ICS 11.020
C 50

团　　体　　标　　准

T/SHIA 012—2024

跨 CA 机构多证照身份认证应用接口规范

Cross-Certificate Authority and Electronic Certificate Authority Identity Authentication Application Interface Specification

2024-02-20 发布　　2024-03-20 实施

四川省卫生信息学会 发布

目　　次

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。

本文件由四川省卫生信息学会提出并归口。

本文件的主要起草单位：四川省卫生健康信息中心、四川省数字证书认证管理中心有限公司、成都市第三人民医院、成都市第六人民医院、四川大学华西医院、四川省妇幼保健院、彭州市第四人民医院、自贡市第三人民医院、成都市第八人民医院、四川护理职业学院附属医院（四川省第三人民医院）、北京数字认证股份有限公司、上海市数字证书认证中心有限公司、陕西省数字证书认证中心股份有限公司、东方中讯数字证书认证有限公司。

本文件主要起草人：林晓东、支红杰、黄路非、杨飞、尹才敏、张红、毕永东、郭坤玲、黄山、刘秋月、毛云鹏、彭先清、邱洪明、冉茂呈、宋海兰、王云洲、吴天智、张新屹。

引　言

《四川省卫生健康信息化三年行动计划（2023-2025 年）》中明确要求统筹加强身份认证、电子印章等基础支撑，推进电子证照建设应用及电子签名应用，为了统一医疗行业电子证照融合 CA 认证服务，本接口规范的制定能够为医疗机构应用系统提供标准统一的电子签名、签章和电子证照的应用接口，促进身份认证、电子签章等基础设施建设，推进电子证照的应用。

当前医疗行业缺乏基于执业主体身份、电子执业执照，面向全省执业机构、人员发行电子证照的应用接口规范，来规范面向医疗机构提供标准统一的电子证照及电子认证服务，而医疗机构在开展线上线下医疗服务的过程中又迫切需要对医疗人员的执业证照进行认证，并且通过 CA 认证来满足医疗机构全程电子化建设要求，而现有的医疗机构存在使用多个 CA 机构服务的情况，为了最大限度节约医疗机构成本，也需要兼容多 CA 机构的数字证书，保障医疗机构公平的选择权利，在区域内实现跨机构的 CA 认证可以实现执业信息的互通和共享，因此制订全省统一的《跨 CA 机构多证照身份认证应用接口规范》，实现一套统一接口规范，支持医疗机构中的多身份认证迫在眉睫。

借助跨证书认证服务机构身份认证应用接口规范，构建全省电子证照融合电子认证服务体系，改变不同区域、医联体、医疗机构电子证照及电子签名等身份认证不统一的现状，提高基础资源的利用效率，优化医疗信息化服务模式，提高医疗信息化水平，降低医疗信息化建设成本，为医疗机构提供更好的基础支撑服务。这对于提高医疗机构信息化建设效率，满足医疗信息化需求，推动医疗行业信息化发展具有重要的意义。

跨 CA 机构多证照身份认证应用接口规范

1 范围

本文件规定了跨 CA 机构多证照身份认证应用接口规范的通讯协议和应用接口，并定义了通讯协议请求方法和 URL 规则、授权类型、状态信息、回调数据结构，明确了身份认证服务的接口、接口调用参数和电子签章服务的接口、接口参数。本文件的电子签名采用代理签名模式。本文件涉及到的密码为国家密码管理部门核准的密码。

本文件适用于医疗机构的应用系统接入卫生健康基础资源链身份认证服务，为执业主体（医疗机构、医生、护士等）提供电子证照、CA 认证服务，来满足医护人员、医疗机构电子执业证照存证上链，执业主体在线认证和亮证执业。

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。

GB/T 33560 信息安全技术 密码应用标识规范

GB/T 25064 信息安全技术 公钥基础设施 电子签名格式规范

GB/T 19713 信息技术 安全技术 公钥基础设施 在线证书状态协议

GB/T 19714 信息技术 安全技术 公钥基础设施 证书管理协议

GB/T 25056 信息安全技术证书认证系统密码及其相关安全技术规范

GB/T 20520 信息安全技术 公钥基础设施 时间戳规范

GB/T 35285 信息安全技术 公钥基础设施 基于数字证书的可靠电子签名生成及验证技术要求

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 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GB/T 38540 信息安全技术 安全电子签章密码技术规范

GM/T 0109 基于云计算的电子签名服务技术要求

GM/T 0120 基于云计算的电子签名服务技术实施指南

GB/Z 21716.1 健康信息学 公钥基础设施（PKI） 第1部分：数字证书服务综述

GB/Z 21716.2 健康信息学 公钥基础设施（PKI） 第2部分：证书轮廓

GB/Z 21716.3 健康信息学 公钥基础设施（PKI） 第3部分：认证机构的策略管理

GM/Z0001 密码术语

GB/T 36901 电子证照 总体技术架构

GB/T 36902 电子证照 目录信息规范

GB/T 36903 电子证照 元数据规范

GB/T 36904 电子证照 标识规范

GB/T 36905 电子证照 文件技术要求

GB/T 36906 电子证照 共享服务接口规范

PKCS #7 密码消息语法(Cryptographic message syntax)

PKCS #1 RSA Cryptography Specifications

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字证书 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、机构证书和设备证书，按用途可分为签名证书和加密证书。

[来源：GB/T 25056—2018]

3.2

证书认证机构 certification authority (CA)

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。

[来源：GB/T 25056—2018]

3.3

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。

[来源：GM/Z 0001-2013]

3.4

证书验证 certificate validation

按照验证策略确认证书有效性和真实性的过程。

[来源：GM/Z 0001-2013]

3.5

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。

[来源：GM/Z 0001-2013]

3.6

时间戳 time stamp(TS)

对时间和其它待签名数据进行签名得到的数据，用于表明数据的时间属性。

[来源：GM/Z 0001-2013]

3.7

电子签章 digitally seal

使用电子印章签署电子文件的过程。

[来源：GM/Z 0001-2013]

3.8

电子印章 digital stamp

一种由制作者签名的包括持有者信息和图形化内容的数据，可用于签署电子文件。

[来源：GM/Z 0001-2013]

3.9

证照 certificate

由机关、团体、企事业单位颁发的、能够证明资格或权利等的凭证类文件。

注：证照包括证件和执照等。

[来源：GB/T 36901-2018]

3.10

电子证照 electronic certificate

由计算机等电子设备形成、传输和存储的证照数据文件。

[来源：GB/T 36901-2018]

3.11

电子证照文件 electronic certificate file

以版式文档表示的电子证照，该文件既包含照面固定版式效果，又包含证照元数据及标识，并应用密码技术保障这些内容的真实性和完整性。

[来源：GB/T 36901-2018]

3.12

电子证照有效性 electronic certificate validity

电子证照的凭证效力被其颁发机构继续认可的性质。

[来源：GB/T 36906-2018]

3.13

电子证照文件完整性 electronic certificate file integrity

电子证照文件的内容，结构和背景信息齐全且没有破坏、变异或丢失的性质。

[来源：GB/T 36906-2018]

3.14

电子证照文件真实性 electronic certificate file authenticity

电子证照文件中的内容、结构和背景信息与形成时的原始状态相一致的性质。

[来源：GB/T 36906-2018]

3.15

带密钥的杂凑算法 keyed-hash message authentication code (HMAC)

一种密码杂凑算法，密钥作为其输入参数参与运算。

[来源：GM/Z 0001-2013]

3.16

代理签名 delegated signature mechanism

签名方将密钥托管在云服务，授权云服务完成电子签名的机制。

[来源：GM/T 0120-2022]

4 缩略语

API	Application Program Interface 应用程序接口,简称应用接口
CA	Certification Authority 证书认证机构
HMAC	Keyed-hash message authentication code 一种密码杂凑算法。
JSON	JavaScript Object Notation JS 对象标记
HTTP	Hyper Text Transfer Protocol 超文本传输协议
HTTPS	Hyper Text Transfcr Protocol over SecurcSocket Layer 安全 HTTP 协议
PIN	Personal Identification Number 个人标识码
P7	PKCS#7 Public Key Cryptography Standards#7
P1	PKCS#1 Public Key Cryptography Standards#1

5 身份认证服务应用接口调用说明

5.1 接口调用说明

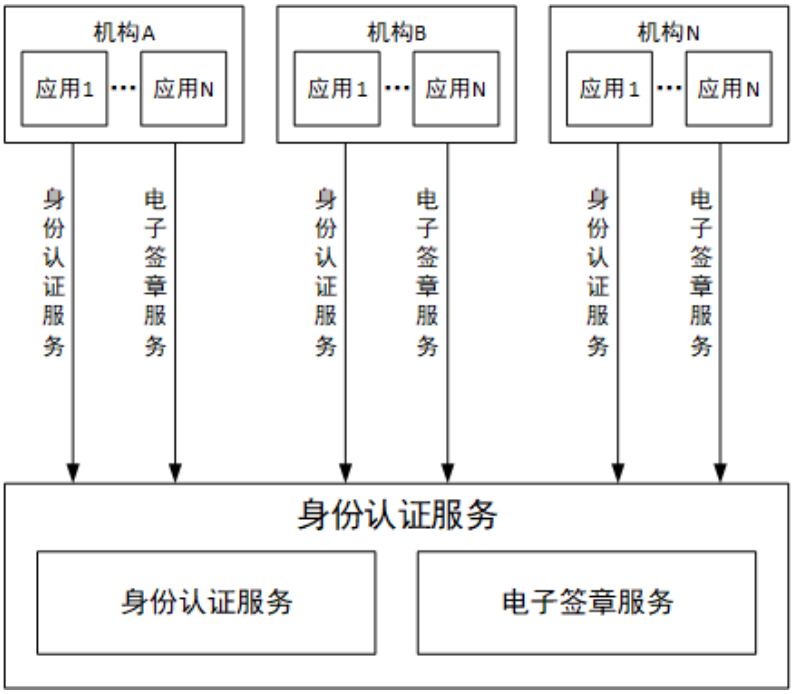

图 1 身份认证服务接口说明

身份认证服务为机构的应用系统提供 API 接口服务（如图 1），其中包括身份认证服务、电子签章服务。

a）身份认证服务为机构的应用系统提供基于数字证书的电子签名、签名验证、时间戳、及电子证照等基础服务。

b）电子签章服务为机构的应用系统提供基于数字证书的电子签章服务，以确保电子文档来源真实性以及文档的完整性，防止对文档未经授权的篡改，并确保签章行为的不可否认性。

c）机构的应用系统在接入之前，需要提出接入申请，获取应用的 app_id 和 app_secret，才能使用身份认证服务。

5.2 参数约束定义

表 1 参数约束定义

参数	描述
0..1	可选项，可以没有，也可以有 1 项
0..n	可选项，可以没有，也可以有多项
1..n	必选项，至少有一项，也可以有多项
1	必选项，且只能填 1 项

6 通讯协议和数据结构

6.1 通讯协议

身份认证服务和应用系统基于 HTTPS 协议，报文格式定义如下：

a）请求数据封装格式：application/json

b）返回数据封装格式：application/json

c）请求和响应参数组成结构说明如下：

接口请求和响应的均为 JSON 格式数据报文，数据报文由公共参数和业务参数两部分构成，请求报文需要由应用系统使用 HMAC 签名算法进行签名计算，支持 HMAC-SM3 的签名算法。

6.2 请求方法和 URL 规则

支持 HTTPS GET POST 方法。

——使用 GET 方法时，输入参数附加在请求的 URL 上，输出参数为 JSON 格式。

示例如下：

https://*{ip:port}*/open/{signature}?{paramkey}={paramValue}

——使用 POST 方法时，输入和输出参数均采用 JSON 格式。

示例如下：

https://*{ip:port}*/open/{signature}

注：*{斜体}*为可变内容域，是身份认证服务网络地址，下同。

6.3 授权类别

——trusted，当前支持的授权类别必须经过验证签名。

6.4 认证信息

应用系统在与身份认证服务通讯时，应提供认证信息，用于鉴别其身份。可以通过验证签名的方式鉴别各个接入的应用系统的身份。

——身份认证服务向申请接入的应用系统分配的唯一 app_id 和 app_secret。

——通过接口传输数据时，调用方应通过 HMAC-SM3 算法对请求数据进行加签计算。

——开放接口采用 https 协议。

公共参数放入请求头中进行传输，请求的 Header 中包含认证信息如下：

参数名	参数类型	参数说明
app_id	string	接入应用系统 app_id,由身份认证服务统一分配。
signature	string	参数签名值，由分配 app_secret 和请求参数计算得出结果，采用 HEX 编码
timestamp	string	请求发送的时间戳(Unix Timestamp, 毫秒)
nonce	string	请求随机数，每笔业务在一定时间内唯一(2 分钟)

签名值生成规则:

——JSON 提交

a）JSON 字符串后面拼接随机数(nonce 对应值，随机数在前)和时间戳（timestamp 对应值）得到字符串。

b）将 a 得到的字符串进行 HMAC-SM3 运算，计算后将结果转换为 16 进制(小写)，即为签名信息，放入请求头(signature)中。

6.5 状态信息

身份认证服务 API 返回状态信息，状态信息包含字符形式的状态码和状态描述。状态码见附录 A 的规定。

6.6 回调数据

因部分操作是异步操作，当异步操作完成后，身份认证服务向应用系统的回调地址发送回调数据。回调数据格式：

参数名	参数类型	参数说明
result_code	string	结果码，0 表示成功
result_msg	string	结果描述
success	bool	成功失败，成功：true，失败：false
body	object	响应内容

回调数据样例：

```
{
    "result_code":"0",
    "result_msg":"请求成功",
    "success":true,
    "body":{}
}
```

7 身份认证服务接口

7.1 接口列表

表 2 身份认证服务接口列表

编号	接口功能	接口 URL 对象	方法	授权	备注
1	数字证书签名	https://*{ip:port}*/open/signature/sign	POST	trusted	
2	数字证书查询	https://*{ip:port}*/open/digitalCert/list	POST	trusted	
3	数字签名验证	https://*{ip:port}*/open/signature/verify	POST	trusted	
4	生成时间戳	https://*{ip:port}*/open/timestamp/sign	POST	trusted	
5	验证时间戳有效性	https://*{ip:port}*/open/timestamp/verify	POST	trusted	
6	二维码生成	https://*{ip:port}*/open/qrcode/applyQrCode	POST	trusted	
7	二维码状态查询	https://*{ip:port}*/open/qrcode/qrCodeStatusQuery	POST	trusted	
8	二维码回调	由业务系统提供	POST	trusted	
9	解析二维码信息	https://*{ip:port}*/open/qrcode/qrCodAnalysis	POST	trusted	
10	电子证照信息检索(医生和护士)	https://{ip:port}/open/elecCert/personRetrieval	POST	trusted	
11	电子证照信息检索(机构)	https://{ip:port}/open/elecCert/orgRetrieval	POST	trusted	
12	电子证照查证	https://*{ip:port}*/open/elecCert/query	POST	trusted	
13	电子证照真伪验证	https://*{ip:port}*/open/elecCert/verifySeal	POST	trusted	
14	电子证照类型列表	https://*{ip:port}*/open/elecCert/queryTypeList	POST	trusted	

编号	接口功能	接口 URL 对象	方法	授权	备注
15	待签署数据推送	https://*{ip:port}*/open/sign/pushData	POST	trusted	
16	待签署 Pdf 文件推送	https://*{ip:port}*/open/sign/pushPdf	POST	trusted	
17	认证服务签署状态查询接口	https://*{ip:port}*/open/sign/querySignStatus	POST	trusted	
18	认证服务签署状态通知	{接口由业务系统提供}/pushcallback	POST	trusted	
19	获取数据签署 H5 链接地址	https://*{ip:port}*/open/signature/h5Sign	POST	trusted	
20	获取pdf签署H5链接地址	https://*{ip:port}*/open/signature/h5SignPdf	POST	trusted	
21	H5或接口签署信息查询接口	https://*{ip:port}*/open/sign/queryApiSignInfo	POST	trusted	
22	H5 签署状态通知	{接口由业务系统提供}/pushcallback	POST	trusted	
23	免密签署状态查询	https://*{ip:port}*/open/digitalCert/pinSaveStatus	POST	trusted	

7.2 数字证书签名

URL：https://{ip:port}/open/signature/sign

调用方法：POST

功能描述：采用已经申请有效数字证书对签名原文进行数字签名，支撑基于电子证照的数字签名。

参数分类	参数名	参数类型	约束	参数说明
输入参数：	dataType	string	1	签名原文类型 PLAIN|HASH
	elecCertId	string	0..1	证照标识(通过证照签名时候必传)
	cardNumber	string	1	单位唯一标识或个人唯一标识
	signatureAlgID	string	1	签名算法，此处为 SM2
	hashAlgID	string	1	HASH 算法，此处为 SM3
	userType	string	1	1 个人 2 单位
	toSign	string	1	签名原文
	transId	string	1	业务流水号，业务系统内保持唯一
	pin	string	0..1	证书 PIN 码(如果设置了免密，则不需要传)
	busiType	string	1	业务类型：SIGN:签名；LOGIN:登录
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	1	返回对象
body 对象：	signP7	string	1	P7 签名值
	signP1	string	1	P1 签名值

参数分类	参数名	参数类型	约束	参数说明
	certBase64	string	1	证书 base64 编码
	signatureAlgID	string	1	签名算法

返回内容示例：

{

"result_code":"0",

"result_msg":"请求成功",

"success":true,

"body":{

"signP7":"
MIIE+gYJKoZIhvcNAQcCoIIE6zCCBO.....UXtTTr4dRMi7iNG2W5ZcUYBysPPM8fpwPFyfEZV2wwIh
AMB7vAK1n1xIl2+LRJSYaicmGqBMRZFSOc6YZkKFRRqS ",

"signP1":"QcCoIIE6zCCBO.....UXtTTr4dRW5ZcUYBysPPM8AK1n1xIl2RqS ",

"certBase64":"
MIIDjDCCAzCgAwIBAgIUfT7uMyQfR…..mBggrBgEFBQcCAEbHkaZ/UxNYdMAXGeda4NWJOpqROOVAD
8NX+ii+MK4 ",

"signatureAlgID":"SM2"

}

}

7.3 数字证书查询

URL：https://{ip:port}/open/digitalCert/list

调用方法：POST

功能描述：查询主体的数字证书信息。

参数分类	参数名	参数类型	约束	参数说明
输入参数：	cardNumber	string	1	单位唯一码或个人唯一码
	userType	string	1	1 个人 2 单位
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	array	0..n	证书对象数组
body 对象:	digitalCertId	string	1	证书 id
	digitalCertCN	string	1	证书主体
	digitalCertSN	string	1	证书序列号
	notAfter	string	1	数字证书有效期不晚于，YYYY-MM-dd HH:mm:ss
	notBefore	string	1	数字证书有效期不早于，YYYY-MM-dd HH:mm:ss

参数分类	参数名	参数类型	约束	参数说明
	certBase64	string	1	证书 base64 编码

返回内容示例：

{

"result_code":"0",

"result_msg":"请求成功",

"success":true,

"body":[{

"digitalCertId":" 123",

"certBase64":"
MIIDjDCCAzCgAwIBAgIUfT7uMyQfR…..mBggrBgEFBQcCAEbHkaZ/UxNYdMAXGeda4NWJOpqROOVAD
8NX+ii+MK4 ",

"digitalCertCN":"mnn 公司" ,

"digitalCertSN":"1ddfdfasdlfksjdflj3",

"notAfter":"2023-01-05 13:20:21",

"notBefore":"2022-01-06 13:20:21"

}]

}

7.4 数字签名验证

URL：https://{ip:port}/open/signature/verify

调用方法：POST

功能描述：用户进行数字签名后,调用此接口进行签名有效性验证。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	toSign	string	1	签名原文
	elecCertId	string	0..1	证照标识(证照签名时候才传)
	cardNumber	string	0..1	单位唯一标识或个人唯一标识
	signatureAlgID	string	1	签名算法，此处为 SM2
	hashAlgID	string	1	HASH 算法，此处为 SM3
	transId	string	0..1	业务流水号，业务系统内保持唯一,不传则不返回 CertInfo、SignInfo 对象
	signature	string	1	签名值,Base64 编码
	signatureType	string	1	签名值类型：P1 或 P7
	certBase64	string	0..1	签名值类型为“P1”验签时必传
输出参数：	result_code	string	1	正常状态码

参数分类	参数名称	参数类型	约束	参数说明
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	1	返回对象
body 对象：	isVerify	bool	1	true 成功 false 失败
	certInfo	object	0..1	证书信息(CertInfo 对象)
CertInfo 对象：	certBase64	string	1	签名数字证书， Base64 编码
	signatureAlgID	string	1	签名算法（如 SM2）
	certIssuer	String	1	证书颁发者
	certNo	String	1	证书序列号
	certNotBefore	String	1	证书有效期起
	certNotAfter	String	1	证书有效期止
	certCN	String	1	证书主体
	signInfo	object	0..1	签名信息(SignInfo 对象)
SignInfo 对象：	timeData	String	1	时间戳签名值
	signTime	string	1	签名时间（yyyy-MM-DD HH:mm:ss）

返回内容示例：


```
{
     "result_code":"200",
     "result_msg":"验签成功",
     "success":true,
     "body":{
             isVerify：true，
          "certInfo":{
                    "certBase64":"base64",
                    "signatureAlgID":"3333",
                    "certIssuer":"四川 ca",
                    "certNo":"3333",
                    "certNotAfter":"2023-10-12 00:00:00",
                    "certNotBefore":"2022-10-12 00:00:00",",
                    "certCN":"张三",
          },
          "signInfo":{
                    "timeData":"dfsdsldhfsdj",
                    "signTime":"2020-12-12 00:00:00"
           }
     }
}
```


7.5 生成时间戳

URL：https://{ip:port}/open/timestamp/sign

调用方法：POST

功能描述：按照国家标准生成时间戳。

参数分类	参数名	参数类型	约束	参数说明
输入参数:	dataType	string	1	签名原文类型，PLAIN|HASH
	toSign	string	1	签名原文
	signatureAlgID	string	1	签名算法，此处为 SM2
	hashAlgID	string	1	HASH 算法，支持 SM3
	transId	string	1	业务流水号，业务系统内保持唯一
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	1	返回对象
body 对象：	timeData	string	1	时间戳签名值

返回内容示例：

{

"result_code":"0",

"result_msg":"请求成功",

"success":true,

"body":{

"timeData":"
MIIE+gYJKoZIhvcNAQcCoIIE6zCCBO.....UXtTTr4dRMi7iNG2W5ZcUYBysPPM8fpwPFyfEZV2wwIh
AMB7vAK1n1xIl2+LRJSYaicmGqBMRZFSOc6YZkKFRRqS"

}

}

7.6 验证时间戳有效性

URL：https://{ip:port}/open/timestamp/verify

调用方法：POST

功能描述：验证时间戳是否有效。

参数分类	参数名	参数类型	约束	参数说明
输入参数：	timeData	string	1	时间戳签名值
	toSign	string	1	签名原文
	signatureAlgID	string	1	签名算法，此处为 SM2
	hashAlgID	string	1	HASH 算法，支持 SM3
	transId	string	1	业务流水号，业务系统内保持唯一
输出参数：	result_code	string	1	正常状态码

	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	1	返回对象
body 对象：	time	string	1	时间戳签名签署时间，国家标准时间（yyyy-MM-DD HH:mm:ss）

返回内容示例：


```
{
    "result_code":"0",
    "result_msg":"请求成功",
    "success":true,
    "body":{
            "time":"2023-01-05 13:20:21"
    }
}
```


7.7 二维码生成

URL：https://{ip:port}/open/qrcode/applyQrCode

调用方法：POST

功能描述：通过二维码进行登录或签名时，通过调用此接口获取对应的二维码。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	busiType	string	1	业务类型, SIGN:证书签名 LOGIN:证书登录 ElECSIGN:证照签名 ElECLOGIN:证照登录
	transId	string	1	业务流水号，业务系统内保持唯一
	toSign	string	1	签名原文(Base64 编码)
	busiName	string	1	业务名称
	busiDesc	string	0..1	业务描述
	callBackUrl	string	1	业务回调地址,扫码后业务通知
	qrType	bool	0..1	是否可以重复使用，默认 false
	expireTime	long	0..1	过期时间，单位：秒，默认不过期
	extParams	string	0..1	扩展参数，JSON 格式，用于回调时返回
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	1	返回对象

参数分类	参数名称	参数类型	约束	参数说明
body 对象：	qrCode	string	1	二维码（Base64 编码）
	qrCodeUid	string	1	二维码唯一标识

返回内容示例：


```
{
        "result_code":"0",
        "result_msg":"请求成功",
        "success":true,
        "body":{
                "qrCode":"DEVDFALDKFKALSDJFJD---",
                "qrCodeUid":"123343546675"
            }
}
```


7.8 二维码状态查询

URL：https://{ip:port}/open/qrcode/qrCodeStatusQuery

调用方法：POST

功能描述：用于二维码状态查询。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	qrCodeUid	string	1	二维码唯一标识
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	1	结果信息
body 对象：	status	string	1	SCANING:扫码中 SCANED:已扫码 WAIT:待扫码

返回内容示例：


```
{
        "result_code":"0",
        "result_msg":"请求成功",
        "success":true,
        "body":{
                "status":"SCANING"
        }
```

}

7.9 二维码回调

URL：由业务系统提供的回调地址。

调用方法：https://{ip:port}/{业务系统提供}

功能描述：用于二维码扫描签名或登录完成后的应用系统回调，应用系统获取签名值和原文后进行签名验证。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	busiType	string	1	二维码类型, SIGN:证书签名 LOGIN:证书登录 ElECSIGN:证照签名 ElECLOGIN:证照登录
	transId	string	1	业务流水号，业务系统内保持唯一,与二维码生成保持一致
	cardNumber	string	1	单位唯一码或个人唯一码
	userType	string	1	1 个人 2 单位
	toSign	string	1	签名原文(Base64 编码)
	signature	string	1	签名值 PKCS7(Base64 编码)
	extParams	string	0..1	扩展参数，JSON 格式，用于回调时返回
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
body 对象：	body	object	0..1	返回对象（具体内容由业务系统提供）

7.10 解析二维码信息

URL：https://{ip:port}/open/qrcode/qrCodAnalysis

调用方法：POST

功能描述：用于二维码信息解析。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	qrCodeUid	string	1	二维码唯一标识
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	1	结果信息
body 对象：	busiType	string	1	业务类型, SIGN:证书签名 LOGIN:证书登录 ElECSIGN:证照签名

参数分类	参数名称	参数类型	约束	参数说明
				ElECLOGIN:证照登录
	toSign	string	1	签名原文
	extParams	string	0..1	扩展参数，JSON 格式，用于回调时返回

返回内容示例：


```
{
        "result_code":"0",
        "result_msg":"请求成功",
        "success":true,
        "body":{
                "busiType":"SIGN",
                "toSign":"签名原文"
        }
}
```


7.11 执业人员的电子证照检索

URL：https://{ip:port}/open/elecCert/personRetrieval

调用方法：POST

功能描述：通过持有人证件号码获取医生和护士证照信息

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	elecCertHolderCode	string	1	持证主体代码（身份证）
	elecCertType	string	0..1	证照类型编码，多个编码间以英文逗号“,”分隔（护士执业证：NURSE ，医师执业证：DOCTOR）
	elecCertTypeName	string	0..1	证照类型名称(护士执业证,医师执业证）
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	array	0..n	证照列表
body 数组：	elecCertId	string	1	证照唯一标识
	elecCertName	string	1	证照名称
	elecCertHolder	string	1	持证主体（姓名）
	elecCertHolderCode	string	1	持证主体代码（身份证）
	techPost	string	1	技术职称（医生为空）
	elecCertType	string	1	证照类型编码 （护士执业证：NURSE ，医师执业证：DOCTOR）
	elecCertTypeName	string	1	持有者证件类型名称

参数分类	参数名称	参数类型	约束	参数说明
	sex	string	1	性别 （男 丨女）
	birthday	string	1	出生年月
	elecCertNumber	string	1	证照编号
	elecCpetCode	string	1	执业证书编码
	practiceScope	string	1	执业范围
	practiceLevel	string	1	证照级别（护士执业证为空）
	practiceClass	string	1	执业类别
	practiceAreaName	string	1	执业地点
	practiceOrgName	string	1	主要执业机构名称
	practiceOrgId	string	1	主要执业机构代码
	issueDept	string	1	证照颁发机构
	workOffice	string	1	工作科室
	issueDeptCode	string	1	证照颁发机构代码
	issueDate	string	1	证照颁发日期
	validityStart	string	1	证照有效期起始（如果为空则为长期有效）
	validityEnd	string	1	证照有效期截止（如果为空则为长期有效）
	state	string	1	证照状态： 1-有效， 0-证照已注销

返回内容示例：


```
{
   "result_code":"0",
   "result_msg":"请求成功",
   "success":true,
   "body":[
     {        "elecCertId": "1234567890",
              "elecCertName":"医师执业证",
              "elecCertHolder": "张医生",
              "elecCertHolderCode": "522228199612100611",
              "techPost": "",
              "elecCertType": "DOCTOR",
              "elecCertTypeName":"医师执业证",
               "sex":"男",
              "birthday":"1999-10-01",
```

```
            "elecCertNumber": "1262235241",
            "elecCpetCode":"20015111013020319760713151l",
            "practiceScope":"外科专业",
            "practiceLevel":"执业医师",
            "practiceClass":"临床",
            "practiceAreaName":"青羊区",
            "practiceOrgId":"88EFE14F-119A-406E-8967-3D33E7D2B93E",
            "issueDept": "成都市青羊区卫生和计划生育局",
            "issueDeptCode": "370100004188602",
            "issueDate": "2019-10-14",
            "validityStart": "2019-10-14",
            "validityEnd": "2019-10-14",
            "state": "1"
    } ]
}
```


7.12 机构的电子证照检索

URL：https://{ip:port}/open/elecCert/orgRetrieval

调用方法：POST

功能描述：通过单位唯一标识获取单位证照信息

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	elecCertHolderCode	string	1	持证主体代码（单位唯一编码）
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	array	0..n	证照列表
body 数组：	elecCertId	string	1	证照唯一标识
	elecCertName	string	1	证照名称
	elecCertHolder	string	1	持证主体（单位名称）
	elecCertHolderCode	string	1	持证主体代码（单位唯一编码）
	elecCertNumber	string	1	证照编号
	specialtiesName	string	1	诊疗科目
	areaName	string	1	行政区域
	legalPerson	string	1	法定代表人
	holderCardNumber	string	1	持证者证件号

参数分类	参数名称	参数类型	约束	参数说明
	adress	string	1	地址
	chargeRepresentative	string	1	主要负责人
	natureBusiness	string	1	经营性质
	setFormedName	string	1	组建负责人
	telNum	string	1	电话
	category	string	1	机构类别
	secondName	string	1	机构第二名称
	level	string	1	医院级别
	rankName	string	1	医院等次
	adminOrgName	string	1	主管单位名称
	issueDept	string	1	证照颁发机构
	issueDeptCode	string	1	证照颁发机构代码
	issueDate	string	1	证照颁发日期
	validityStart	string	0..1	证照有效期起始（如果为空则为长期有效）
	validityEnd	string	1	证照有效期截止（如果为空则为长期有效）
	state	string	1	证照状态：1-有效， 0-证照已注销

返回内容示例：


```
{
    "result_code":"0",
    "result_msg":"请求成功",
    "success":true,
    "body":[{   "elecCertId": "1234567890",
                "elecCertName":"xxx 医疗机构执业许可证",
                "elecCertHolder": "xx 医疗机构",
                "elecCertHolderCode": "12323232",
                "elecCertNumber": "1262235241",
                "specialtiesName":"内科、外科",
                "areaName":"锦江区",
                "legalPerson":"张三",
                "holderCardNumber":"23434324334343343",
                "adress":"四川省成都市锦江区 xxx 路 xxx 号",
                "chargeRepresentative":"xxx",
```

```
            "natureBusiness":"",
            "setFormedName":"xxx",
            "telNum":"028-xxx",
            "category":"",
            "secondName":"",
            "level":"三甲",
            "rankName":"",
            "adminOrgName":"",
            "issueDept": "成都市青羊区卫生和计划生育局",
            "issueDeptCode": "370100004188602",
            "issueDate": "2019-10-14",
            "validityStart": "2019-10-14",
            "validityEnd": "2019-10-14",
            "state": "1"
    }]
}
```


7.13 电子证照查证

URL：https://{ip:port}/open/elecCert/query

调用方法：POST

功能描述：通过电子证照标识，获取电子证照 pdf 文件。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	elecCertId	string	1	电子证照标识
	userType	string	1	用户类型（1 个人或 2 单位）
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	0..1	证照对象
body 对象：	elecPdfBase64	string	1	电子证照文件 base64 编码

返回内容示例：


```
{
    "result_code":"0",
    "result_msg":"请求成功",
    "success":true,
```

```
    "body":{
                    "elecPdfBase64": "DFDFSDDFS***="
    }
}
```

7.14 电子证照真伪验证

URL：https://{ip:port}/open/elecCert/verifySeal

调用方法：POST

功能描述：电子证照签章验证，验证章的有效性。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	elecCertId	string	1	电子证照标识
	fileEntity	string	1	电子证照文件 base64 编码
	userType	string	1	用户类型（1 个人或 2 单位）
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	1	结果信息
body 对象:	verifyResult	bool	1	文件整体验证结果 ture 或 false
	fileName	string	1	验证文件名称
	verifyList	array	0..n	签章验证列表
verifyList 数组：	signIndex	int	1	签名或签章序号，标识文档中出现的第几个签名或签章，从 1 开始编号。
	signStd	string	1	“es.GBT38540”GB/T 3854 标准 “es.GMT0031” GM/T 0031 标准 “ds.GBT35275”GB/T 35275 标准 “ds.PKCS7” PKCS#7 数字签名 “unknown” 未识别的签名标准
	verify	string	1	单个印章或签名验证结果“true/false”， 当 signStd 类型为 es.GMT0031 或 ds.PKCS7 时，不做验证，该值为“unknown”
	errorCode	string	1	错误码
	errorMsg	string	1	错误原因
	certInfo	object	0..1	证书信息(CertInfo 对象)
CertInfo 对象：	certBase64	string	1	签名证书， Base64 编码
	signatureAlgID	string	1	签名算法（如 SM2）
	certIssuer	string	1	证书颁发者
	certNo	string	1	证书序列号

参数分类	参数名称	参数类型	约束	参数说明
	certNotBefore	string	1	证书有效期起
	certNotAfter	string	1	证书有效期止
	certCN	string	1	证书主体
	signInfo	object	0..1	签名信息(SignInfo 对象)
SignInfo 对象：	timeData	string	1	时间戳签名值
	signTime	string	1	签名时间（yyyy-MM-DD HH:mm:ss）

返回内容示例：


```
{
"result_code":"0",
"result_msg":"请求成功",
"success":true,
"body":{
    " verifyResult ":"true",
        "fileName ":"ddd.pdf",
        "verifyList":[{
        "signIndex":1,
        "signStd":"ds.PKCS7",
        "verify":"unknown",
        "errorCode":"c803302",
        "errorMsg":"该数字签名为 rsa 签名",
        "certInfo":{
                  "certBase64":"base64",
                  "signatureAlgID":"3333",
                  "certIssuer":"四川 ca",
                  "certNo":"3333",
                  "certNotAfter":"2023-10-12 00:00:00",
                  "certNotBefore":"2022-10-12 00:00:00",",
                  "certCN":"张三",
        },
        "signInfo":{
                  "timeData":"dfsdsldhfsdj",
                  "signTime":"2020-12-12 00:00:00"
         }

      }]
   }
}
```


7.15 电子证照类型列表

URL：https://{ip:port}/open/elecCert/queryTypeList

调用方法：POST

功能描述：获取电子证照类型列表。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	无	无	无	无
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	array	0..n	证照类型列表
body 数组:	elecCertType	string	1	证照类型（护士执业证：NURSE ，医师执业证：DOCTOR,机构执业证：ORG）
	elecCertTypeName	string	1	证照类型名称（护士执业证，医师执业证，机构执业证）

返回内容示例：

```
{
    "result_code":"0",
    "result_msg":"请求成功",
    "success":true,
    "body":[{
                "elecCertType": "NURSE",
                "elecCertTypeName": "护士执业证"
    }]
}
```

7.16 待签署数据推送

URL：https://{ip:port}/open/sign/pushData

调用方法：POST

功能描述：机构的应用系统可以将数据同步到身份认证服务，在移动设备上完成签署（移动设备上的移动 APP、小程序为身份认证服务提供）。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	signType	string	1	签署类型，1 仅签署人（如医生）签 2 仅患者签 3 签署人和患者签（医生和患者）
	isSignOrder	string	1	签署顺序（1 有序 2 无序）
	isQrSign	string	0..1	是否返回签署二维码，通过扫码来签署（1 返回，0 或空不返回），如果传 1，则只能通过扫码签署或在移动端手动签署
	dataCatalogCode	string	1	签署数据种类编码（见表 A.2）

参数分类	参数名称	参数类型	约束	参数说明
	patientInfo	object	1	患者信息
patientInfo 对象	name	string	1	患者姓名
	age	string	1	患者年龄
	sex	string	1	患者性别（1 男 2 女）
	no	string	1	患者就诊卡号
	personCard	string	1	患者身份证号码
	doctorSignInfo	array	1	签署人（如医生）对象数组
doctorSignInfo 对象	personCard	string	1	签署人（如医生）身份证号
	signOrder	string	1	签署顺序
	dataSource	object	1	签署数据源
dataSource 对象:	dataName	string	1	数据名称
	data	array	1	签署数据数组
data 对象	key	string	1	名称
	value	string	1	key 对应值
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	1	返回对象
body 对象：	qrCode	string	0..1	二维码 base64 扫码签返回
	dataId	string	1	数据 id

输入参数示例：


```
{
    "patientInfo":{
        "name":"张三",
        "age":"100",
        "sex":"1",
        "no":"patient_no_001",
        "personCard":"333---"
    },
    "signType":"1",
    "isSignOrder":"0",
    "doctorSignInfo":[{
          "personCard":"333--",
          "signOrder":"1"
    }],
```

```
    "dataCatalogCode":" recipe",
    "datasource":{
        "dataName":"处方",
        "data":[
              {
                      "key":"症状",
                      "value":"发热"
              },
              {
                       "key":"体温",
                       "value":"39 度"
               }
           ]
       }
}
```


返回内容示例：


```
{
        "result_code":"0",
        "result_msg":"请求成功",
        "success":true,
        "body":{
                  "dataId":"12344 ",
                  "qrCode":"base64"
        }
}
```


7.17 待签署 Pdf 文件推送

URL：https://{ip:port}/open/sign/pushPdf

调用方法：POST

功能描述：机构的应用系统 pdf 版式文件同步到身份认证服务，签署人在移动设备上完成签署（移动设备上的移动 APP、小程序为身份认证服务提供）。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	signType	string	1	签署类型，1 仅签署人（如医生）签 2 患者签 3 签署人和患者签（医生和患者）
	isSignOrder	string	1	签署顺序（1 有序 2 无序）
	isQrSign	string	0..1	是否返回签署二维码，通过扫码来签署（1 返回，其他值 不返回），如果传 1，则只能通过扫码签署或在移动端手动签署
	docCatalogCode	string	1	签署文件种类编码（见表 A.2）
	patientInfo	object	1	患者信息
patientInfo 对象	name	string	1	患者姓名
	age	string	1	患者年龄
	sex	string	1	患者性别（1 男 2 女）
	no	string	1	患者卡号（如患者就诊卡号）
	personCard	string	1	患者身份证号码
	doctorSignInfo	array	1	签署人医生对象数组
doctorSignInfo 对象	personCard	string	1	签署人医生身份证号
	signOrder	string	1	签署顺序
	signInfo	object	1	签名坐标信息
signInfo 对象：	fillStyle	string	1	填充类型（2 图片，目前医生只支持 2）
	keyword	string	0..1	关键字（关键字和坐标二选一）
	keywordIndex	string	0..1	关键字索引（关键字和坐标二选一）
	x	string	0..1	坐标 x（关键字和坐标二选一）
	y	string	0..1	坐标 y（关键字和坐标二选一）
	pageNumber	int	0..1	坐标签署必传
	patientSignInfo	array	1	患者对象数组
patientSignInfo 对象:	fillStyle	string	0..1	填充类型（//1 文本 2 图片 3 语音 4 手写签名）,如果是手写签名情况该字段必传
	keyword	string	0..1	关键字（关键字和坐标二选一）
	keywordIndex	string	0..1	关键字索引（关键字和坐标二选一）
	x	string	0..1	坐标 x（关键字和坐标二选一）
	y	string	0..1	坐标 y（关键字和坐标二选一）
	pageNumber	int	0..1	坐标签署必传
	signContentTitle	string	1	签署内容标题
	pdfInfo	object	1	pdf 信息对象
pdfInfo 对象：	fileName	string	1	文件名称
	pdfBase64	string	1	pdf 文件 base64 编码（5M 以内）
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	1	返回对象
body 对象：	qrCode	string	0..1	二维码 base64 编码,扫码签才返回

参数分类	参数名称	参数类型	约束	参数说明
	dataId	string	1	数据 id

输入参数示例：


```
{
        "patientInfo":{
                        "name":"张三",
                        "age":"100",
                        "sex":"1",
                        "no":"patient_no_001",
                        "personCard":"333---"
        },
        "signType":"1",
        "isSignOrder":"0",
        "doctorSignInfo":[
            {
                "personCard":"333--",
                "signOrder":"1",
                 "signInfo": {
                            "keyword": "1 号医生签署",
                            "keywordIndex": 1,
                            "x": "",
                            "y": "",
                           "pageNumber": 2,
                            "fillStyle": "2"
                 }
            }
        ],
        "patientSignInfo":[
            {
                "keyword":"患者签名",
                "keywordIndex":1,
```

```
                "x":40,
                "y":0,
                "fillStyle":"1"
            }
        ],
        "pdfInfo":{
                "fileName":"afc.pdf",
                "pdfBase64":"base64"
        }
}
```


返回内容示例：


```
{
        "result_code":"0",
        "result_msg":"请求成功",
        "success":true,
        "body":{
                    "qrCode":"base64",
                    "dataId":"12344 "
        }
}
```


7.18 认证服务签署状态查询接口

URL：https://{ip:port}/open/sign/querySignStatus

调用方法：POST

功能描述：业务系统把数据/文件推送到身份认证服务，在移动设备上签署时的状态查询（移动设备上的移动 APP、小程序为身份认证服务提供），返回签署信息。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	dataId	string	1	签署数据 id
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	1	对象

参数分类	参数名称	参数类型	约束	参数说明
body 对象:	dataId	string	1	签署数据 id
	docContentBase64	string	0..1	pdf 文档内容, Base64 编码数据（数据签署时候为空）
	signStatus	string	1	当前文档状态,1: 医生签署, 2: 患者签署, 3 已完成, 4: 作废
	patientSignInfo	object	1	患者签署信息
patientSignInfo 对象	no	string	1	患者就诊卡号
	name	string	1	患者姓名
	seal	string	0...1	患者签章图片(可以为空)
	signTime	long	1	患者签署时间戳
	timeData	string	1	时间戳签名值
	signed	bool	1	患者是否已经签署此文档
	signChannel	string	1	医生签署此文档的方式，微信小程序: WX, 平板电脑: PAD、app:APP、自动签署:AUTO
	signerName	string	1	签署人姓名
	signature	string	0..1	签名值，数据签才返回
	holders	array	0..n	解析出来的动态占位符列表，数据格式为{Key:Value}形式，key 为动态占位符的名称，value 为患者填充的值,PDF 签署才有
	doctorSignInfo	object	1..n	医生签署对象
doctorSignInfo 对象	cardNumber	string	1	医生身份证
	name	string	1	医生姓名
	seal	string	1	医生签章图片
	signTime	long	1	医生签署时间
	timeData	string	1	时间戳签名值
	signed	bool	1	医生是否已经签署此文档
	signature	string	0..1	签名值，数据签才返回
	signChannel	string	1	医生签署此文档的方式,微信小程序: MINI, 平板电脑: PAD、app:APP、自动签署:AUTO

返回内容示例：


```
{
        "id": "1303172585906810882",
        "signStatus": 0,
        "docContentBase64": "…",
        "doctorSignInfo":[{
                "cardNumber":"007",
```

```
                "name":"张三医生",
                "seal":"...",
                "signTime":1597225333000,
                "timeData":"
MIIE+gYJKoZIhvcNAQcCoIIE6zCCBO.....UXtTTr4dRMi7iNG2W5ZcUYBysPPM8fpwPFyfEZV2wwIh
AMB7vAK1n1xIl2+LRJSYaicmGqBMRZFSOc6YZkKFRRqS",
                "siend":true,
                "signChannel":"APP",
                "signature":"MIIFBgYJKoZIhvc……8BC75zXwcOPZGLNIsrUtj2tm2"
        }],
        "patientSignInfo": {
            "no":"123456",
            "name":"李四患者",
            "signerName":"李四亲属",
            "seal":"...",
            "signature":"MIIFBgYJKoZIhvc……8BC75zXwcOPZGLNIsrUtj2tm2",
            "signTime":1597225833000,
            "timeData":"MIIE+gYJKoZIhvcNAQcCoIIE6zCCBO.....UXtTTr4dRMi7iNG2W5Zc
            UYBysPPM8fpwPFyfEZV2wwIhAMB7vAK1n1xIl2+LRJSYaicmGqBMRZFSOc6YZkKFRRq
            S",
            "signed":true,
            "signChannel":"WX",
            "holders":{
                "双方关系":"朋友",
                "联系电话":"19090909090"
            }
        }
}
```


7.19 认证服务签署状态通知

URL：{接口由业务系统提供}/pushcallback

调用方法：POST

功能描述：业务系统把数据/文件推送到身份认证服务，用户在移动设备上签署/废弃数据后，身份认证服务通过此接口通知第三方系统，返回数据格式遵循“6.6 回调数据”格式标准.

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	dataId	string	1	签署数据 id
	docContentBase64	string	0..1	pdf 文档内容，Base64 编码数据，数据签署时候为空
	signStatus	string	1	当前文档状态，1：医生签署，2：患者签署，3 已完成，4：作废

参数分类	参数名称	参数类型	约束	参数说明
	patientSignInfo	object	1	患者签署信息
patientSignInfo 对象	no	string	1	患者就诊卡号
	name	string	1	患者姓名
	seal	string	0..1	患者签章图片(可以为空)
	signTime	long	1	患者签署时间戳
	timeData	string	1	时间戳签名值
	signed	bool	1	患者是否已经签署此文档
	signChannel	string	1	医生签署此文档的方式，微信小程序: WX, 平板电脑: PAD、app:APP、自动签署:AUTO
	signerName	string	1	签署人姓名
	signature	string	0..1	签名值，数据签才返回
	holders	array	0..n	解析出来的动态占位符列表， 数据格式为{Key:Value}形式， key 为动态占位符的名称, value 为患者填充的值，PDF 签署才有
	doctorSignInfo	object	1	医生签署对象
doctorSignInfo 对象	cardNumber	string	1	医生身份证
	name	string	1	医生姓名
	seal	string	1	医生签章图片
	signTime	long	1	医生签署时间
	timeData	string	1	时间戳签名值
	signed	bool	1	医生是否已经签署此文档
	signature	string	0..1	签名值，数据签才返回
	signChannel	string	1	医生签署此文档的方式，微信小程序: WX, 平板电脑: PAD、app:APP、自动签署:AUTO
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败,成功:true,失败:false
body 对象:	body	object	0..1	返回对象（具体内容由业务系统提供）

输入参数示例：


```
{
        "id": "1303172585906810882",
        "signStatus": 0,
        "docContentBase64": "…",
        "doctorSignInfo":[{
            "cardNumber":"007",
            "name":"张三医生",
```

```
            "seal":"...",
            "signTime":1597225333000,
             "timeData":"MIIE+gYJKoZIhvcNAQcCoIIE6zCCBO.....UXtTTr4dRMi7iNG2W5Z
cUYBysPPM8fpwPFyfEZV2wwIhAMB7vAK1n1xIl2+LRJSYaicmGqBMRZFSOc6YZkKFRRqS",
            "siend":true,
            "signChannel":"APP",
            "signature":"MIIFBgYJKoZIhvc……8BC75zXwcOPZGLNIsrUtj2tm2"
        }],
        "patientSignInfo": {
            "no":"123456",
            "name":"李四患者",
            "signerName":"李四亲属",
            "seal":"...",
            "signature":"MIIFBgYJKoZIhvc……8BC75zXwcOPZGLNIsrUtj2tm2",
            "signTime":1597225833000,
             "timeData":"MIIE+gYJKoZIhvcNAQcCoIIE6zCCBO.....UXtTTr4dRMi7iNG2W5Z
              cUYBysPPM8fpwPFyfEZV2wwIhAMB7vAK1n1xIl2+LRJSYaicmGqBMRZFSOc6YZkKF
              RRqS",
            "signed":true,
            "signChannel":"WX",
            "saveType":2,
            "holders":{
                "双方关系":"朋友",
                "联系电话":"19090909090"
            }
        }
}
```


7.20 获取数据签署 H5 链接地址

URL：https://{ip:port}/open/signature/h5Sign

调用方法：POST

功能描述：应用系统调用此接口,返回一个签署界面 url 链接地址，用户在 url 对应界面上对数据进行签署。

参数分类	参数名	参数类型	约束	参数说明
输入参数：	dataType	string	1	签名原文类型 PLAIN|HASH
	elecCertId	string	0..1	证照标识(通过证照签名时候必传)
	cardNumber	string	1	单位唯一标识或个人唯一标识
	signatureAlgID	string	1	签名算法，此处为 SM2
	hashAlgID	string	1	HASH 算法，支持 SM3
	userType	string	1	1 个人 2 单位

参数分类	参数名	参数类型	约束	参数说明
	toSign	string	1	签名原文
	transId	string	1	业务流水号，业务系统内保持唯一
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	1	返回对象
body 对象：	htmlUrl	string	1	h5 链接地址

返回内容示例：


```
{
        "result_code":"0",
        "result_msg":"请求成功",
        "success":true,
        "body":{
          "htmlUrl": "https://www.{....}.com"
        }
    }
```


7.21 获取 pdf 签署 H5 链接地址

URL：https://{ip:port}/open/signature/h5SignPdf

调用方法：POST

功能描述：应用系统调用此接口,返回一个签署界面 url，用户在 url 对应界面上对 PDF 文件进行签署。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	userType	string	1	用户类型（1 个人或 2 单位）
	personCard	string	0..1	个人唯一码(如身份证，当用户类型 1 时，personCard 必填)
	orgCode	string	0..1	单位唯一码(用户类型为 2 时,orgCode 必填)
	sealId	string	1	印章标识
	orgName	string	0..1	单位名称
	file	string	1	文件 base64 编码（5M 以内）
	digitalCertId	string	1	数字证书唯一标识
	isQf	string	0..1	是否盖骑缝章，默认非骑缝
	qfPossition	string	0..1	骑缝章盖章位置
	sealType	string	1	关键字或者坐标
	sealInfo	object	1	签章参数对象
	transId	string	1	业务流水号，业务系统内保持唯一

参数分类	参数名称	参数类型	约束	参数说明
sealInfo 对象：	keyword	string	0..1	关键字 sealType 为：关键字时必传
	pageConfigList	array	0..n	关键字位置 sealType 为：关键字时必传
pageConfigList 数组：	pageNo	string	1	签章页码，用”,”隔开（英文状态） sealType 为：关键字时必传
	keyWordIndex	string	1	当前页面第几个 sealType 为：关键字时必传
坐标数组	x	string	0..1	sealType 为：坐标时必传，用”,”隔开
	y	string	0..1	sealType 为：坐标时必传，用”,”隔开
	pageNo	string	0..1	签章页码，用”,”隔开（英文状态）
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	1	返回对象
body 对象：	htmlUrl	string	1	html 连接

关键字输入参数示例：


```
{
    "userType": 1,
    "personCard": "",
    "orgCode": "",
    "sealId": "1673983799422935041",
    "digitalCertId": "",
    "orgName": "测试医疗机构",
    "sealType": "关键字",
    "isQf": true,
    "qfPossition": 0.8,
    "sealInfo": [
        {
            "keyword": "医生签名",
            "pageConfigList": [
                {
                    "pageNo": 1,
                    "keyWordIndex": 1
                }
            ]
```

```
        },
        {
            "keyword": "患者意见",
            "pageConfigList": [
                {
                    "pageNo": 1,
                    "keyWordIndex": 1
                }
            ]
        }
    ],
    "file": ""
}
```

7.22 H5 或接口签署信息查询接口

URL：https://{ip:port}/open/sign/queryApiSignInfo

调用方法：POST

功能描述：业务系统通过“7.21 获取 pdf 签署 H5 链接地址、7.20 获取数据签署 H5 链接地址、7.2 数字证书签名、 8.3 电子签章”进行签署时，签署信息查询，返回签署信息。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	transId	string	1	业务流水号，业务系统内保持唯一
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	1	对象
body 对象:	signStatus	string	1	当前状态，1:已签署 0 未签署
	certInfo	object	0..1	证书信息(CertInfo 对象)
CertInfo 对象：	certBase64	string	1	签名证书， Base64 编码
	signatureAlgID	string	1	签名算法（如 SM2）
	certIssuer	string	1	证书颁发者
	certNo	string	1	证书序列号
	certNotBefore	string	1	证书有效期起
	certNotAfter	string	1	证书有效期止
	certCN	string	1	证书主体
	signInfo	object	0..1	签名信息(SignInfo 对象)

参数分类	参数名称	参数类型	约束	参数说明
SignInfo 对象：	timeData	string	1	时间戳签名值
	signTime	string	1	签名时间（yyyy-MM-DD HH:mm:ss）
	signP7	string	0..1	P7 签名值(数据签署时候才返回)
	seal	string	0..1	签章图片
	toSign	string	0..1	签名原文（pdf 签署时候为空）
	docContentBase64	string	0..1	pdf 文档内容，Base64 编码数据（数据签署时候为空）

返回内容示例：


```
{
    "result_code":"0",
    "result_msg":"请求成功",
    "success":true,
    "body":{
            "signStatus": 0,
            "certInfo":{
                "certBase64":"base64",
                "signatureAlgID":"3333",
                "certIssuer":"四川 ca",
                "certNo":"3333",
                "certNotAfter":"2023-10-12 00:00:00",
                " certNotBefore":"2022-10-12 00:00:00",
                "certCN":"张三",
            },
            "signInfo":{
                "timeData":"dfsdsldhfsdj",
                 "signTime":"2020-12-12 00:00:00",
                 "signP7":"dddfdf",
                 "seal":"base64",
                 "docContentBase64": "base64",
                 "toSign": "签名原文"
            }
        }
}
```


7.23 H5 签署状态通知

URL：{接口由业务系统提供}/pushcallback

调用方法：POST

功能描述：h5 签署数据或 pdf 时，返回的状态通知，数据格式遵循“6.6 回调数据”数据标准。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	signStatus	string	1	当前状态，1:已签署 0 未签署
	signInfo	object	0..1	签名信息SignInfo对象(未签署返回空)
SignInfo对象：	seal	string	0..1	签名图片
	signTime	long	1	签署时间戳
	timeData	string	1	时间戳签名值
	signP7	string	0..1	P7签名值(数据签署时候才返回)
	toSign	string	0..1	签名原文（pdf签署时候为空）
	docContentBase64	string	0..1	pdf 文档内容， Base64 编码数据（数据签署时候为空）
	certInfo	object	0..1	证书信息CertInfo对象(未签署返回空)
CertInfo对象：	certBase64	string	1	签名证书， Base64编码
	signatureAlgID	string	1	签名算法（如SM2）
	certIssuer	string	1	证书颁发者
	certNo	string	1	证书序列号
	certNotBefore	string	1	证书有效期起
	certNotAfter	string	1	证书有效期止
	certCN	string	1	证书主体

输入参数示例：

```
{
    "docContentBase64": "base64",
    "signStatus": 0,
    "certInfo":{
        "certBase64":"base64",
        "signatureAlgID":"3333",
        "certIssuer":"四川ca",
        "certNo":"3333",
        "certNotAfter":"2023-10-12 00:00:00",
        " certNotBefore":"2022-10-12 00:00:00",
        "certCN":"张三",
    },
    "signInfo":{
        "timeData":"dfsdsldhfsdj",
        "signTime":"2020-12-12 00:00:00",
        "signP7":"dddfdf",
        "seal":"base64",
        "docContentBase64": "base64",
        "toSign": "签名原文"
    }
}
```

7.24 免密签署状态查询

URL：https://*{ip:port}*/open/digitalCert/pinSaveStatus

调用方法：POST

功能描述：查询免密签署是否开启，用户免密操作，如果开启，在“7.2 数字证书签名”和“8.3 电子签章”接口则可以不传入 pin 码。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	cardNumber	string	1	个人唯一标识
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	1	返回对象
body 对象：	pinStatus	int	1	1 开启 0 未开启

返回内容示例：

```
{
    "result_code":"200",
    "result_msg":"成功",
    "success":true,
    "body":{ pinStatus：1 }
}
```

8 电子签章服务接口

8.1 接口列表

表 3 电子签章服务接口列表

编号	接口功能	接口 URL 对象	方法	授权	备注
1	电子印章查询	https://{ip:port}/open/signature/sealQuerysealQue	POST	trusted	
2	电子签章	https://{ip:port}/open/signature/signPdf	POST	trusted	
3	电子印章 pdf 验证接口	https://{ip:port}/open/signature/verifyPdf	POST	trusted	

8.2 电子印章查询

URL：https://{ip:port}/open/signature/sealQuerysealQue

调用方法：POST

功能描述：查询单位或个人电子印章。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	userType	string	1	用户类型（1 个人或 2 单位）
	personCard	string	0..1	个人唯标识(如身份证，当用户类型 1 时,必填)
	orgCode	string	0..1	单位唯标识（用户类型为 2 时，orgCode 必填）
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	array	0..n	结果信息
body 数组：	sealId	string	1	印章标识
	sealData	string	1	印章数据 Base64 编码，遵循 GB/T 38540
	makeEsealTime	string	1	制章时间
	defaultSeal	int	1	是否默认，1-是，0-否

返回内容示例：


```
{
        "result_code":"0",
        "result_msg":"请求成功",
        "success":true,
        "body":{[
              "sealId":"12343243",
              "sealData":"DEF****==",
              "makeEsealTime":"2022-10-20 12:00:00" ,
               "defaultSeal":"1"
        ]}
}
```


8.3 电子签章

URL：https://{ip:port}/open/signature/signPdf

调用方法：POST

功能描述：应用系统调用此签章接口完成 PDF 文件的文件签署。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	userType	string	1	用户类型（1 个人或 2 单位）
	transId	string	1	业务流水号，业务系统内保持唯一
	personCard	string	0..1	个人唯一码(如身份证，当用户类型 1 时必填)
	orgCode	string	0..1	单位唯一码（用户类型为 2 时必填）
	sealId	string	1	印章标识

参数分类	参数名称	参数类型	约束	参数说明
	orgName	string	0..1	单位名称
	file	string	1	文件 base64 编码（5M 以内）
	digitalCertId	string	1	数字证书唯一标识
	pin	string	0..1	数字证书 pin 码(个人如果设置了免密，则不需要传,否则必传)
	isQf	string	0..1	是否盖骑缝章，默认非骑缝
	qfPossition	string	0..1	骑缝章盖章位置
	sealType	string	1	关键字或者坐标
	sealInfo	object	1	签章参数对象
sealInfo 对象：	keyword	string	0..1	关键字 sealType 为：关键字时必传
	pageConfigList	array	0..n	关键字位置 sealType 为：关键字时必传
pageConfigList 数组：	pageNo	string	1	签章页码，用”,”隔开（英文状态） sealType 为：关键字时必传
	keyWordIndex	string	1	当前页面第几个 sealType 为：关键字时必传
坐标数组	x	string	0..1	sealType 为：坐标时必传，用”,”隔开
	y	string	0..1	sealType 为：坐标时必传，用”,”隔开
	pageNo	string	0..1	签章页码，用”,”隔开（英文状态）
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	1	返回对象
body 对象：	sealId	string	1	印章标识
	signData	string	1	签章文件 base64 编码
	sealTime	string	1	签章时间（yyyy-MM-DD HH:mm:ss）
	timeData	string	1	时间戳签名值

关键字输入参数示例：


```
{
    "userType": 1,
    "personCard": "",
    "orgCode": "",
    "sealId": "1673983799422935041",
    "digitalCertId": "",
    "pin": "123456",
    "orgName": "测试医疗机构",
    "sealType": "关键字",
    "isQf": true,
```

```
    "qfPossition": 0.8,
    "sealInfo": [
        {
            "keyword": "医生签名",
            "pageConfigList": [
                {
                    "pageNo": 1,
                    "keyWordIndex": 1
                }
            ]
        },
        {
            "keyword": "患者意见",
            "pageConfigList": [
                {
                    "pageNo": 1,
                    "keyWordIndex": 1
                }
            ]
        }
    ],
    "file": ""
}
```


坐标输入参数示例：


```
{
    "userType": 1,
    "personCard": "",
    "orgCode": "",
    "sealId": "1673983799422935041",
    "digitalCertId": "",
    "pin": "123456",
```

```
    "orgName": "测试医疗机构",
    "sealType": "坐标",
    "isQf": true,
    "qfPossition": 0.5,
    "sealInfo": [
        {
            "pageNo": 1,
            "x": 0.4,
            "y": 0.1
        }
    ],
    "file": "2Jq/F3CpS"
}
```


返回内容示例：


```
{
        "result_code":"0",
        "result_msg":"请求成功",
        "success":true,
        "body":{
                    "sealId":"12344 ",
                    "requestId":"12345",
                    "signData":"DFDF***===",
                    "sealTime":"2022-12-09 10:00:00"   ,
                     "timeData":"MIIE+gYJKoZIhvcNAQcCoIIE6zCCBO.....UXtTTr4dRMi7
            iNG2W5ZcUYBysPPM8fpwPFyfEZV2wwIhAMB7vAK1n1xIl2+LRJSYaicmGqBMRZFSO
            c6YZkKFRRqS",

        }
}
```


8.4 电子签章 pdf 验证接口

URL：https://{ip:port}/open/signature/verifyPdf

调用方法：POST

功能描述：电子签章 pdf 验证，验证 pdf 签章的有效性，并获取签章签署信息。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	file	string	1	电子签章文件 base64 编码
	transId	string	0..1	业务流水号，业务系统内保持唯一，不传则不返回 CertInfo、SignInfo 对象
输出参数：	result_code	string	1	正常状态码
	result_msg	string	1	正常响应描述
	success	bool	1	成功失败，成功：true，失败：false
	body	object	1	结果信息
body 对象:	verifyResult	bool	1	文件整体验证结果 ture 或 false
	verifyList	array	0..n	签章验证列表
verifyList 数组：	signIndex	int	1	签名或签章序号，标识文档中出现的第几个签名或签章，从 1 开始编号。
	signStd	string	1	“es.GBT38540”GB/T 3854 标准 “es.GMT0031” GM/T 0031 标准 “ds.GBT35275”GB/T 35275 标准 “ds.PKCS7” PKCS#7 数字签名 “unknown” 未识别的签名标准
	verify	string	1	单个印章或签名验证结果 “true/false”，当 signStd 类型为 es.GMT0031 或 ds.PKCS7 时，不做验证，该值为“unknown”
	errorCode	string	1	错误码
	errorMsg	string	1	错误原因
	certInfo	object	0..1	证书信息(CertInfo 对象)
CertInfo 对象：	certBase64	string	1	签名证书， Base64 编码
	signatureAlgID	string	1	签名算法（如 SM2）
	certIssuer	string	1	证书颁发者
	certNo	string	1	证书序列号
	certNotBefore	string	1	证书有效期起
	certNotAfter	string	1	证书有效期止
	certCN	string	1	证书主体
	signInfo	object	0..1	签名信息(SignInfo 对象)
SignInfo 对象：	timeData	string	1	时间戳签名值
	signTime	string	1	签名时间（yyyy-MM-DD HH:mm:ss）

返回内容示例：


```
{
  "result_code":"0",
  "result_msg":"请求成功",
  "success":true,
  "body":{
    "verifyResult ":"true",
```

```
  " fileName ":"ddd.pdf",
  "verifyList":[{
      "signIndex":1,
      "signStd":"ds.PKCS7",
      "verify":"unknown",
      "errorCode":"c803302",
      "errorMsg":"该数字签名为 rsa 签名",
      "certInfo":{
          "certBase64":"base64",
          "signatureAlgID":"3333",
          "certIssuer":"四川 ca",
          "certNo":"3333",
          "certNotAfter":"2023-10-12 00:00:00",
          " certNotBefore":"2022-10-12 00:00:00",",
          "certCN":"张三",
       },
       "signInfo":{
          "timeData":"dfsdsldhfsdj",
          "signTime":"2020-12-12 00:00:00"
       }
    }]
  }
}
```

附录 A

（资料性附录）

表 A.1 接口返回状态码定义

消息代码	消息描述
0	成功
1000	应用 ID 为空
1001	应用 ID 未匹配任何应用
1002	参数签名为空
1003	参数签名值错误
1103	参数错误
1104	数据重复
1105	权限验证错误
1107	二维码生成失败
1299	应用负载超过设定值
1202	调用内部服务出错
1205	非法 IP 调用
2001	用户不存在
2003	签名验证失败
2006	二维码登录失败
3001	网络错误
9001	重复提交
9998	操作失败
9999	其它错误

表 A.2 签署数据种类编码/签署文件种类编码

签署数据种类编码/签署文件种类编码	描述信息
recipe	处方
viewport	影像
diagnosis	诊断报告
medicalRecord	病历
consultation	会诊意见书
laboratory	检验模板参数
docCode_001	病历概要
docCode_002	门（急）诊病历
docCode_003	急诊留观病历
docCode_004	西药处方

签署数据种类编码/签署文件种类编码	描述信息
docCode_005	中药处方
docCode_006	检查报告
docCode_007	检验报告
docCode_008	治疗记录
docCode_009	一般手术记录
docCode_010	麻醉术前访视记录
docCode_011	麻醉记录
docCode_012	麻醉术后访视记录
docCode_013	输血记录
docCode_014	待产记录
docCode_015	阴道分娩记录
docCode_016	剖宫产记录
docCode_017	一般护理记录
docCode_018	病重（病危）护理记录
docCode_019	手术护理记录
docCode_020	生命体征测量记录
docCode_021	出入量记录
docCode_022	高值耗材使用记录
docCode_023	入院评估
docCode_024	护理计划
docCode_025	出院评估与指导
docCode_026	手术知情同意书
docCode_027	麻醉知情同意书
docCode_028	输血治疗同意书
docCode_029	特殊检查及特殊治疗同意书
docCode_030	病危（重）同意书
docCode_031	其他知情同意书
docCode_032	住院病案首页
docCode_033	中医住院病案首页
docCode_034	入院记录
docCode_035	24 小时内入出院记录
docCode_036	24 小时内入院死亡记录
docCode_037	首次病程记录
docCode_038	日常病程记录
docCode_039	上级医师查房记录
docCode_040	疑难病例讨论记录

签署数据种类编码/签署文件种类编码	描述信息
docCode_041	交接班记录
docCode_042	转科记录
docCode_043	阶段小结
docCode_044	抢救记录
docCode_045	会诊记录
docCode_046	术前小结
docCode_047	术前讨论
docCode_048	术后首次病程记录
docCode_049	出院记录
docCode_050	死亡记录
docCode_051	死亡病例讨论记录
docCode_052	住院医嘱
docCode_053	出院小结