安徽省公共资源交易平台数字证书（手机扫码）互认对接指南

（试行）

2021 年 7 月

目 录

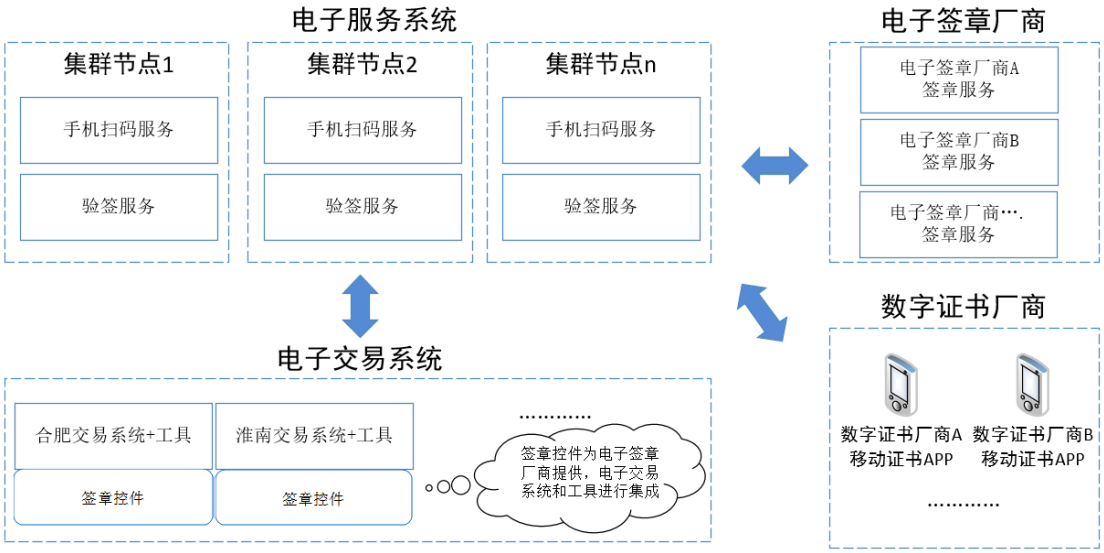
一、总体架构

安徽省公共资源交易监管平台（省电子服务系统）制定数字证书手机扫码身份认证、电子签名、加解密等通用接口规范，提供数字证书 APP、平台系统（交易、服务、监管系统）等信息交互的安全通道，以及电子签名验签服务。

数字证书厂商按照接口规范开发数字证书 APP，实现身份认证、电子签名、加解密，以及手机扫码互认等功能。

电子签章厂商按照接口规范提供签章控件及签章服务，实现签章、撤章和离线验签等功能。

电子交易系统集成签章控件，按照接口规范生成二维码，通过手机扫码完成份认证、电子签名、加解密等。



二、技术实现

1 接口约定

接口采用 https 协议进行通信。

1.1 数据格式

如接口未做格式特殊说明，则按照如下格式：

1、上传格式：Content-type: APPlication/x-www-for

m-urlencoded;utf-8 格式。

2、返回格式：Content-type:APPlication/json;utf-8 格式。

1.2 数据字典

类型	可选值	说明
操作状态（status）	0:未处理 1:已扫码 2:已确认 3:已取消 4:二次放入签章 hash 5:签章控件获取证书信息成功	
操作类型（type）	1:签名 2:加密 3:解密 4:登录 5:签章 6:撤章	
CA 类型（certType）	0 或空: 任何证书 1: 机构证书 2: 个人证书	

2 手机扫码服务类接口

2.1 获取操作授权码

接口地址：/grantToken

输入参数：

名称	中文名称	备注
accountName	用户名称	
password	密码	
guid	需要绑定的操作主键	此值可为空；为空，只能调用初始化接口，并且调用初始化接口后，默认绑定到初始化后的操作主键。

返回信息：

名称	中文名称	备注
token	授权码	有效期半个小时
invokeCode	调用状态	1:成功　其它值均为失败
failMessage	失败信息	调用失败时返回中文消息

2.2 初始化信息接口

接口地址：/initMessage

输入参数：

名称	中文名称	备注
type	类型	参见数据字典
message	需处理的信息	【此值定义根据操作业务不同，格式也有不同，具体定义详见各业务接口“参数定义说明”】
title	显示的标题	在手机 APP 中显示的标题
certType	需要的证书类型	参见数据字典

名称	中文名称	备注
token	授权码	获取操作授权码接口返回的 token
extMessage	扩展信息	扩展信息

返回信息：

名称	中文名称	备注
guid	主键	
invokeCode	调用状态	1:成功，401：无　其它值均为失败
failMessage	失败信息	调用失败时返回中文消息

2.3 获取初始化信息接口

接口地址：/getInitMessage

输入参数：

名称	中文名称	备注
guid	主键	
token	授权码	

返回信息：

名称	中文名称	备注
invokeCode	调用状态	1:成功，401：无　其它值均为失败
failMessage	失败信息	调用失败时返回中文消息
title	显示的标题	在手机 APP 中显示的标题
certType	需要的证书类型	参见数据字典

名称	中文名称	备注
extMessage	扩展信息	扩展信息
type	类型	参见数据字典
message	需处理的信息	【此值定义根据操作业务不同，格式也有不同，具体定义详见各业务接口“参数定义说明”】

2.4 获取操作结果

接口地址：/getCaMessageResult

输入参数：

名称	中文名称	备注
guid	主键	
token	授权码	

返回信息：

名称	中文名称	备注
status	状态	参加数据字典
value	处理后的值	【此值定义根据操作业务不同，格式也有不同，具体定义详见各业务接口“参数定义说明”】
invokeCode	调用状态	1:成功　其它值均为失败
failMessage	失败信息	调用失败时返回中文消息

2.5 二维码规则

1、二维码示例

2、二维码格式

二维码中为 json 信息，如下：

名称	含义	说明
guid	初始化信息的唯一键	
url	手机扫码服务地址	
city	使用者所在地市、平台	用于 APP 区分证书在哪个地市使用

city 说明：

平台编码	含义	说明
P3401000001	合肥市公共资源交易平台	
P3402000002	芜湖市公共资源交易平台	
P3403000003	蚌埠市公共资源交易平台	
P3404000004	淮南市公共资源交易平台	
P3405000005	马鞍山市公共资源交易平台	
P3406000006	淮北市公共资源交易平台	

平台编码	含义	说明
P3407000007	铜陵市公共资源交易平台	
P3408000008	安庆市公共资源交易平台	
P3410000009	黄山市公共资源交易平台	
P3411000010	滁州市公共资源交易平台	
P3412000011	阜阳市公共资源交易平台	
P3413000012	宿州市公共资源交易平台	
P3415000013	六安市公共资源交易平台	
P3416000014	亳州市公共资源交易平台	
P3417000015	池州市公共资源交易平台	
P3418000016	宣城市公共资源交易平台	
Z340000000F	综合评标评审专家库系统	
ZXSPPT00001	投资项目在线审批监管平台	
P3402000018	长江产权交易所电子交易系统	
P3401000019	优质采电子招标投标与采购平台	
P3401000020	安徽省产权交易中心电子交易系统	
……	……	

2.6 获取初始化信息

接口地址：/getInitMessage

输入参数：

名称	中文名称	备注
guid	主键	
token	授权码	

返回信息：

名称	中文名称	备注
message	需处理的信息	【此值定义根据操作业务不同，格式也有不同，具体定义详见各业务接口“参数定义说明”】
type	类型	1:签名 2：加密 3:解密 4:登录
title	标题	需要显示的标题
invokeCode	调用状态	1:成功 其它值均为失败

2.7 保存处理结果

接口地址：/saveCaMessageResult

输入参数：

名称	中文名称	备注
guid	主键	
value	值	【此值定义根据操作业务不同，格式也有不同，具体定义详见各业务接口“参数定义说明”】
status	状态	参见数据字典

名称	中文名称	备注
extMessage	附加信息	
token	授权码	

返回信息：

名称	中文名称	备注
invokeCode	调用状态	1:成功　其它值均为失败
failMessage	失败信息	调用失败时返回中文消息

2.8 获取签章图片

接口地址：/getSealImg

输入参数：

名称	中文名称	备注
guid	签章操作主键	
token	授权码	

返回参数：APPlication/json

名称	中文名称	备注
invokeCode	调用状态	1:成功　其它值均为失败
failMessage	失败信息	调用失败时返回中文消息
signInfos	印章数据	Jsonarry

Json 参数定义说明

signInfos 说明：

名称	类型	中文名称
signName	String	印章名称
signWidth	String	印章宽度（cm）
signHeight	String	印章高度（cm）
img	String	印章图片数据（base64）
description	String	印章相关描述

3 签章服务类接口

3.1 获取印章数据接口

接口地址：/api/getSeal

输入参数：

名称	中文名称	备注
caSerialId	证书序列号	必填
accountName	授权账号	必填
password	授权密码	必填

返回参数：APPlication/json

名称	中文名称	备注
code	错误码	“0”正常，其他异常
message	错误描述	
userInfo	用户数据	Json
signInfos	印章数据	Jsonarry

Json 参数定义说明

userInfo 说明：

名称	类型	中文名称
userId	String	用户唯一标识
APPlyDate	String	启用日期
overDate	String	过期日期
userName	String	用户名称
phone	String	联系方式

signInfos 说明：

名称	类型	中文名称
signName	String	印章名称
signWidth	String	印章宽度（cm）
signHeight	String	印章高度（cm）
signExt	String	印章图片后缀
signData	String	印章图片数据（base64）
description	String	印章相关描述
APPlyDate	String	启用日期
overDate	String	过期日期
signType	String	印章类型

三、应用场景

1 登录

1.1 流程说明

1、电子交易系统生成随机数，调用手机扫码服务获取授权码并初始化登录操作，获取操作唯一键。

获取 token 调用示例：

curl -X POST -H 'Content-Type: APPlication/x-www-form-urlencoded' -i '手机扫码服务/grantToken' --data 'accountName=xxx&password=xxx'

返回数据：

{"token":"36b6a611-0c97-47f3-a070-7d3d0ffaddd4","invokeCode":1}

http 调用初始化信息示例：

curl -X POST -H 'Content-Type: APPlication/x-www-form-urlencoded' -i '手机扫码服务/initMessage' --data 'type=4&message=f7c54891-adad-4f32-9994-83d70a7204a2&title=xx 系统登录&certType=0&token=36b6a611-0c97-47f3-a070-7d3d0ffaddd4'

返回数据：

{"guid":"bf1af3f2-97b0-4b04-a054-ad7ba824eb70","invokeCode":1}

2、电子交易系统按照规则生成二维码并展示，启动轮询获取操作状态。轮询超过五分钟则停止轮询，提示二维码过期。轮询间隔建议 3-5s。

http 调用示例：

curl -X GET -H 'Content-Type: APPlication/x-www-form-urlencoded' -i '手机扫码服务地址/getCaMessageResult? guid=bf1af3f2-97b0-4b04-a054-ad7ba824eb70&token=36b6a611-0c97-47f3-a070-7d3d0ffaddd4'

返回数据：

{"status":0,"invokeCode":1,"value":null,"extMessage":null}

3、APP 扫描二维码，根据二维码信息调用扫码服务获取授权 token 并初始化信息。

http 调用示例：

curl -X POST -H 'Content-Type: APPlication/x-www-form-urlencoded' -i '手机扫码服务地址/getInitMessage' --data 'guid=bf1af3f2-97b0-4b04-a054-ad7ba824eb70&token=36b6a611-0c97-47f3-a070-7d3d0ffaddd4'

返回数据：

{"message":"f7c54891-adad-4f32-9994-83d70a7204a2","title":"xx 系统登录","invokeCode":1,"certType":0,"type":"4"}

4、APP 判断为登录操作，对存入的随机数进行 p7 附原文签名，将签名值存入到手机扫码服务中。

http 调用示例：

curl -X POST -H 'Content-Type: APPlication/x-www-form-urlencoded' -i '手机扫码服务地址/saveCaMessageResult' --data ' guid=bf1af3f2-97b0-4b04-a054-ad7ba824eb70&value= 签 名 值 &extMessage= 扩 展 值 &status=2&token=36b6a611-0c97-47f3-a070-7d3d0ffaddd4 '

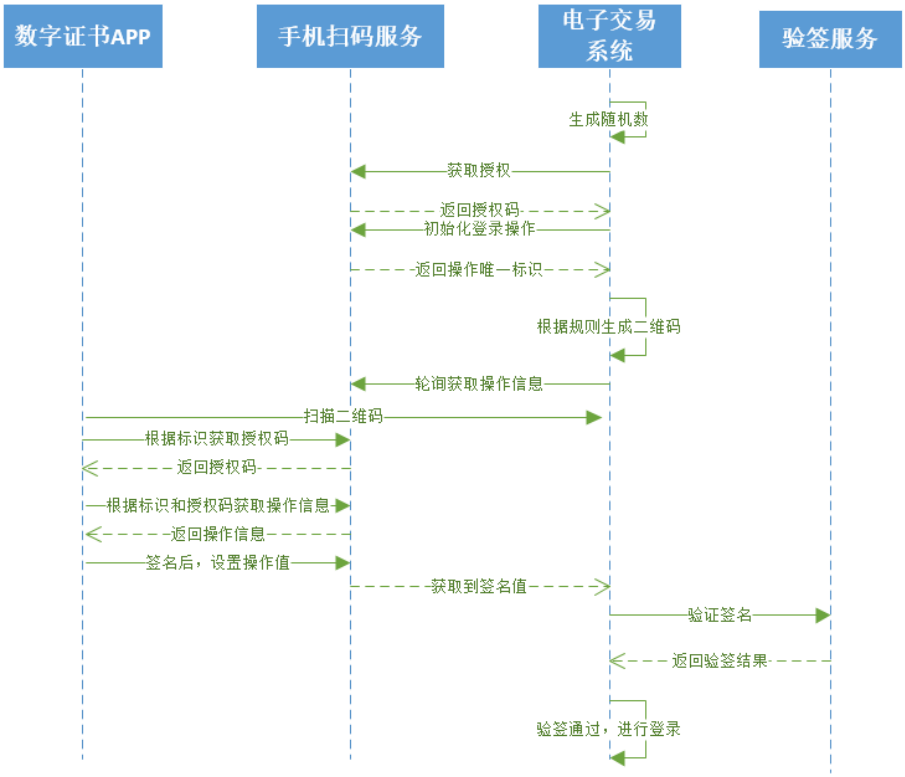
返回数据：

{"invokeCode":1}

5、电子交易系统，调用验签服务器签名值进行验签，并比较签名值与存入的是否一致。

6、验签与比较通过，通过签名值获取到公钥证书，进行登录操作。

1.2 调用流程图



1.3 参数定义说明

名称	对应接口名称	说明
message	初始化信息接口	String 类型，登录的随机数
value	保存处理结果&获取操作结果	JSON 格式的字符串，JSON 描述见下表。

value 描述

名称	中文名称	备注
signStr	签名值	针对随机数的签名值
pubCert	公钥证书	

2 签名

2.1 流程说明

1、电子交易系统调用手机扫码服务，获取授权码并初始

化签名操作，获取操作唯一键。

2、电子交易系统按照规则生成二维码展示，并启动轮询获取操作状态。轮询超过五分钟则停止轮询，提示二维码过期。轮询间隔建议 3-5s。

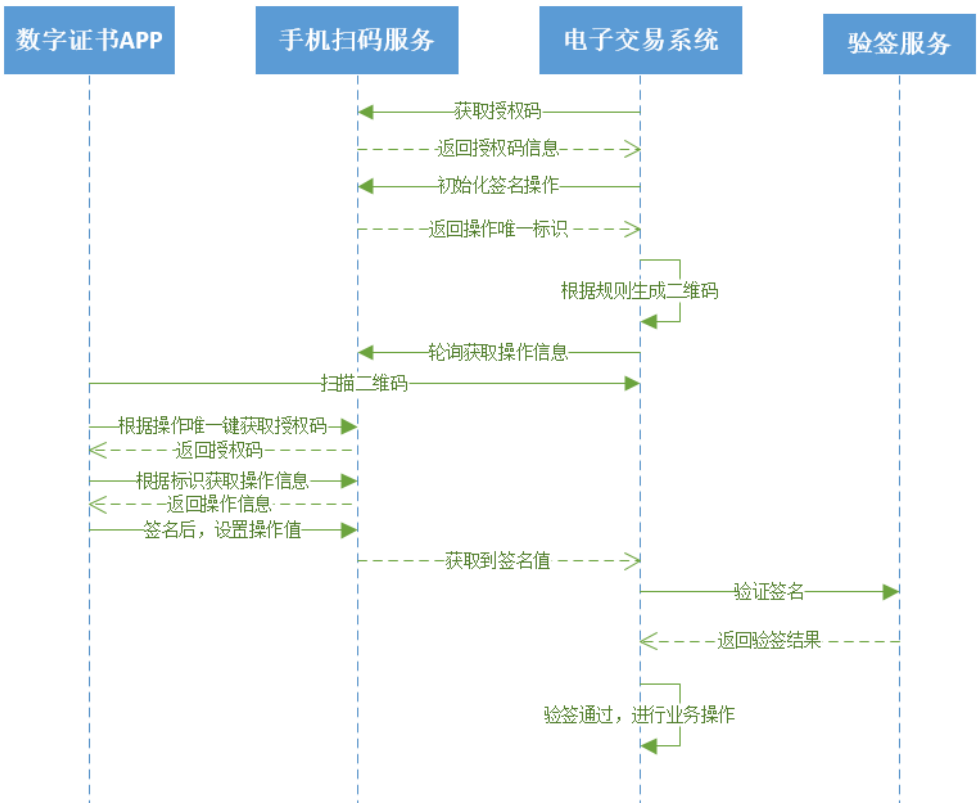
3、APP 扫描二维码，根据二维码信息获取授权码并获取初始化信息。

4、APP 判断为签名操作，对存入的值进行 p7 附原文签名，并存入手机扫码服务中。

5、电子交易系统，调用验签服务器签名值进行验签，并比较签名值与存入的是否一致。

6、验签通过，进行业务操作。

2.2 调用流程图



2.3 参数定义说明

名称	对应接口名称	说明
message	初始化信息接口	String 类型，签名原文
value	保存处理结果&获取操作结果	String 类型，签名值

3 加密

3.1 流程说明

1、电子交易系统调用手机扫码服务，获取授权码并初始化加密操作，获取操作唯一键。

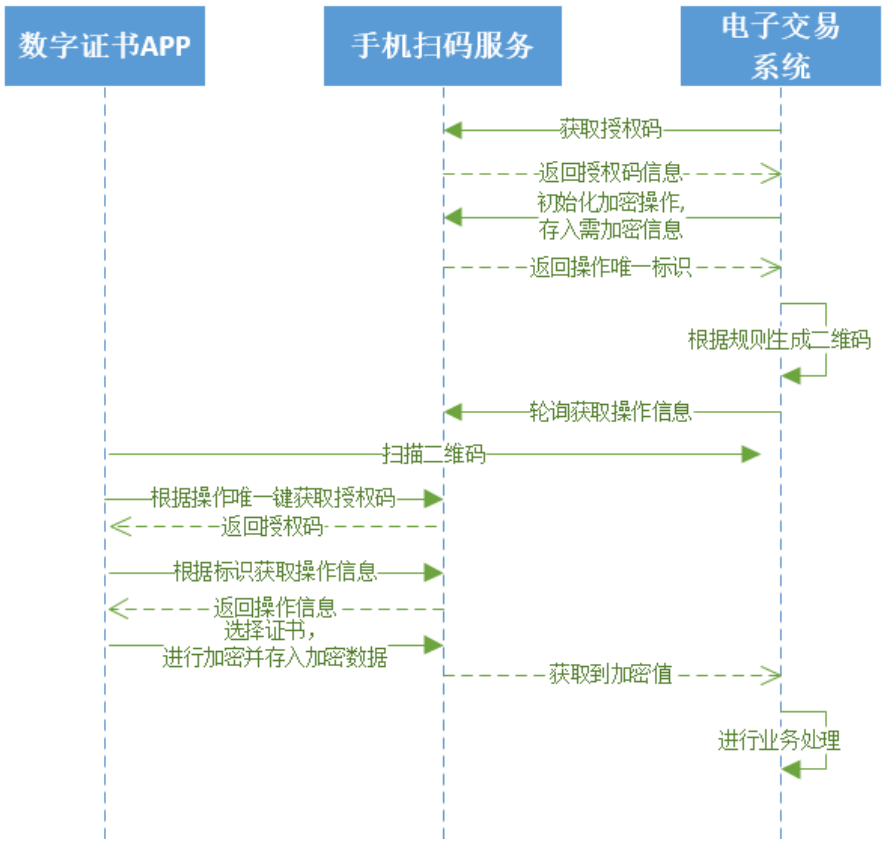
2、电子交易系统按照规则生成二维码展示，并启动轮询获取操作状态。轮询超过五分钟则停止轮询，提示二维码过期。轮询间隔建议 3-5s。

3、APP 扫描二维码，根据二维码信息获取授权码并初始化信息。

4、APP 判断为加密操作，读取证书的公钥信息存入到手机扫码服务中。

5、电子交易系统轮询接口获取证书公钥信息后调用本地的加密包 API 进行加密操作。

3.2 调用流程图



3.3 参数定义说明

名称	对应接口名称	说明
message	初始化信息接口	String 类型，需加密的字符串
value	保存处理结果&获取操作结果	String 类型，证书公钥信息

4 解密

4.1 流程说明

1、电子交易系统调用手机扫码服务，获取授权码并初始化解密操作，存入需解密信息，获取操作唯一键。

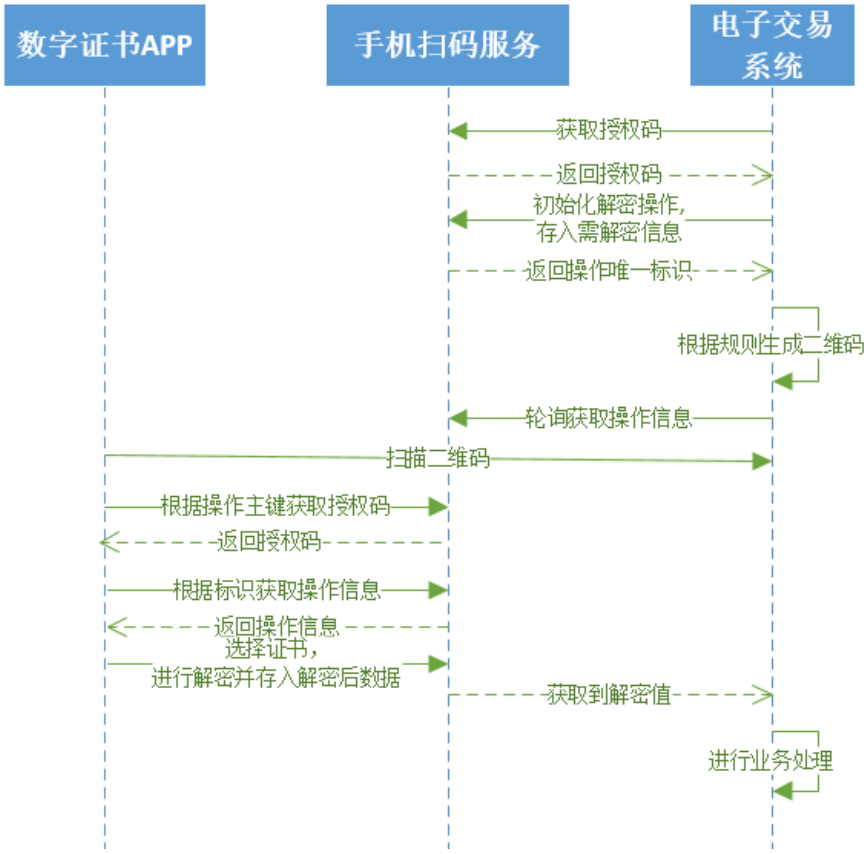
2、电子交易系统按照规则生成二维码展示，并启动轮询获取操作状态。轮询超过五分钟则停止轮询，提示二维码过期。轮询间隔建议 3-5s。

3、APP 扫描二维码，根据二维码信息获取授权码并获取初始化信息。

4、APP 判断为解密操作，对存入的值进行解密并将解密的接口存入到手机扫码服务中。

5、电子交易系统轮询到操作结果中的解密值，进行业务操作。

4.2 调用流程图



4.3 参数定义说明

名称	对应接口名称	说明
message	初始化信息接口	String 类型。需解密的字符串
value	保存处理结果&获	String 类型。解密后的字符串。

名称	对应接口名称	说明
	取操作结果	

5 签章

5.1 流程说明

1、电子交易系统集成签章控件到页面。

2、用户点击签章，获取授权码并调用控件接口设置授权码。

获取 token 调用示例：

curl -X POST -H 'Content-Type: APPlication/x-www-form-urlencoded' -i '手机扫码服务/grantToken' --data 'accountName=xxx&password=xxx'

返回数据：

{"token":"36b6a611-0c97-47f3-a070-7d3d0ffaddd4","invokeCode":1}

3、签章控件调用手机扫码服务， 初始化签章操作。

http 调用初始化信息示例：

curl -X POST -H 'Content-Type: APPlication/x-www-form-urlencoded' -i '手机扫码服务/initMessage' --data 'type=5&message=f7c54891-adad-4f32-9994-83d70a7204a2&title=xx 系统签章&certType=0&token=36b6a611-0c97-47f3-a070-7d3d0ffaddd4'

返回数据：

{"guid":"bf1af3f2-97b0-4b04-a054-ad7ba824eb70","invokeCode":1}

4、签章控件根据接口规范生成二维码，触发盖章动作时启动轮询，获取签名图片信息。轮询超过五分钟则停止轮询，提示二维码过期。轮询间隔建议 3-5s。

5、APP 扫描二维码，获取授权码后获取初始化信息。

http 调用示例：

curl -X POST -H 'Content-Type: APPlication/x-www-form-urlencoded' -i '手机扫码服务地址/getInitMessage' --data 'guid=bf1af3f2-97b0-4b04-a054-ad7ba824eb70&token=36b6a611-0c97-47f3-a070-7d3d0ffaddd4'

返回数据：

{"message":"f7c54891-adad-4f32-9994-83d70a7204a2","title":"xx 系统签章","invokeCode":1,"certType":0,"type":"5"}

6、APP 判断为扫码操作，将签章公司 code,存入到手机扫码服务，启动轮询，获取 pdf 合并签章图片后的文件 hash 值，进行签名操作。

http 调用示例：

curl -X POST -H 'Content-Type: APPlication/x-www-form-urlencoded' -i '手机扫码服务地址/saveCaMessageResult' --data 'guid=bf1af3f2-97b0-4b04-a054-ad7ba824eb70&value={"signatureCompanyCode":"xx"}&extMessage={"caSerialId":"xx"}&status=2&token=36b6a611-0c97-47f3-a070-7d3d0ffaddd4 '

返回数据：

{"invokeCode":1}

7、签章控件调用手机扫码服务获取签章图片。

http 调用初始化信息示例：

curl -X POST -H 'Content-Type: APPlication/x-www-form-urlencoded' -i '手机扫码服务/getSealImg' --data 'guid=xxxx&token=36b6a611-0c97-47f3-a070-7d3d0ffaddd4'

返回数据：

{"invokeCode":1,"signInfos":[{"signName":"xx","signWidth":"xx","signHeight":"xxx","img":"xxxxx","description":"xxx"}]}

8、手机扫码服务通过签章公司 code 获取到签章服务地址，调用签章服务（签章服务需各签章公司提供，具体签章服务规范说明详见第六章）接口地址获取图片，返回结果。

9、签章控件展示印章列表，用户选择印章签章，并计算出 pdf 合并签章图片后的文件 hash，调用手机扫码服务接口进行存储。

10、APP 使用 ca 对传入的文件 hash 进行签名。

http 调用示例：

curl -X POST -H 'Content-Type: APPlication/x-www-form-urlencoded' -i '手机扫码服务地址/saveCaMessageResult' --data 'guid=bf1af3f2-97b0-4b04-a054-ad7ba824eb70&value=hash&extMessage=xxx&status=2&token=36b6a611-0c97-47f3-a070-7d3d0ffaddd4 '

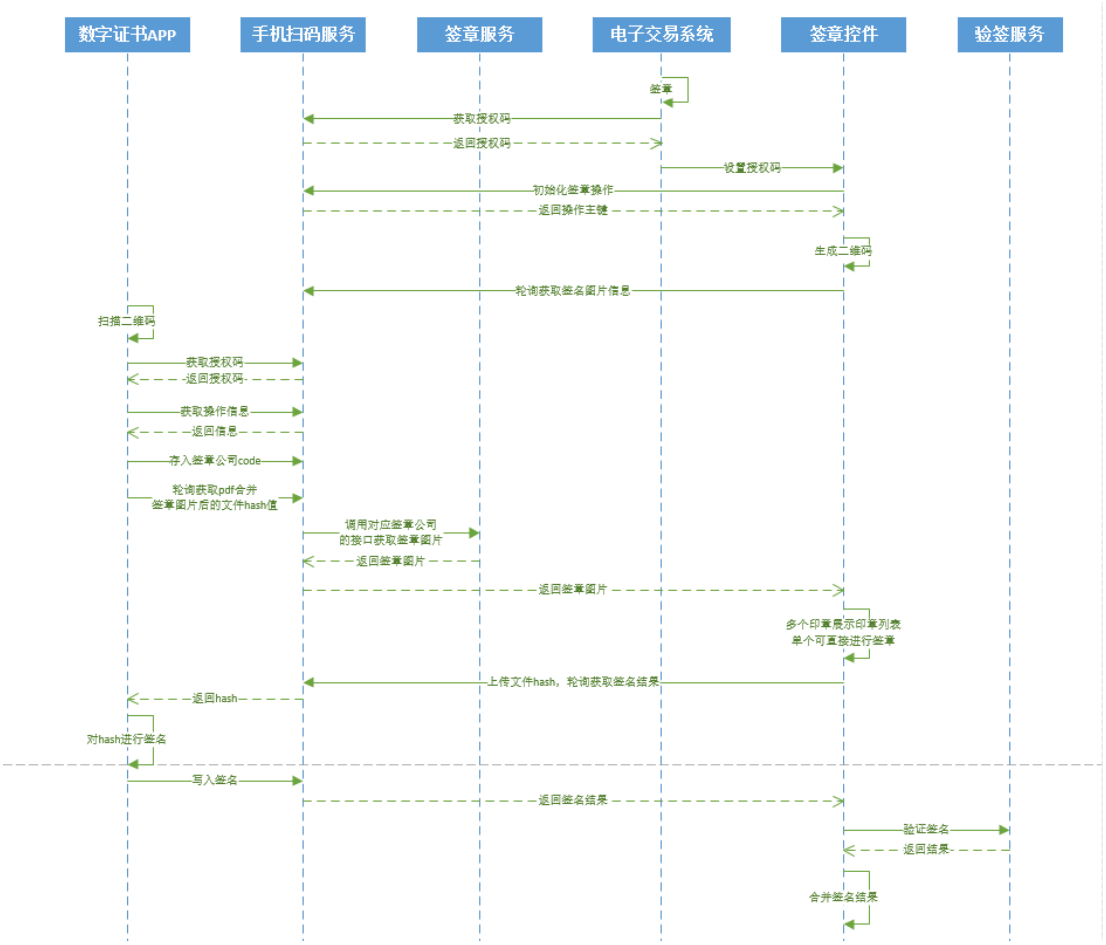
返回数据：

{"invokeCode":1}

11、签章控件轮询到签名完成状态，调用验签服务接口进行验签并解析出来公钥证书。

12、签章控件将签名结果、文件进行合并进行签章。

5.2 调用流程图



5.3 参数定义说明

名称	对应接口名称	说明
message	初始化信息接口	文件 hash 值
value	保存处理结果&获取操作结果	json 格式的字符串。具体描述见下表

value 格式描述：

名称	中文名称	备注
signStr	签名值	针对文件 hash 的签名值
signatureCompanyCode	签章公司编码	

名称	中文名称	备注
pubCert	公钥证书	

6 撤章

6.1 流程说明

1、用户点击右键，进行撤章。

2、电子交易系统监听到撤章操作，调用扫码服务获取授权码后，设置控件授权码。

3、签章控件响应撤章操作，获取被撤章的信息。

4、签章控件获得签章信息中的文件 hash（既签名原文）并初始化撤章操作，获得操作主键，生成撤章二维码并启动轮询获取操作结果。轮询超过五分钟则停止轮询，提示二维码过期。轮询间隔建议 3-5s。

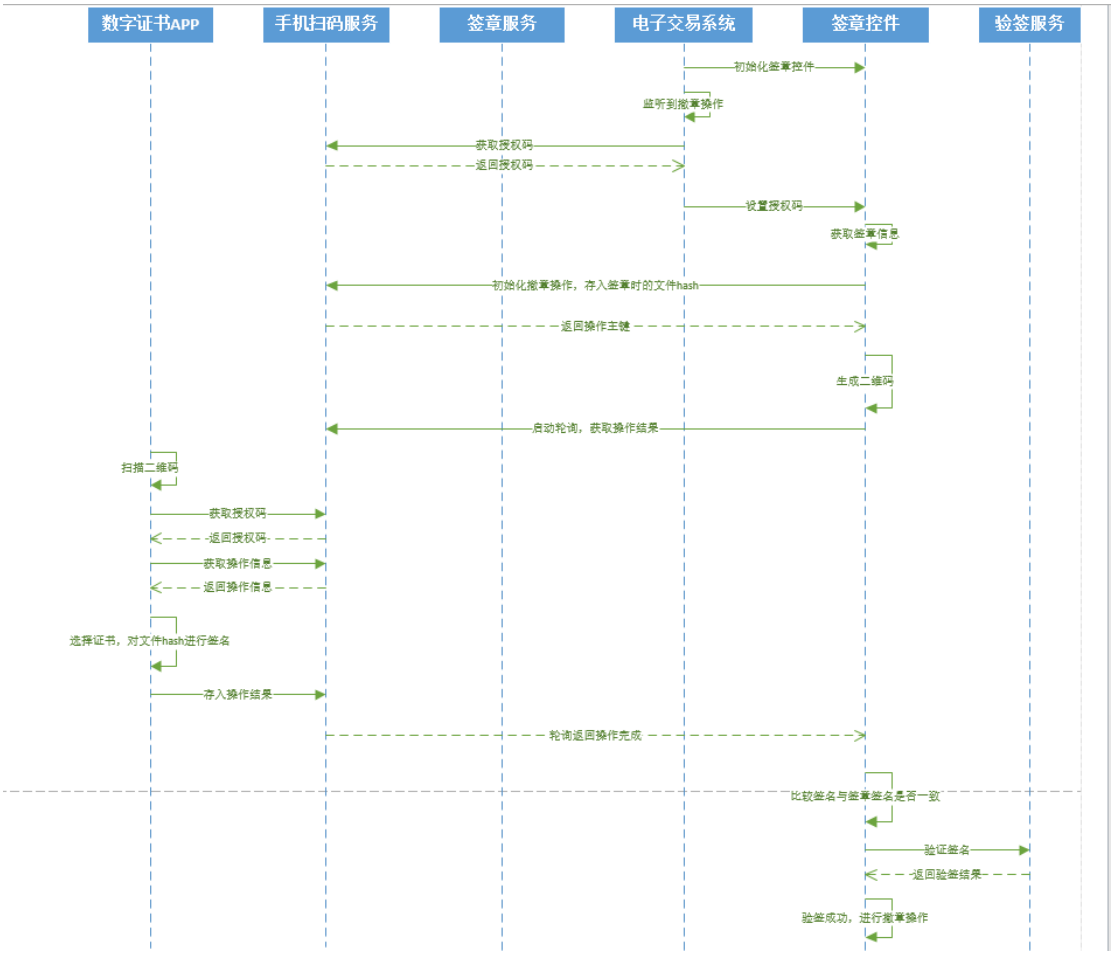
5、APP 扫描二维码，从手机扫码服务获取授权码后再获取操作信息。

6、APP 判断为撤章操作，对操作信息中的文件 hash 进行 p7 附原文签名。

7、APP 操作完成，存入操作结果到手机扫码服务中。

8、签章控件获取到操作结果，进行验签操作。并比较签名值是否一致；如一致，进行撤章；否则，返回撤章失败。

6.2 调用流程图



6.3 参数定义说明

名称	对应接口名称	说明
message	初始化信息接口	String 类型，文件 hash 值
value	保存处理结果&获取操作结果	String 类型，文件 hash 值的签名结果