
"taskCode":"1021",
"taskData": {
"approveUnitCode": "",
"operatorIdcard": "360822199007043121",
"keyState": 1,
"mspUniqueCode": "f74e2df839f94a19ae726e975bfc3875",
"mspUnitNameFew": "壮族",
"mspUnitDistrict": "120104",
"signDate": "",
"deviceId": "",
"mspUnitAddress": "北京市东城区和平里",
"operator": "用户",
"businessLicence": "seal-manager/1540952625907_1815",
"mspUnitZipcode": "274300",
"pushState": 2,
"password": "9cbf8a4dcb8e30682b927f352d6559a0",
"rejectReason": "",
"mspState": 1,
"mspUnitCode": "12530201981382PL95",
"mspUnitPhone": "010-32145698",
"mspUnitLegalPersonId": "360822199007043121",
"mspUnitCity": "120100",
"mspUnitProvice": "120000",

```

```

"approveUnitName": "审批测试",
"mspUnitLegalPerson": "测试",
"mspUnitNameEn": "Tom",
"mspUnitNameCn": "测试数据",
"lastCheckDate": "",
"roleId": "10",
"mspUnitLegalPersonPhone": "18810970400",
"signValue": "",
"specialTrades": "seal-manager/1540952622291_7740",
"signMasterPK": "",
"mspSn": 190,
"keyPlus": "MIIC4DCCAOsGAWIBAgIIEQArpxrlxbEwDAYIKoEcz1UBg3UFADCBhzEfMBOGA1UECwwWRGV2ZWxvcG11bnQgRG
VwYXJ0bWVudDERMA8GA1UECgwIU2VjdXJpdHkxEDA0BgNVBAGMBOJ1aUppbmcxEDA0BgNVBACMBOJ1aUppbmcxDzANBgNVBAMMBkd
vbWFPbjELMAkGA1UEBgcwQ04xDzANBgNVBACMBOJ1aUppbmcxEDA0BgNVBAGMBOJ1aUppbmcxEDA0BgNVBACMBOJ1aUppbmcx
VQDDbVljYHkuozkuInmtYvor5X1iLbkvZzngnrnkuIkkDzANBgNVBACMBjEYMDAwMDEPMA0GA1UECAwGMTIwMDAwMSQwIgyYDVQKQD
Bv1jYHkuozkuInmtYvor5X1iLbkvZzngnrnkuIkkJDAiBgNVBAsMG+WngeS6j0S4ieali+ivleWItuS9n0eCueS4iTBZMBMGBYqGSM
49AgEGCCqBHM9VAYItA0IABDJtNBPdhUqLXUNZz0yMH9iooqBT01Q3QzZNC210hPMkNisqV91r9VWdIMMTaB2nrffyfoLmgSJauBsI
bggo4fZeJgcgwgUwDAYDVROTAQH/BAIwADAAdBgNVHQ4EFgQUrJjvypefsEeEIXxMTA8W3310oT8wgZUGA1UdIwSBjTCBioAUMrkw
osHqMHD+1cssuNTM/fYmGS+hbaRrMGkxDzANBgNVBAsMBkd1b0JhbJERMA8GA1UECgwIU2VjdXJpdHkxEDA0BgNVBAGMBOJ1aUppb
mcxEDA0BgNVBACMBOJ1aUppbmcxEjAQBgNVBAMMCUd1b0JhbJBDQTELMakGA1UEBgcwQ06CAxAAADAMBggqRzPVQGDdQUAA0gAME
UCIAvmF1RihOkBiEPAfo2a2ueQT7UxNRt3gkmoAnz819aJAiEAo0951Xm5vfVJgAG49K+qMdaa50VBCYDo7yTMz5paiF0=",
"applyDate": "2018-12-05 11:44:24"}
}

```

业务返回报文:

```

{
"message_header": {
"businessstype": "onlinePush",
"syscode": "HBECS",
"version": "1.0",
"errorCode": "1",
"errorInfo": "推送成功"},
"message_content": {}
}

```

示例3: 电子印章信息备案获取随机数接口示例

请求URL示例
请求方法: POST
请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:

```

{
"message_header": {
"syscode": "HBECS",
"authcode": "hjHjkja666sdfuuaUyydsa77654Ja",
"businessstype": "getRandom",
"sign": "1333D3DFAFSDFASDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
"version": "1.0",
"ctime": "1498627266000",
"random": "550e8400e29b41d4a716446655440000",
"hmac": "Ubypy0Gxk5JKTs8A5Sf18B0R/LRLe61W099NQHuzew4="},
"message_content": {
"taskCode": "applyRandom",
"version": "1.0",
"randomA": "1234567890123456"}
}

```

业务返回报文:


```

{
  "message_header":{
    "businesstype":"getRandom",
    "syscode":" HBECS ",
    "version":"1.0",
    "errorCode":"1 ",
    "errorInfo":"获取随机数成功"},
  "message_content":{
    randomB: "1234567890123456"
  }
}

```

示例4: 电子印章上传备案信息接口示例

请求URL示例
 请求方法: POST
 请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:

```

{
  "message_header":{
    "syscode":"HBECS",
    "authcode":"hjhjkja666sdfuuaUyydsa77654Ja",
    "businesstype":"uploadRecordInfos",
    "sign":"1333D3DFAFSDFASDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
    "version":"1.0"
  },
  "ctime": "1498627266000"
  "random":550e8400e29b41d4a716446655440000"
  "hmac":"UppybOGxk5JKTs8A5Sf18BOR/LRLe61W099NQHZUew4="},
  "message_content":{
    "taskCode ":"uploadRecordInfos",
    "version ":"1.0",
    "tokenInfo":"randomA+randomB",
    "taskTypeCode":"0",
    "data": [
      {"sealEncCert":"BASE64编码的电子印章加密证书",
        "sealSignCert":" BASE64编码的电子印章签名证书",
        "sealData":{
          "yzmc": "印章名称",
          "yzbm": "印章编码",
          "yzzzdwbm": "印章制作单位编码",
          "yzlxdm": "印章类型代码",
          "jbr_xm": "经办人姓名",
          "jbr_zjlx": "经办人证件类型",
          "jbr_zjhm": "经办人证件号码",
          "zzrq": "制作日期",
          "ymlx": "印模类型",
          "ymsd": "印模数据",
          "yzsydw_dwmc": "印章使用单位_单位名称",
          "yzsydw_dwssmzwzmc": "印章使用单位_单位少数民族文字名称",
          "yzsydw_dwywmc": "印章使用单位_单位英文名称",
          "yzzzdw_dwmc": "印章制作单位_单位名称",
          "yzzzdw_dwssmzwzmc": "印章制作单位_单位少数民族文字名称",
          "yzzzdw_dwywmc": "印章制作单位_单位英文名称",
          "yzsydw_tyshxydm": "印章使用单位_统一社会信用代码"},
        "districtCode": "行政区划代码"},
      {.....电子印章备案信息列表.....}
    ]
  },
  "signInfo": {

```

```

"signAlgorithm": "1.2.156.10197.1.501",
"signValue ": "BASE64编码的签名值"}
}
}

```

业务返回报文:

```

{
"message_header": {
"businesstype": "uploadRecordInfos ",
"syscode": "HBECS ",
"version": "1.0",
"errorCode": "1",
"errorInfo": "备案成功"},
"message_content": {
"taskCode ": "uploadRecordInfos",
"version ": "1.0",
"resultCode ": "1",
"resultCodeMsg ": "备案信息上传成功",
"taskTypeCode": "0",
"data": {"taskId ": "abcdefg123456"},
"signInfo": {
"signAlgorithm ": "1.2.156.10197.1.501",
"signValue ": "BASE64编码的签名值"}
}
}
}

```

示例5: 业务查询、下载公安部门下发数据接口示例

请求URL示例

请求方法: POST

请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:

```

{
"message_header": {
"syscode": "HBECS",
"authcode": "hjhjkja666sdfuualyydsa77654Ja",
"businesstype": "checkResult",
"sign": "1333D3DFAFSDFASDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
"version": "1.0"
"ctime": "1498627266000"
"random": "550e8400e29b41d4a716446655440000"
"hmac": "UbpybOGxk5JKTs8A5Sf18BOR/LRLe61W099NQHzUew4="},
"message_content": {
"taskCode ": "checkResult",
"version ": "1.0",
"taskTypeCode": "0",
"data": {"taskId ": "abcdefg123456"},
"signInfo": {
"signAlgorithm ": "1.2.156.10197.1.501",
"signValue ": "BASE64编码的签名值"}
}
}
}

```

业务返回报文:

```

{
"message_header": {
"businesstype": "checkResult ",
"syscode": "HBECS ",

```

```

"version": "1.0",
"errorCode": "1 ",
"errorInfo": "业务查询成功",
"message_content": {
"taskCode ": "checkResult",
"version ": "1.0",
"resultCode ": "0",
"resultCodeMsg ": "查询任务结果成功",
"taskTypeCode": "0",
"data": [{
"errorCode": "0",
"package": {
"yzbm": "印章编码",
"appSymKeyEnc": "BASE64 编码的应用维护对称密钥密文",
"dataSymKeyEnc": "BASE64 编码的数据加密对称密钥密文",
"encFile": "公安部门下发的加密文件"}
}]
}
}

```

示例6: 上传保护密钥更新信息接口示例

请求URL示例

请求方法: POST

请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:

```

{
"message_header": {
"syscode": "HBECS",
"authcode": "hjhjkja666sdfuuaUyydsa77654Ja",
"businesstype": "updateProtectKey",
"sign": "1333D3DFAFSDFASDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
"version": "1.0"
"ctime": "1498627266000"
"random": "550e8400e29b41d4a716446655440000"
"hmac": "Ubpyb0Gxk5JKTs8A5Sf18BOR/LRLe61W099NQHzUew4="},
"message_content": {
"taskCode ": "updateProtectKey",
"version ": "1.0",
"tokenInfo": "randomA+randomB",
"taskTypeCode": "1",
"data": [
{"yzbm": "印章编码",
"sealEncCert": " BASE64编码的电子印章加密证书",
"sealSignCert": " BASE64编码的电子印章签名证书",
"deviceCode ": "设备编码",
"encDeviceCode ": "BASE64编码的设备编码密文"},
{.....保护密钥更新信息列表....}
]
"signInfo": {
"signAlgorithm ": "1.2.156.10197.1.501",
"signValue ": " BASE64编码的签名值"}
}
}

```

业务返回报文:

```

{
"message_header": {
"businesstype": "updateProtectKey ",

```

```

"syscode": "HBECS",
"version": "1.0",
"errorCode": "1",
"errorInfo": "上传密钥更新信息成功",
"message_content": {
"taskCode": "updateProtectKey",
"version": "1.0",
"resultCode": "1",
"resultCodeMsg": "信息上传成功",
"taskTypeCode": "1",
"data": {"taskId": "abcdefg123456"},
"signInfo": {
"signAlgorithm": "1.2.156.10197.1.501",
"signValue": "BASE64编码的签名值"}
}

```

示例7：上传电子印章撤销接口示例

请求URL示例
 请求方法：POST
 请求URL：http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文：

```

{
"message_header": {
"syscode": "HBECS",
"authcode": "hjhjkja666sdfuualyydsa77654Ja",
"businessstype": "revocationSealInfo",
"sign": "1333D3DFAFSDFSADFASFDFASDF1234234213421ABSFADSFASDFASDF",
"version": "1.0",
"ctime": "1498627266000",
"random": "550e8400e29b41d4a716446655440000",
"hmac": "Ubpyb0Gxk5JKTs8A5Sf18B0R/LRLe61W099NQHHzUew4="},
"message_content": {
"taskCode": "revocationSealInfo",
"version": "1.0",
"tokenInfo": "randomA+randomB",
"taskTypeCode": "2",
"data": [{
"yzbm": "印章编码",
"deviceCode": "设备编码",
"encDeviceCode": "base64 编码的设备编码密文"},
{.....待撤销的印章设备编码列表.....}
],
"signInfo": {
"signAlgorithm": "1.2.156.10197.1.501",
"signValue": "BASE64编码的签名值"}
}
}

```

业务返回报文：

```

{
"message_header": {
"businessstype": "revocationSealInfo",
"syscode": "HBECS",
"version": "1.0",
"errorCode": "1",
"errorInfo": "电子印章撤销成功"},
"message_content": {

```

```

"taskCode ":"revocationSealInfo ",
"version":"1.0",
"resultCode ":"0",
"resultCodeMsg ":"信息上传成功",
"taskTypeCode":"2",
"data":{" taskId ":"abcdefg123456"},
"signInfo": {
"signAlgorithm ":"1.2.156.10197.1.501",
"signValue ":" BASE64编码的签名值"}
}

```

示例8: 申请电子印章唯一赋码接口示例

请求URL示例

请求方法: POST

请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:

```

{
"message_header":{
"syscode":"HBECS",
"authcode":"hjhjkja666sdfuuaUyydsa77654Ja",
"businesstype":"applySealCode",
"sign":"1333D3DFAFSDFASDFASDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
"version":"1.0"
"ctime": "1498627266000"
"random":550e8400e29b41d4a716446655440000"
"hmac":"UbpybOGxk5JKTs8A5Sf18BOR/LRLe61W099NQHZUew4="},
"message_content":{
"taskCode ":"applySealCode",
"version ":"1.0",
"tokenInfo":"randomA+randomB",
"taskTypeCode":"3",
"data": {"areaNumber": "110"}
"signInfo": {
"signAlgorithm ":"1.2.156.10197.1.501",
"signValue ":" BASE64编码的签名值"}
}
}

```

业务返回报文:

```

{
"message_header":{
"businesstype":"applySealCode",
"syscode":"HBECS ",
"version":"1.0",
"errorCode":"1 ",
"errorInfo":"申请电子印章唯一赋码成功"
},
"message_content":{
"taskCode ":"applySealCode",
"version ":"1.0",
"resultCode ":"1",
"resultCodeMsg ":"申请业务成功",
"taskTypeCode":"3",
"data":{
"sealCode ":"000000001",
}
"signInfo": {
"signAlgorithm ":"1.2.156.10197.1.501",

```

```

"signValue ":"BASE64编码的签名值"
}
}

```

示例9：确认回执接口示例

请求URL示例
请求方法：POST
请求URL：http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文：

```

{
"message_header":{
"syscode":"HBECS",
"authcode":"hjhjkja666sdfuuaUyydsa77654Ja",
"businesstype":"confirmReceipt",
"sign":"1333D3DFAFSDFASDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
"version":"1.0"
"ctime": "1498627266000"
"random":550e8400e29b41d4a716446655440000"
"hmac":"Ubpyb0Gxk5JKTs8A5Sf18B0R/LRLe61W099NQHwUew4="},
"message_content":{
"taskCode ":"confirmReceipt",
"version ":"1.0",
"tokenInfo":"randomA+randomB",
"taskTypeCode":"0或1",
"data": [
{"taskId ":"abcdefg123456",
"yzbm": "印章编码",
"deviceCode": "设备编码",
"encDeviceCode": "BASE64编码的设备编码密文" },
{.....确认信息列表.....}
],
"signInfo": {
"signAlgorithm":"1.2.156.10197.1.501",
"signValue":"BASE64编码的签名值"}
}
}

```

业务返回报文：

```

{
"message_header":{
"businesstype":"confirmReceipt",
"syscode":"HBECS ",
"version":"1.0",
"errorCode":"1 ",
"errorInfo":"确认回执成功"},
"message_content":{
"taskCode":"confirmReceipt",
"version":"1.0",
"tokenInfo":"randomA+randomB",
"taskTypeCode":"0或1",
"data": [
{"taskId ":"abcdefg123456",
"yzbm": "印章编码",
"deviceCode ": "设备编码",
"encDeviceCode ": "BASE64编码的设备编码密文"},
{.....确认信息列表.....}
]
}
}

```

```
}
}
```

示例10：身份认证接口示例

请求URL示例

请求方法：POST

请求URL：http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文：

```
{
  "message_header":{
    "syscode":"HBECS",
    "authcode":"hjhjkja666sdfuuaUyydsa77654Ja",
    "businesstype":"reciveAuthServer",
    "sign":"1333D3DFAFSDFSADFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
    "version":"1.0",
    "ctime":"1498627266000",
    "random":"550e8400e29b41d4a716446655440000",
    "hmac":"Ubpyb0Gxk5JKTs8A5Sf18BOR/LRLe61W099NQHZUew4="},
  "message_content":{
    "idA":"dcccscs",
    "random":"1234567890123456"}
}
```

业务返回报文：

```
{
  "message_header":{
    "businesstype":"reciveAuthServer",
    "syscode":"HBECS",
    "version":"1.0",
    "errorCode":"1",
    "errorInfo":"身份认证成功"},
  "message_content":{
    "result":"0",
    "msg":"请求成功",
    "token":"随机数、签名值和国家政务服务平台电子印章系统状态发布系统数字证书拼接的字符串"}
}
```

示例11：数据传输接口示例

请求URL示例

请求方法：POST

请求URL：http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文：

```
{
  "message_header":{
    "syscode":"HBECS",
    "authcode":"hjhjkja666sdfuuaUyydsa77654Ja",
    "businesstype":"msgCenterDoubleServer",
    "sign":"1333D3DFAFSDFSADFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
    "version":"1.0",
    "ctime":"1498627266000",
    "random":"550e8400e29b41d4a716446655440000",
    "hmac":"Ubpyb0Gxk5JKTs8A5Sf18BOR/LRLe61W099NQHZUew4="},
  "message_content":{
    "data":"MIICrzCCA1KgAwIBAgIIEQAQ/10oe78wDAYIKoEcz1UBg3UFADC BhzEfMBOGA1UECwwWRGV2ZWxvcG11bnQgRGVw
YXJ0bWVudDERMA8GA1UECgwIU2VjdXJpdHkxEDA0BgNVBAGMBOJ1aUppbmcxEDA0BgNVBACMBOJ1aUppbmcxZANBgNVBAMMBkdvb
WFpbjELMAkGA1UEBgcwQ04xDzANBgNVBAQMBkEwMDEwMTAeFw0xODEwMzAwNzE1MzJaFw0xOTEwMzAwNzE1MzJaMGMAxGDAWBgNVBA
MMD+Wcs0aWueWpkeW4g+S6jDEPMA0GA1UEBwwGMTAwMTAwMQ8wDQYDVQQIDAYxMTAwMDAxGTAxBGNVBAoMEDEwLjEwMC4xLjM1Ojg
```

```

30DcxCjAIBgNVBAsMATIwWTATBgqhkJOPQIBggqRzPVQGCLQNCAAQSc7kLOUXcuJOIVaWsm6+J5KLMbQvk9NaCivFwHvecOBqn
CGmSQW0IEYYqISOjuIqztN77ID3ALCAsLiLs74S8o4HIMIHFMAwGA1UdEwEB/wQCMAAwHQYDVROBBYEF0ZCzovdKgaO4VMX/PpCA
pnR05ZFMIGVbGwVHSMegY0wgYqAFDK5MKLB6jBw/tXLLljUzP32JhkvoW2kazBpMQ8wDQYDVQQLDAZHdW9CYW4xETAPBgNVBAoMCF
NlY3VyaXR5MRAwDgYDVQQIDAdCZW1KaW5nMRAwDgYDVQQHDAcCZW1KaW5nMRIwEAYDVQQDDA1HdW9CYW4gQ0ExCzAJBgNVBAYMAkN
OggMAAAAwDAYIKoEcz1UBG3UFAANJADBGAIeAriUOIaCh527GdryjRoJae7pg8SHCs4ppFVnbJO9sWfKCIQCdr38siAB+RW1xkVJ6
ONuM/4jJtRZ+zpsN4/Y+67H6wQ==||1234567890123457||{"taskCode":"209","taskData":{"invalidType":"\
"3","certStartTime":"","invalidEffectTime":"2018-09-20","signature":"","sealCreditCode\
":"Q20000039012312316","signCert":"","errorInfo":"","receiveTime":"2018-10-18 19:27:55\
","cancelDescribe":"挂失印章","sealName":"人社业务印章","creator":"","11","applyDate":"20
18-09-20","cancelReason":"1","certEndTime":"","sealCode":"2364107191015","taskId":"84
8b7658f58d4a72a0771c20c799113b","status":"-1"}}|AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAADGqH5
K3BCzDGgaNfCiM/SZxOLaxl+yT9NpRx9AcJoPRQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAB+6F9td2z7U6nsfi/+k1
3hCnypsE05yzVgCecjekri8=}
}

业务返回报文:
{
  "message_header":{
    "businessstype":"msgCenterDoubleServer",
    "syscode":"HBECS",
    "version":"1.0",
    "errorCode":"1",
    "errorInfo":"数据传输成功"
  },
  "message_content":{
    "success":"true"
  }
}

```

示例12: 获取 Token 接口示例

```

请求URL示例
请求方法: POST
请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:
{
  "message_header":{
    "syscode":"HBECS",
    "authcode":"hjhjkja666sdfuualyydsa77654Ja",
    "businessstype":"DB.oauth.token",
    "sign":"1333D3DFAFSDFASDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
    "version":"1.0",
    "ctime":"1498627266000",
    "random":"550e8400e29b41d4a716446655440000",
    "hmac":"Ubpyb0Gxk5JKTs8A5Sf18BOR/LRLe61W099NQHHzUew4="},
  "message_content":{
    "method":"DB.oauth.token",
    "username":"DBAdmin",
    "password":"50f009f32093b88a693573fb77bca6bb6a05b923",
    "client_id":"1000000",
    "client_secret":"448856e7fed3433eb0a5e4896a4179d1",
    "grant_type":"password",
    "version":"1.0",
    "timestamp":"20181031163733"
  }
}

业务返回报文:
{
  "message_header":{

```



```

"businesstype": "DB. oauth. token ",
"syscode": "HBECS ",
"version": "1.0",
"errorCode": "1 ",
"errorInfo": "获取Token成功",
"message_content": {
"method": "DB. oauth. token",
"requestId": "9e100afd-3f7e-4f55-aaee-7alf9bce71c8",
"code": 0,
"data": [
{"access_token": "dfb7a692-7e98-48bb-97da-6d3ccc97fd97",
"token_type": "bearer",
"expires_in": 28799,
"scope": "server"}
],
"message": "调用接口成功"
}
}

```

示例13：注册用户印章状态查询接口

请求URL示例
 请求方法：POST
 请求URL：http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文：

```

{
"message_header": {
"syscode": "HBECS",
"authcode": "hjhjkja666sdfuuaUyydsa77654Ja",
"businesstype": "DB. seal. status. query ",
"sign": "1333D3DFAFSDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
"version": "1.0",
"ctime": "1498627266000",
"random": "550e8400e29b41d4a716446655440000",
"hmac": "UbpYb0Gxk5JKTs8A5Sf18BOR/LRLe61W099NQHzUew4="},
"message_content": {
"appKey": "1000000",
"format": "json",
"method": "DB. seal. status. query",
"queryTime": "2018-08-06 02:14:04",
"sealCode": "3304060000002",
"sealName": "111",
"sign": "F82C421FC286ABF1719F957DA053CB55",
"timestamp": "20181101203409",
"token": "17964625-afbc-424e-bf30-a9c33989916a",
"type": "sync",
"username": "DBAdmin",
"version": "1.0"}
}

```

业务返回报文：

```

{
"message_header": {
"businesstype": "DB. seal. status. query ",
"syscode": "HBECS ",
"version": "1.0",
"errorCode": "1 ",
"errorInfo": "印章状态查询成功"},

```

```

"message_content":{
"method": "DB. seal. status. query",
"requestId": "9e100afd-3f7e-4f55-aaee-7alf9bce71c8",
"code": 0,
"data": [
{"sealName": "测试章",
"queryTime": "2020-05-05 00:00:00",
"sealStatus": "1"}
],
"message": "调用[印章状态查询接口]成功!"
}

```

示例14：非注册用户印章状态查询接口示例

请求URL示例
 请求方法：POST
 请求URL：http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文：

```

{
"message_header":{
"syscode":"HBECS",
"authcode":"hjhjkja666sdfuuaUyydsa77654Ja",
"businessstype":"DB. seal. status. query ",
"sign":"1333D3DFAFSDFASDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
"version":"1.0",
"ctime": "1498627266000",
"random":"550e8400e29b41d4a716446655440000",
"hmac":"Ubpyb0Gxk5JKTs8A5Sf18BOR/LRLe61W099NQHHzUew4="},
"message_content":{
"format":"json",
"method":"DB. seal. status. query",
"queryTime":"2018-08-06 02:14:04",
"sealCode":"3304060000002",
"sealName":"111",
"sign":"4CA052663B21D4D6D75AB824F788EB96",
"timestamp":"20181101203407",
"type":"sync",
"version":"1.0"}
}

```

业务返回报文：

```

{
"message_header":{
"businessstype":"DB. seal. status. query ",
"syscode":"HBECS ",
"version":"1.0",
"errorCode":"1",
"errorInfo":"印章状态查询成功"},
"message_content":{
"method": "DB. seal. status. query",
"requestId": "9e100afd-3f7e-4f55-aaee-7alf9bce71c8",
"code": 0,
"data": [
{"sealName": "测试章",
"queryTime": "2020-05-05 00:00:00",
"sealStatus": "1"}
],
"message": "调用[印章状态查询接口]成功!"
}

```

}

示例15：印章吊销查询接口

请求URL示例

请求方法：POST

请求URL：http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文：

```
{
  "message_header":{
    "syscode":"HBECS",
    "authcode":"hjhjkja666sdfuuaUyydsa77654Ja",
    "businesstype":"DB. seal. deactivate. list. query ",
    "sign":"1333D3DFAFSDFASDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
    "version":"1.0",
    "ctime": "1498627266000",
    "random":"550e8400e29b41d4a716446655440000",
    "hmac":"Ubyyb0Gxk5JKTs8A5Sf18BOR/LRL61W099NQH4Uew4="},
  "message_content":{
    "appKey":"1000000",
    "format":"json",
    "method":"DB. seal. deactivate. list. query",
    "pageNow":"1",
    "pageSize":"10",
    "queryEndTime":"2019-01-01 00:00:00",
    "queryStartTime":"2015-01-01 00:00:00",
    "sign":"8A502136325C3CF46C53794CFAAAB902",
    "timestamp":"20181101204023",
    "token":"17964625-afbc-424e-bf30-a9c33989916a",
    "type":"sync",
    "username":"DBAdmin",
    "version":"1.0"}
}
```

业务返回报文：

```
{
  "message_header":{
    "businesstype":"DB. seal. deactivate. list. query",
    "syscode":"HBECS ",
    "version":"1.0",
    "errorCode":"1 ",
    "errorInfo":"印章吊销查询成功"
  },
  "message_content":{
    "method": " DB. seal. deactivate. list. query ",
    "requestId": "9e100afd-3f7e-4f55-aaee-7alf9bce71c8",
    "code": 0,
    "data": [
      {"version": "V1.0",
        "invalidEffectTime": "2018-05-29 17:04:36",
        "nextUpdateTime": "2018-06-29 17:04:36",
        "signature": "wdwqweqwewl1dqw=",
        "signAlgorithm": "SM2",
        "signHashAlgorithm":"SM3",
        "secretKey": "JKJDKAJDKAJKJAKAD",
        "awardCompany": "国家电子政务服务平台",
        "revocationList": [
          {"sealCode": "1234567890123456789",
```

```

"sealName": "测试章1",
"revocationTime": "2018-05-08 00:00:00"},
{"sealCode": "12345671012345678",
"sealName": "测试章2",
"revocationTime": "2018-05-08 00:00:00"},
{"sealCode": "123456713123456789",
"sealName": "测试章3",
"revocationTime": "2018-05-08 00:00:00"}
],
"total": "10",
"size": "3"}
],
"message": "调用[印章吊销列表获取]接口成功!"
}

```

示例16: 印章注册接口示例

请求URL示例
请求方法: POST
请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:

```

{
"message_header":{
"syscode":"HBECS",
"authcode":"hjhjkja666sdfuuaUyydsa77654Ja",
"businessstype":"applySeal ",
"sign":"1333D3DFAFSDFASDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
"version":"1.0",
"ctime": "1498627266000",
"random":"550e8400e29b41d4a716446655440000",
"hmac":"Ubpyb0Gxk5JKTs8A5Sf18B0R/LRLe61W099NQHHzUew4="},
"message_content":{
"sealName":"122"
"templateName":"se_name",
"photoData":"1232312312adfasfsdfasdfsdfsafsaf",
"certDN":"cn=test, OU=xxx, C=CN"}
}

```

业务返回报文:

```

{
"message_header":{
"businessstype":" applySeal",
"syscode":"HBECS ",
"version":"1.0",
"errorCode":"1",
"errorInfo":"印章注册成功"},
"message_content":{}
}

```

示例17: 印章获取接口示例

请求URL示例
请求方法: POST
请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:

```

{
"message_header":{
"syscode":"HBECS",
"authcode":"hjhjkja666sdfuuaUyydsa77654Ja",

```

```

"businesstype": "getSeal ",
"sign": "1333D3DFAFSDFSADFASFDASDFSADFASDF1234234213421ABSFADSFASDFSADF",
"version": "1.0",
"ctime": "1498627266000",
"random": "550e8400e29b41d4a716446655440000",
"hmac": "UbpybOGxk5JKTs8A5Sf18BOR/LRLe61W099NQHzUew4=",
"message_content": {
"certDN": "证书DN"
}
}

```

业务返回报文:

```

{
"message_header": {
"businesstype": " getSeal",
"syscode": "HBECS ",
"version": "1.0",
"errorCode": "1 ",
"errorInfo": "印章获取成功",
"message_content": {
"Seal": "印章信息base64编码"}
}
}

```

示例18: 印章状态查询接口示例

请求URL示例

请求方法: POST

请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:

```

{
"message_header": {
"syscode": "HBECS",
"authcode": "hjhjkja666sdfuuaUyydsa77654Ja",
"businesstype": "getSealStatus",
"sign": "1333D3DFAFSDFSADFASFDASDFSADFASDF1234234213421ABSFADSFASDFSADF",
"version": "1.0",
"ctime": "1498627266000",
"random": "550e8400e29b41d4a716446655440000",
"hmac": "UbpybOGxk5JKTs8A5Sf18BOR/LRLe61W099NQHzUew4=",
"message_content": {
"certDN": "证书DN"
}
}
}

```

业务返回报文:

```

{
"message_header": {
"businesstype": " getSealStatus ",
"syscode": "HBECS ",
"version": "1.0",
"errorCode": "1 ",
"errorInfo": "印章状态获取成功"},
"message_content": {
"SealStatus": "0-不可用1-可用"}
}
}

```

示例19: 签章验证接口示例

请求URL示例

请求方法: POST

请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:

```
{
  "message_header":{
    "syscode":"HBECS",
    "authcode":"hj hjk ja666sdfuuaUyydsa77654Ja",
    "businesstype":"verifyFile",
    "sign":"1333D3DFAFSDFASDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
    "version":"1.0",
    "ctime": "1498627266000",
    "random":"550e8400e29b41d4a716446655440000",
    "hmac":"Ubpyb0Gxk5JKTs8A5Sf18B0R/LRLe61W099NQHHzUew4="},
  "message_content":{
    "data":"PDF、OFD文件数据base64编码"}
}
```

业务返回报文:

```
{
  "message_header":{
    "businesstype":"verifyFile",
    "syscode":"HBECS ",
    "version":"1.0",
    "errorCode":"1 ",
    "errorInfo":"签章验证成功"
  },
  "message_content":{
    "verifySealResults": [
      {"status": "true",
        "info": "null",
        "sealId": "273dacbd-aa94-4165-8aad-f62e0fb918a9",
        "sealName": "wang123",
        "certDN": "0=人力资源社会保障部信息中心, CN=ESM_Sign, C=CN"}
    ]
  }
}
```

示例20: 位置签章接口示例

请求URL示例

请求方法: POST

请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:

```
{
  "message_header":{
    "syscode":"HBECS",
    "authcode":"hj hjk ja666sdfuuaUyydsa77654Ja",
    "businesstype":" positionSealSign",
    "sign":"1333D3DFAFSDFASDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
    "version":"1.0",
    "ctime": "1498627266000",
    "random":"550e8400e29b41d4a716446655440000",
    "hmac":"Ubpyb0Gxk5JKTs8A5Sf18B0R/LRLe61W099NQHHzUew4="},
  "message_content":{
    "data":"待签文件数据base64编码",
    "signList":[{
      "pageNum": "页号 整数",
      "zx": "左上坐标X",

```

```

"zy": "左上坐标Y",
"sealId": "印章ID",
"certDN": "签名服务器公钥证书DN项, 根据具体服务器填写, 可为空",
"secretKey": "签名服务器密钥索引, 根据具体服务器填写, 可为空",
"keyPin": "签名服务器密钥索引保护PIN, 根据具体服务填写, 可为空",
{.....}
],
"BIZNUM": "业务编号, 为空时系统自动生成, 整个文档业务编号唯一"}
}
}

```

业务返回报文:

```

{
"message_header":{
"businesstype":" positionSealSign ",
"syscode":"HBECS ",
"version":"1.0",
"errorCode":" 1 ",
"errorInfo":"位置签章成功"},
"message_content":{
"signedData": "签章后的文件, 按base64编码"}
}

```

示例21: 关键字签章接口示例

请求URL示例
 请求方法: POST
 请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:

```

{
"message_header":{
"syscode":"HBECS",
"authcode":"hjhjkja666sdfuualyydsa77654Ja",
"businesstype":"keyWordSealSign",
"sign":"1333D3DFAFSDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
"version":"1.0",
"ctime": "1498627266000",
"random":"550e8400e29b41d4a716446655440000",
"hmac":"Ubpyb0Gxk5JKTs8A5Sf18BOR/LRLe61W099NQHZUew4="},
"message_content":{
data:待签文件数据base64编码
signList:[{
"keyword": "盖章关键字",
"keywordModel: 关键字类型(1:首个,0:末个,-1:全部,-:区间,,:自定义页号) ",
"sealId": "传入该页文档所使用的印章ID",
"certDN": "签名服务器公钥证书DN项, 根据具体服务器填写, 可为空",
"secretKey": "签名服务器密钥索引, 根据具体服务器填写, 可为空",
"keyPin": "签名服务器密钥索引保护PIN, 根据具体服务填写, 可为空",
{.....}],
"BIZNUM": "业务编号, 为空时系统自动生成, 整个文档业务编号唯一"}
}
}

```

业务返回报文:

```

{
"message_header":{
"businesstype":" keyWordSealSign ",
"syscode":"HBECS ",

```

```

"version": "1.0",
"errorCode": "1 ",
"errorInfo": "关键字签章成功",
"message_content": {
"signedData": "签章后的PDF文件, 按base64编码"}
}

```

示例22: 骑缝章接口示例

请求URL示例
请求方法: POST
请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:

```

{
"message_header": {
"syscode": "HBECS",
"authcode": "hjhjkja666sdfuuaUyydsa77654Ja",
"businesstype": "pagingSealSign ",
"sign": "1333D3DFAFSDFASDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
"version": "1.0",
"ctime": "1498627266000",
"random": "550e8400e29b41d4a716446655440000",
"hmac": "Ubpyb0Gxk5JKTs8A5Sf18B0R/LRLe61W099NQHHzUew4="},
"message_content": {
"data": "待签文件数据base64编码"
"signList": [{
"sealId: 传入该页文档所使用的印章ID,
page: 骑缝页数,
y: 骑缝章Y坐标,
"certDN": "签名服务器公钥证书DN项, 根据具体服务器填写, 可为空",
"secretKey": "签名服务器密钥索引, 根据具体服务器填写, 可为空",
"keyPin": "签名服务器密钥索引保护PIN, 根据具体服务填写, 可为空",
{.....}],
"PBIZNUM": "业务编号, 为空时系统自动生成, 整个PDF业务编号唯一"}
}

```

业务返回报文:

```

{
"message_header": {
"businesstype": " pagingSealSign",
"syscode": "HBECS ",
"version": "1.0",
"errorCode": "1 ",
"errorInfo": "骑缝签章成功"},
"message_content": {
signedData: "签章后的PDF文件, 按base64编码"}
}

```

示例23: 电子证照锁定签名接口示例

请求URL示例
请求方法: POST
请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:

```

{
"message_header": {
"syscode": "HBECS",
"authcode": "hjhjkja666sdfuuaUyydsa77654Ja",
"businesstype": " lockSign ",

```



```

"sign": "1333D3DFAFSDFSADFASFDASDFASDF1234234213421ABSFADSFASDFASDF",
"version": "1.0",
"ctime": "1498627266000",
"random": "550e8400e29b41d4a716446655440000",
"hmac": "UbpybOGxk5JKTs8A5Sf18BOR/LRLe61W099NQHzUew4=",
"message_content": {
"data": "待签文件数据base64编码",
"certDN": "签名服务器公钥证书DN项, 根据具体服务器填写, 可为空",
"secretKey": "签名服务器密钥索引, 根据具体服务器填写, 可为空",
"keyPin": "签名服务器密钥索引保护PIN, 根据具体服务器填写, 可为空",
"BIZNUM": "业务编号, 为空时系统自动生成, 整个OFD业务编号唯一"}
}

```

业务返回报文:

```

{
"message_header": {
"businesstype": "lockSign",
"syscode": "HBECS",
"version": "1.0",
"errorCode": "1",
"errorInfo": "锁定签名成功"},
"message_content": {
"signedData": "签名后的文件, 按base64编码"}
}

```

示例24: 电子证照删除锁定签名接口示例

请求URL示例

请求方法: POST

请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:

```

{
"message_header": {
"syscode": "HBECS",
"authcode": "hjhjkja666sdfuuaUyydsa77654Ja",
"businesstype": "delLockSign",
"sign": "1333D3DFAFSDFSADFASFDASDFASDF1234234213421ABSFADSFASDFASDF",
"version": "1.0",
"ctime": "1498627266000",
"random": "550e8400e29b41d4a716446655440000",
"hmac": "UbpybOGxk5JKTs8A5Sf18BOR/LRLe61W099NQHzUew4=",
"message_content": {
"data": "待操作文件数据base64编码",
"BIZNUM": "业务编号, 为空时系统自动生成, 整个OFD业务编号唯一"}
}
}

```

业务返回报文:

```

{
"message_header": {
"businesstype": "delLockSign",
"syscode": "HBECS",
"version": "1.0",
"errorCode": "1",
"errorInfo": "删除锁定签名成功"},
"message_content": {
"signedData": "删除锁定签名后的OFD文件, 按base64编码"}
}

```

示例25: 电子证照签章并锁定签名接口示例

请求URL示例

请求方法: POST

请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:

```
{
  "message_header":{
    "syscode":"HBECS",
    "authcode":"hjhjkja666sdfuuaUyydsa77654Ja",
    "businesstype":" signAndLockSign ",
    "sign":"1333D3DFAFSDFASDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
    "version":"1.0"
    "ctime": "1498627266000",
    "random":"550e8400e29b41d4a716446655440000"
    "hmac":"Ubpyb0Gxk5JKTs8A5Sf18B0R/LRLe61W099NQHHzUew4="},
  "message_content":{
    "data": "待签章电子证照文件",
    "signList":[{
      "sealId": "传入该页文档所使用的印章ID",
      "page": "签章页数",
      "zx": "签章左上X坐标",
      "zy": "签章左上Y坐标",
      "certDN": "签名服务器公钥证书DN项, 根据具体服务器填写, 可为空",
      "secretKey": "签名服务器密钥索引, 根据具体服务器填写, 可为空",
      "keyPin": "签名服务器密钥索引保护PIN, 根据具体服务填写, 可为空"
      "ismain": "是否作为锁定签名证书"},
    {.....}]
    "BIZNUM": " 业务编号, 为空时系统自动生成, 整个OFD业务编号唯一"
  }
}
```

业务返回报文:

```
{
  "message_header":{
    "businesstype":" signAndLockSign",
    "syscode":"HBECS ",
    "version":"1.0",
    "errorCode":"1 ",
    "errorInfo":"签章及锁定签名成功"},
  "message_content":{
    "signedData": "签章及锁定签名后的OFD文件, 按base64编码"
  }
}
```

示例26: 电子证照验签接口示例

请求URL示例

请求方法: POST

请求URL: http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文:

```
{
  "message_header":{
    "syscode":"HBECS",
    "authcode":"hjhjkja666sdfuuaUyydsa77654Ja",
    "businesstype":" verifyEleSign ",
    "sign":"1333D3DFAFSDFASDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
    "version":"1.0",
    "ctime": "1498627266000",
    "random":"550e8400e29b41d4a716446655440000",
    "hmac":"Ubpyb0Gxk5JKTs8A5Sf18B0R/LRLe61W099NQHHzUew4="},
}
```

```

"message_content":{
"data": "待验证电子证照文件"
"isSingle": "是否只返回第一个校验不通过的签章校验信息，false则验证所有"
"BIZNUM": "业务编号，为空时系统自动生成，整个文档业务编号唯一"}
}

```

业务返回报文：

```

{
"message_header":{
"businesstype": "verifyEleSign",
"syscode": "HBECS ",
"version": "1.0",
"errorCode": "1 ",
"errorInfo": "验证成功"},
"message_content":{
"verifySealResults": [
{"status": "true",
"info": "null",
"sealId": "273dacbd-aa94-4165-8aad-f62e0fb918a9",
"sealName": "wang123",
"certDN": "0=人力资源社会保障部信息中心, CN=ESM_Sign, C=CN"}
]
}
}

```

示例27：电子证照加注并锁定签名接口示例

请求URL示例

请求方法：POST

请求URL：http://域名或IP:端口号/seal/v1/electricSeal

业务请求报文：

```

{
"message_header":{
"syscode": "HBECS",
"authcode": "hjhjkja666sdfuuaUyydsa77654Ja",
"businesstype": "watermarkAndLockSign",
"sign": "1333D3DFAFSDFASDFASDFASDF1234234213421ABSFADSFASDFASDF",
"version": "1.0",
"ctime": "1498627266000",
"random": "550e8400e29b41d4a716446655440000",
"hmac": "UbpybOGxk5JKTs8A5Sf18BOR/LRLe61W099NQHzUew4="},
"message_content":{
"data": "待加注文件数据base64编码",
"certDN": "签名服务器公钥证书DN项，根据具体服务器填写，可为空",
"secretKey": "签名服务器秘钥索引，根据具体服务器填写，可为空",
"keyPin": "签名服务器秘钥索引保护PIN，根据具体服务填写，可为空"
"copyCreator": "加注件作者",
"copyCause": "加注内容",
"year": "加注有效年限从当前日期开始，整数类型",
"BIZNUM": "业务编号，为空时系统自动生成，整个文档业务编号唯一"}
}

```

业务返回报文：

```

{
"message_header":{
"businesstype": "watermarkAndLockSign",
"syscode": "HBECS ",
"version": "1.0",

```

```
"errorCode": "1",  
"errorInfo": "加注并锁定签名成功",  
"message_content": {  
"signedData": "加注及锁定签名后的OFD文件, 按base64编码"}  
}
```

参 考 文 献

- [1] GB/T 32905—2016 信息安全技术 SM3密码杂凑算法
 - [2] GB/T 32918(所有部分) 信息安全技术 SM2椭圆曲线公钥密码算法
 - [3] GB/T 35291—2017 信息安全技术智能密码钥匙应用接口规范
-