

# 湖南省公共资源交易中心文件

湘资〔2021〕46号

---

## 湖南省公共资源交易中心 关于印发《湖南省公共资源交易中心 CA证书及电子签章服务机构接入 管理办法（试行）》的通知

各市州交易中心、CA证书及电子签章服务机构、市场交易主体：

现将《湖南省公共资源交易中心CA证书及电子签章服务机构接入管理办法（试行）》印发给你们，请认真遵照执行。

湖南省公共资源交易中心

2021年11月4日

# 湖南省公共资源交易中心 CA 证书及电子签章服务机构接入 管理办法（试行）

## 第一章 总则

**第一条** 为全面贯彻落实省委关于清廉湖南建设的工作要求，推进优化营商环境、“放管服”改革重要部署，更好服务全省“三高四新”战略，构建公正、透明、标准的 CA 证书及电子签章服务体系，打破技术垄断，简化市场主体办理事项，降低交易成本，实现 CA 证书及电子签章全省范围“一次办理、全省通用”，依据《中华人民共和国电子签名法》、《电子认证服务管理办法》、《湖南省优化营商环境攻坚行动方案》，结合省交易中心的实际情况，制定本办法。

**第二条** 本办法适用于接入湖南省公共资源交易中心（以下简称“省交易中心”）开发建设系统的 CA 证书服务机构、电子签章服务机构、CA 证书与电子签章资源共享平台服务机构。

**第三条** 本办法所称 CA 证书及电子签章服务机构是指提供符合《中华人民共和国电子签名法》及国密算法，能够与省交易中心信息化系统无缝对接，用以登录系统、签名、加密电子招标投标文件的数字证书及配套软硬件的服务机构。CA 证书与电子签章资源共享平台服务机构是指依据公平合法、标准开放、兼容

互联、资源共享原则，受省交易中心委托，依托新兴信息化技术手段搭建 CA 证书及电子签章资源共享平台的技术服务机构。

**第四条** CA 证书与电子签章资源共享平台服务机构不得对所有 CA 证书及电子签章使用人收取任何费用，不得对 CA 证书及电子签章服务机构对接工作收取任何费用。CA 证书及电子签章制证费用由各 CA 证书及电子签章服务机构按市场原则自行制定，任何人不得以指定、授意、暗示等方式干预市场主体选择。

**第五条** 省交易中心网络安全和数字化领导小组负责 CA 证书及电子签章服务机构接入事务的审批，综合管理办公室负责 CA 证书及电子签章服务机构驻场开展业务相关事宜，技术管理办公室负责协调 CA 证书及电子签章服务机构接入的技术事项。

## **第二章 机构准入管理**

**第六条** CA 证书及电子签章服务机构按照自愿原则，申请与 CA 证书与电子签章资源共享平台进行对接。省交易中心的信息系统通过 CA 证书与电子签章资源共享平台对接实现移动端、PC 端的多 CA 证书、多电子签章兼容互联使用。CA 证书及电子签章服务机构应满足以下条件：

（一）CA 证书及电子签章服务机构应依法设立，具有独立法人资格，有能力提供相应服务，符合《电子认证服务管理办法》要求。

（二）遵守国家有关法律、法规和规章，具有良好的商业信

誉和健全的财务管理制度，财务状况良好。

**第七条** CA 证书与电子签章资源共享平台服务机构应满足以下条件：

（一）CA 证书与电子签章资源共享平台服务机构应依法设立，具有独立法人资格，有能力提供相应服务。

（二）具备完善的网络信息存储、传输、处理安全保护机制，取得公安部信息安全等级保护第三级或者更高级别保护认证。

（三）提供健全密码保障体系，实施并通过商用密码应用安全性评估。

（四）具有较强的技术开发和标准服务能力。面向 CA 证书及电子签章服务机构提供标准化对接服务。面向市场主体提供在线化、通用化、移动化 CA 证书及电子签章应用服务。面向交易业务提供不可篡改、可追溯的 CA 证书及电子签章使用信息存证服务。

**第八条** 符合要求意向对接的 CA 证书及电子签章服务机构，应向技术管理办公室提交准入申请，并按以下要求提供申报材料报技术管理办公室组织论证，确认可行后交综合管理办公室统筹，提交网络安全和数字化领导小组审批，审批同意后按照统一的接入标准，开展接入 CA 证书与电子签章资源共享平台相关事宜。需提供的材料及要求如下：

（1）《CA 证书及电子签章服务机构接入申请表》；

(2)《CA 证书及电子签章服务机构接入服务承诺书》;

(3)营业执照复印件;

(4)具有国家信息产业部电子认证服务许可资质、电子政务电子认证服务机构、电子认证服务使用密码许可证等相关资质(提供相关资质复印件),且须符合《中华人民共和国电子签名法》、《电子认证服务管理办法》和其他法律、行政法规的规定;

(5)CA 证书及电子签章服务机构简介。

**第九条** CA 证书及电子签章服务机构可向省交易中心申请设置一个现场业务咨询席位,填写《CA 证书及电子签章服务机构驻场服务申请表》,经交综合管理办公室统筹后,提交业务分管领导签署意见,报网络安全和数字化领导小组审批,审批同意后安排现场业务咨询人员入场,并纳入省交易中心驻场人员统一管理。

省交易中心所设置的业务咨询席位只提供 CA 证书及电子签章业务咨询,不得从事 CA 证书及电子签章销售、推广等与业务咨询无关的事宜。

### **第三章 服务管理**

**第十条** CA 证书及电子签章服务机构对于其所提供的服务应保证合法、合规、公开、透明,通过 CA 证书及电子签章资源共享平台面向社会进行公开,包括但不限于以下事项:

(一) 服务内容与服务地点；  
(二) CA 证书及电子签章业务办理流程；  
(三) CA 证书及电子签章服务产品各项收费标准与收费价格；

(四) CA 证书及电子签章服务机构技术支持方式；

**第十一条** CA 证书及电子签章服务机构应在湖南省内设有专门的驻场服务窗口，具备为市场主体提供线下与线上新办、续办业务的能力，保证市场主体可通过网络完成 CA 证书及电子签章业务办理。CA 证书及电子签章服务机构的各项服务价格必须向社会公开，接受社会监督。

**第十二条** CA 证书及电子签章服务机构应提供 7x24 小时应用支持服务，及时解决 CA 证书及电子签章在使用过程中出现的各类问题，业务与技术服务电话统一接入省交易中心智慧客服系统。

**第十三条** CA 证书及电子签章服务机构须向用户提供免费培训，不准向用户进行虚假宣传，不准向用户推荐、销售本公司其他产品，不准攻击、诋毁其他 CA 证书及电子签章服务机构的产品，不准以不正当手段进行竞争。

**第十四条** CA 证书与电子签章资源共享平台服务机构应按照国家交易中心统一接口要求，公开其所采用的技术标准，确保技术的开放性与兼容性，确保接入的各类 CA 证书与电子签章均可

在公共资源交易业务中正常使用。

**第十五条** CA 证书与电子签章资源共享平台服务机构承担 CA 证书与电子签章服务的兼容与互联互通共享服务，不得从事 CA 证书与电子签章销售、制证等服务业务。

**第十六条** CA 证书与电子签章资源共享平台服务机构应提供完善的技术支持服务，确保 CA 证书与电子签章服务机构技术对接工作的顺利进行，及时解决 CA 证书与电子签章接入的各项技术问题。

**第十七条** CA 证书服务机构、电子签章服务机构、CA 证书与电子签章资源共享平台服务机构均应积极配合省交易中心 CA 证书与电子签章接入管理工作，服从省交易中心的 CA 证书与电子签章兼容互联、移动化应用的整体工作安排，配合完成评标区内评标专家的无介质证书使用配套的手写信息数字签名板设备的联调测试。

## **第四章 安全运维管理**

**第十八条** CA 证书服务机构、电子签章服务机构、CA 证书与电子签章资源共享平台服务机构均应采取安全措施，加强数据资源保护，确保数据安全，未经审批不得访问后台数据。

**第十九条** CA 证书服务机构、电子签章服务机构、CA 证书与电子签章资源共享服务机构必须提供故障应急处理机制，对因系统、网络、误操作、CA 证书、电子签章自身问题等特殊情况

导致无法编制招投标文件、开评标现场无法解密等情况时对制定解决措施，确保出现紧急问题时能够立即响应，第一时间解决。相关应急处置机制，突发问题解决情况报告交技术管理办公室备案。

**第二十条** CA 证书服务机构、电子签章服务机构不得私设后台，非法收集、提供、篡改、泄露用户数据；CA 证书与电子签章资源共享服务机构不准利用平台优势、开发便利条件、设置技术门槛、搞变相垄断，限制排斥其他 CA 证书与电子签章服务机构对接，诱导潜在相关交易主体购买指定产品，索拿卡要，谋取与开发建设无关利益。

**第二十一条** CA 证书服务机构、电子签章服务机构、CA 证书与电子签章资源共享服务机构不准调派未经培训、临时招聘人员上岗，未经允许不得擅自更换主要技术服务人员造成安全隐患。

## **第五章 法律责任**

**第二十二条** 市场主体在申领、变更、注销数字证书及注册使用 CA 证书与电子签章时，应当提供合法、真实、有效的证件或者证明材料，不得弄虚作假，由于自身原因导致的问题由市场主体自行承担。

**第二十三条** 市场主体应当妥善保管 CA 证书与电子签章，



并对使用 CA 证书与电子签章行为负责。因市场主体自身原因导致遗失、泄露 CA 证书与电子签章等情况而未通知 CA 证书与电子签章服务机构及时处理的，市场主体自行承担相应责任。

**第二十四条** 因 CA 证书与电子签章不符合国家相关技术规范的，在保质期内因质量问题造成市场主体或者省交易中心利益损害的，相应 CA 证书及电子签章服务机构应当承担相应责任。

**第二十五条** CA 证书服务机构、电子签章服务机构、CA 证书与电子签章资源共享平台服务机构存在以下情况，情节较轻的，省交易中心责令其立即改正；情节较重的，相关 CA 证书、电子签章产品进行下架处理，相应机构应承担相应的经济法律责任：

- （一）不配合省交易中心 CA 证书与电子签章管理工作的；
- （二）使用未经安全审查或安全审查未通过的产品及服务；
- （三）故意泄露数据的；
- （四）造成系统瘫痪，导致交易活动无法正常进行的；
- （五）造成无法进行正常投标、开标、评标等重大损失的；
- （六）服务质量差，时效性低，被市场主体投诉的；
- （七）其他影响省交易中心开、评标工作或给省交易中心造成不良影响的情形的。

**第二十六条** CA 证书服务机构、电子签章服务机构、CA 证书与电子签章资源共享平台服务机构在工作中滥用职权、玩忽职

守、徇私舞弊，或者泄露、非法向他人提供在履行职责中知悉的保密信息、个人隐私的，依法予以处罚；涉嫌犯罪的，移送司法机关处理。

**第二十七条** 本办法自 2021 年 11 月 5 日起执行。

附件：1. 《CA 证书与电子签章资源共享服务机构接入申请表》

2. 《CA 证书与电子签章资源共享服务机构驻场服务申请表》

3. 《CA 证书与电子签章资源共享服务机构接入服务承诺书》

4. 《CA 证书与电子签章资源共享平台对接技术标准 ( V1.0 )》

附件 1

# CA 证书与电子签章资源 共享服务机构接入申请表

申 请 单 位（盖公章）：\_\_\_\_\_

法定代表人或负责人（签字或盖章）：\_\_\_\_\_

地 址：\_\_\_\_\_

联 系 电 话：\_\_\_\_\_

日 期：\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日

# 法定代表人/负责人授权委托书

本授权委托书声明：\_\_\_\_\_（申请人名称），现  
授权委托 \_\_\_\_\_（姓名）为我司代理人，以单位名义参加  
湖南省公共资源交易中心 CA 证书及电子签章服务机构接入  
CA 证书与电子签章资源共享平台工作。

代理人在接入过程中所签署的一切文件和处理与之有  
关的一切事务，我司均予以承认，授权有效期\_\_\_\_\_天。

法定代表人或其委托代理人无转委托。特此委托。

申请单位：\_\_\_\_\_（公章）

法定代表人或负责人：\_\_\_\_\_（签字）

日 期：\_\_\_\_\_年\_\_\_\_月\_\_\_\_日

附：1. 法定代表人/负责人和委托代理人身份证复印件

2. 电子认证服务许可证、电子认证服务使用密码许可证复印件

接入申请审批表

申请单位名称		
单位地址		
单位联系人	姓名：                      手机号码：	
认证许可证	营业执照证件编号	
	电子认证服务许可证编号	
	电子认证服务使用密码许可证编号	
湖南省境内窗口 服务地址		
单位主要情况		
申请理由		
技术管理 办公室意见	签字：                      日期：	
综合管理 办公室意见	签字：                      日期：	
网络安全和数字化 领导小组意见	签字：                      日期：	

附件 2

驻场服务申请表

申请单位名称	
申请时间	
申请驻场 服务时限	
驻场服务 人员信息	姓名：                      手机号码：
申请单位	签字：                      日期：
综合管理 办公室意见	签字：                      日期：
分管领导意见	签字：                      日期：
网络安全和数字化 领导小组意见	签字：                      日期：

### 附件 3

## CA 证书与电子签章资源共享平台 接入服务承诺书

湖南省公共资源交易中心：

我司承诺自愿接入湖南省公共资源交易中心 CA 证书与电子签章资源共享平台，为平台提供的数字认证或者电子签章服务，满足湖南省公共资源交易中心平台接入相关规范。

1、满足中心《CA 证书与电子签章资源共享平台对接技术标准》的要求。

2、按照中心提供的接入要求和技术规范及时提供满足要求的接口和接口文档。

3、对接完成以后能实现提供的数字认证或者电子签章服务能全省范围内使用，一次办理全省通用。

4、从递交申请文件之日起，向贵方提供所有与本项目有关的数据、情况和技术资料真实有效。

5、遵守《湖南省公共资源交易中心 CA 证书及电子签章服务机构接入管理办法》中的各项条款及一切有关规定，并遵守签署《十不准廉洁承诺书》。

特此承诺。

承诺单位（盖章）：

日 期：

附件 4

# **CA 证书与电子签章资源共享平台 对接技术标准（V1.0）**

湖南省公共资源交易中心

2021 年 10 月



# 前 言

《CA 证书与电子签章资源共享平台对接技术标准（V1.0）》是《CA 证书及电子签章服务机构接入管理办法（试行）》的配套文件，规定了 CA 证书与电子签章资源共享平台与 CA 证书、电子签章移动端、PC 端在湖南省公共资源交易建设的电子交易系统进行集成接入的内容、方法和准则，以及配套的手写信息数字签名板设备参数以及标准接口。

《CA 证书与电子签章资源共享平台对接技术标准（V1.0）》分为三部分：

第 1 部分 《CA 证书与电子签章资源共享平台对接技术标准（移动端）》

第 2 部分 《手写信息数字签名板设备参数以及标准接口》

第 3 部分 《CA 证书与电子签章资源共享平台对接技术标准（PC 端）》

本标准第 1 部分、第 2 部分。

# 第 1 部分

## CA 证书与电子签章资源共享平台 对接技术标准（移动端）

湖南省公共资源交易中心

2021 年 10 月

## 目 次

1. CA 证书与电子签章资源共享平台对接技术标准.....	10
1.1. 范围.....	10
1.2. 规范性引用文件.....	10
1.3. 术语和定义.....	11
1.4. CA 证书与电子签章资源共享平台对接技术规范.....	- 14 -
2. CA 证书与电子签章资源共享平台 CA 证书接口信息.....	- 18 -
2.1. 集成服务接口.....	- 18 -
2.2. 证书申请.....	- 20 -
2.3. 证书续期.....	- 27 -
2.4. 证书吊销.....	- 29 -
2.5. 证书附件上传.....	- 31 -
2.6. 证书恢复申请接口.....	- 34 -
2.7. 证书更新.....	- 38 -
3. CA 证书与电子签章资源共享平台电子签章接口信息.....	- 41 -
3.1. oauth2.0 认证接口.....	- 41 -
3.2. 签章接口.....	- 54 -
附 1.....	- 70 -

# 1. CA 证书与电子签章资源共享平台对接技术标准

## 范围

本规范明确了 CA 证书与电子签章资源共享平台的集成业务要求。

本规范适用于与 CA 证书与电子签章资源共享平台进行业务集成的证书服务机构，用于规范证书服务机构开展 CA 证书移动化应用的业务集成操作。

## 1.1. 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（包括所有的修订单）适用于本文件。

GM/Z 0001 密码术语

GM/T 0009-2012 SM2 密码算法使用规范

GM/T 0015 基于 SM2 密码算法的 CA 证书格式规范

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0017 智能密码钥匙密码应用接口数据格式规范

GM/T 0018 密码设备应用接口规范

GM/T 0019 通用密码服务接口规范

GM/T 0020 证书应用综合服务接口规范

GM/T 0028 密码模块安全技术要求

GM/T 0034 基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范

GM/T 0054 信息系统密码应用基本要求

## 1.2. 术语和定义

GM/Z 0001 确立的以及下列术语和定义适用本文件。

### 1.3.1.

加密 encipherment/encryption

对数据进行密码变换以产生密文的过程。

### 1.3.2.

加密证书 encipherment certificate/exchange certificate

用于证明加密公钥的 CA 证书。

### 1.3.3.

密码算法 cryptographic algorithm

描述密码处理过程的运算规则。

### 1.3.4.

密钥 key

控制密码算法运算的关键信息或参数。

### 1.3.5.

证书更新 Certificate update

指在不改变密钥的情况下，用一个新证书来代替旧证书的过程。

### 1.3.6.

密钥更新 key update

用一个新密钥来代替旧密钥的过程，通常指证书与密钥同时更新。

### 1.3.7.

密钥恢复 key recovery

将归档或备份的密钥恢复到可用状态的过程。

#### 1.3.8.

签名证书 signature certificate

用于证明签名公钥的 CA 证书。

#### 1.3.9.

身份鉴别/实体鉴别 authentication/entity authentication

确认一个实体所声称身份的过程。

#### 1.3.10.

数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果,该结果只能用签名者的公钥进行验证,用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

#### 1.3.11.

CA 证书 digital certificate

也称公钥证书,由证书认证机构(CA)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。按类别可分为个人证书、机构证书,按用途可分为签名证书和加密证书。

#### 1.3.12.

私钥 private key

非对称密码算法中只能由拥有者使用的不公开密钥。

#### 1.3.13.

SM2 算法 SM2 algorithm

一种椭圆曲线公钥密码算法，其密钥长度为 256 比特。

#### 1.3.14.

证书撤销列表 certificate revocation list (CRL)

由证书认证机构 (CA) 签发并发布的被撤销证书的列表。

#### 1.3.15.

证书认证机构 certification authority (CA)

对 CA 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。

#### 1.3.16.

证书注册机构 registration authority (RA)

受理 CA 证书的申请、更新、恢复和注销等业务的实体。

#### 1.3.17.

证书依赖方 certificate dependent

依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。

依赖方可以是也可以不是一个证书持有者。

#### 1.3.18.

移动 CA 证书 mobile digital certificate

由移动设备承载并实现完整功能的 CA 证书。

#### 1.3.19.

移动 CA 证书平台 mobile digital certificate platform

与证书认证机构完成技术集成，利用移动设备实现证书认证机构所签发的 CA 证书的各项功能的技术平台，并提供移动 CA 证书 APP 应用。

### **1.3. CA 证书与电子签章资源共享平台对接技术规范**

#### **1.3.1. 移动 CA 证书集成服务**

CA 证书与电子签章资源共享平台提供的 CA 证书集成服务包括以下五类。

##### **1.3.1.1. 移动 CA 证书申请**

移动 CA 证书申请是通过移动端 APP，向证书注册机构申请办理 CA 证书业务。

##### **1.3.1.2. 移动 CA 证书恢复**

移动 CA 证书恢复是指在移动 CA 证书有效期内，CA 证书持有者出现承载移动 CA 证书的设备损坏或丢失时，将移动 CA 证书恢复至其它移动设备的操作。

##### **1.3.1.3. 移动 CA 证书续期**

移动 CA 证书续期是指密钥不变，移动 CA 证书有效期延长。当用户移动 CA 证书有效期届满，需要继续使用证书时，进行证书续期操作。

##### **1.3.1.4. 移动 CA 证书变更**

移动 CA 证书变更是指用户要求认证机构对已签发的 CA 证书进行证书信息变更。如单位名称、法人信息等内容的变更。

##### **1.3.1.5. 移动 CA 证书撤销**

CA 证书与电子签章资源共享平台或证书持有者在发生下列情况时，申请撤销 CA 证书：

1. 个人 CA 证书持有者不从事原岗位工作。
2. 司法机构要求撤销 CA 证书持有者证书。



3. CA 证书持有者提供的信息不真实。
4. CA 证书持有者没有或无法履行有关规定和义务。
5. CA 证书与电子签章资源共享平台或最终 CA 证书持有者有理由相信或强烈怀疑一个证书持有者的私钥安全已经受到损害。
6. 企业有理由相信或强烈怀疑其下属机构 CA 证书、人员 CA 证书的私钥安全已经受到损害。
7. 与 CA 证书持有者达成的证书持有者协议已经终止。
8. CA 证书持有者请求撤销其证书。
9. 法律、行政法规规定的其他情况。

### 1.3.2. 移动 CA 证书类型

CA 证书与电子签章资源共享平台需要提供以下类型的 CA 证书：

#### 1. 机构证书

用以代表参与公共资源交易业务的企事业单位、社会团体或其他组织的身份，如：代表单位和部门等机构身份证书。

#### 2. 个人证书

为参与公共资源交易业务的相关人员颁发的证书，用以代表个体的身份，如：评标专家、项目经理或参加交易的个人的身份证书等。

以上各类 CA 证书格式应遵循 GM/T 0015，在标识实体名称时，应保证实体身份的唯一性，且名称类型应支持 X.500、RFC-822、X.400 等标准协议格式。

### 1.3.3. 移动 CA 证书服务集成业务要求

移动 CA 证书用户利用移动 APP，在 CA 证书与电子签章资源共享平台

完成 CA 证书的申请、使用、恢复、续期、变更、撤销等业务操作。

平台接受用户操作请求后会转发至证书认证机构。

证书认证机构应满足以下业务要求。

#### **1.3.3.1. 移动 CA 证书签发要求**

##### **1. 密钥类型**

证书认证机构签发的证书应为支持 SM2-256、RSA-1024、RSA-2048 密钥类型的企业证书、个人证书。

##### **2. CSR 信息**

CA 证书的 CSR 信息应符合 PKCS#10 协议。

##### **3. CA 证书的结构**

CA 证书的组成结构应符合 X.509 标准。

##### **4. 数字信封**

数字信封由证书认证机构使用 CSR 文件的签名公钥进行加密后产生，并符合《GMT 0009-2012 SM2 密码算法使用规范》的要求。

##### **5. CA 证书信息**

CA 证书的信息以 Base64 编码格式提供。

#### **1.3.3.2. 移动 CA 证书恢复要求**

##### **1. 密钥对操作**

恢复后的加密 CA 证书的公钥和私钥与原加密 CA 证书应保持一致，不允许发生变化，以满足对加解密业务的持续支持能。

##### **2. CA 证书有效期操作**

CA 证书有效期与原 CA 证书一致，不允许发生变化。

### 3. 数字信封操作

CA 证书恢复后，数字信封应使用新的签名公钥重新生成。

#### 1.3.3.3. 移动 CA 证书续期要求

##### 1. 密钥对操作

续期后的加密 CA 证书的公钥和私钥与原加密 CA 证书应保持一致，不允许发生变化，以满足对加解密业务的持续支持能。

##### 2. 证书有效期操作

续期后，CA 证书的有效期限应从原 CA 证书有效期到期日进行更新。

##### 3. 签名 CA 证书操作

续期后，签名 CA 证书应根据原 CSR 文件重新生成。

##### 4. 数字信封操作

续期后，数字信封应使用新的签名公钥重新生成。

#### 1.3.3.4. 移动 CA 证书变更要求

##### 1. 证书有效期操作

移动 CA 证书变更后，证书有效期不发生变化。

##### 2. 变更信息更新操作

CA 证书认证机构应将变更后的 CA 证书信息提交至 CA 证书与电子签章资源共享平台进行更新。

##### 3. 签名 CA 证书操作

移动 CA 证书变更后，签名 CA 证书根据更新后的 CA 证书 CSR 文件重新生成。

##### 5. 数字信封操作

移动 CA 证书变更后，数字信封应使用新的签名公钥重新生成。

### 1.3.3.5. 移动 CA 证书撤销要求

#### 1. 移动 CA 证书撤销受理

CA 证书与电子签章资源共享平台在接到证书持有者的撤销请求后，应对其身份进行鉴别并确认其为证书持有者本人或得到了证书持有者的授权。

#### 2. CA 证书撤销操作

CA 证书认证机构应在 24 小时内，撤销符合条件的证书并发布到证书撤销列表。

#### 3. CA 证书撤销告知

CA 证书撤销后，CA 证书认证机构应通过有效方式及时告知证书持有者或依赖方证书撤销结果。

### 1.3.4. 附件上传

当存在附件时，CA 证书认证机构以 base64 编码格式提交。

## 2. CA 证书与电子签章资源共享平台 CA 证书接口信息

### 2.1. 集成服务接口

获取 Token

CA 系统分配的 appKey 和 appSecret，之后的接口需要在请求头中增加 token 标识头，token 有效期一天。

需要 token 的头信息示例如下：

Origin: chrome-extension://aejoelaoggembCAhagimdiliamlcdfm

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)  
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.142  
Safari/537.36

token:

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJhdWQiOiIwMDEiLCJleHAiOjE1NjQxOTIwMTd9.pmaQVc3PR\_COZB9V4VvqtTTZszVfHDnOWuyR1-kFA4o

Content-Type: appliCation/json

Accept: \*/\*

接口定义:

服务名称: /api/token

请求方式: GET

请求头是否需要 token: \*\*否\*\*

请求示例:

http://127.0.0.1:8008/CA/api/token/?appKey=001&appSecret=123456

输入参数

参数名称	参数说明	类型	是否必填	备注
appKey	CA 系统分配的 key	string	是	
appSecret	CA 系统分配的密钥	string	是	

输出结果

参数名称	参数说明	类型	备注
token	CA 系统生成的 token	string	

```
{
  "code": "200",
  "data": {
    "token":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJhdWQiOiIwMDEiLCJleHAiOjE1NjQyMTY3ODN9.hp-jsuG0pTAcMAgNabZG7WzPw0xrTpbAFcLTow7-tiI"
  },
  "message": "获取 token 成功"
}
```

## 2.2. 证书申请

说明：用户 CA 证书的申请

服务名称：/api/cert/apply

请求方式：POST

请求头是否需要 token：是

输入参数

参数名称	参数说明	类型	长	必	备注
------	------	----	---	---	----

			度	填	
userName	用户名称	String	128	是	个人：用户名，单位：企业名称
certType	证书类型	String	2	是	1. 个人证书，2. 机构(企业)证书
CArdID	证件号码	String	64	是	certType 为 1 时，填充个人身份证件号码。 certType 为 2 时，填充企业统一社会信用代码。
deviceNo	设备编号	String	128	否	硬件设备的编号,如果能够获取需要填写
circle	证书有效期	String	2	是	单位年
algorithm	证书算法	String	2	是	1. RSA, 2. SM2
keyLength	秘钥长度	String	6	是	当 algorithm 为 1 时,可指定 1024 或者 2048。SM2

					默认 256
mobile	联系人手机号码	String	11	是	
userEmail	邮箱	String	128	否	
userOrganization	单位名称	String	128	否	
userOrgunit	部门名称	String	128	否	
userCountry	国家	String	64	否	
userState	省份	String	64	否	
userLocality	城市	String	64	否	
userStreet	街道	String	64	否	



userTitle	职位	String	64	否	
operator	经办人名字	String	64	否	
operatorCA rdId	经办人证件号 码	String	64	否	

输入示例：

```
{
  "userName": "啊哈 test",
  "circle": "1",
  "algorithm": "2",
  "keyLength": "256",
  "certType": "2",
  "CArdID": "91110000700218641X",
  "deviceNo": "",
  "mobile": "15111111111",
  "userEmail": "123@qq.com",
  "userOrgunit": "111144414421",
  "operator": "aha2",
```

```
"operatorCardId": "130282199706243529"
}
```

#### 输出参数

参数名称	参数说明	类型	备注
bussinessCode	业务受理号	String	

#### 输出示例

```
{
  "code": "200",
  "message": "success",
  "data": {
    "bussinessCode": "8776789273782"
  }
}
```

#### 证书制作下发

说明： 根据证书申请的 code 来下发证书

服务名称： /api/cert/make

请求方式： POST

请求头是否需要 token: 是

### 输入参数

参数名称	参数说明	类型	长度	必填	备注
businessNo	受理编号	String	128	是	申请证书返回信息
csr	证书请求 CSR 字符串类型 (cfCA 传 p10)	String	4000	是	字符串类型

### 输出参数

参数名称	参数说明	类型	备注
bussinessCode	业务受理号	String	
signCert	签名证书 (补发证书则为空)	String	
signCertSerial	签名证书序列号 (补发证书则为空)	String	
cryptPrivKey	加密私钥 (使用签名公钥加密后的数据)	String	

encryptCert	加密证书	String	
encryptCertSerial	加密证书序列号	String	

返回示例

```
{
  "code": "200",
  "message": "success",
  "data": {
    "bussinessCode": "9887329382983",
    "signCert": "签名证书",
    "signCertSerial": "签名证书序列号",
    "cryptPrivKey": "加密私钥-使用签名证书加密后的数据，需要使用签名私钥解密",
    "encryptCert": "加密证书",
    "encryptCertSerial": "加密证书序列号"
  }
}
```

### 2.3. 证书续期

说明：以年为单位续期证书

服务名称：/api/cert/update

请求方式：POST

请求头是否需要 token：是

输入参数

参数名称	参数说明	类型	长度	必填	备注
certNumber	加密证书序列号	String	128	是	
signNumber	签名证书序列号	String	128	是	
time	续期年数	String	2	是	
csr	证书请求 CSR 字符串 类型	String	4000	是	

输入示例

```
{  
  
    "time":1,  
  
    "certNumber":"4414878232503860559778300024729333797214586706"
```

87",

"signNumber": "4414878232503860559778300024729333797214586706

87",

"csr": ""

}

输出参数

参数名称	参数说明	类型	备注
bussinessCode	业务受理号	String	
signCert	签名证书（补发证书则为空）	String	
signCertSerial	签名证书序列号（补发证书则为空）	String	
cryptPrivKey	加密私钥（使用签名公钥加密后的数据）	String	
encryptCert	加密证书	String	
encryptCertSerial	加密证书序列号	String	

输出示例

{

```
"code": 200,

"message": "success",

"data": {

    "encryptCert": "",

    "encryptCertSerial":

"582469728037039673872388448552626487607555436263",

    "signCert": "",

    "cryptPrivkey": "",

    "signCertSerial":

"208489358780430331463424674665939033214414107131",

    "bussinessCode": "00202010210000039"

}

}
```

#### 2.4. 证书吊销

说明：用于注销证书

服务名称：/api/cert/revoke

请求方式：POST

请求头是否需要 token: 是

输入参数

参数名称	参数说明	类型	长度	必	备注
------	------	----	----	---	----

				填	
certNumber	加密证书序列号	String	128	是	
signNumber	签名证书序列号	String	128	是	
reason	吊销原因	String	2	是	无原因 0，默认传 0

输入示例

```
{
  "certNumber": "329947057022382728755732045912693629292715204849",
  "signNumber": "329947057022382728755732045912693629292715204849",
  "reason": "0"
}
```

输出参数

参数名称	参数说明	类型	备注
code	返回编码	String	200 注销成功
message	返回信息	String	



data	返回主要内容	String	参数 bussinessCode
------	--------	--------	------------------

输出示例

```
{
  "code": 200,
  "message": "success",
  "data": {
    "bussinessCode": "202002281335531627113"
  }
}
```

## 2.5. 证书附件上传

说明：有需要附件的可以提供附件上传接口

服务名称：/api/cert/upload

请求方式：POST

请求头是否需要 token: 是

输入参数

参数名称	参数说明	类型	长度	必填	备注
certType	证书类型	Str	40	是	1: 个人证书, 2:

		ing			机构证书
bussinessCode	申请流水号	String	40	是	
authorCertificate	申请材料 (base64)	String		是	申请表或者授权书
creditCodeOrIdCard	申请材料 (base64)	String		是	证书类型为机构证书：统一社会信用代码证图片（加盖公章），证书类型为个人证书：申请人身份证正面；
applicantPhoto	申请材料 (base64)	String		是	申请人大头照
idCardReverse	申请材料 (base64)	String		否	如果为个人证书填写身份证反面，机构证书则不填写

creditCodeOrIdCardSuffix	creditCodeOrIdCard 的后缀格式	String	10	是	pdf 或者 jpg 或者 png
authorCertificateSuffix	authorCertificate 后缀	String			为 pdf 或者 jpg 或者 png
idCardReverseSuffix	idCardReverse 后缀	String			默认按照图片处理
applicantPhotoSuffix	applicantPhoto 后缀	String			默认按照图片处理

输入示例

```
{
  "certType": "1",
  "businessCode": "jdbc20200221161255739030",
  "authorCertificate": "",
  "creditCodeOrIdCard": "",
  "applicantPhoto": "",
  "idCardReverse": ""
}
```

输出示例

```
{
  "code" : "200",
  "message" : "success",
  "data" : {
    "bussinessCode": "jdbc20200221161255739030"
  }
}
```

## 2.6. 证书恢复申请接口

说明：证书恢复申请，用于上传用户恢复证书信息，之后在调用证书制作下发接口

服务名称：/api/cert/recoverApply

请求方式：POST

请求头是否需要 token: 是

输入参数

参数名称	参数说明	类型	长度	必填	备注
userName	用户名称（单位：企	Str	128	是	

	业名称)	ing			
certType	证书类型	String	2	是	1. 个人证书, 2. 机构(企业)证书
CArdID	证件号码	String	64	是	certType 为 1 时, 填充个人身份证件号码。 certType 为 2 时, 填充企业统一社会信用代码。
deviceNo	设备编号	String	128	否	硬件设备的编号, 如果能够获取需要填写
circle	证书有效期	String	2	是	单位年
algorithm	证书算法	String	2	是	1. RSA, 2. SM2
keyLength	秘钥长度	String	6	是	当 algorithm 为 1 时, 可指定 1024

					或者 2048 。 SM2 默认 256
mobile	联系人手机号码	String	11	是	
userEmail	邮箱	String	128	否	
userOrganization	单位名称	String	128	否	
userOrgunit	部门名称	String	128	否	
userCountry	国家	String	64	否	
userState	省份	String	64	否	
userLocality	城市	String	64	否	
userStreet	街道	String	64	否	

		ing			
userTitle	职位	String	64	否	
recoverReason	补发原因	String	64	否	
encryptCertSerial	需要补发的加密证书序列号	String	64	是	
recoverCode	需要补发的证书 bussinessCode	String	64	是	
encryptSignSerial	需要补发的签名证书序列号	String	64	是	

#### 输出参数

参数名称	参数说明	类型	备注
bussinessCode	业务受理号	String	

#### 输出示例

```
{  
  
  "code": "200",  
  
  "message": "success",  
  
  "data": {  
  
    "bussinessCode": "8776789273782"  
  
  }  
  
}
```

## 2.7. 证书更新

说明：用于更新证书主体信息 cn 项

服务名称：/api/cert/modify

请求方式：POST

请求头是否需要 token：是

输入参数

参数名称	参数说明	类型	长度	必填	备注
certNumber	加密证书序列号	String	128	是	
signNumber	签名证书序列号	String	128	是	



csr	证书请求 CSR 字符串类型	String	4000	是	
newName	新的企业名称	String	50	是	

输入示例

```
{
    "newName": "更新 001",
    "certNumber": "123076676459790128570726",
    "signNumber": "123076676459790128570725",
    "csr": ""
}
```

输出参数

参数名称	参数说明	类型	备注
bussinessCode	业务受理号	String	
signCert	签名证书 （补发证书则为空）	String	
signCertSerial	签名证书序列号 （补发证书则为空）	String	

cryptPrivKey	加密私钥（使用签名公钥加密后的数据）	String	
encryptCert	加密证书	String	
encryptCertSerial	加密证书序列号	String	

输出示例

```
{
  "code": 200,
  "message": "success",
  "data": {
    "encryptCert": "",
    "encryptCertSerial":
"582469728037039673872388448552626487607555436263",
    "signCert": "",
    "cryptPrivkey": "",
    "signCertSerial":
"208489358780430331463424674665939033214414107131",
    "bussinessCode": "00202010210000039"
  }
}
```

### 3. CA 证书与电子签章资源共享平台电子签章接口信息

#### 3.1. oauth2.0 认证接口

##### 3.1.1. 申请二维码数据

##### 3.1.1.1. 功能说明

该接口用于，当用户授权完成后。由标信服务器重定向到第三方服务器，如果正确，请求端和第三方服务器可以拿到 token 和 openId。

该接口用于第三方想自己展示标信二维码登录页面时，请求二维码数据字符串接口。该二维码用于标信客户端扫码授权。同时支持多种二维码类型

注意事项：响应的 header 中包含 errorCode 和 errorDesc,errorCode 为 0 时表示请求成功，errorCode 不为 0 时，errorDesc 为请求失败的描述信息 errorCode 定义详见附件 1。

接口协议：HTTP 协议

请求方式：post

接口服务地址：http(s)://ip:port/auth/applyQrCode

### 3.1.1.2. 接口说明

### 3.1.1.3. 请求消息

消息流向：第三方→oauth 服务

参数说明：

参数名称	字段类型	说明	必填
appId	String	客户端 id	是
appKey	String	客户端密钥	是
qrCodeType	Integer	二维码类型，取值（1.2..10） 1：登录二维码 2：普华签章二维码 3：CA 签章二维码 4：加密二维码 6：平台绑定二维码 7：预解密二维码 8：hash 上链二维码 9：撤销 hash 上链二维码 10 保存指纹二维码	是
qrContent	List	扩展数据，申请二维码所上传的键值对集合，客户端在扫码	否

		后可以拿到该集合内容。该内容具体需要客户端和申请二维码方商定。	
key	String	扩展数据库 key	否
value	String	扩展数据 value	否

请求 JSON 示例 (post):

```
{
  "appId": "客户端 id",
  "appKey": "客户端密钥"
  "qrCodeType": 1 ,
  "qrContent": [
    {
      "key": "23232",
      "value": "23232"
    }
  ]
}
```

#### 3.1.1.4. 响应消息

消息流向：oauth 服务→第三方服务

响应参数列表

参数名称	字段类型	说明	必填
qrCode	String	二维码信息字符串	是
expireTime	Integer	二维码过期时间，单位秒	是
intervalTime	Integer	轮训的间隔时间单位秒	是
businessid	String	一次会话的唯一标识	是

返回 JSON 示例：

```
{  
    "qrCode": "二维码信息",  
    "expireTime": 300, //二维码过期时间，单位秒  
    "intervalTime": 2, //轮训的间隔时间单位秒  
    "businessid": "xxx" // 一次会话的唯一标识  
}
```

### 3.1.2. 检测是否授权状态

#### 3.1.2.1. 功能说明

该接口用在第三方客户端上，以间隔一定时间去轮训标信服务器，查看是否授权成功。该接口配合 1.3 接口获取二维码之后，查询二维码值接口。

#### 3.1.2.2. 接口说明

响应的 header 中包含 errorCode 和 errorDesc, errorCode 为 0 时表示请求成功，errorCode 不为 0 时，errorDesc 为请求失败的描述信息  
errorCode 定义详见 附录 1

该接口应该轮训调用，轮训间隔时间应为，接口 1.3 中 intervalTime 中的值，如果访问周期小于该时间，则会认为非法操作，强行终止本授权。

协议：HTTP 协议

请求方式：post

接口服务地址：http(s)://ip:port/auth/queryQrStatus

#### 3.1.2.3. 请求消息

消息流向：第三方→oauth 服务

参数说明：

参数名称	字段类型	说明	必填
appId	String	客户端 id	是
appKey	String	客户端密钥	是
qrCode	String	二维码信息，取值为 1.3 接口返回的 qrCode	是

请求 JSON 示例 (post)：

```
{  
  
  "appId": "xxxx"  
  
  "appKey": "xxx"  
  
  "qrCode": "xxx"  
  
}
```

#### 3.1.2.4. 响应消息

消息流向：oauth 服务—>第三方服务

响应参数列表



参数名称	字段类型	说明	必填
qrCodeStatus	String	<p>二维码状态取值（1. 2. 3. 4. 5）</p> <p>1: 初始化</p> <p>2: 已扫码</p> <p>3: 已授权</p> <p>4: 拒绝授权</p> <p>5: 二维码已过期</p> <p>返回值 qrCodeStatus 当为 3 的时候表示成功。 当为 1 和 2 时应继续轮训</p>	是
token	String	客户端密钥	否
openId	String	<p>是指标信发放针对用户在第三方平台下的唯一 id。举例</p> <p>标信用户 id 和组关系的 id 为 a</p> <p>有三个第三方平台 A B C</p> <p>则，在 A 平台下的用户 openId</p>	否

		为 Aa  在 B 平台下的用户 openId 为 Ba  在 C 平台下的用户 openIdwei CA	
url	String	第三方申请 app 时, 提供的 url	否
companyName	String	企业名称	否

返回 JSON 示例:

```
{
  "qrCodeStatus":1, //二维码状态 取值范围 1: 初始化 2 已扫码
  3 已授权 4 拒绝授权 5 二维码已过期
  "token":"200189a0f4bf0f63deebb9f6f186f92f4a7f",
  "openId":"255454445DDSA",
  "url":"xxx",
  "companyName":"xxx"
}
```

### 3.1.3. 获取用户详细信息

#### 3.1.3.1. 功能说明

用户 oauth 认证通过后，且配置该资源权限。即可访问该接口获取用户相关信息。

#### 3.1.3.2. 接口说明

注意事项： 接口调用的传入参数和返回参数以 json 形式组成，在 header 中添加 token 字段，内容为 token；响应的 header 中包含 errorCode 和 errorDesc，errorCode 为 0 时表示请求成功，errorCode 不为 0 时，errorDesc 为请求失败的描述信息，errorCode 定义详见 附录 1

协议：HTTP 协议

请求方式：post

接口服务地址：http(s)://ip:port/auth/getUserInfoDetail

#### 3.1.3.3. 请求消息

消息流向：第三方—>标信服务

参数说明：

请求 JSON 示例 (post)：

无需传参，在 head 中添加 token 即可

### 3.1.3.4. 响应消息

消息流向：oauth 服务→第三方服务

响应参数列表

参数名称	字段类型	说明	必填
name	String	用户姓名	否
businessType	Integer	业务类型取值（1.2..10）  1：登录二维码  2：普华签章二维码  3：CA 签章二维码  4：加密二维码  5：解密二维码  6：平台绑定二维码  7：预解密二维码  8：hash 上链二维码  9：撤销 hash 上链二维码  10 保存指纹二维码	是

sex	Integr	性别信息，取值范围  1：男  其他：女	否
userId	String	用户唯一标识	是
nation	String	民族	否
address	String	地址	否
telephone	String	手机号码	是
companyName	String	公司名称	是
licenseNumber	String	公司营业执照号码	否
orgCode	String	组织机构代码	是
CAUserId	String	用户 CA 唯一标识	是
cert	String	证书编码	是
algorithmLength	Integr	算法长度	是
algorithmType	Integr	算法	是

		1: SM2_256 2: RSA_1024 3: RSA_2048	
CAType	Integr	CA 类型 1:RSA 签名证书 2:SM2 签名证书 3: SM2 加密证书	是
status	Integr	CA 状态 1: 启用 2: 禁用 3: 撤销 4: 过期	是

注：//一个 CA 包含 签名和加密证书.CAuserid 标识一个 CA

返回 JSON 示例：

```
{

    "name": "姓名",

    "nation": "民族",

    "sex": 1,

    "businessType": 1,

    "address": "地址",

    "telephone": "手机号码",

    "companyName": "公司名称",

    "licenseNumber": "公司营业执照号码",

    "orgCode": "组织机构代码",

    "CA": [

        {

            "CAUserId": "xxx",

            "cert": "证书编码",

            "algorithmLength": 1024,

            "algorithmType": 1,

            "CAType": 1,
```

```
        "status":1
    }
]
}
```

### 3.2. 签章接口

签章所有接口需要在 header 中添加 token, token 的值为 OAuth 授权成功后返回的 token (参照接口 1.4 检测是否授权状态 的响应结果)

所有接口都会在响应的 header 中返回 errorCode 和 errorDesc; errorCode 为 0 表示成功, 否则失败, 具体失败原因参照对应接口的响应错误码列表; errorDesc 为错误信息, 由于包含中文, 所以需要 URLDecode 解码后才能正常显示。

#### 3.2.1. 获取通道唯一标识

##### 3.2.1.1. 功能说明

扫码登录成功后, 获取通道唯一标识 (uuid), uuid 作为一次交易的唯一标识, 在通道未关闭前可通过 uuid 调用其他交易接口;



### 3.2.1.2. 接口说明

接口协议：HTTP 协议

请求方式：POST

请求数据类型：appliCation/json

接口服务地址：http(s)://ip:port/trade/getSignId

### 3.2.1.3. 参数说明

参数名称	字段类型	说明	必填
qrCode	String	请求 OAuth 登录二维码时返回的 qrCode	是
contractNumbers	String	合同编号列表	否

请求示例：

```
{  
  
    "qrCode" : "xxx" ,  
  
    "contractNumbers" : "[\ "xxx\" ]"  
  
}
```

#### 3.2.1.4. 响应消息

字段	类型	说明
uuid	String	一次交易通道的唯一标识

返回 JSON 示例：

```
{  
  
  "uuid" : "xxx"  
}
```

#### 3.2.1.5. 响应错误码

4329327035370 服务器内部错误

### 3.2.2. 获取印章及 CA（轮询）

#### 3.2.2.1. 功能说明

获取用户所在单位的印章和 CA，用于签章过程；

#### 3.2.2.2. 接口说明

接口协议：HTTP 协议

请求方式：POST

请求数据类型：applicAtion/json

接口服务地址：http(s)://ip:port/trade/getStampInfo

### 3.2.2.3. 参数说明：

参数名称	字段类型	说明	必填
uuid	String	通道唯一标识	是

请求示例：

```
{  
  
    "uuid" : "xxx"  
  
}
```

### 3.2.2.4. 响应消息

字段	类型	说明
status	Integer	轮询状态：为 0 表示需要继续轮询，为 1 则结束轮询
userName	String	用户姓名

signType	Integer	签名类型，1: CA 证书签名，2: 普华签名
list	Json	<pre>[{     "stampList": [{         "stampName": "xxx",    // 印章名称         "stampDataBase64": "xxx" // 印章 base64     }],     "cert": "xxx",    // 签名证书, 普华签名时为 null     "certAlgorithmType": 1, // 证书算法类型: 1 (sm2 256)、2 (rsa 1024)、3 (rsa2048) }]</pre>

返回 JSON 示例:

```
{
```

```

“status”：0, // 0 表示需要继续轮询，1 表示有结果

“userName”： “”,

“signType”：1, // 1: CA 证书签名, 2: 普华签名

“list”： [{

    “stampList”： [{

“stampName”： “xxx”,

“stampDataBase64”： “xxx” // 印章 base64

}],

    “cert”： “xxx”, // 签名证书, 普华签名时为 null

“certAlgorithmType”：1, //证书算法类型：1 (sm2 256)、2 (rsa 1024)、

3 (rsa2048)

}]

}

```

### 3.2.2.5. 响应错误码

4329327035369 非法的 uuid

4329327035370 服务器内部错误

4329327035372 没有可用的印章

4329327035373 没有可用的 CA 证书

4329327035387 用户取消此次操作

### 3.2.3. 上传需要签名的文件摘要

#### 3.2.3.1. 功能说明

上传需要签名的文件摘要以及告知本次签名之后是否结束；文件摘要需要 SM3 算法处理；

#### 3.2.3.2. 接口说明

接口协议：HTTP 协议

请求方式：POST

请求数据类型：appliCAtion/json

接口服务地址：http(s)://ip:port/trade/uploadFileDigest

#### 3.2.3.3. 参数说明：

参数名称	字段类型	说明	必填
uuid	String	通道唯一标识	是
fileDigest	String	文件摘要	是

cert	String	签名证书，普华签名时为 null	否
status	Integer	签名状态，0 表示签名未结束， 1 表示本次为最后一次签名，-1 表示取消本次签名	是

请求示例：

```
{
    "uuid": "xxx",    // 通道唯一标识
    "fileDigest": "xxx",    // 文件摘要
    "cert": "xxx",    // 签名证书，普华签名时为 null
    "status": 0        // 0 表示签名未结束，1 表示本次为最后一次签名，
-1 表示取消本次签名
}
```

### 3.2.3.4. 响应消息

字段	类型	说明
channelStatus	Integer	当前通道状态：0 表示正常、1 表示用户已 关闭此次流程

返回 JSON 示例：

```
{  
  
    "channelStatus": 1 // 通道状态：0 表示正常、1 表示用户已关闭  
  
    此次流程  
  
}
```

### 3.2.3.5. 响应错误码

4329327035369 非法的 uuid

4329327035370 服务器内部错误

### 3.2.4. 查询签名结果（轮询）

#### 3.2.4.1. 功能说明

轮询获取用户在 App 端对文件摘要的签名结果；

#### 3.2.4.2. 接口说明

接口协议：HTTP 协议

请求方式：POST

请求数据类型：application/json

接口服务地址：http(s)://ip:port/trade/getSignResult



#### 3.2.4.3. 参数说明：

参数名称	字段类型	说明	必填
uuid	String	通道唯一标识	是

请求示例：

```
{  
  
    "uuid": "xxx"    // 通道唯一标识  
  
}
```

#### 3.2.4.4. 响应消息

字段	类型	说明
status	Integer	轮询状态：为 0 表示需要继续轮询，为 1 则结束轮询
cert	String	签名证书
fileDigest	String	文件摘要
signDigest	String	对摘要签名后的结果

t		
channelStatus	Integer	当前通道状态：0 表示正常、1 表示用户已关闭此次流程

返回 JSON 示例：

```
{
  "status": 0, // 0 表示需要继续轮询，1 表示有结果
  "cert": "xxx", // 签名证书
  "fileDigest": "xxx", // 文件摘要
  "signDigest": "xxx", // 对摘要签名后的结果
  "channelStatus": 1 // 通道状态：0 表示正常、1 表示用户已关闭此次流程
}
```

### 3.2.4.5. 响应错误码

4329327035369 非法的 uuid

4329327035370 服务器内部错误

4329327035391 用户签名失败

4329327035387 用户取消此次操作

### 3.2.5. 查询通道状态

#### 3.2.5.1. 功能说明

根据 uuid 查询当前通道状态；

#### 3.2.5.2. 接口说明

接口协议：HTTP 协议

请求方式：POST

请求数据类型：appliCation/json

接口服务地址：http(s)://ip:port/trade/getChannelStatus

#### 3.2.5.3. 参数说明：

参数名称	字段类型	说明	必填
uuid	String	通道唯一标识	是

请求示例：

```
{  
  
    "uuid": "xxx"    // 通道唯一标识  
  
}
```

#### 3.2.5.4. 响应消息

字段	类型	说明
status	Integer	轮询状态：为 0 表示需要继续轮询，为 1 则结束轮询

返回 JSON 示例：

```
{  
  
  "status": 0  // 0 表示需要继续轮询，1 表示结束  
  
}
```

#### 3.2.5.5. 响应错误码

4329327035369 非法的 uuid

4329327035370 服务器内部错误

### 3.2.6. 上报签章结果

#### 3.2.6.1. 功能说明

告知签章是否成功

### 3.2.6.2. 接口说明

接口协议：HTTP 协议

请求方式：POST

请求数据类型：appliCation/json

接口服务地址：http(s)://ip:port/trade/notifySignetResult

### 3.2.6.3. 参数说明：

参数名称	字段类型	说明	必填
uuid	String	通道唯一标识	是
stampName	String	印章名称	是
operateType	Integer	操作类型：1：签章、2：删除 签章	是
status	Integer	1:成功, 0: 失败	是

请求示例：

```
{  
  
    "uuid": "xxx", // 通道唯一标识  
  
    "stampName": "xxx",
```

```
“operateType” : 1,  
“status” : 1  
}
```

#### 3.2.6.4. 响应消息

无

#### 3.2.6.5. 响应错误码

4329327035369 非法的 uuid

4329327035370 服务器内部错误

### 3.2.7. 完成此次交易通道

#### 3.2.7.1. 功能说明

完成此次交易流程；

#### 3.2.7.2. 接口说明

接口协议：HTTP 协议

请求方式：POST

请求数据类型：appliCation/json

接口服务地址：http(s)://ip:port/trade/finishTradeChannel

### 3.2.7.3. 参数说明

参数名称	字段类型	说明	必填
uuid	String	通道唯一标识	是
status	Integer	状态：0 表示失败，1 表示成功	是

请求示例：

```
{  
  
    "uuid" : "xxx" ,    // 通道唯一标识  
  
    "status" : 0        // 0 表示失败，1 表示成功  
  
}
```

### 3.2.7.4. 响应消息

返回 JSON 示例：

```
{}
```

### 3.2.7.5. 响应错误码

4329327035369 非法的 uuid

4329327035370 服务器内部错误

#### 附 1

errorCode 码	errorDesc
0	成功
1001	appId 或者 appKey 不匹配
1002	二维码已失效
1003	扫码初始状态
1004	用户已扫码
1005	用户拒绝授权
1006	用户同意扫码
1007	用户权限不够
1008	回调地址与填写地址不一致
1009	该平台已被禁用
1010	用户没有权限访问该接口



## 第 2 部分

# 手写信息数字签名板 设备参数以及标准接口

湖南省公共资源交易中心

2021 年 10 月

## 目 次

1. 设备参数.....	73	-
2. 标准接口.....	75	-
2.1. 初始化签名.....	75	-
2.2. 设置业务参数.....	76	-
2.3. 设置数据签名原文.....	76	-
2.4. 设置签名人信息.....	77	-
2.5. 采集签名证据数据.....	77	-
2.6. 获取签名证据数据.....	78	-
2.7. 获得加密包数据.....	79	-
2.8. 获得服务端签名包.....	79	-
2.9. 验证数据签名.....	80	-
2.10. 设备人证比对接口.....	81	-
2.11. 获取错误码.....	81	-

## 1. 设备参数

模块	项目	参数
核心系统	CPU	国产 CPU，四核，1.8GHz
	操作系统	Android 7.1
	系统内存	2GB（可扩容至 4G）
	存储容量	16GB（可扩容至 64G）
	TF 卡扩展（可选）	最支持 128GB
显示屏	尺寸	10.1 寸
	屏幕类型	IPS LCD
	显示比例	16：10
	分辨率	1280*800
	亮度	250cd/m <sup>2</sup>
	对比度	800：1
	颜色质量	24 位真彩色
	可视角度	水平 $\geq 170^{\circ}$ ，垂直 $\geq 170^{\circ}$

触控屏	特征	电磁电容一体屏
	触控	5 点触控
	电子签名加密	支持
	无故障点击次数	$\geq 100$ 万次
	电子签名感应方式	电磁感应
	电子签名压感	$\geq 2048$
	电子签名最高读取速率	$\geq 220$ 点/秒
电磁笔	无源电磁笔	支持
人像红外双目摄像头 DC13	型号	彩色
	传感器尺寸	1/3"
	分辨率	2048*1536
	像素	300 万
	帧率	2048*1536@20fps
指纹仪	普通指纹仪	指纹仪具体信息：图像大小： 256*288pixel,

		图像分辨率：50,0dpi
二代证阅读器	公安部	支持
语音模块	拾音器	支持
	麦克风	支持
USB 速度	USB 连接	支持，USB HID 免驱

## 2. 标准接口

### 2.1. 初始化签名

接口函数：AS\_InitSign

接口作用：初始化所有签名数据，声明签名类型

接口声明：

a、签名：long AS\_InitSign(long signType);

b、参数：signType: 签名类型; 0 为 pdf 签名, 1 为数据签名;

c、默认值：无;

d、返回值：0 为成功，其他值为错误码;

e、是否必选：是;

接口说明：每次业务的开始，必须调用。

## 2.2. 设置业务参数

接口函数：AS\_SetBusinessParam

接口作用：设置业务的基本参数

接口声明：

a、签名：long AS\_SetBusinessParam (LONG ParamType, BSRT Param);

b、参数：ParamType: 参数类型;1, 代表工单号;2 代表渠道号; Param: 标识具体内容;

c、默认值：无;

d、返回值：0 为成功，其他值为错误码;

e、是否必选：是;

接口说明：初始化签名之后，必须调用。PDF 签名必须设置工单号和渠道号,工单号是业务系统自定的。

数据签名只需要设置渠道号，每个项目的渠道都不同，必须按照项目规定的渠道号进行设置。

## 2.3. 设置数据签名原文

接口函数：AS\_SetSignPlain

接口作用：设置签名数据原文

接口声明：

a、签名：long AS\_SetSignPlain(BSTR plainBase);

b、参数：plainBase:原文的 base64 数据；

c、默认值：无；

d、返回值：0 为成功，其他值为错误码；

e、是否必选：是；

接口说明：外传原文数据不能超过 6M ，如果要传大文件，可以在配置文件中修改 SignFileMaxSize 选项。

## 2.4. 设置签名人信息

接口函数：AS\_SetSignerInfo

接口作用：设置手写签名人的信息

接口声明：

a、签名：long AS\_SetSignerInfo(BSTR name, BSTR IDType, BSTR ID)；

b、参数：name: 签名人姓名；IDType: 证件类型，1 为身份证，2 为军官证，3 为护照，4 为户口本，5 为其他证件 ID: 证件号码

c、默认值：无；

d、返回值：0 为成功，其他值为错误码；

e、是否必选：是；

接口说明：每次签名或批准之前必须调用。

## 2.5. 采集签名证据数据

接口函数：AS\_AddSignEvidenceData

接口作用：采集签名证据数据

接口声明：

- a、签名：long AS\_AddSignEvidenceData();
- b、参数：无；
- c、默认值：无；
- d、返回值：0 为成功，其他值为错误码；
- e、是否必选：是；

接口说明：打开对话框,采集手写签名图片、轨迹，以及指纹图片、照片，可以在签名后调用 AS\_GetSignEvidenceData() 来获取相关证据数据。每次签名前都会有合规性提示，同意后才能进行 手写签名。

前置条件：设置了原文，设置了业务参数，设置了签名人信息，pdf 签名还需设置签名位置。

## 2.6. 获取签名证据数据

接口函数：AS\_GetSignEvidenceData

接口作用：获取当前签名证据数据

接口声明：

- a、签名：BSTR AS\_GetSignEvidenceData(long dataType);
- b、参数：dataType:指定获取的数据类型： 0 为手写图片 1 为批注图片 2 为指纹图片 3 为拍照图片 4 为手写轨迹 5 为 OCR 6 为扩展项
- c、默认值：无；



d、返回值：再次采集签名数据后, 签名证据数据会被覆盖;

e、是否必选：是;

接口说明：再次采集签名数据后, 签名证据数据会被覆盖

## 2.7. 获得加密包数据

接口函数：AS\_GetBusinessString

接口作用：获得签名后的加密包，包含了手写签名及证据数据，业务系统使用这个包去签名服务器进行 pdf 签名或数据签名。

接口声明：

a、签名：BSTR AS\_GetBusinessString();

b、参数：无;

c、默认值：无;

d、返回值：返回加密包数据, 加密包格式为 json 格式;

e、是否必选：是;

接口说明：该函数在签名完成之后调用，会对此前签名的相关数据进行加密封装并返回给调用者。加密包属于中间过程产生的数据，完成签名后，加密包不需要保存。

## 2.8. 获得服务端签名包

接口函数：AS\_GetSignPackage

接口作用：发送加密包到信手书服务器，并获得服务端签名包，数据签名专用。

接口声明：

- a、签名：BSTR AS\_GetSignPackage(BSTR businessString);
- b、参数：businessString: 加密包数据，通过 AS\_GetBusinessString

接口获取；

- c、默认值：无；
- d、返回值：服务端签名包；
- e、是否必选：是；

接口说明：获得服务端签名包

前置条件：调用 AS\_GetBusinessString 接口获取加密包数据

## 2.9. 验证数据签名

接口函数：AS\_VerifySign

接口作用：验证数据签名。

接口声明：

- a、签名：long AS\_VerifySign(BSTR signValue, BSTR plainBase64);
- b、参数：signValue: 签名包（AS\_GetSignPackage 接口的返回值），或者签名包中的某一个签名。

BSTR plainBase64: 签名原文的 base64 数据，需要和 AS\_SetSignPlain 设置的签名原文一致；

- c、默认值：无；
- d、返回值：0 为成功，其他值为错误码；

e、是否必选：是；

接口说明：无

## 2.10. 设备人证比对接口

接口函数：AS\_IdentifyVerification

接口作用：人证比对接口

接口声明：

a、签名：BSTR AS\_IdentifyVerification()；

b、参数：无；

c、默认值：无；

d、返回值：返回二代证的 json 结构数据，为空时表示读二代证失败，通过 AS\_GetLastError 获取错误信息；

e、是否必选：是；

接口说明： 1、调用次接口设备自动获取二代证信息。

2、“双目摄像头”拍照同时做活体检测，并与二代证照片比对，比较通过自动设置签名人信息。

3、“单摄像头”只做拍照并和二代证照片比对，比较通过自动设置签名人信息。

前置条件：无

## 2.11. 获取错误码

接口函数：AS\_GetLastError

接口作用：获取返回值为 BSTR 的接口调用失败的错误码

接口声明：

a、签名：LONG AS\_GetLastError(void);

b、参数：无；

c、默认值：无；

d、返回值：具体的错误代码；

e、是否必选：否；

接口说明：对于返回值为 BSTR 的接口，在调用失败后，不能获知具体的错误原因，若想获取具

体的错误码，在 BSTR 的接口返回 “” 后可调用此接口。