

SZSD

数 字 山 东 工 程 标 准

SZSD02 0014—2024

政务服务数字认证平台 (企业和个人电子签章) 开发接入规范

Digital Authentication Platform For Government Services
Development Specification

2024-04-15 发布

2024-06-01 实施

青岛市大数据发展管理局 发 布

目 次

前 言.....	II
1. 范围.....	1
2. 规范性引用文件.....	1
3. 术语和定义.....	1
3.1 接入应用	1
3.2 前置服务	1
3.3 “政务服务数字认证平台” 基础服务能力.....	2
3.4 第三方可信用户信息源	2
4. 缩略语.....	2
5. 应用接入要求.....	2
5.1 网络环境	2
5.2 接入应用	2
5.3 安全要求	3
5.4 性能要求	3
5.5 兼容性要求	3
6. 接入申请及操作流程.....	4
6.1 应用接入申请流程	4
6.2 应用接入部署流程	4
附录 A （规范性） 前置服务接口信息	7
A.1 获取认证方式接口.....	8
A.2 企业章签署发起接口.....	9
A.3 签署信息查询接口.....	13
A.4 签署文件下载接口.....	14
A.5 H5 页面验签接口	15
A.6 签署完成通知接口.....	16
A.7 个人章签署发起接口.....	17
附录 B （规范性） HMAC 签名算法示例.....	21
B.1 签名值 signature 生成的通用步骤.....	21
B.2 报文请求及响应示例.....	21
附录 C （规范性） 前置服务部署配置	23

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则》的规定起草。

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专利的责任。

本文件由青岛市大数据发展管理局提出并归口。

本标准起草单位：青岛市大数据发展管理局、山东亚微软件股份有限公司。

本标准主要起草人：孙磊志、李佳、孙燕双、江河、陈英航、赵云林、曹晓华、陈良、陈硕、张庆浩、李超等。

政务服务数字认证平台（企业和个人电子签章） 开发接入规范

1. 范围

本文件规定了“政务服务数字认证平台”的接入申请流程、接入方式、接口规范。

本文件适用于政府单位相关应用接入企业及个人电子印章。确保电子签章使用合法、安全、可靠，并提高应用接入的效率。

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 39044-2020 政务服务平台接入规范

GB/T 39047-2020 政务服务平台基本功能规范

3. 术语和定义

下列术语和定义适用于本文件。

3.1

接入应用 **access application**

需要接入到“政务服务数字认证平台”中的各类应用，类型包括 H5 页面、app、小程序、PC 端等。

3.2

前置服务 **prepose services**

前置服务提供统一业务处理入口，与业务应用部署在统一环境，在调用前置服务接口可以不使用签名值验证，前置服务与接口网关交互时会自行做签名值校验。

3.3

“政务服务数字认证平台”基础服务能力 basic service capabilities of " Digital Authentication Platform For Government Services"

指“政务服务数字认证平台”提供的公共服务能力，业务应用接入前置服务后，按照要求即可通过前置服务调用“政务服务数字认证平台”基础服务，当业务应用没有文档签章要求时，业务应用通过安全策略可以直接调用“政务服务数字认证平台”基础服务。

3.4

第三方可信用户信息源 third-party trusted user information sources

整个“政务服务数字认证平台”体系，用户信息的获取不能以 app 或者小程序传入的为准，即用户信息的获取必须依赖第三方可信用户源。

4. 缩略语

以下缩略语适用于本文件。

api 网关：API 托管服务 (Application Programming Interface Gateway)

appId：应用程序标识符 (Application Identification)

deviceId：设备标识 (device Identification)

H5：构建 Web 内容的一种语言描述方式 (HyperText Markup Language 5)

5. 应用接入要求

5.1 网络环境

业务应用需具备对接青岛市政务云的网络访问基础。

5.2 接入应用

各业务应用在接入“政务服务数字认证平台”前需进行相应改造，实现与“政务服务数字认证平台”平台业务互访。

a) H5 应用：

需修改前置服务中的 apiUrl、license，实现与“政务服务数字认证平台”网络互通后，按本规范附录 A（规范性）前置服务接口信息进行对接。

b) app 应用：

1) 用户通过 app 使用证书下载、印章申领、印章授权、扫码授权签章等服务功能；

2) app 应用需集成认证签名移动端模块（简称：移动端 sdk）完成证书下载、并通过 H5 页面进入“政务服务数字认证平台”页面，以实现印章申领、扫码签章功能。

c) 小程序应用：

1) 用户通过小程序使用证书下载、印章申领、印章授权、扫码授权签章等服务功能；

2) 小程序需要集成“政务服务数字认证平台”H5 小程序插件实现证书下载并且通过页面跳转小程序 H5 “政务服务数字认证平台”页面，实现印章申领、扫码签章功能。

5.3 安全要求

按照以下安全要求进行接入：

——接入“政务服务数字认证平台”的应用必须符合信息系统安全等级保护三级标准中的所有技术要求；

——所有非直接内网调用前置服务的请求都需要使用申请账号进行 HMAC 签名值计算，防止数据在传输过程中被拦截篡改。HMAC 签名算法示例见附录 B（规范性）HMAC 签名算法示例。

5.4 性能要求

按照以下性能要求进行接入：

——保障签章效率以及实现大文件签章，业务应用需要提供前置服务部署的基础环境，参照附录 C（规范性）前置服务部署配置；

——支持 7*24 小时无间断运行；

——每年因系统本身故障导致停机时间累计不超过 1 小时，故障次数不超过 10 次。

5.5 兼容性要求

应用接入时，应符合以下兼容性要求。

a) app 移动端兼容：

1) android: 4.0 以上系统版本；

2) IOS: 任意系统版本；

3) 鸿蒙: 任意系统版本。

b) 页面浏览器兼容：

1) 当前 chrome 浏览器、IE 浏览器、火狐浏览器及国产浏览器等。

c) 终端适配要求：

1) 当前主流手机、PC 电脑及平板电脑等。

6. 接入申请及操作流程

6.1 应用接入申请流程

6.1.1 应用评估

接入单位梳理本单位的应用服务，明确使用业务签章的用户体系，用户体系需分为：法定代表人、法定代表人授权的印章操作人和自然人，明确应用场景、应用范围。

评估应用接入的可行性，包括是否高频、是否便民、是否重复、网络互通、安全性等多方面角度。通过评估通过后启动接入工作。

6.1.2 账号申请

接入单位提交接入方基本客户资料如客户名称、客户联系人和电话，向“政务服务数字认证平台”项目组线下申请接入参数（appId、deviceId、secret）及license文件。

6.1.3 前置服务部署包

在前置服务license文件具备后，“政务服务数字认证平台”项目组会同步将前置服务部署包、部署文档、接口文档等一并提供给接入单位。

6.2 应用接入部署流程

6.2.1 概述

接入操作流程包含网络实现互访、按需调用基础服务能力、联调测试和前置服务参数部署以及配置环节，见图 1。

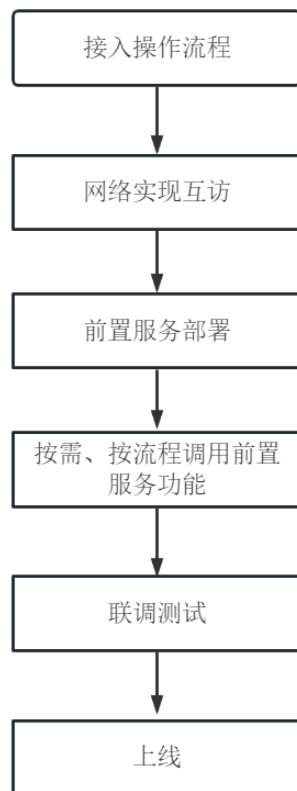


图1 第三方应用接入操作流程示意图

6.2.2 网络实现互访

业务应用需具备对接政务云的网络访问基础。业务应用可开通前置服务服务器与接入应用服务器之间的网络策略与“政务服务数字认证平台”平台网络互通，达到与“政务服务数字认证平台”平台网络互通目的。

6.2.3 前置服务部署

参考附录 C（规范性）前置服务部署配置，实现前置服务部署。

6.2.4 调用前置服务功能

业务应用与“政务服务数字认证平台”基础服务能力交互可以通过前置服务和直接调用 API 网关完成，其中直接调用网关主要是完成用户注册、企业注册及印章申领等业务，不能直接完成签章业务，签章业务必须依赖于前置服务。

集成开发要求参照附录 A（规范性）前置服务接口信息

6.2.5 联调测试

业务应用按照标准完成接入及完成自身业务改造后, 可通过申请预发布环境 app 或者小程序使用权限, 与自身业务应用进行联调测试。

6.2.6 应用上线

平台对接工作完成, 预发布环境联调测试完成后, 即可根据实际业务需要安排上线时间, 上线后需要做上线回归测试。

附录 A

(规范性)

前置服务接口信息

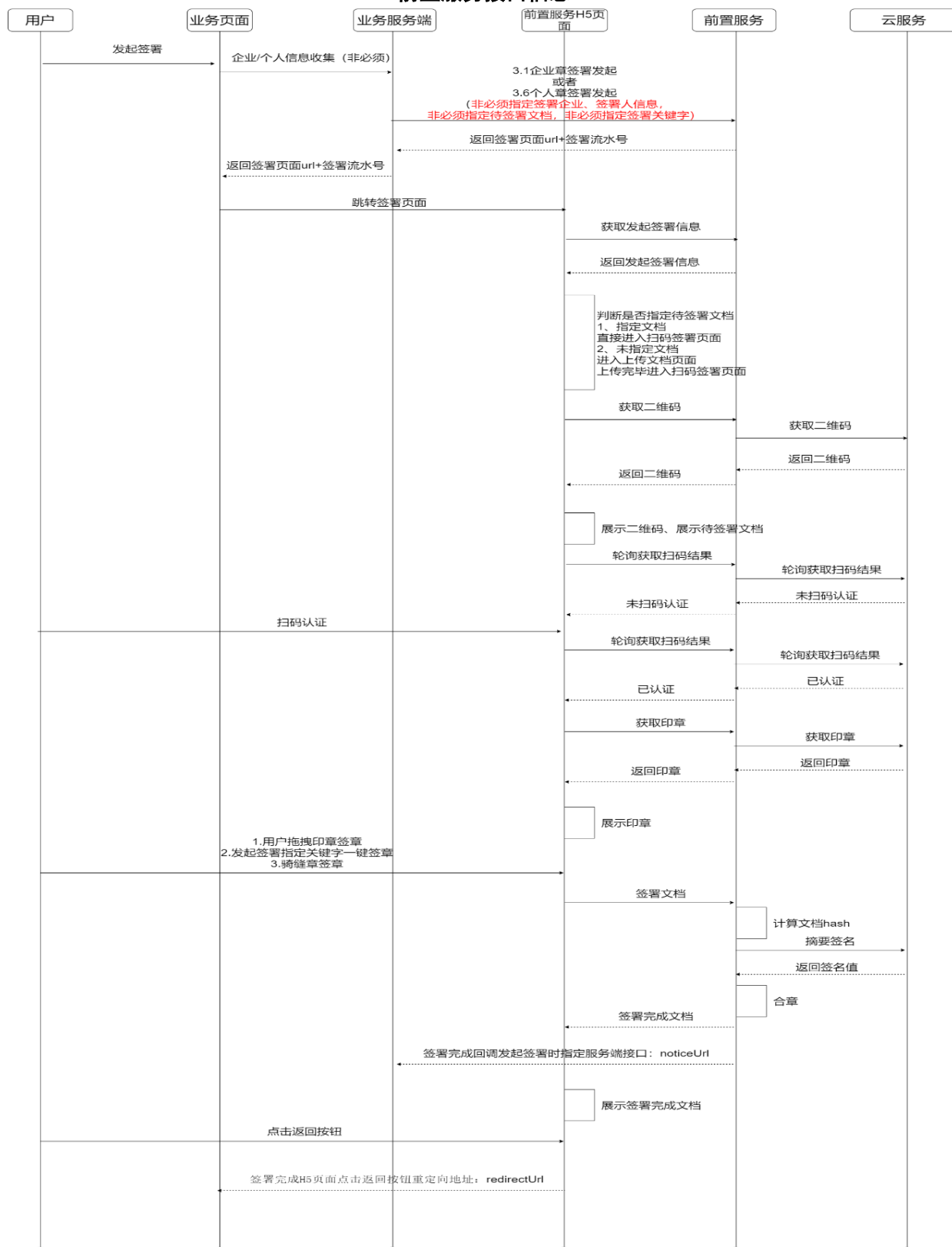


图2 接口接入流程图

A. 1 获取认证方式接口

A. 1. 1 功能说明

HMAC 签名算法示例认证类型，以便页面提供相应的授权认证所需信息。

A. 1. 2 接口定义

http://ip:port/h5sign/auth

A. 1. 3 请求类型

GET

A. 1. 4 参数说明

A. 1. 5 请求示例

名称	参数类型	类型	必填	示例值	描述
appId	query	字符型	是	APP_4E4E0490D21C44C7A439F847A77 44D29	标识业务应用的唯一标识

http://ip:port/ipAddress/h5Sign/auth?appId=APP_4E4E0490D21C44C7A439F847A7744D29

A. 1. 6 返回值

属性名	属性类型	描述
status	整型	响应码，成功是 200，其他错误为 8 位错误码
message	字符型	响应信息
trace	字符型	错误栈信息，用于显示错误的深层次原因，
transId	字符型	请求流水号
data	数据类型	返回业务信息
authType	集合型	认证类型：暂时为 SIGN ：扫码

A. 1. 7 响应示例

```
{
  "status": 200,
  "message": "SUCCESS",
  "transId": null,
  "data": { "authType": ["SIGN" ] }}
```

A. 2 企业章签署发起接口

A. 2. 1 功能说明

该接口供业务应用发起企业章签署请求，企业 ofd 签署仅支持拖拽签章。

A. 2. 2 接口定义

http://ip:port/h5sign

A. 2. 3 请求类型

POST

A. 2. 4 参数说明

参数名称		类型	必填	描述
appId		字符型	是	标识业务应用的唯一标识
configInfo 签署配置信息	noticeUrl	字符型		回调通知地址（签署完成后由 H5 签署组件调用此 URL 进行状态通知，详见签署完成通知接口），默认使用系统配置地址
	redirectUrl	字符型		签署完成 H5 页面点击返回按钮重定向地址，默认签署完成停在当前页面
signSealAlgoType		字符型	是	SM3withSM2 SHA256withRSA SHA1withRSA
sealTitles		集合型		印章名称 参考枚举 GZ-公章、CWZ-财务专用章、HTZ-合同专用章、FRZ-法定代表人章、FPZ-发票专用章、GRZ-个人章。传 code 码
ext		字符型		可用于自定义扩展

参数名称		类型	必填	描述
timeFontColor		字符型		字颜色，默认 RED 白色:WHITE, 浅灰色:LIGHT_GRAY, 灰色:GRAY, 深灰色:DARK_GRAY, 黑色:BLACK, 红色:RED, 粉色:PINK, 橘色:ORANGE, 黄色:YELLOW, 绿色:GREEN, 紫红色:MAGENTA, 青色:CYAN, 蓝色:BLUE,
authTypes		集合型		企业签署传固定值：ENTSIGN;企业代理人签署传固 定值：SIGN
fileTypePlan		字符型		计划上传文件类型（PDF OFD），默认 PDF
fileStampList		集合型		文件和印章信息 当传该对象时文件必须传，不传时需要在上传页面手动上传
	fileList	集合型		文件信息（结构体类型具体参考第 5 章）
	sealList	集合型		印章信息（结构体类型具体参考第 5 章）
uniqueNum		字符型		社会统一信用代码，签署时指定签署企业，此时仅能用当前企业的印章签章
clientSign		字符型		mobile: 移动端签署、pc: pc 端签署，默认 pc
showSignTime		字符型		true:展示时间 false: 不展示时间（默认）。Pdf 文件签署时印章签署时间展示，OFD 暂不支持
timeEntity		数据型		showSignTime=true 时必传

参数名称		类型	必填	描述
	signTimeFormat	字符型		时间格式 "yyyy-MM-dd HH:mm:ss"（默认） "yyyy-MM-dd" "yyyy/MM/dd HH:mm:ss" "yyyy/MM/dd"
	timeFontSize	整型		字大小，默认 40，单位 px
	timeMoveSpace	浮点型		相对印章偏移量，可为正、负值，单位 mm，默认 0mm

A. 2. 5 请求示例

```
{
  "appId": "APP_4E4E0490D21C44C7A439F847A7744D29",
  "authTypes": [ "SIGN" ],
  "configInfo": {
    "noticeUrl": "http://ip:port/getRedirectUrl/123456789",
    "redirectUrl": "http://ip:port/getRedirectUrl/123456789"
  },
  "ext": "string",
  "fileStampList": [{
    "fileList": [
      {
        "title": "测试",
        "fileB64": "xxxx",
        "fileType": "PDF",
        "fileDesc": "签章"
      }
    ],
    "sealList": [
      {
        "ruleInfo": {
          "keyWordRule": {
            "keyword": "你好",
            "moveType": "CENTER",
            "searchOrder": "DESC"
          },
          "ruleType": "KEYWORD",
```

```

        "version": "1.0"
    },
    "sealInfo": {
        "sealTitle": "HTZ"
    }
}

]

}],
"sealTitles": [ "GZ", "FPZ", "HTZ", "CWZ", "FRZ" ],
"signSealAlgoType": "SM3withSM2",
"startType": "PAGE"
}

```

A. 2. 7 返回值

属性名		属性类型	描述
status		整型	响应码，成功是 200，其他错误为 8 位错误码
message		字符型	响应信息
trace		字符型	错误栈信息，用于显示错误的深层次原因，帮助调用者解决错误
transId		字符型	请求流水号
data		数据类型	返回业务字段
	url	字符型	该地址作为签署当前业务的 H5 页面地址嵌入接入方系统中完成页面文件签署动作。
	businessId	字符型	签署业务 ID 业务应用需留存后续用于 1. 业务应用接收签署完成通知时可根据此 ID 区分具体业务； 2. 业务应用在签署文件下载接口中利用此 ID 下载签署后的文件；

A. 2. 8 响应示例

```

{
    "status": 200,
    "message": "SUCCESS",
    "transId": null,
    "data": {
        "url":
            "http://ip:port/ecSign/tools/#/sso/index?businessId=1294519964845252610&businessType=h5send",
        "businessId": "1294519964845252610"
    }
}

```

A.3 签署信息查询接口

A.3.1 功能说明

根据签署业务 ID（businessId）查询业务信息。

A.3.2 接口定义

http://ip:port/h5sign/{businessId}

A.3.3 请求类型

GET

A.3.4 参数说明

名称	参数类型	类型	必填	示例值	描述
appId	query	字符型	是	456455645656dfd	标识业务应用的唯一标识
businessId	path	字符型	是	456455645656dfd	签署业务 ID

A.3.5 返回值

属性名		属性类型	描述
status		整型	响应码，成功是 200，其他错误为 8 位错误码
message		字符型	响应信息
trace		字符型	错误栈信息，用于显示错误的深层次原因，
transId		字符型	请求流水号
data		数据型	返回业务信息
	signTime	字符型	签署时间
	status	字符型	签署状态
	fileList	数组型	签署文件列表
	fileId	字符型	上传文件 id
	signFileId	字符型	签署完成的文件 ID
	fileName	字符型	文件名称

A.3.6 请求示例

http://ip:port/ipAddress/h5sign/1294513569148194817?appId=app-1

A. 3. 7 响应示例

```
{
  "status": 200,
  "message": "SUCCESS",
  "transId": null,
  "data": {
    "signTime": "2020-08-15 14:18:57",
    "status": "1",
    "fileList": [
      {
        "fileId": "9e74390b-84a3-4ea3-8807-2a3f2a33ddac",
        "signFileId": "1294514346080088066",
        "fileName": "申请材料-张三.pdf"
      }
    ]
  }
}
```

A. 4 签署文件下载接口

A. 4. 1 功能说明

根据相关签署业务 ID 加签署文件 ID 下载签署完成的文件。

A. 4. 2 接口定义

http://ip:port/h5sign/downloadFiles/{businessId}

A. 4. 3 请求类型

GET

A. 4. 4 参数说明

名称	参数类型	类型	必填	示例值	描述
appId	query	字符型	是	456455645656dfd	标识业务应用的唯一标识
businessId	path	字符型	是	456455645656dfd	签署业务 ID
signFileId	query	字符型	是	456455645656dfd	签署文件 ID

A. 4. 5 返回值

下载成功则返回文件二进制格式的数据流。

正常 HTTP 响应头：（下载成功 HTTP status code 等于 200）

HTTP/1.1 200

Content-Type: application/octet-stream

异常 HTTP 响应头：（下载失败 HTTP status code 不等 200）

HTTP/1.1 404

Content-Length: 0

A. 4. 6 请求示例

http://ip:port/ipAddress/h5sign/downloadFiles/1294513569148194817?appId=app-1&signFileId=129451434608008806

A. 5 H5 页面验签接口

A. 5. 1 功能说明

接入系统通过接口先获取验签 url，然后再打开验签页面，完成对已签署的文档验证功能。

A. 5. 2 接口定义

http://ip:port/h5sign/validate

A. 5. 3 请求类型

GET

A. 5. 4 参数说明

名称	参数类型	类型	必填	示例值	描述
appId	query	字符型	是	456455645656dfd	标识业务应用的唯一标识
fileType	query	字符型		0FD	计划验签的文件类型，默认 PDF

A. 5. 5 请求示例

http://ip:port/ipAddress/h5sign/validate?appId=appid-01&fileType=0FD

A. 5. 6 返回值

属性名	属性类型	描述
status	整型	响应码，成功是 200，其他错误为 8 位错误码
message	字符型	响应信息
trace	字符型	错误栈信息，用于显示错误的深层次原因，
transId	字符型	请求流水号
data	数据类型	返回业务信息
url	字符型	返回的验签的 url

A. 5. 7 响应示例

```
{
  "status": 200,
  "message": "SUCCESS",
  "transId": null,
  "data": {
    "url": "http:// ip:port/ipAddress/h5sign/ecSign?appId=appid-01"
  }
}
```

A. 6 签署完成通知接口

A. 6. 1 功能说明

由于文件签署涉及大量数字签名、文档操作等耗时操作，签署任务的执行采用异步方式进行，完成后通过 HTTP 协议 get 请求回调的方式通知业务应用签署结果，此接口需要业务应用实现供 H5 组件调用。

A. 6. 2 请求类型

GET

A. 6. 3 接口定义

接入方在调用签署发起接口时传入的 noticeUrl 地址

A. 6. 4 参数说明

名称	类型	必填	示例值	描述
businessId	字符型	是	b6a3bf93626b54abb303ea	签署业务 ID
signTime	字符型	是	2020-07-11 23:59:59	签署时间格式 yyyy-MM-dd HH:MM:SS 北

名称	类型	必填	示例值	描述
				京时间
status	整型	是	1	1:签署完成 2:签署未完成
message	字符型	是	服务器内部异常	签署失败异常消息
timestamp	字符型	是	1263967486940	回调通知时间戳毫秒级 北京时间

A. 7 个人章签署发起接口

A. 7. 1 功能说明

个人章业务入口。

个人 ofd 签署仅支持拖拽签章。

A. 7. 2 请求类型

POST

A. 7. 3 接口定义

http://ip:port/h5sign/personal/signStart

A. 7. 4 参数说明

参数名称		类型	必填	描述
appId		字符型	是	标识业务应用的唯一标识
code		字符型		分配 code
token		字符型		外传 token
configInfo	noticeUrl	字符型		回调通知地址（签署完成后由 H5 签署组件调用此 URL 进行状态通知，详见签署完成通知接口），默认使用系统配置地址
	redirectUrl	字符型		签署完成 H5 页面点击返回按钮重定向地址，默认签署完成停留在当前页面
signSealAlgoType		字符型	是	SM3withSM2 SHA256withRSA SHA1withRSA

参数名称		类型	必填	描述
sealTitles		集合型		印章名称 参考枚举 GZ-公章、CWZ-财务专用章、HTZ-合同专用章、FRZ-法定代表人章、FPZ-发票专用章、GRZ-个人章 请传 code 码
ext		字符型		可用于自定义扩展
authTypes		集合型		跟据接口获取认证方式
fileTypePlan		字符型		计划上传文件类型（PDF OFD），默认 PDF
fileStampList		集合型		文件和印章信息 当传该对象时文件必须传，不传时需要在上传页面手动上传
	fileList	集合型		文件信息（结构体类型具体参考第 5 章）
	sealList	集合型		印章信息（结构体类型具体参考第 5 章）
clientSign		字符型		mobile: 移动端签署、pc: pc 端签署，默认 pc
timeFontColor		字符型		字颜色，默认 RED 白色:WHITE, 浅灰色:LIGHT_GRAY, 灰色:GRAY, 深灰色:DARK_GRAY, 黑色:BLACK, 红色:RED, 粉色:PINK, 橘色:ORANGE, 黄色:YELLOW, 绿色:GREEN, 紫红色:MAGENTA, 青色:CYAN, 蓝色:BLUE,
showSignTime		字符型		Pdf 文件签署时印章签署时间展示，OFD 暂不支持 true:展示时间 false: 不展示时间（默认）

参数名称		类型	必填	描述
timeEntity		数据型		showSignTime=true 时必传
	signTimeFormat	字符型		时间格式 "yyyy-MM-dd HH:mm:ss"（默认） "yyyy-MM-dd" "yyyy/MM/dd HH:mm:ss" "yyyy/MM/dd"
	timeFontSize	整型		字大小，默认 40，单位 px
	timeMoveSpace	浮点型		相对印章偏移量，可为正、负值，单位 mm，默认 0mm
	timeMove	字符型		相对印章字位置，默认 BOTTOM BOTTOM：印章下方，TOP：印章上方，LEFT：印章左侧， RIGHT：印章右侧
	timeFontStyle	整型		正常：0（默认），斜体：2

A. 7. 5 请求示例

```
{
  "appId": "APP_A86EAB029724438C8E2CAC04C63F63BC",
  "authTypes": [ "SIGN" ],
  "configInfo": {
    "noticeUrl": "http://ip:Port/getRedirectUrl/123456789",
    "redirectUrl": "http://ip:Port/getRedirectUrl/123456789"
  },
  "ext": "string",
  "sealTitles": [ "GZ", "FPZ", "HTZ", "CWZ", "FRZ" ],
  "signSealAlgoType": "SM3withSM2",
  "startType": "PAGE"
}
```

A. 7. 6 返回值

属性名	属性类型	描述
status	整型	响应码，成功是 200，其他错误为 8 位错误码
message	字符型	响应信息

属性名		属性类型	描述
trace		字符型	错误栈信息，用于显示错误的深层次原因，帮助调用者解决错误
transId		字符型	请求流水号
data		数据类型	返回业务字段
	url	字符型	该地址作为签署当前业务的 H5 页面地址嵌入接入方系统中完成页面文件签署动作。
	businessId	字符型	签署业务 ID 业务应用需留存后续用于 3. 业务应用接收签署完成通知时可根据此 ID 区分具体业务； 4. 业务应用在签署文件下载接口中利用此 ID 下载签署后的文件；

A. 7. 7 响应示例

```

{
  "status": 200,
  "message": "SUCCESS",
  "transId": null,
  "data": {
    "url": "http://ip:Port/ecSign/tools/#/sso/index?businessId=1294519964845252610&businessType=h5p
sSend",
    "businessId": "1294519964845252610"
  }
}

```

附录 B

（规范性）

HMAC 签名算法示例

所有非直接内网调用前置服务的请求都需要使用申请账号进行 HMAC 签名值计算，防止数据在传输过程中被拦截篡改；

B.1 签名值 signature 生成的通用步骤

第一步

设所有发送或者接收到的数据为集合 M，将集合 M 内非空参数值的参数按照参数名 ASCII 码从小到大排序（字典序），使用 URL 键值对的格式（即 key1=value1&key2=value2...）拼接成字符串 stringA。

特别注意以下重要规则：

- ◆ 参数名 ASCII 码从小到大排序（字典序）；
- ◆ 如果参数的值为空不参与签名，且请求报文中也不要带此参数；
- ◆ 参数名区分大小写；

第二步

对 stringA 对进行 HMAC 运算，得到 hmac 的值后再做 Base64 编码，最后得到 sign 值 signature。

```
String signTemp = hmac(stringA, secret);
```

```
String signature = Base64(signTemp);
```

B.2 报文请求及响应示例

接口请求响应示例：

- ◆ 以调用添加签名任务接口为例，请求报文如下：

```
{
  "version": "1.0",
  "appId": "APP_52E0099A69414266B84DFAB4999E1299",
  "signAlgo": "HMAC",
  "data": "Q29zcyBTaWduIERhdGEgRm9yIFRlc3Qu"
}
```

其中：

- ◆ 对示例请求的参数按照 key=value 的格式，并按照参数名 ASCII 字典序排序后字符串如下：

```
stringA=SM3withSM2&appId=APP_52E0099A69414266B84DFAB4999E1299&data=Q29zcyBTaWduIERhdGEgRm9yIFRlc3Qu&
signAlgo=HMAC&transId=20190531001&version=1.0
```

◆ 计算签名值 signature:

```
String signTemp = hmac(stringA, secret);

String signature = Base64(signTemp);
```

◆ 对上述待签名原文进行 HMAC-SHA256 签名的签名值结果如下:

```
wyLPhb2JwrcT6WPMdx/61BMKdSVZc5gpaU21n/bfgA=
```

◆ 待发送报文如下:

```
{

  "version": "1.0",

  "appId": "APP_52E0099A69414266B84DFAB4999E1299",

  "signAlgo": "HMAC",

  "title": "测试长签名",

  "description": "签名描述",

  "dataType": "DATA",

  "algo": "SM3withSM2",

  "data": "Q29zcyBTaWduIERhdGEgRm9yIFRlc3Qu",

  "signature": "P2yQKZuDdFFoatgBXlMSsBttnczNuDAGWyTSu/U4pwM="

}
```

◆ 响应报文如下:

```
{

  "status": 200,

  "message": "SUCCESS",

  "data": {

    "signDataId": "SD_56770b9f-80b6-4efd-a4b2-c7305cc16f82",

    "qrCode": "KHEODgQEUHoQY3VneGVkZ18SXBRtCgBTDmBnNjYlXQRGIgAdUg9+Y2YzDEFTFHgAEh0a0SojNU1KRyEJdX

      4TG8mITxNSkdQbBBGVEo+0jw+TUpHQ24CEkw="

  }

}
```

附录 C
（规范性）
前置服务部署配置

部署前置服务之前需要业务应用具备相关的服务器资源，建议主要配置要求如下：

CPU	≥8Core，主频≥2.3GHz
内存	≥16G
存储	≥300G
台数	≥2 台
文件存储	NAS、本地共享磁盘、NFS 共享盘
操作系统	信创操作系统