

DB36

江西省地方标准

DB36/T 1349—2020

统一电子印章平台应用接入技术规范

Unified electronic seal platform application access technical specification

XXXX—XX—XX 发布

XXXX—XX—XX 实施

江西省市场监督管理局

发布

目 次

目 次	I
前 言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 电子印章平台接入概述	3
5 电子印章平台接入流程	4
6 电子印章平台接入通用要求	6
7 电子印章平台接口调用	7
附 录 A （规范性附录） 获取电子印章信息接口说明	8
附 录 B （规范性附录） 签章接口说明	10
附 录 C （规范性附录） 验章接口说明	13

前 言

本文件按照GB/T 1.1-2020《标准化工作导则第1部分：标准的结构和编写》给出的规则编制。

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。

本文件由江西省发展和改革委员会提出并归口。

本文件起草单位:江西省信息中心。

本文件起草人:杜军龙、孙杨、鲁战利、黄振、侯文刚、王伟、王均传、王鑫。

统一电子印章平台应用接入技术规范

1 范围

本文件规定了省统一电子印章平台（以下简称电子印章平台）的概述、接口说明和接入流程。

本文件适用于全省各级政府部门政务服务系统（以下简称政务服务系统）与电子印章平台对接技术实现。

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，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式
GB/T 32905 信息安全技术 SM3密码杂凑算法
GB/T 32918(所有部分) 信息安全技术 SM2椭圆曲线公钥密码算法
GM/T 0031-2014 安全电子签章密码技术规范
C0118-2019 国家政务服务平台统一电子印章 总体技术架构
C0119-2019 国家政务服务平台统一电子印章 签章技术要求
C0120-2019 国家政务服务平台统一电子印章 印章技术要求
C0121-2019 国家政务服务平台统一电子印章 接入测试方法
C0122-2019 国家政务服务平台统一电子印章 系统接口要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

电子印章应用系统 `electronic seal application system`

具有签章或验章功能的系统或软件的统称。

3.2

电子印章 `electronic seal`

电子印章以先进的数字技术模拟传统实物印章，其管理、使用方式符合实物印章的习惯和体验，其加盖的电子文件具有与实物印章加盖的纸张文件相同的外观、相同的有效性和相似的使用方式。

3.3

印章信息 `seal information`

通过统一社会信用代码获取到归属于该统一社会信用代码下的印章信息列表，包含：印章编码、印章名称、印章类型、印章状态、印章base64转码数据等。

3.4

印章名称 seal name

印章在电子印章服务器中存储的唯一名称。

3.5

印章编码 seal code

印章在国家平台备案后由国家平台赋予的唯一编码，存储在印章服务器中。

3.6

印章状态 seal status

印章在服务器中存储的状态，包含：已删除、未制作、已冻结和正常。

3.7

印章类型 seal type

印章包含6中类型，分别为：电子法定名称章、电子财务专用章、电子发票专用章、电子合同专用章、电子名章、业务专用章。

3.8

对称密钥 symmetric key

对称密钥加密又叫专用密钥加密或共享密钥加密，即发送和接收数据的双方必使用相同的密钥对明文进行加密和解密运算。

3.9

电子印章印文图像数据 electronic seal print image

电子印章的不含辅助识别特征的印文图像数据。

3.10

证书认证机构 certificate authority

对数字证书进行全生命周期管理的实体，也称为电子认证服务机构。本标准中是指由国家认可的，具有权威性、可信性和公正性的证书认证机构（CA）。

3.11

数字证书 digital certificate

由证书认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。

3.12

SM2 算法 SM2 cryptographic algorithm

由GB/T 32918(所有部分)定义的一种算法。

4 电子印章平台接入概述

4.1 系统接入架构

电子印章平台对接国家政务服务平台统一电子印章平台,为全省的各级政府部门提供统一的电子印章制发、电子印章应用服务。电子印章平台接入架构见图1。



图1 接入架构示意图

4.2 电子印章平台组成

电子印章平台由电子印章制作系统、电子印章状态发布系统、电子印章应用系统、电子印章应用服务接口组成，具体描述如下：

- 电子印章制作系统提供电子印章制作的相关服务，部署在省电子政务云平台；
- 电子印章状态发布系统提供电子印章状态发布、查询、下载及变更服务；
- 电子印章应用系统实现电子印章签章、验章等相关服务；
- 电子印章应用系统提供电子印章客户端软件，支持对PDF或OFD格式的版式文件进行签章或验章；
- 电子印章应用服务接口包括电子印章信息获取、文件签章、文件验章接口，提供给第三方系统调用。

4.3 电子印章平台功能对接

4.3.1 获取印章信息

业务调用方通过appid、salt和单位的统一社会信用代码等参数信息，详见附录A（规范性附录）获取电子印章信息接口说明，可获取印章信息，印章信息中包含印章编码、印章名称、印章图片数据、印章状态等，以json格式返回。

4.3.2 签章

签章的模式主要分为分散式和集中式两种，电子印章使用主体可根据自身情况选择采用哪种模式：

- a) 分散式用章：电子印章存储在电子印章使用主体的智能密码钥匙中，电子印章使用主体使用电子印章客户端软件对 PDF 或 OFD 格式的版式文件进行签章或验章，并可完成离线或在线电子签章和验章操作；
- b) 集中式用章：业务系统通过调用发布在省电子政务共享数据统一交换平台的服务接口，向电子印章平台发送 PDF 或 OFD 格式的版式文件，或指定版式文件路径、印章标识、签章页面、签章位置坐标，电子印章平台完成对该版式文件的签章操作，并返回签署后的版式文档给业务系统。

4.3.3 验章

业务系统通过调用接口，向电子印章平台发送 PDF 或 OFD 格式的版式文件，电子印章平台对文档进行验章，并将验签结果返回给对接业务系统。

5 电子印章平台接入流程

5.1 总体流程

电子印章平台接入流程示意图，见图2。

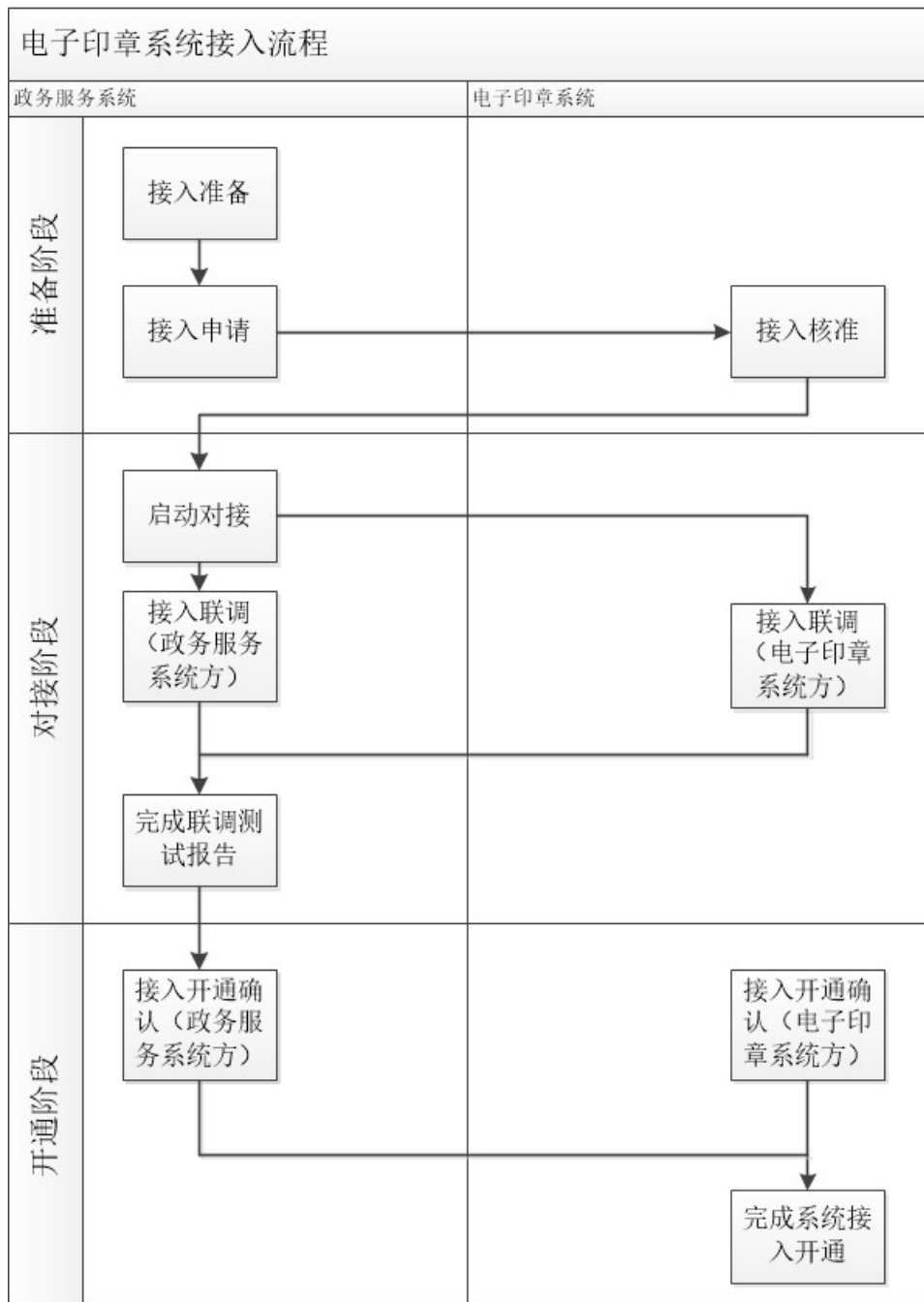


图2 电子印章平台接入流程示意图

5.2 接入准备

各级政府部门政务服务系统应开通网络安全策略，保证和电子印章平台网络互通。

5.3 接入申请

访问省电子政务共享数据统一交换平台申请接口权限。

5.4 接入核准

开设对接部门的appid和salt，禁止泄露调用印章服务接口所需的appid和salt，确保只在调用印章服务接口的后台服务中配置appid和salt。

5.5 启动对接

各级政府部门政务服务系统根据《江西省统一电子印章平台接入规范》进行对接，调用电子印章平台盖章接口实现对在线文档加盖电子印章。

5.6 接入联调

各级政府部门政务服务系统与电子印章平台完成接入联调，由对接系统建设方对电子印章平台的盖章和验证等功能进行测试。

印章制作单位根据提交的申请材料开通电子印章服务接口的使用授权，交付接口指引与授权使用信息给电子印章使用单位。

5.7 接入开通

各级电子印章平台建设方、各级政府部门政务服务系统和电子印章平台三方共同确认完成系统接入准备工作，正式开通电子印章各项服务功能，电子印章使用单位技术人员把业务系统发布到生产环境。

6 电子印章平台接入通用要求

6.1 申领电子印章

电子印章的申领流程如下图：

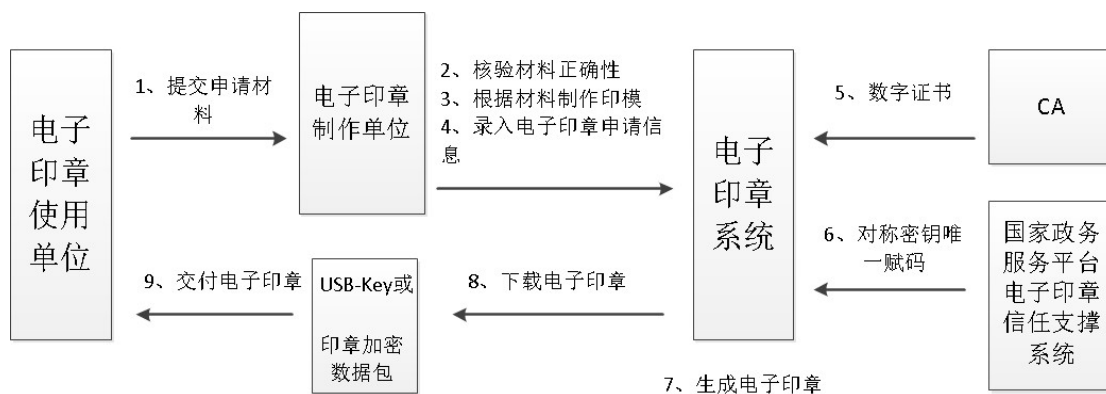


图3 申领流程示意图

流程说明

- c) 电子印章使用单位向电子印章制作单位提交申领材料；
- d) 电子印章制作单位核验申领材料正确性；
- e) 电子印章制作单位根据提交的申领材料制作电子印章印文图像，印文图像规格和样式在 1:1 打印下应遵循实物印章有关规定和标准；
- f) 电子印章制作单位登录电子印章平台根据申请单位提交的材料，录入提交电子印章申请信息，包括：单位统一社会信用代码、单位行政区划码、单位类型（国家行政机关或事业单位）、单位名称、单位地址、经办人姓名、经办人公民身份号码、经办人手机号码、印章名称、实物印章直径、电子印章印文图像；

- g) 由 CA 机构为电子印章颁发数字证书（一个数字证书对应一枚电子印章）；
- h) 通过省统一电子印章平台从国家政务服务平台电子印章信任支撑系统获取电子印章唯一赋码、公安对称密钥、公安印章信息，并完成印章备案；
- i) 电子印章平台根据申请材料生成电子印章；
- j) 电子印章制作单位下载制作完成的电子印章；
- k) 电子印章制作单位向电子印章使用单位交付电子印章。

7 电子印章平台接口调用

7.1 总则

电子印章平台接口API按照HTTP接口方式，UTF-8编码，通过HTTP协议的GET方法或POST方法提交请求。使用GET方法，请求参数通过URL查询参数（QueryParam）提供。使用POST方法，请求公共参数通过URL查询参数（QueryParam）提供，接口专用参数通过请求正文（Body）、按照json格式封装提供。

7.2 接口主要功能

- 7.2.1 获取印章信息接口：通过统一社会信用代码可获取该代码下所有印章的印章信息。
- 7.2.2 签章接口：通过 sealCode（印章编号）对 PDF/OFD 文档进行签章。
- 7.2.3 验章接口：对文档加盖的印章进行合法有效的验证。

7.3 接口调用

7.3.1 获取印章信息接口

步骤如下：

- 接口调用方根据电子印章平台提供的 appid，生成随机数；
- 把随机数和 salt 组合后取摘要并进行 base64 转码生成 checkcode 码；
- 再把 appid、checkcode、keysn（统一社会信用代码）以 json 格式封装；
- 把封装的参数传给签章应用系统调用获取印章信息接口获取该 keysn 下全部印章信息；
- 获取印章信息接口见附录 A 表 A。

7.3.2 签章接口

步骤如下：

- 通过获取印章信息接口获取 keysn 下全部印章信息；
- 通过印章信息中 sealstatus（印章状态）和 sealname（印章名称）筛选指定的 sealcode（印章编号）；
- 再把 sealcode、checkcode、需要盖章的页码以及盖章定位以 json 格式封装；
- 把封装的参数传给签章应用系统调用签章接口实现签章操作；
- 签章接口见附录 B 表 B。

7.3.3 验章接口

步骤如下：

- 接口调用方根据电子印章平台提供的 appid，生成随机数；
- 把随机数和 salt 组合后加密生成 checkcode 码；
- 再把 appid、checkcode、盖章文档传给签章应用系统调用验章接口实现签章操作；
- 验章接口见附录 C 表 C。

附 录 A
(规范性附录)
获取电子印章信息接口说明

获取电子印章信息接口表见表A。

表 A 获取电子印章信息接口表

服务名称	获取电子印章信息			
方法说明	通过统一社会信用代码可获取该代码下所有印章的印章信息			
请求方法	POST			
URL 地址	\$host/api/getSeals			
请求头	参数名	必选	值	描述
	host	是	\$host/api/getSeals	
	content-type	是	application/json	
	content-length	否	包体总长度	请求的包体大小
输入参数	参数名	必选	类型范围	说明
	appid	是	String	接入项目的唯一标识，在应用管理中获取
	randomN	是	String	由获取随机数接口获取到的随机数字符
	checkCode	是	String	随机数+salt 的 SHA256 摘要值，base64 编码
	unifiedSocialCreditCode	是	String	单位企业统一社会信用代码
	appid	是	String	接入项目的唯一标识，在应用管理中获取
输出参数	参数名		类型	描述
	code		String	错误码
	message		String	错误描述
	items		Array(item)	印章列表

表 A 获取电子印章信息接口表（续）

	参数名	类型	描述
items 说明	sealCode	String	印章编码
	sealName	String	印章名称
	width	int	印章宽度
	height	int	印章高度
	startTime	String	生效日期
	endTime	String	失效日期
	sealData	byte[]	印章图片数据
	sealStatus	String	印章状态：-1：已删除, 0：未制作, 1：正常, 2：已冻结
	错误码	返回值	对应说明
0		正常	
1		参数 appid 不能为空!	
2		参数 unifiedSocialCreditCode 不能为空!	
3		授权码未发放	
4		授权码已禁用	
5		checkCode 验证不一致	
请求示例	POST http://{API_ROOT}/api/getSeals Content-Type: application/json <pre>{ "appid":appid, "unifiedSocialCreditCode":keysn, "randomN":randomN, "checkCode":checkCode }</pre>		
返回示例	<pre>{ "code": 0, "message": "OK", "items": [{"sealCode": "36010000002588", "sealName": "赣江新区行政审批局。", "width": 42, "height": 42, "sealType": "1", "storeType": "1", "startTime": "2020-06-10 16:41:33", "endTime": "2023-06-10 16:41:33", "sealStatus": "1", "sealData": sealData; "keysn": "11360000MB1A12045P"}] }</pre>		

附 录 B
(规范性附录)
签章接口说明

签章接口表见表B

表 B 签章接口表

服务名称	签章			
方法说明	通过印章编号对版式文档进行签章			
请求方法	POST			
URL 地址	\$host/api/stampSeal			
请求头	参数名	必选	值	描述
	host	是	\$host/api/stampSeal	
	content-type	是	multipart/form-data	
输入参数	参数名	必选	类型范围	说明
	appid	是	String	授权码，在应用管理中获取
	randomN	是	String	由获取随机数接口获取到的随机数字符
	checkCode	是	String	randomN+盐值的 SHA256 摘要值，base64 编码
	orderId	是	String	业务系统生成的业务号，同一业务系统号下，所有业务号的编号必选唯一
	title	是	String	文档标题，方便以后查询使用
	file	是	byte[]	文件内容
	fileType	是	String	文档类型：PDF、OFD
	signList	是	Array(item)	签章信息，json 数组
	certContext	否	String	证书内容，base64 编码
	signAlgorithm	否	String	签名算法 oid: 1.2.156.10197.1.501

表 B 签章接口表 (续)

输入参数	signatureValue	否	String	SM2 带公钥签名, 格式: 64 个字节, base64 编码返回。 需签名的内容: appid+ orderId + title + fileType + signList
signList 说明	参数名	必选	类型范围	说明
	sealCode	是	String	印章编码
	page	是	String	签章页码 所有页用 0 表示
	positionType	是	int	定位模式 1: 坐标定位, PDF 左下角为原点, OFD 左上角为原点 2: 文本定位
	x	否	float	坐标定位 X 轴
	y	否	float	坐标定位 Y 轴
	text	否	String	文本定位, 文本内容
输出参数	参数名		类型	
	code		String	
	message		String	
错误码	返回值		对应说明	
	0		正常	
	1		参数 appid 不能为空!	
	2		参数 unifiedSocialCreditCode 不能为空!	
	3		授权码未发放	
	4		授权码已禁用	
5		checkCode 验证不一致		

表 B 签章接口表

请求示例	<pre> POST http://{API_ROOT}/api/stampSeal Content-Type: multipart/form-data { "appid":appid, "checkCode":checkCode, "orderId":"test", "title":"test", "file":"d:/JXGBPDFSignTest/in/演示文档.pdf", "fileType":"PDF", "signList": { 'sealCode' :sealCode, 'page' : ' 0' , 'positionType' : ' 1' , 'x' : ' 200' , 'y' : ' 200' } } </pre>
返回示例	<pre> { "code": 0, "message": "OK" } </pre>

附 录 C
(规范性附录)
验章接口说明

验章接口表见表C

表 C 验章接口表

服务名称	验章			
方法说明	对文档加盖的印章进行合法有效的验证			
请求方法	POST			
URL 地址	\$host/api/verify			
请求头	参数名	必选	值	描述
	host	是	\$host/api/verify	
	content-type	是	multipart/form-data	
输入参数	参数名	必选	类型范围	说明
	appid	是	String	接入项目的唯一标识,在应用管理中获取
	randomN	是	String	由获取随机数接口获取到的随机数字符
	checkCode	是	String	randomN+盐值的 SHA256 摘要值, base64 编码
	file	是	byte[]	文件内容
	fileType	是	String	文档类型: PDF、OFD
输出参数	参数名		类型	描述
	code		String	错误码
	message		String	错误描述
	items		Array(item)	印章列表
items 说明	参数名		类型	描述
	sealCode		String	印章编码
	sealName		String	印章名称
	validityResult		boolean	签章有效性
	cadata		jsonObject	证书信息
	failReason		String	失败原因

表 C 验章接口表 (续)

	参数名	类型	描述
cadata 说明	version	String	版本号
	subjectDN	String	
	issuerDN	String	
	sigAlg	String	加密类型
	notBefore	String	有效时间
	notAfter	String	结束时间
	错误码	返回值	对应说明
0		正常	
1		参数 appid 不能为空!	
2		参数 unifiedSocialCreditCode 不能为空!	
3		授权码未发放	
4		授权码已禁用	
5		checkCode 验证不一致	
请求示例	POST http://{API_ROOT}/api/stampSeal Content-Type: multipart/form-data <pre>{ "appid":appid, "checkCode":checkCode, "file":"d:/JXGPDFSignTest/out/演示文档.pdf", "fileType":"PDF", }</pre>		
返回示例	<pre>{ "code": 0, "message": "OK", "items":{ 'sealCode' :sealCode, 'sealName' :sealName, 'validityResult' :' true' , 'cadata' :cadata } }</pre>		