

证书在线服务平台 CA 证书申请操作手册

(V1.4)

一、注册证书在线服务平台

(一) 注册账号

1. 访问证书在线服务平台

可通过浏览器直接访问地址：<http://120.223.240.14:8083/#/login>，打开后点击登录按钮左下方“注册单位”。



2. 输入相关企业注册信息

*项为必填项，输入完成后点击“立即注册”。

单位信息可在输入统一信用代码或单位名称后点击红框搜索对应企业信息并自动填充（数据来源为招采平台已注册单位信息）。如信息有误请自行修改正确。

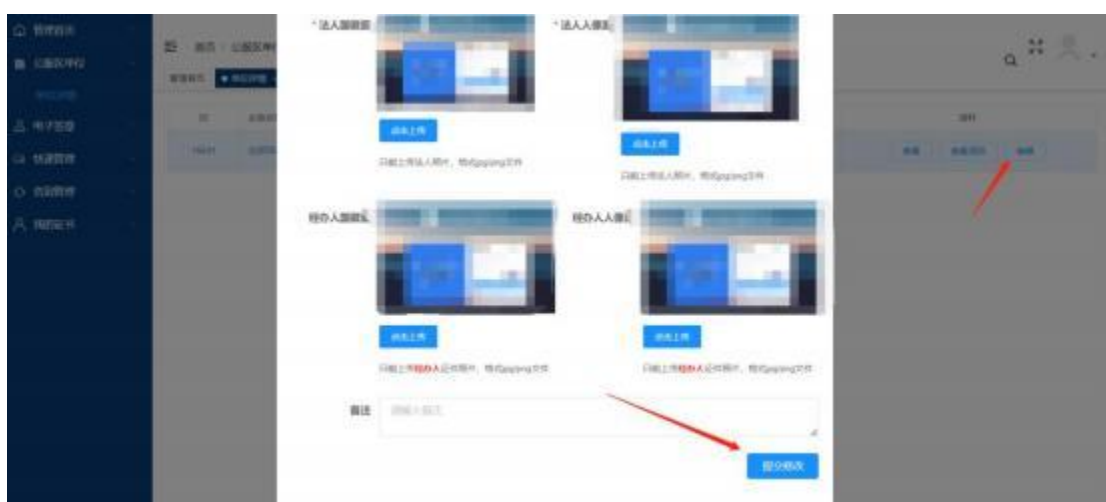
3. 点击“立即注册”后，账号即可注册成功，返回上一页填写账号密码，登录系统。等待管理员后台核验单位资料，通过后即可去“我的证书”列表申请证书。

（二）信息修改

1. 如核验不通过，单位信息驳回后，在“公服区单位”-“单位详情”中可查看被驳回的原因，点击“编辑”对单位信息修改。



2. 重新编辑单位信息后，点击“提交修改”，等待管理员核验。



二、申请 CA 证书

(一) 用户登录

单位注册核验通过后，登录证书在线服务平台首页，输入用户名、密码、验证码，点击“登录”。



(二) 证书申请

1. 依次点击“我的证书”-“证书列表”，点击“申请证书”。提交成功即可。



2. 选择“自领取”可选填信息。选择“邮寄(到付)”时，须准确填写收件人、收货电话、收货地址，收货地址务必按省市县格式准确填写，否则有可能无法准确寄出。选择

“第三方寄付”时（三方订购平台购买含快递服务的），同上填写收件人、收货电话、收货地址。点击“确定”即可。

3. 点击“证书列表”查看已申请的证书状态。

三、注册电子签章

（一）自助制图

ID	印模类型	印模名称	卡号	公司
32739	公章	公章	32739000000000000000	
32738	公章	外办(2019)0000000000	32738000000000000000	外办(2019)0000000000
32737	公章	公章	02	公章
32736	公章	公章	02	公章
32735	公章	公章	02	公章
32734	公章	公章	02	公章
32733	公章	公章	02	公章
32732	公章	公章	020	公章

用户登录证书在线服务平台，电子签章模块下 → 采集印章菜单下。参考“PS印章处理教程”获取实体印章的印模图片，保存印模图片到本地电脑备用。（获取印模图片时

， 将印章清晰地加盖在空白纸上， 以便获取的印模图片更加完整和清晰。)

（二）采集印章

进入“印章管理”-“采集印章”， 点击“添加印模”， 输入印模名称， 选择印章类型、所属证书， 添加印模图片， 以上信息确认无误后， 点击“确定”提交添加申请。

四、使用要求

（一）CA证书是各单位在招采平台的安全可信身份凭证之一，CA证书是招采平台安全的认证方式，请各单位务必重视CA证书安全管理，严禁私自转借他人使用，若因保管、使用不当造成的损失由各单位自行负责；

（二）发放首个CA证书后，各单位因管理、工作分工需要或发生证书介质损坏等情况的，需自行通过正规渠道采购符合医保网络安全和信息化标准规范（数字证书存储介质）（见附件）的CA证书设备。

五、常见问题

（一）CA证书管理默认PIN码随介质标明。

（二）外省申领的CA证书介质PIN码被锁，无法在我省解锁，请联系原申领地解锁。如不确定申领地时，可通过CA证书介质外观序列号查询。

（三）技术联系电话：

CA技术支持电话1:13256777350

CA技术支持电话2:13001717570

CA技术支持电话3:13256777385

CA技术支持电话4:13256777352

CA技术支持电话5:13256777330

附件：

线上购买渠道

- 一、<http://sdkey.xahuadao.com>
- 二、<http://salekey.uniondept.com>
- 三、<http://shopping.jnrxf.com/>

医保数字证书存储介质标准规范

以下标准规范内容节选自国家医疗保障局《医保网络安全和信息化标准医疗保障信息平台身份认证与授权管理第5部分：证书存储设备规范》。

一、基本要求

- 1. 自带驱动程序，支持 SM2 等国产系列算法；
- 2. 外壳按统一外观封装，外观颜色分为黄色和绿色两种，黄色用在核心业务区，绿色用在公共服务区，外壳统一印制20位标准序列号；
- 3. 私钥调用有 PIN 码保护，遵循统一的 PIN 码长度及规则（8-12 位数字加字母的组合）；
- 4. 经医保身份认证与授权管理系统测试通过，能够被证书综合管理系统识别、初始化、分配序列号、远程解锁等。

二、规格要求

参数项	参数值
工作电压	5V
工作电流	50-200mA
工作温度	0~ 70° C
存储温度	-20~ 85° C
工作湿度	20%—90%
存储湿度	16%—95%
处理器	32 位国产智能卡芯片
芯片内存储空间	128KB 及以上
可擦写次数	10 万次以上
数据存储年限	10 年以上
支持算法	DES、3DES、SHA-1、SM1、SM2、SM3、SSF33
闪存存储空间	2M-8M
接口类型	USB 2.0
可插拔次数	5 万次以上

三、性能要求

参数项	参数值
芯片CPU位数	32位
片内存储空间	≥128KB
文件读写性能参数（私有接口测试数据）	
写文件（片内空间）	≥4.06KB/秒
读文件（片内空间）	≥63.44KB/秒
对称算法性能参数（私有接口测试数据）	
DES加解密（ECB）	≥32.52KB/秒
3DES加解密（ECB）	≥33.60KB/秒
SSF33加解密（ECB）	≥31.50KB/秒
SM1加解密（ECB）	≥33.60KB/秒
SM2性能参数（COS接口测试数据）	
SM2密钥对生成	≤0.09秒/次
SM2私钥签名	≥79.49次/秒
SM2公钥验证	≥50.94次/秒
SM2签名+验证	≥24.06次/秒

参数项	参数值
SM2公钥加密	$\geq 6.07\text{KB/秒}$
SM2私钥解密	$\geq 11.85\text{KB/秒}$
硬件杂凑算法	$\geq \text{SM3: } 1.97\text{K/秒}$

四、安全要求

1. PIN 码安全

- (1) PIN 码长度不少于 6 个字节；
- (2) PIN 码在设备和本接口之间的传输过程中应采取保护措施，防止 PIN 码泄露；
- (3) PIN 码在设备中应安全存储，不可从设备中导出。

2. 密钥安全

- (1) 设备内产生的随机数应为真随机数，应符合随机性检测的要求；
- (2) 设备内产生的会话密钥应使用随机数；
- (3) 设备内产生非对称密钥使用的素数应满足素性要求；
- (4) 设备内的密钥应具备有效的密钥保护机制防止解剖、探测和读取；
- (5) 设备内的密钥应按权限要求使用；
- (6) 除公钥外的密钥不能以明文形式出现在设备外；
- (7) 签名私钥必须在设备中产生；
- (8) 容器内的私钥不能以任何形式导出设备；
- (9) 删除容器时必须销毁该容器内所有的密钥。