ICS 11.020
C 50

团　　体　　标　　准

T/SHIA 013—2024

认证服务机构接入接口规范

Authentication service Authority Access 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

《国家“十四五”全民健康信息化规划》中明确构建卫生健康行业网络可信体系，实现医患可信身份电子认证和电子签名，保证访问、处理数据的用户身份真实；拓展电子证照应用领域。本接口规范的制定是为了规范认证服务机构采用标准统一的接口进行接入，以便能够为医疗机构提供相应的数字证书和电子证照实体，保障卫生健康行业网络可信体系建设，拓展电子证照应用领域；认证服务机构包括电子认证服务机构（CA 机构）和按照法定职责签批颁发电子证照的各级政务服务部门或取得法定资质的第三方机构。

目前，国内卫生行业各认证服务机构（CA 机构、电子证照认证机构）在对外提供数字证书及电子证照实体时，由于缺少认证服务机构接入的统一标准，从而导致认证服务机构重复多次开发，不利于形成融合的认证服务提供合作生态，导致认证服务机构间的恶性竞争、服务成本增加，因此制定认证服务机构接入的接口规范势在必行。

认证服务机构（CA 机构、电子证照认证机构）使用统一接入接口规范，可以有效屏蔽认证服务机构之间的差异，避免认证服务机构提供电子证照融合 CA 认证时，标准的不统一、接入规则的无序变动，从而构建开放的合作生态为医疗机构提供电子证照融合 CA 认证服务。

认证服务机构接入接口规范

1 范围

本文件规定了身份认证服务的认证服务提供者接入跨 CA 多证照身份认证服务，提供数字证书认证及电子证照认证服务所应遵守的接口标准。

本文件适用于认证服务机构接入身份认证服务来提供数字证书服务、电子证照服务，认证服务机构包括：证书认证机构、电子证照认证机构。

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

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

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

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]

3.7

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]

3.8

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]

3.9

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]

3.10

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]

3.11

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]

3.12

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]

3.13

认证服务机构 authentication service authority

本文件定义的认证服务机构指为身份认证服务的提供者，提供数字证书、电子证照的服务机构，包括证书认证机构（CA）、电子证照认证机构。

4 缩略语

下列缩略语适用于本文件。

CA　Certification Authority 证书认证机构

CRL　Certificate revocation list 证书撤销列表

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

API　Application Program Interface 应用程序接口,简称应用接口

5 认证服务机构接入接口说明

5.1 接入接口说明

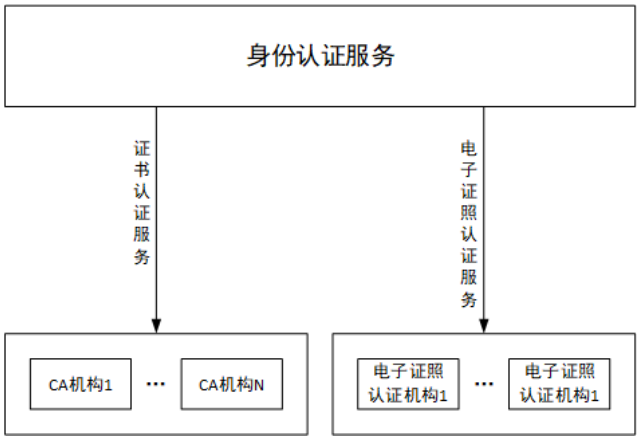

图 1 认证服务机构接入接口说明

身份认证服务可以向上层应用系统提供多种身份认证方式（如图 1），包括数字证书认证、电子证照认证。认证服务机构可以遵循本文件的定义接入身份认证服务。本文件的认证服务机构包括：证书认证机构、电子证照认证机构。

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

认证服务机构应按如下的通讯协议和数据结构与身份认证服务进行信息交换。

身份认证服务和认证服务机构基于 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，请求报文需要由身份认证服务使用 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，是认证服务机构服务网络地址，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

各接入的认证服务机构在与身份认证服务通讯时，身份认证服务提供认证信息，用于鉴别其身份。可以通过验证签名的方式鉴别身份。

——认证服务机构向身份认证服务分配唯一的 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。

——认证服务机构提供的开放接口采用 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，认证服务机构分配。
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)

6.5 状态信息

认证服务机构 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。

7 证书认证机构（CA）接入接口

7.1 接口列表

证书认证机构（CA）应该按照下列标准提供相应的 API 接口，供身份认证服务调用。

表 2 证书认证机构接入接口

编号	接口功能	接口 URL 对象	方法	授权	备注
1	个人证书申请	https://*{ip:port}*/open/digitalCert/person/apply	POST	trusted	
2	机构证书申请	https://*{ip:port}*/open/digitalCert/enterpise/apply	POST	trusted	
3	证书更新	https://*{ip:port}*/open/digitalCert/update	POST	trusted	
4	证书吊销	https://*{ip:port}*/open/digitalCert/ revoke	POST	trusted	
5	证书验证	https://*{ip:port}*/open/digitalCert/effective	POST	trusted	

7.2 机构证书数据结构

表 3 机构证书数据结构

证书域名	含义	说明		字段内容（示例）
Version	版本号	证书版本号		V3
Serial Number	序列号	由颁发机构指定		证书序列号
Signature	签名算法	符合国家标准		符合国家标准
Issuer	颁发者	C	国家	CN
		O	单位	Xx
		OU	部门	xx
		CN	二级 CA 通用名	xx CA
Validity	有效期限			最长 2 年
notBefore	有效期起始日期	签发日期		年月日+时分秒
notAfter	有效期终止日期	起始日期＋x 个月		年月日+时分秒
Subject	主体	C	国家	CN
		S	省份	持证人所在省份，如：广东
		L	城市	持证人所在城市，如：深圳
		O	用户单位/机构	xx 卫生厅（局）
		OU	部门名称	信息中心（可选字段）
		CN	用户通用名	xx 卫生厅（局）xx 部门（单位名称全称）
		Email	电子邮件	（可选字段）
Subject Public Key Information	公钥	包括加密算法及公钥值		采用 SM2 算法
Extensions	扩展域			
KeyUsage	密钥用法	关键扩展项		Digital Signature, keyEncipherment； 根据证书用途，分“签名”或“加密”证书
SubjectUniqueID	实体唯一标识	非关键扩展项		OID：1.2.156.xxxx，OID 对应的值如：1@1001JJ0123456789
SubjectKeyIdentifier	主体密钥标识符	关键扩展项		用户证书公钥的哈希值
AuthorityKeyIdentifier	颁发机构密钥标识符	关键扩展项		颁发单位证书公钥的哈希值
CRLDistributionPoints	CRL 分发点	非关键扩展项		[1]CRL Distribution Point Distribution Point

证书域名	含义	说明	字段内容（示例）
			Name: Full Name: Directory Address: DN… [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ldap.xxca.org.cn/crl/ caxcrlxx.crl
SignatureAlgorithm	签名算法	对证书基本信息的数字签名的签名算法	
Issuer’s Signature	签名值	颁发机构对证书基本信息的数字签名	数字签名值

7.3 个人证书数据结构

表 4 个人证书数据结构

证书域名	含义	说明		字段内容（示例）
Version	版本号	证书版本号		V3
Serial Number	序列号	由颁发机构指定		证书序列号
Signature	签名算法	符合国家标准		符合国家标准
Issuer	颁发者	C	国家	CN
		O	单位	xx
		OU	部门	xx
		CN	二级 CA 通用名	xx CA
Validity	有效期限			最长 2 年
notBefore	有效期起始日期	签发日期		年月日+时分秒
notAfter	有效期终止日期	起始日期＋x 个月		年月日+时分秒
Subject	主体	C	国家	CN
		S	省份	持证人所在省份，如：广东
		L	城市	持证人所在城市，如：深圳
		O	用户单位/机构	xx 卫生厅（局）
		OU	部门名称	信息中心（可选字段）
		CN	用户通用名	张三（个人姓名）
		Email	电子邮件	（可选字段）

证书域名	含义	说明	字段内容（示例）
Subject Public Key Information	公钥	包括加密算法及公钥值	如：采用 SM2 算法
Extensions	扩展域		
KeyUsage	密钥用法	关键扩展项	Digital Signature, keyEncipherment； 根据证书用途，分“签名”或“加密”证书
SubjectUniqueID	实体唯一标识	非关键扩展项	OID 如：1.2.156.xxx8，OID 对应的值如：1@1001SF03422221972050536 18
SubjectKeyIdentifier	主体密钥标识符	关键扩展项	用户证书公钥的哈希值
AuthorityKeyIdentifier	颁发机构密钥标识符	关键扩展项	颁发单位证书公钥的哈希值
CRLDistributionPoints	CRL 分发点	非关键扩展项	[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: DN… [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ldap.xxca.org.cn/crl/ caxcrlxx.crl
SignatureAlgorithm	签名算法	对证书基本信息的数字签名的签名算法	
Issuer’s Signature	签名值	颁发机构对证书基本信息的数字签名	数字签名值

7.4 个人证书申请

URL：https://{ip:port}/open/digitalCert/person/apply

调用方法：POST

功能描述：当用户办理证书新办业务时，调用本接口申请证书。

参数分类	参数名	参数类型	约束	说明
输入参数：	transId	string	1	流水号
	time	string	1	发送时间
	busiType	string	1	业务类型：新增-enroll， 变更-reChange，补办-reEnroll
	serialnumberSign	string	0..1	签名证书序列号，业务类型为变更，补办时需要
	name	string	1	姓名
	idType	string	1	证件类型：1-居民身份证
	idNumber	string	1	证件号码
	phone	string	0..1	手机号
	orgName	string	1	持证人所在的单位名称
	deptName	string	0..1	持证人所在部门名称
	csr	string	1	证书申请请求文件
	certValidays	string	1	证书申请天数业务类型为变更，补办时此参数填入 0，服务端根据原证书进行
	province	string	0..1	持证人所在的省份
	city	string	0..1	持证人所在的城市
	audit	object	1	证书鉴证审核信息
audit 对象：	auditMemo	string	1	审核的备注信息
	auditTime	string	1	审核时间 yyyy-MM-dd HH:mm:ss
	auditType	string	1	审核方式 1 现场人工审核 2 线上资料审核 3 身份证 OCR 比对 4 调用公安部接口 5 活体检测 6 第三方平台审核
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	返回数据对象
body 对象：	serialnumberSign	string	1	签名证书序列号
	digitaCert	string	1	签名证书 Base64 编码
	digitalCertChain	string	1	签名证书证书链
	notBefore	string	1	签名证书有效期开始日期（日期字符串）
	notAfter	string	1	签名证书有效期结束日期(日,期字符串）

返回内容示例：


```
{
    "result_code":"0",
    "result_msg":"请求成功",
    "success":true,
    "body":{
      "serialnumberSign":"3342342342377238",
      "digitaCert":"
```

MIIDjDCCAzCgAwIBAgIUfT7uMyQfR…..mBggrBgEFBQcCAEbHkaZ/UxNYdMAXGeda4NWJOpqROOVAD8NX+ii+MK4 ",
"digitalCertChain":"dfskjhdfkshjdfhssdk",
"notBefore":"2022-10-21 10:00:00",
"notAfter":"2023-10-21 10:00:00"
}
}

7.5 机构证书申请

URL：https://{ip:port}/open/digitalCert/enterpise/apply

调用方法：POST

功能描述：当机构申请数字证书时，调用本接口申请证书。

参数分类	参数名	参数类型	约束	说明
输入参数：	transId	string	1	流水号
	time	string	1	发送时间
	busiType	string	1	业务类型：新增-enroll，变更-reChange，补办-reEnroll
	serialnumberSign	string	0..1	签名证书序列号，业务类型为变更，补办时需要
	orgName	string	1	单位名称
	socialcreditcode	string	1	统一社会信用代码
	personName	string	1	法定代表人姓名
	personIdType	string	0..1	证件类型：1-居民身份证
	personIdNumber	string	0..1	法定代表人证件号码
	transName	string	0..1	经办人姓名
	transPhone	string	0..1	经办人手机号
	transNumber	string	0..1	经办人身份证号
	csr	string	1	证书申请请求文件
	certValidays	string	1	证书申请天数；业务类型为变更、补办时此参数填入 0，服务端根据原证书有效期进行自动计算
	province	string	0..1	持证人所在的省份
	city	string	0..1	持证人所在的城市
	audit	object	1	鉴证审核信息
audit 对象：	auditMemo	string	1	审核的备注信息
	auditTime	string	1	审核时间 yyyy-MM-dd HH:mm:ss
	auditType	string	1	审核方式 1 现场人工审核 2 线上资料审核 3 身份证 OCR 比对 4 调用公安部接口 5 活体检测 6 第三方平台审核
输出参数：	result_code	string	1	正常状态码

参数分类	参数名	参数类型	约束	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 对象：	body	object	1	返回数据对象
	serialnumberSign	string	1	签名证书序列号
	digitalCert	string	1	签名证书
	digitalCertChain	string	1	签名证书证书链
	notBefore	string	1	签名证书有效期开始日期（日期字符串）
	notAfter	string	1	签名证书有效期结束日期(日,期字符串）

返回内容示例：


```
{
    "result_code":"0",
    "result_msg":"请求成功",
    "success":true,
    "body":{
      "serialnumberSign":"3342342342377238",
      "digitalCert":"
MIIDjDCCAzCgAwIBAgIUfT7uMyQfR…..mBggrBgEFBQcCAEbHkaZ/UxNYdMAXGeda4NWJOpqROOVAD
8NX+ii+MK4 ",
       "digitalCertChain":"dfskjhdfkshjdfhssdk",
       "notBefore":"2022-10-21 10:00:00",
       "notAfter":"2023-10-21 10:00:00"
    }
}
```


7.6 证书更新

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

调用方法：POST

功能描述：本接口用于证书更新延期。

参数分类	参数名	参数类型	约束	说明
输入参数：	transId	string	1	流水号
	time	string	1	发送时间
	serialnumberSign	string	1	签名证书序列号
	certValidays	string	1	证书更新天数(整数)
	audit	object	1	鉴证审核信息
audit 对象：	auditMemo	string	1	审核的备注信息
	auditTime	string	1	审核时间 yyyy-MM-dd HH:mm:ss
	auditType	string	1	审核方式 1 现场人工审核 2 线上资料审核 3 身份证 OCR 比对 4 调用公安部接

参数分类	参数名	参数类型	约束	说明
				口 5 活体检测 6 第三方平台审核
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	返回数据对象
body 对象:	serialnumberSign	string	1	签名证书序列号
	digitalCert	string	1	签名证书
	digitalCertChain	string	1	签名证书证书链
	notBefore	string	1	签名证书有效期开始日期（日期字符串）
	notAfter	string	1	签名证书有效期结束日期（日,期字符串）

返回内容示例：


```
{
    "result_code":"0",
    "result_msg":"请求成功",
    "success":true,
    "body":{
      "serialnumberSign":"3342342342377238",
      "digitalCert":"
MIIDjDCCAzCgAwIBAgIUfT7uMyQfR….mBggrBgEFBQcCAEbHkaZ/UxNYdMAXGeda4NWJOpqROOVAD
8NX+ii+MK4 ",
       "digitalCertChain":"dfskjhdfkshjdfhssdk",
       "notBefore":"2022-10-21 10:00:00",
       "notAfter":"2023-10-21 10:00:00"
    }
}
```


7.7 证书吊销

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

调用方法：POST

功能描述：当证书彻底废弃不再使用时，可以进行证书吊销，需调用本接口进行证书吊销。

参数分类	参名数	参数类型	约束	说明
输入参数：	transId	string	1	流水号
	serialnumberSign	string	1	签名证书序列号
	revokeReason	string	1	吊销原因
	audit	object	1	鉴证审核信息
audit 对象：	auditMemo	string	1	审核的备注信息
	auditTime	string	1	审核时间 yyyy-MM-dd HH:mm:ss
	auditType	string	1	审核方式 1 现场人工审核 2 线上资料

参数分类	参名数	参数类型	约束	说明
				审核 3 身份证 OCR 比对 4 调用公安部接口 5 活体检测 6 第三方平台审核
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	返回数据对象(改对象为空)
body 对象：	isRevoke	bool	1	true 吊销成功 false 失败

返回内容示例：

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

7.8 证书验证

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

调用方法：POST

功能描述：本接口用于通过服务端验证证书有效性。

参数分类	参数名	参数类型	约束	说明
输入参数：	transId	string	1	流水号
	time	string	1	发送时间
	digitalCert	string	1	证书 base64 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	object	1	返回数据对象
body 对象：	isEffective	bool	1	true 有效 false 无效

返回内容示例：

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

```
    }
}
```

8 电子证照认证机构接入接口

8.1 接口列表

电子证照认证服务机构应该按照下列标准提供相应的 API 接口，供身份认证服务调用。

表 5 电子证照认证机构接入接口

编号	接口功能	接口 URL 对象	方法	授权	备注
1	电子证照申领	https://*{ip:port}*/open/elecCert/apply	POST	trusted	
2	电子证照亮证	https://*{ip:port}*/open/elecCert/show	POST	trusted	
3	电子证照查证	https:// *{ip:port}*/open/elecCert/query	POST	trusted	
4	电子证照真伪验证	https://*{ip:port}*/open/elecCert/verifySeal	POST	trusted	
5	电子证照类型列表	https://*{ip:port}*/open/elecCert/queryTypeList	POST	trusted	

8.2 电子证照申领

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

调用方法：POST

功能描述：通过身份标识（身份证号码或统一社会信用代码）申领电子证照，获取电子证照元数据、照面数据以及电子证照的版式文件，在需要亮证的业务场景中使用。

参数分类	参数名	参数类型	约束	说明
输入参数：	elecCertHolderCode	string	1	证照持有主体代码（如：公民身份证号码、统一社会信用代码）
	elecCertHolderType	string	0..1	证照持有主体代码类型
	elecCertType	string	1	证照类型
	useFor	string	1	用途描述，不超过 200 字
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	返回数据对象
body 对象：	elecCertID	string	1	电子证照标识
	elecCertInfo	object	1	证照照面数据
	fileFormat	string	1	证照文件格式
	fileUrl	string	1	文件下载地址
	elecCertMeta	object	1	返回数据对象
证照元数据对象：	elecCertType	string	1	证照名称
	issueDept	string	1	颁发单位

参数分类	参数名	参数类型	约束	说明
	elecCertNumber	string	1	证照编号
	issueDate	string	1	证照颁发时间

返回内容示例：


```
{
    "result_code":"0",
    "result_msg":"请求成功",
    "success":true,
    "body":{
            "elecCertID":"3342342342377238",
            "elecCertInfo":" MI4 ",
            "fileFormat":"",
            "fileUrl":"https://ddjd.pdf",
            "elecCertMeta":{
                    "elecCertType":"",
                    "issueDept":"四川卫健委",
                    "elecCertNumber":"3434",
                    "issueDate":"2022-10-11 10:00:00"
             }
        }
}
```


8.3 电子证照亮证

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

调用方法：POST

功能描述：通过电子证照标识，获取证照文件下载路径和证照二维码。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	elecCertId	string	1	电子证照标识
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:	qrCodeImgBase64	string	0..1	证照二维码图片
	fileUrl	string	1	证照文件下载路径

返回内容示例：


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

```
"success":true,
"body":{
        "qrCodeImgBase64":"base==",
        "fileUrl":"https://ddjd.pdf"
    }
}
```


8.4 电子证照查证

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

调用方法：POST

功能描述:应用系统在需要使用电子证照的业务场景中,通过本接口获取电子证照的元数据、照面数据。

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	证照持有主体代码（如：公民身份证号码、统一社会信用代码）
	elecCertTypeCode	string	0..1	证照持有主体代码类型
	elecCertHolderType	string	0..1	证照类型名称
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	aarry	1	证照列表
body 数组：	qrCodeImgBase64	string	0..1	证照二维码图片
	fileUrl	string	1	证照文件下载路径
	elecCertId	string	1	证照唯一标识
	elecCertType	string	1	证照类型名称
	sourceId	string	1	证照源标识
	certypeDtlName	string	1	证照明细名称
	certypeDtlId	string	1	证照明细编码
	elecCertName	string	1	证照名称
	elecCertHolder	string	1	持证主体
	elecCertHolderCode	string	1	持证主体代码
	elecCertHolderType	string	1	持有者证件类型
	elecCertHolderCategory	string	1	持有者类型
	issueDept	string	1	证照颁发机构
	elecCertNumber	string	1	证照编号
	issueDeptCode	string	1	证照颁发机构代码
	issueDate	string	1	证照颁发日期

参数分类	参数名称	参数类型	约束	参数说明
	elecCertLevel	string	1	证照等级
	validityStart	string	1	证照有效期起始
	validityEnd	string	1	证照有效期截止
	state	string	1	证照状态： 0-未签章证照，1-签章证照，11-证照已变更，21-证照已注销，22-证照已废止

返回内容示例：


```
{
        "result_code":"0",
        "result_msg":"请求成功",
        "success":true,
        "body":[
           {"elecCertId": "1.2.156.3005.2..37010056F5F25F9A271.1.X",
                      "sourceId": "1.2.156.3005.2..370100025F9A271.1.X",
                      "elecCertNumber": "1262235241",
                      "certypeDtlName": "变更照面测试 3",
                      "certypeDtlId": "5B56C2C3C216454680B51E7780FAACE8",
                      "elecCertType": "中华人民共和国外国人工作许可证",
                      "elecCertTypeCode": "111000000000013063F001",
                      "issueDept": "济南市发展和改革委员会",
                      "issueDeptCode": "370100004188602",
                      "elecCertHolder": "测试",
                      "elecCertHolderCode": "522228199612100611",
                      "elecCertHolderType": "51",
                      "elecCertHolderCategory": "",
                      "issueDate": "2019-10-14",
                      "validityStart": "2019-10-14",
                      "validityEnd": "2019-10-14",
                      "state": "0",
                      "version": 1,
                      "elecCertLevel": "A",
```

" qrCodeImgBase64": "Afdfdhfhlds****hlfh==",

" fileUrl ": "https:***dddd.pdf",

}]

}

8.5 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	0..1	电子证照文件 base64 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	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。
	signType	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” 未识别的签名类型
	verify	string	1	单个印章或签名验证结果 “true/false”，当 signType 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

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,
                    "signType":"ds.PKCS7",
                    "verify":"unknown",
                    "errorCode":"c803302",
                    "errorMsg":"该数字签名为 rsa 签名"
                }]
        }
}
```


8.6 电子证照类型列表

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

调用方法：POST

功能描述：电子证照类型列表获取。

参数分类	参数名称	参数类型	约束	参数说明
输入参数：	elecCertTypeName	string	0..1	证照类型名称
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	1	证照类型列表，body 对象数组
body 对象:	elecCertTypeCode	string	1	证照类型编码
	elecCertTypeName	string	1	证照类型名称
	defineAuthorityName	string	1	定义部门代码
	defineAuthorityLevel	string	1	定义部门等级
	defineAuthorityCode	string	1	定义部门名称
	category	string	1	证照类型,1 证照
	elecCertHolderCategory	string	1	持证人类型 1 自然人 2 法人 3 混合 4 其他
	validityRange	string	1	有效期
	dtlNum	string	1	该证照类型包含的明细数量
	isStandard	string	1	是否为国家标准类型 1 是 2 否

返回内容示例：

```
{
        "result_code":"0",
        "result_msg":"请求成功",
        "success":true,
        "body":[{
               "elecCertTypeCode": "111000000000013127D012",
               "defineAuthorityName": "中华人民共和国公安部",
               "defineAuthorityLevel": "1",
               "isStandard": "1",
               "defineAuthorityCode": "11100000000013127D",
               "category": "",
               "elecCertHolderCategory": "",
               "subjectId": "",
               "elecCertTypeName": "出海船民证",
               "validityRange": "",
               "dtlNum": 10
           }]
}
```

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