**附件**

**一、原招标文件第一章 招标公告**

5.1招标范围：本项目共1个包，包含：电子签名系统医师签（APP/小程序）、移动端前置CA服务器、移动端后台管理云服务系统、签名验签时间戳服务器、证书管理服务系统、电子签章系统、个人数字证书、移动数字证书（医护）、单位数字证书、设备数字证书、证书存储介质、患者签名终端（有线）、患者签名终端（无线）、患者签名终端证书、手写签名服务系统、院内业务系统接口、合作研发等。包含以上所有货物及服务的采购、供货、运输、保险、装卸、安装、检测、调试、试运行、验收交付、培训、技术支持、软件升级、售后保修及相关伴随服务等。

**更正为**

5.1招标范围：本项目共1个包，包含：移动电子认证软件（移动端软件）、CA安全认证服务器、移动安全认证系统、时间戳服务系统、数字身份管理系统、电子签章系统、手写数字签名系统、统一电子认证系统（含服务器）、个人数字证书、移动数字证书（医护）、单位数字证书、设备数字证书、证书存储介质、患者签名终端（有线）、患者签名终端（无线）、事件性数字证书、系统可靠性方案、院内业务系统接口、合作研发等。包含以上所有货物及服务的采购、供货、运输、保险、装卸、安装、检测、调试、试运行、验收交付、培训、技术支持、软件升级、售后保修及相关伴随服务等。

**二、原招标文件第二章 投标人须知前附表**

|  |  |  |
| --- | --- | --- |
| 7.5.1 | 履约保证金 | 是否提交履约保证金：否 |

**更正为**

|  |  |  |
| --- | --- | --- |
| 7.5.1 | 履约保证金 | 是否提交履约保证金：是，合同价的5% |

**三、原招标文件第二章 投标人须知前附表**

|  |  |
| --- | --- |
| 10.4 | 付款条件：1. 本合同签订，乙方按甲方要求将本项目相关硬件设备交付给甲方安装部署后，经甲方签收检查合格后，10个工作日内，甲方向乙方支付合同总计金额的 50 %，即人民币： 元（大写： ）；2.项目验收合格后， 10 个工作日内，甲方向乙方支付合同总计金额的 40 %，即人民币： 元（大写： ）3.项目验收满1年后支付项目剩余10%。即:人民币 （大写：）4.乙方根据付款方式和甲方财务要求及时向甲方出具发票。因乙方发票出具不及时或存在问题，而造成的损失，由乙方承担。 |

**更正为**

|  |  |
| --- | --- |
| 10.4 | 付款条件：1.合同签订前，乙方向甲方支付合同总额的5%，作为履约保证金。合同签订后，乙方按甲方要求将本项目相关硬件设备交付给甲方安装部署后，经甲方签收检查合格后，15个工作日内，甲方向乙方支付合同总计金额的 50 %；2.项目验收合格后， 15 个工作日内，甲方向乙方支付合同总计金额的 45 %；3.项目验收满1年后支付项目剩余5%。履约保证金退还时间按合同约定执行；4.乙方根据付款方式和甲方财务要求及时向甲方出具发票。因乙方发票出具不及时或存在问题，而造成的损失，由乙方承担。 |

**四、原招标文件第三章 评标方法和标准**

（三）评标办法

|  |  |
| --- | --- |
| 技术部分（30分） | 评标委员会根据投标人所投产品技术参数响应情况进行评审，此项不作为无效处理。1.加“★”项技术参数评审：加“★”项技术参数满分19.5分。技术参数中加“★”项完全满足要求的，得19.5分；每有一项加“★”项不满足的扣1.5分。2.非“★”项技术参数评审：非加“★”项技术参数满10.5分。技术参数中非加“★”项完全满足要求的，得10.5分；每有一项非加“★”项不满足的扣0.05分。 |

**更正为**

|  |  |
| --- | --- |
| 技术部分（30分） | 评标委员会根据投标人所投产品技术参数响应情况进行评审，此项不作为无效处理。1.加“★”项技术参数评审：加“★”项技术参数满分18分。技术参数中加“★”项完全满足要求的，得18分；每有一项加“★”项不满足的扣1.5分。2.非“★”项技术参数评审：非加“★”项技术参数满12分。技术参数中非加“★”项完全满足要求的，得12分；每有一项非加“★”项不满足的扣0.05分。 |

**五、原招标文件第四章 合同（格式）**

4.1 本合同签订，乙方按甲方要求将本项目相关硬件设备交付给甲方安装部署后，经甲方签收检查合格后，10个工作日内，甲方向乙方支付合同总计金额的 50 %，即人民币： 元（大写： ）；

4.2项目验收合格后， 10 个工作日内，甲方向乙方支付合同总计金额的 40 %，即人民币： 元（大写： ）

4.3项目验收满1年后支付项目剩余10%。即:人民币 （大写：）

**更正为**

4.1 合同签订前，乙方向甲方支付合同总额的5%，作为履约保证金。合同签订后，乙方按甲方要求将本项目相关硬件设备交付给甲方安装部署后，经甲方签收检查合格后，15个工作日内，甲方向乙方支付合同总计金额的 50 %；

4.2项目验收合格后， 15 个工作日内，甲方向乙方支付合同总计金额的 45 %；

4.3项目验收满1年后支付项目剩余5%。

**六、原招标文件第四章 合同（格式）**

**增加：**

4.5履约保证金的退还：

项目验收合格满5年后，无息退还在扣除乙方违约金（包括但不限于工期、质量、维保等违约金）后的余额部分。

**七、原招标文件第六章 采购需求**

|  |  |  |
| --- | --- | --- |
| **编号** | **产品名称** | **数量** |
|  | 电子签名系统医师签（APP/小程序） | 1套 |
|  | 移动端前置CA服务器 | 1台 |
|  | 移动端后台管理云服务系统 | 1套 |
|  | 签名验签时间戳服务器 | 2台 |
|  | 证书管理服务系统 | 1套 |
|  | 电子签章系统 | 1套 |
|  | 个人数字证书 | 4100张 |
|  | 移动数字证书（医护） | 4100张 |
|  | 单位数字证书 | 1张 |
|  | 设备数字证书 | 3张 |
|  | 证书存储介质 | 4100个 |
|  | 患者签名终端（有线） | 204台 |
|  | 患者签名终端（无线） | 10台 |
|  | 患者签名终端证书 | 214张 |
|  | 手写签名服务系统 | 1套 |
|  | 院内业务系统接口 | 1批 |
|  | 合作研发 | 1项 |

1. **产品参数**
	1. **电子签名系统医师签（APP/小程序）**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
|  | 支持CA数字证书签发和续期请求、文件移动电子签名请求等； |  |
|  | 支持面容ID、指纹认证登录app、授权业务系统登录、文件签署； |  |
|  | 支持通过客户端扫描屏幕上的二维码，实现身份认证，完成登录。 |  |
|  | 支持申请证书、证书查看、证书删除、支持数字证书的冻结与启用 |  |
|  | 支持医务人员登录成功后，在授权时间内无需再次扫码，即可实现电子签名。 |  |
|  | 支持移动CA证书签发，实现数字证书申请/签发/冻结/吊销等全生命周期管理服务。 |  |
|  | 提供支持活体人脸核身、手机短信验证码认证、手机号三要素验证等多种校对方式。 |  |
|  | 支持多种文件预览和批量签署功能，用户可在移动端查看文件详情，确认文件内容。 |  |
|  | 支持批量签名，全面解决医院无纸化安全的需求，满足医院病案工作发展的需要。 |  |
|  | 支持集成密码模块的移动端应用，实现数字证书认证和电子签名 |  |
|  | 具有查看以往签名记录的功能，查看签名列表，查询签名记录和时间； |  |
|  | 支持签名统计，显示每日签名的数量的列表； |  |
|  | 支持待签文件数量提醒、弹窗提醒； |  |
|  | 移动端查看文件时，具有防止截屏功能； |  |
|  | ★移动端待签或已签署文件内容查看时，文件页面应能够通过显示水印等措施提高安全性，水印信息包含用户姓名、日期等；**（提供截图证明）** |  |
|  | ★具有授权签署功能，可根据客户需求实现同科室授权或跨科室授权；支持手动终止授权；**（提供截图证明）** |  |
|  | 医生在手机完成手写数字签名后，其签署文档即通过数字签名技术进行保护，可以进行签署者身份校验和完整性校验，当文档发生篡改，则文档签名验证提示不通过。 |  |
|  | 支持扫描、解析本地图片，支持远程扫描二维码授权业务系统登录  |  |
|  | 支持手写签名更新，客户端已签名后也放开采集签名图片的入口，可以通过前后端配合控制是否允许医护编辑签名 |  |
|  | 为医护人员提供移动电子签名服务，实现移动端证书APP、小程序的私钥分割协同运算，实现数字签名、数据加解密等通用密码服务 |  |
|  | 用户数字签名时，支持随机键盘/人脸核身/指纹校验，提升密钥安全性；（提供截图证明） |  |
|  | 具有签署时添加备注功能，允许跳过备注； |  |
|  | 支持多应用商店下载，如oppo、vivo、华为、小米、苹果、应用宝等； |  |
|  | 支持院内第三方APP、微信小程序等应用使用移动数字证书授权登录； |  |
|  | 完成与鸿蒙系统适配，**提供相关证明文件；** |  |
| **序号** | **非功能指标要求** |  |
| 1 | 私钥加密存储，密钥存储、使用能够按不同应用进行区分，并防止非法读取与导出，证书卸载时能够确保删除所有密钥 |  |
| 2 | 支持基于SM2的合作签名与加解密算法，SM3, SM4国密算法，支持Pkcs7等格式的数字签名和验证功能； |  |
| 3 | 支持合作签名、标准签名、签名验证、非对称加密、合作非对称解密、标准非对称解密、数据摘要、随机数生成等密码服务 |  |
| 4 | 采用门限分割的密钥管理技术，证书密钥由客户端密钥因子和云端密钥因子共同组成，两端协同完成电子签名运算，实现用户对签名密钥的专有控制 |  |
| 5 | 支持各类主流Android、IOS移动端、微信小程序平台，**提供相关证明文件**； |  |
| 6 | ★**移动签体系完成了信息系统安全等级保护三级备案，提供备案证明；** |  |
| 7 | **★移动签体系需完成商用密码应用安全性评估，提供密码管理局出具的备案回执证明。** |  |
| **序号** | **产品资质要求** |  |
| 1 | **密码模块具备《软件著作权证书》（分别提供Android和IOS移动端平台的证书）** |  |

* 1. **移动端前置CA服务器**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 密钥存储：用户密钥对及密钥加密密钥 KEK 使用系统保护密钥加密保护，以密文的形式存储在密码卡的存储芯片中。 |  |
| 2 | 采用密钥协同运算技术、数字证书、身份信息核验等多重手段，支持APP、PC等全终端可信身份认证，通过扫码、口令等方式保障登录身份安全 |  |
| 3 | 处理医院业务系统端的请求，为客户终端提供数字签名、电子签章、加盖时间戳、密钥管理等服务。 |  |
| 4 | 实现证书申请、制作、下载等全生命周期管理功能 |  |
| 5 | 预设医生签名信息，通过扫码等形式实现快捷电子签名。在PC中，支持预登录后，后台批量签署电子病历功能 |  |
| 6 | 支持对时间、次数、角色等细粒度的授权管理。对所有登录、签名、签章、授权等行为自动记录日志。 |  |
| 7 | 提供移动电子认证服务，调用数字证书认证、电子签名等应用功能，实现跨终端的数字证书应用 |  |
| 8 | 支持证书的启动自检，实现证书的初始化、PIN码、格式化等管理操作。 |  |
| 9 | 支持将待签文件推送至移动端预览、签署； |  |
| 10 | 具备电子签名值存证功能； |  |
| 11 | 提供日志管理功能，可以查询和管理登录日志、签名日志、数据维护日志等；支持签名日志云端同步； |  |
| **序号** | **非功能指标要求** |  |
| 1 | 1.支持ECB、CBC模式的SM1密码算法2.支持SM2密码算法，可在卡内进行加解密、签名验签、密钥对生成3.支持SM3密码算法4.支持ECB、CBC模式的SM4密码算法5.支持数据的安全存储功能6.采用双物理噪声源生成真随机数7.支持密码卡全量密钥备份 |  |
| 2 | 接口要求1.支持个性化接口定制开发，2.支持国内算法3.支持X86、ARM、PowerPC等架构下的API接口库 |  |
| 3 | 密码运算性能要求SM1加解密速度 ≥200Mbps、SM4加解密速度 ≥150Mbps、SM2生密钥≥2300次/秒、SM2签名≥2000次/秒、.SM2验签≥1700次/秒、SM3摘要≥150Mbps、随机数生成≥2Mbps |  |
| **序号** | **产品规格要求** |  |
| 1 | 服务器类型：机架式服务器，配置标准机架安装导轨处理器配置：处理器型号：Intel至强系列或同等级处理器核心数：≥6核，主频≥1.9GHz缓存：≥8.25MBTDP功耗：≤85W内存配置：运行内存：≥64GB DDR4 ECC内存内存插槽：≥16个，支持扩展至≥32个DIMM插槽存储配置：硬盘配置：标配≥4块2.5英寸1200GB SAS 10K硬盘，支持热插拔最大支持≥12个3.5/2.5英寸硬盘扩展RAID控制器：配置硬件RAID卡，支持RAID 0/1/5/10/50/6/60模式缓存≥2GB，支持Cache超级电容保护可选配SAS HBA卡或SAS RAID控制卡网络接口：标配网卡：≥2个千兆电口（RJ45）+ 2个万兆光口（含多模模块）管理网口：1个独立10/100Mbps RJ45管理网口，支持IPMI 2.0远程管理功能要求：支持NC-SI、WOL、PXE功能，可扩展灵活IO卡扩展性要求PCIe扩展槽：≥8个标准PCIe 3.0插槽，支持GPU卡、高速网卡等扩展支持虚拟化加速卡及硬件加密模块电源配置电源功率：≥550W 80Plus铂金级冗余电源冗余设计：双电源模块，支持热插拔 |  |

* 1. **移动端后台管理云服务系统**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 管理客户端，实现单位管理、用户管理、权限管理、系统配置、日志管理、数据统计、账户登录等功能； |  |
| 2 | 接收处理业务系统侧的数据待签请求和验签请求； |  |
| 3 | 医师用户管理：新增用户、编辑医师信息、删除医师信息。支持批量导入信息； |  |
| 4 | ★具备医师手写签名图片管理功能，支持批量、单独管理医生签名图片；支持签名图片预览、审核；**(提供截图证明)** |  |
| 5 | 用户手机证书管理：移动端数字证书下载、绑定移动端数字证书、证书状态查询 |  |
| 6 | 角色权限：固定角色、权限列表、角色对应成员； |  |
| 7 | 账户管理：单位操作成员账户管理，成员基础信息账户管理，增删改查 |  |
| 8 | 单位管理：添加单位、管理单位状态启用/停用。 |  |
| 9 | 日志管理：包括签名日志、扫码日志、申请证书日志、操作日志和登录日志 |  |
| 10 | 统计报表：用户量统计、用户状态统计、签名业务量统计、证书申请统计；★支持折线图、饼状图、柱状图等图表分析，查看使用趋势；(**提供截图证明)** |  |
| **序号** | **产品资质要求** |  |
| 1 | **系统具备信息系统安全等级保护三级备案证明；** | 3 |
| 2 | **系统需经过商用密码应用安全性评估，提供密码管理局出具的备案回执证明** | 4 |

* 1. **签名验签时间戳服务器**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| **1** | **硬件****指标** | 标准机架式服务器设备；支持≥5个千兆网口；具备≥1个RJ45串口管理；具有LCD或LED液晶显示模块，支持显示CPU、内存、IP等实时信息。 |  |
| **2** | **功能指标** | 支持X.509 v3证书，支持全中文证书 ，支持签名证书和加密证书的双证书认证体系。 |  |
| 支持国密SM2、国际RSA等非对称加密算法，支持SHA256、SHA384、SHA512、SM3 等摘要算法。 |  |
| 满足多个时间戳规范，包括国际通用的RFC3161标准、微软 Authenticode和PKCS7副署及验证。 |  |
| 支持签发时间戳，支持通过调用API将数据发送到TSA服务器进行时间戳签名。 |  |
| 支持验证时间戳，支持通过调用API将数据发送到TSA服务器进行时间戳签名验证。 |  |
| ★内部集成时间戳和签名验签服务功能测试模块，便于现场实施或接入开发过程中进行调试。**（提供截图证明）** |  |
| 支持通过NTP协议与第三方授时中心、卫星授权时间源进行时间同步，确保时间戳中时间的有效性。 |  |
| 支持通过选配安装北斗、GPS、CDMA 时间源模块同步卫星时间。 |  |
| 支持设置多个独立的签名验签服务，通过服务端口的不同区分不同的验签服务。 |  |
| 密钥访问控制，密钥库中保存的每一对密钥都各自拥有自己的访问口令，必须 使用正确的口令才使用该密钥进行服务操作。 |  |
| 支持私钥加密、私钥解密、公钥加密、公钥解密、数字信封封包、数字信封解包。 |  |
| 遵循 PKCS、XML 等国际签名规范。支持多标准签名验证，包括PKCS#1、PKCS#7（Attach）、 PKCS#7（Detach）。 |  |
| 具备CRL无差别匹配功能，支持在CRL中通过证书序列号进行检索。 |  |
| 具备WebGUI管理控制台，通过基于WEB形式的图形管理控制界面，实现对设备的管理、维护和监控等操作。 |  |
| 支持多机热备，同时提供自动回切、热备分组、配置同步等功能。 |  |
| 支持通过符合国密标准的密码机、加密卡等硬件加速设备提高密码运算效率。 |  |
| ★具备证书防火墙功能，可根据证书序列号、主题项、证书指纹等多种维度来对使用者的数字证书进行鉴权管理。**（提供截图证明）** |  |
| 3 | **性能指标** | 1.SM2：时间戳签名不小于2800tps，时间戳验签不小于2100tps;2.SM2：签名不小于10000tps，验签不小于5000tps; |  |

* 1. **证书管理服务系统**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 实现证书自动静默更新； |  |
| 2 | 实现证书应用客户端环境自动更新； |  |
| 3 | 提供网页在线帮助功能； |  |
| 4 | 提供查看系统状态、配置系统IP/端口、管理员管理、设备编号管理、日志管理、服务管理、备份恢复等管理功能； |  |
| **序号** | **非功能指标要求** | **备注** |
| 1 | 提供备份恢复功能，可通过界面备份当前所有配置，保证系统瘫痪时的快速恢复； |  |
| 2 | 提供日志记录，可将日志以syslog的方式发送到指定服务器； |  |
| 3 | 应满足卫生部卫生系统电子认证服务相关技术规范。 |  |

* 1. **电子签章系统**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 文件签章：根据电子印章加盖位置信息在相应的位置进行签章，签章时可获取时间戳信息和用章单位数字证书信息。签章后形成带有用章单位电子印章的签章文件。 |  |
| 2 | 签章管理：签章能够完成Office、PDF等文档的盖章功能，并能通过服务端查看系统工作状态和任务状态。 |  |
| 3 | 支持文档的手动盖章、自动盖章和批量盖章支持鼠标定位、坐标定位和关键字符定位等功能，用户能根据实际情况选择合适方便的盖章方式。 |  |
| 4 | 电子签章证据链：根据国家及行业有关规定，电子签章业务对签章过程信息进行电子签名，形成签章证据链信息以便存证 |  |
| 5 | 签章文件验签：实现对已签章文件的验签功能，包括电子印章有效性、签章详细信息等。 |  |
| 6 | 支持批量签章 |  |
| 7 | 文档验证：提供离线、在线、批量验证功能。 |  |
| 8 | 查看印鉴信息：通过电子签章系统查看文档印鉴信息：包括验证结果、盖章时间、盖章人、数字证书、印章外观、印章名称、印章来源、制印时间、制印人、所属单位等印章信息。 |  |
| 9 | 签名验证：电子签章系统具有签名验证功能，其验证方式和操作与功能验证是一致的。 |  |
| 10 | 具备印章管理功能，包括印章模板管理、印章制作、授权、停用、启用等功能 |  |
| 11 | 支持第三方CA机构签发的数字证书 |  |
| **序号** | **产品资质要求** |  |
| 1 | **产品具备《软件著作权证书》** |  |

* 1. **个人数字证书**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 标识医护人员用户网络身份； |  |
| 2 | 由权威合法的第三方CA机构签发，符合《x.509C的国内数字证书格式规范》。证书标准遵循 X.509 V3格式标准； |  |
| 3 | 支持存储于智能USBKEY、IC卡等多类型介质； |  |
| 4 | 数字证书支持RSA、SM2算法； |  |
| 5 | 支持自定义证书扩展域管理。 |  |
| **序号** | **产品资质要求** |  |
| 1 | **通过国家卫计委合规性检测的电子认证机构证明** |  |

* 1. **移动数字证书（医护）**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 标识医护用户网络身份； |  |
| 2 | 由权威合法的第三方CA机构签发，符合《x.509C的国内数字证书格式规范》。证书标准遵循 X.509 V3格式标准； |  |
| 3 | 支持存储于智能USBKEY、IC卡、移动APP客户端等多类型介质； |  |
| 4 | 数字证书支持RSA、SM2算法； |  |
| 5 | 支持自定义证书扩展域管理。 |  |
| **序号** | **产品资质要求** |  |
| 1 | **通过国家卫计委合规性检测的电子认证机构证明** |  |

* 1. **单位数字证书**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 标识单位用户网络身份； |  |
| 2 | 由权威合法的第三方CA机构签发，符合《x.509C的国内数字证书格式规范》。证书标准遵循 X.509 V3格式标准； |  |
| 3 | 支持存储于智能USBKEY、IC卡、移动APP客户端等多类型介质； |  |
| 4 | 数字证书支持RSA、SM2算法； |  |
| 5 | 支持自定义证书扩展域管理。 |  |
| **序号** | **产品资质要求** |  |
| 1 | **通过国家卫计委合规性检测的电子认证机构证明** |  |

* 1. **设备数字证书**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 标识设备网络身份； |  |
| 2 | 由权威合法的第三方CA机构签发，符合《x.509C的国内数字证书格式规范》。证书标准遵循 X.509 V3格式标准； |  |
| 3 | 数字证书支持RSA、SM2算法； |  |
| 4 | 支持自定义证书扩展域管理。 |  |
| **序号** | **产品资质要求** |  |
| 1 | **通过国家卫计委合规性检测的电子认证机构证明** |  |

* 1. **证书存储介质**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标** | **备注** |
| 1 | USBKey智能密码钥匙，实现数字证书的安全存储与使用； |  |
| 2 | 标准USB2.0规范，兼容USB1.1，兼容3.0规范接口； |  |
| 3 | 提供标准安全中间件 CSP 及 PKCS#11 v2.11 接口，硬件实现数字签名，支持X.509 v3标准证书格式； |  |
| 4 | 支持Window2000/2003/2008/XP/Vista/Win7/Win8等32位和64位中文、英文、繁体操作系统； |  |
| 5 | 硬件支持1024/2048位RSA和SM2非对称算法，支持SSF33、SM1、SM3、SM4等国密算法。支持DES、3DES等对称算法和SHA-1、SHA256摘要算法； |  |
| 6 | 智能卡芯片CPU至少32位，用户可用空间（Byte）不低于64K，可存放多张证书； |  |
| 7 | USBKey自身的安全要求：具备完善的PIN校验保护功能； |  |
| 8 | 支持标准的RSA和国产商用密码算法； |  |
| 9 | 数据存储时间不小于10年，可读写次数(次)不小于10万次。 |  |
| **序号** | **非功能性指标** |  |
| 1 | RSA（1024）密钥对生成时间<2秒，RSA（2048）密钥对生成时间<12秒；SM2密钥对平均生成时间<2秒； |  |
| 2 | RSA（1024）签名速度≥15次/s，RSA（1024）验签速度≥20次/s，RSA（2048）签名速度≥5次/s，RSA（2048）验签速度≥20次/s，SM2私钥签名≥4次/s，SM2公钥验证≥2次/s； |  |
| 3 | RSA（1024）加密速度≥20次/s，RSA（1024）解密速度≥15次/s，RSA（2048）加密速度≥20次/s，RSA（2048）解密速度≥5次/s，SM2公钥加密≥2次/s，SM2私钥解密≥4次/s。 |  |

* 1. **患者签名终端（有线）**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 电磁屏技术类型：无线无源；电磁笔：无电池无源笔；压感：≥8192级；≥10.1寸高清显示屏；分辨率≥1280\*800； |  |
| 2 | 能记录客户在签名设备上的完整轨迹，无断点； |  |
| 3 | 签名时轨迹同步在屏幕上展示，延迟小于0.5秒； |  |
| 4 | 平均无故障时间：大于18000小时； |  |
| 5 | 能以原始轨迹数据、矢量图片方式保存签名数据 |  |
| 6 | ★支持图像加签验签技术:可以对签字图像指纹图像，进行原RGB级别SM3+SM2加密封装，确保图像原始RGB不被篡改，并可F5隐写如RGB中形成不可变水印，并且数据链条可加时间戳确保时间的可溯源性。 |  |
| 7 | 支持原笔迹签名及手书功能，可进行原笔迹签名功能及手写输入指定文字；笔迹图像存储及原笔迹数据存储；手写输入数据可以保存为图片，矢量图片及原笔迹数据； |  |
| 8 | 具备同屏显示功能，上位机可将当前显示内容推送到签批设备上，并且上位机也能实施查看签批设备显示操作状态；文件合成功能；设备可根据功能规则（如XYP数据，关键字数据）进行签字名图片的对指定格式的文件进行插入操作。 |  |
| 9 | 系统：Linux（支持Windows、安卓、国产麒麟、统信等系统平台交互） |  |
| 10 | **★产品具有计算机软件著作权登记证书** |  |

* 1. **患者签名终端（无线）**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 显示模块：≥10.1寸高清显示屏；分辨率≥1280\*800；亮度：≥250cd/m²；摄像头：≥前置200万像素，后置≥500万像素；  |  |
| 2 | 数字证书申请功能，支持与第三方CA机构对接，下发合规的数字证书； |  |
| 3 | 支持用户在多个移动终端设备上使用同一个用户身份； |  |
| 4 | 数据签名功能，提供数据签名服务接口，与业务系统对接，支持业务系统发起签名请求，并调用签名接口对患者签名信息、指纹信息进行数字签名，并加盖时间戳； |  |
| 5 | 支持按照科室维度登录应用，查看该科室有待签文件的患者、待签文件数量； |  |
| 6 | 支持缓存机制，支持网络不佳状态下，缓存患者已提交签署的文件。待网络稳定后文件状态自动更新； |  |
| 7 | 支持记录当前已签署的文件数量，可查看已签署文件详情； |  |
| 8 | 提供身份认证服务，支持对患者进行可靠身份认证，并基于可信身份实现可靠签署； |  |
| 9 | PIN重置功能，支持忘记证书PIN码向管理端发起重置PIN码申请； |  |
| 10 | 支持对终端移动终端进行管理：包括设备的查看、挂起、停用； |  |
| 11 | 文件推送交互和全屏签署功能：可在交互终端上进行PDF等板式文件的推送和信息交互，能在浏览后进行签署； |  |
| 12 | 具备数字证书登录功能； |  |
| **序号** | **非功能指标要求** |  |
| 1 | 指纹模块：传感器类型：半导体电容式，传感器尺寸：≥23.0\*35.0mm，有效图像尺寸；≥12.8\*18mm，图像大小；≥256\*360pixel,图像分辨率：≥508dpi，比对方式：1：1/1：N，认假率（FAR）；<0.0001%; |  |
| 2 | CPU：国产高性能CPU，处理器核心数量≥4核，主频≥1.8G；系统：安卓（支持Windows、安卓、国产麒麟、统信等系统平台交互）；内存：≥2GB；存储：≥16GB； |  |
| 3 | 电池：电池类型：聚合物高密度安全电池；电池容量：标配≥8000mAH；待机时长：≥12h；工作时长：≥7.5h； |  |

* 1. **患者签名终端证书**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 标识患者智能签名终端网络身份； |  |
| 2 | 由权威合法的第三方CA机构签发，符合《x.509C的国内数字证书格式规范》。证书标准遵循 X.509 V3格式标准； |  |
| 3 | 数字证书支持RSA、SM2算法； |  |
| 4 | 支持自定义证书扩展域管理。 |  |
| **序号** | **产品资质要求** |  |
| 1 | **通过国家卫计委合规性检测的电子认证机构证明** |  |

* 1. **手写签名服务系统**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标** | **备注** |
| 1 | 申请和获取签名数字证书。根据签名业务及签名主体鉴证信息，向电子认证服务机构证书服务平台申请颁发数字证书； |  |
| 2 | 通过手写数字签名终端，获取签名人手写签字笔迹，作为数字签名可视化展现效果图示； |  |
| 3 | 使用数字签名密码算法，对知情同意书进行密码运算，保护知情同意书的有效性； |  |
| 4 | 提供知情同意书的存储、归档、展现、验证举证服务。支持知情同意书共享、同步到电子病历系统； |  |
| 5 | 系统兼容性良好，提供版本接口，方便与各种应用系统结合； |  |
| 6 | ★提供web管理平台，具备设备信息、签名业务等数据展示；具备设备信息管理、证书申请、日志记录等功能；**（提供平台截图证明）** |  |
| 7 | ★系统支持维护医院科室信息，支持设备绑定科室信息，支持设备、科室状态修改；**（提供系统截图证明）** |  |
| 8 | 系统具备证书过期提醒功能； |  |
| 9 | 支持对签名数据加盖时间戳，保障签名数据的时间权威可靠； |  |
| 10 | 系统支持多院区信息维护，支持院区签名数据统计、查询；支持签名数据分科室、院区、时间段折线图展示； |  |
| 11 | ★支持设备使用状态、科室/病区数量以及签名业务数据总览；**（提供系统截图证明）** |  |
|  | **资质要求** |  |
| 1 | **产品应具有软件著作权证书** |  |

* 1. **院内业务系统接口**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 对接院内业务系统，HIS、LIS、PACS、EMR 、互联网医院系统等； |  |

* 1. **合作研发要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **名称** | **功能指标要求** | **备注** |
| 1 | 电子签名系统合作研发需求 | 投标人应具有与目标医院合作研发电子签名系统条件与能力，根据目标医院现有的业务流程，提出相应的电子签名系统研发方案及合作办法 |  |
| 2 | 电子签名系统合作研发需求 | 1. 研发目的

国家卫生健康委办公厅2017年印发《电子病历系统应用水平分级评价管理办法（试行）》中，明确要求医疗机构积极做好卫生系统电子认证服务体系建设，实现身份认证、授权管理和责任认定；《中华人民共和国电子签名法》明确可靠的电子签名与手写签名或盖章具有同等的法律效力。为满足《中华人民共和国电子签名法》、《电子病历系统应用水平分级评价管理办法（试行）》、《卫生健康领域电子签名应用规范》等法律法规要求，实现医疗文书、处方、检验报告等全流程电子化签名合法性。覆盖门诊/住院电子病历、知情同意书、医嘱、护理记录、互联网医院等业务场景，降低纸质文件流转，缩短患者等待时间。构建符合等保三级标准的可信认证体系，确保签名数据存储、传输、验证全过程防篡改、防抵赖。 |  |
| 3 | 电子签名系统合作研发需求 | 1. 研发办法

采用本地化私有部署，国产商用密码算法（SM2/SM3/SM4）实现数字证书签发；支持与医院现有信息系统（HIS/LIS/PACS/EMR）无缝集成，提供标准化API接口。构建“可信身份、可信行为、可信数据和可信时间”电子认证体系，合作研发支持USBKey/扫码/指纹/人脸多模态生物识别签名；同步国家授时中心可信时间源，签名时间戳误差≤0.1秒；兼容iOS/Android/HarmonyOS系统的移动端签署设备；确保医疗文书的合法性和可追溯性。 |  |
| 4 | 电子签名系统合作研发需求 | 1. 时间周期

中标人需提出合理的时间周期，提出详细的进度安排，有具体的时间保障措施，以确保项目按时、高质量完成。 |  |
| 5 | 电子签名系统合作研发需求 | 1. 双方责权利划分

合作研发项目费用由中标人承担；中标人不得将本合作研发项目委托给任何第三方：中标人保证合作研发过程不侵犯第三人的知识产权；在完成合作研发项目后，中标人交付给目标医院可运行的软件，包括系统技术文档、数据等；中标人需协助目标医院进行软件调试，直至目标医院验收合格；中标人负责为目标医院培训人员；中标人不得将该研发项目的信息资源（包括源代码、系统技术文档、软件、数据等）泄露或许可第三方阅读、使用或复制。目标医院提供合理的建议；完成研发后，目标医院在7天内组织验收，并提出验收意见。该研发项目整个研发产品由目标医院独享专利、著作权等申请权；利用本合作研发项目成果申报的各类奖项，目标医院有作为第一人及第一单位的优先权；中标人作为第二人及第二单位。以上为研发协议签订时的基本内容，未尽事宜待投标人中标后签订研发协议时与目标医院协商确定。 |  |

**更正为**

|  |  |  |
| --- | --- | --- |
| **编号** | **产品名称** | **数量** |
|  | 移动电子认证软件（移动端软件） | 1套 |
|  | CA安全认证服务器 | 1套 |
|  | 移动安全认证系统 | 1套 |
|  | 时间戳服务系统 | 1套 |
|  | 数字身份管理系统 | 1套 |
|  | 电子签章系统 | 1套 |
|  | 手写数字签名系统 | 1套 |
|  | 统一电子认证系统（含服务器） | 1套 |
|  | 个人数字证书 | 4100张 |
|  | 移动数字证书（医护） | 4100张 |
|  | 单位数字证书 | 1张 |
|  | 设备数字证书 | 配套 |
|  | 证书存储介质 | 4100个 |
|  | 患者签名终端（有线） | 204台 |
|  | 患者签名终端（无线） | 10台 |
|  | 事件性数字证书 | 214套 |
|  | 系统可靠性方案 | 1项 |
|  | 院内业务系统接口 | 1批 |
|  | 合作研发 | 1项 |

**产品参数**

* 1. **移动电子认证软件（移动端软件）**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
|  | 支持CA数字证书签发和续期请求、文件移动电子签名请求等； |  |
|  | 支持面容ID、指纹认证登录app、授权业务系统登录、文件签署； |  |
|  | 支持通过客户端扫描屏幕上的二维码，实现身份认证，完成登录。 |  |
|  | 支持申请证书、证书查看、证书删除、支持数字证书的冻结与启用 |  |
|  | 支持医务人员登录成功后，在授权时间内无需再次扫码，即可实现电子签名。 |  |
|  | 支持移动CA证书签发，实现数字证书申请/签发/冻结/吊销等全生命周期管理服务。 |  |
|  | 提供支持活体人脸核身、手机短信验证码认证、手机号三要素验证等多种校对方式。 |  |
|  | 支持多种文件预览和批量签署功能，用户可在移动端查看文件详情，确认文件内容。 |  |
|  | 支持批量签名，全面解决医院无纸化安全的需求，满足医院病案工作发展的需要。 |  |
|  | 支持集成密码模块的移动端应用，实现数字证书认证和电子签名 |  |
|  | 具有查看以往签名记录的功能，查看签名列表，查询签名记录和时间； |  |
|  | 支持签名统计，显示每日签名的数量的列表； |  |
|  | 支持待签文件数量提醒、弹窗提醒； |  |
|  | 移动端查看文件时，具有防止截屏功能； |  |
|  | 移动端待签或已签署文件内容查看时，文件页面应能够通过显示水印等措施提高安全性，水印信息包含用户姓名、日期等；**（提供产品****截图证明）** |  |
|  | 具有授权签署功能，可根据客户需求实现同科室授权或跨科室授权；支持手动终止授权；**（提供产品截图证明）** |  |
|  | 医生在手机完成手写数字签名后，其签署文档即通过数字签名技术进行保护，可以进行签署者身份校验和完整性校验，当文档发生篡改，则文档签名验证提示不通过。 |  |
|  | 支持扫描、解析本地图片，支持远程扫描二维码授权业务系统登录  |  |
|  | 支持手写签名更新，客户端已签名后也放开采集签名图片的入口，可以通过前后端配合控制是否允许医护编辑签名 |  |
|  | 为医护人员提供移动电子签名服务，实现移动端证书APP、小程序的私钥分割协同运算，实现数字签名、数据加解密等通用密码服务 |  |
|  | 用户数字签名时，支持随机键盘/人脸核身/指纹校验，提升密钥安全性；（**提供产品截图证明**） |  |
|  | 具有签署时添加备注功能，允许跳过备注； |  |
|  | 支持多应用商店下载，如oppo、vivo、华为、小米、苹果、应用宝等； |  |
|  | 支持院内第三方APP、微信小程序等应用使用移动数字证书授权登录； |  |
|  | 客户端支持IOS、安卓系统、并已对鸿蒙系统进行适配，以及各类小程序平台。**（提供产品截图证明）** |  |
|  | 客户端支持Windows PC端安装部署，支持Windows7以上操作系统。 |  |
|  | 支持医生在不使用UKEY和手机的情况，直接使用Windows PC端安全密码模块软件就能完成基于数字证书的身份认证登录及电子签名服务 |  |
|  | 提供基于Windows PC客户端的密钥生成、密钥存储、密钥维护、密钥使用（如签名、验证签名）以及数字证书生命周期管理等功能。完成签名私钥的分割产生、分散存储、拆分计算，保证签名私钥的安全性。 |  |
|  | 提供Windows PC端的数字签名、签名验证、证书验证、证书解析、随机数、数据加解密等功能，同时采用密钥分割算法保障私钥的安全存储和调用，并能够针对Windows终端获取对应的特征值与证书进行绑定 |  |
|  | 提供WindowsPC端基于数字证书的安全登录认证流程、签名&验签流程、数据加解密集成支持配合。 |  |
|  | Windows PC客户端可以设置支持安全可靠的免密签名功能。 |  |
|  | 可以灵活配置数字证书在线状态和退出状态，而无需像传统USBkey证书一样频繁插拔。 |  |
|  | **Windows PC终端安全密码模块支持证书信息查阅、验证密码、修改密码、证书设置、证书更新、证书注销以及使用日志查阅功能。** |  |
|  | **★支持纯本地部署方案，在医院互联网断网情况下，能够保证院内数字证书体系正常登录与签名，提供详细解决方案。** |  |
| **序号** | **非功能指标要求** |  |
| 1 | 私钥加密存储，密钥存储、使用能够按不同应用进行区分，并防止非法读取与导出，证书卸载时能够确保删除所有密钥 |  |
| 2 | 支持基于SM2的合作签名与加解密算法，SM3, SM4国密算法，支持Pkcs7等格式的数字签名和验证功能； |  |
| 3 | 支持合作签名、标准签名、签名验证、非对称加密、合作非对称解密、标准非对称解密、数据摘要、随机数生成等密码服务 |  |
| 4 | 采用密钥分割的密钥管理技术，证书密钥由客户端密钥因子和服务端密钥因子共同组成，两端协同完成电子签名运算，实现用户对签名密钥的专有控制 |  |
| 5 | 支持各类主流Android、IOS移动端、微信小程序平台，**提供相关证明文件**； |  |
| **序号** | **产品资质要求** |  |
| 1 | **★具备IOS和Android端电子病历数字签名及IOS和Android端移动电子认证软件著作权证书并提供全部证明文件；** |  |

* 1. **CA安全认证服务器**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 密钥存储：用户密钥对及密钥加密密钥可以使用系统保护密钥加密保护，以密文的形式存储在密码卡的存储芯片中。 |  |
| 2 | 采用密钥运算技术、数字证书、身份信息核验等多重手段，支持APP、PC等全终端可信身份认证，通过扫码、口令等方式保障登录身份安全 |  |
| 3 | 处理医院业务系统端的请求，为客户终端提供数字签名、电子签章、加盖时间戳、密钥管理等服务。 |  |
| 4 | 实现证书申请、制作、下载等全生命周期管理功能 |  |
| 5 | 预设医生签名信息，通过扫码等形式实现快捷电子签名。在PC中，支持预登录后，后台批量签署电子病历功能 |  |
| 6 | 支持对时间、次数、角色等细粒度的授权管理。对所有登录、签名、签章、授权等行为自动记录日志。 |  |
| 7 | 提供移动电子认证服务，调用数字证书认证、电子签名等应用功能，实现跨终端的数字证书应用 |  |
| 8 | 支持证书的启动自检，实现证书的初始化、PIN码、格式化等管理操作。 |  |
| 9 | 支持将待签文件推送至移动端预览、签署； |  |
| 10 | 具备电子签名值存证功能； |  |
| 11 | 提供日志管理功能，可以查询和管理登录日志、签名日志、数据维护日志等； |  |
| **序号** | **非功能指标要求** |  |
| 1 | 1.支持ECB、CBC模式的SM1密码算法2.支持SM2密码算法，可在卡内进行加解密、签名验签、密钥对生成3.支持SM3密码算法4.支持ECB、CBC模式的SM4密码算法5.支持数据的安全存储功能6.采用双物理噪声源生成真随机数7.支持密码卡全量密钥备份 |  |
| 2 | 接口要求1.支持个性化接口定制开发，2.支持国内算法3.支持X86、ARM、PowerPC等架构下的API接口库 |  |
| 3 | 密码运算性能要求SM1加解密速度 ≥200Mbps、SM4加解密速度 ≥150Mbps、SM2生密钥≥2300次/秒、SM2签名≥2000次/秒、.SM2验签≥1700次/秒、SM3摘要≥150Mbps、随机数生成≥2Mbps |  |
| **序号** | **产品规格要求** |  |
| 1 | 服务器类型：2U机架式服务器，配置标准机架安装导轨处理器配置：处理器型号：国产CPU或Intel至强系列或同等级处理器核心数：物理核数≥8核，主频≥2.7GHz内存配置：运行内存：≥64GB内存内存插槽：≥8个，存储配置：硬盘配置：标配≥2块1T固态硬盘，RAID1，支持热插拔。RAID控制器：配置硬件RAID卡，支持RAID 0/1/5/10/50/6/60模式缓存≥2GB，支持Cache超级电容保护可选配SAS HBA卡或SAS RAID控制卡网络接口：标配网卡：≥2个千兆电口（RJ45）+ 2个万兆光口（含多模模块）电源配置电源功率：≥500W 80Plus铂金级冗余电源冗余设计：双电源模块，支持热插拔 |  |

* 1. **移动安全认证系统**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 管理客户端，实现单位管理、用户管理、权限管理、系统配置、日志管理、数据统计、账户登录等功能； |  |
| 2 | 接收处理业务系统侧的数据待签请求和验签请求； |  |
| 3 | 医师用户管理：新增用户、编辑医师信息、删除医师信息。支持批量导入信息； |  |
| 4 | 具备医师手写签名图片管理功能，支持批量、单独管理医生签名图片；支持签名图片预览、审核；**(提供产品截图证明)** |  |
| 5 | 用户手机证书管理：移动端数字证书下载、绑定移动端数字证书、证书状态查询 |  |
| 6 | 角色权限：固定角色、权限列表、角色对应成员； |  |
| 7 | 账户管理：单位操作成员账户管理，成员基础信息账户管理，增删改查 |  |
| 8 | 单位管理：添加单位、管理单位状态启用/停用。 |  |
| 9 | 日志管理：包括签名日志、扫码日志、申请证书日志、操作日志和登录日志 |  |
| 10 | 统计报表：用户量统计、用户状态统计、签名业务量统计、证书申请统计；(**提供产品截图证明)**支持折线图、饼状图、柱状图等图表分析，查看使用趋势；(**提供截图证明)** |  |
| **序号** | **产品资质要求** |  |
| 1 | **★移动签体系具备信息系统安全等级保护三级备案证明** |  |
| 2 | ★**具备移动智能终端签名验签系统服务端（密码模块）及移动智能终端安全密码模块(服务端)的商用产品认证证书并提供证明文件** |  |

* 1. **时间戳服务系统**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 支持X.509 v3证书，支持全中文证书 ，支持签名证书和加密证书的双证书认证体系。 |  |
| 2 | 支持国密SM2、国际RSA等非对称加密算法，支持SHA256、SHA384、SHA512、SM3 等摘要算法。 |  |
| 3 | 满足多个时间戳规范，包括国际通用的RFC3161标准、微软 Authenticode和PKCS7副署及验证。 |  |
| 4 | 支持签发时间戳，支持通过调用API将数据发送到TSA服务器进行时间戳签名。 |  |
| 5 | 支持验证时间戳，支持通过调用API将数据发送到TSA服务器进行时间戳签名验证。 |  |
| 6 | 支持时间戳和签名验签服务功能测试模块，便于现场实施或接入开发过程中进行调试。 |  |
| 7 | 支持通过NTP协议与第三方授时中心、卫星授权时间源进行时间同步，确保时间戳中时间的有效性。 |  |
| 8 | 支持通过选配安装北斗、GPS、CDMA 时间源模块同步卫星时间。 |  |
| 9 | 支持设置多个独立的签名验签服务，通过服务端口的不同区分不同的验签服务。 |  |
| 10 | 密钥访问控制，密钥库中保存的每一对密钥都各自拥有自己的访问口令，必须 使用正确的口令才使用该密钥进行服务操作。 |  |
| 11 | 支持私钥加密、私钥解密、公钥加密、公钥解密、数字信封封包、数字信封解包。 |  |
| 12 | 遵循 PKCS、XML 等国际签名规范。支持多标准签名验证，包括PKCS#1、PKCS#7（Attach）、 PKCS#7（Detach）。 |  |
| 13 | 具备CRL无差别匹配功能，支持在CRL中通过证书序列号进行检索。 |  |
| 14 | 具备WebGUI管理控制台，通过基于WEB形式的图形管理控制界面，实现对设备的管理、维护和监控等操作。 |  |
| 15 | 支持通过符合国密标准的密码机、加密卡等硬件加速设备提高密码运算效率。 |  |
| 16 | 具备证书防火墙功能，可根据证书序列号、主题项、证书指纹等多种维度来对使用者的数字证书进行鉴权管理。**（提供产品截图证明）** |  |
| **序号** | **性能指标要求** |  |
| 1 | 1.SM2：时间戳签名不小于2800tps，时间戳验签不小于2100tps;2.SM2：签名不小于10000tps，验签不小于5000tps; |  |
| **序号** | **产品资质要求** |  |
| 1 | **★具备时间戳服务器商用密码产品认证证书及时间戳服务器信息技术产品安全测试证书。** |  |
| 2 | **★可信时间戳系统符合《信息技术应用创新产品评估规范》，提供省市级适配中心出具的信创产品评估证书** |  |

* 1. **数字身份管理系统**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 实现证书自动静默更新； |  |
| 2 | 实现证书应用客户端环境自动更新； |  |
| 3 | 提供网页在线帮助功能； |  |
| 4 | 提供查看系统状态、配置系统IP/端口、管理员管理、设备编号管理、日志管理、服务管理、备份恢复等管理功能； |  |
| **序号** | **非功能指标要求** | **备注** |
| 1 | 提供备份恢复功能，可通过界面备份当前所有配置，保证系统瘫痪时的快速恢复； |  |
| 2 | 提供日志记录，可将日志以syslog的方式发送到指定服务器； |  |
| 3 | 应满足卫生部卫生系统电子认证服务相关技术规范。 |  |

* 1. **电子签章系统**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 文件签章：根据电子印章加盖位置信息在相应的位置进行签章，签章时可获取时间戳信息和用章单位数字证书信息。签章后形成带有用章单位电子印章的签章文件。 |  |
| 2 | 签章管理：签章能够完成PDF等版式文档的盖章功能，并能通过服务端查看系统工作状态和任务状态。 |  |
| 3 | 支持文档的手动盖章、自动盖章和批量盖章支持鼠标定位、坐标定位和关键字符定位等功能，用户能根据实际情况选择合适方便的盖章方式。 |  |
| 4 | 电子签章证据链：根据国家及行业有关规定，电子签章业务对签章过程信息进行电子签名，形成签章证据链信息以便存证 |  |
| 5 | 签章文件验签：实现对已签章文件的验签功能，包括电子印章有效性、签章详细信息等。 |  |
| 6 | 支持批量签章 |  |
| 7 | 文档验证：提供离线、在线、批量验证功能。 |  |
| 8 | 查看印鉴信息：通过电子签章系统查看文档印鉴信息：包括验证结果、盖章时间、盖章人、数字证书、印章外观、印章名称、印章来源、制印时间、制印人、所属单位等印章信息。 |  |
| 9 | 签名验证：电子签章系统具有签名验证功能，其验证方式和操作与功能验证是一致的。 |  |
| 10 | 具备印章管理功能，包括印章模板管理、印章制作、授权、停用、启用等功能 |  |
| 11 | 支持第三方CA机构签发的数字证书 |  |
| **序号** | **产品资质要求** |  |
| 1 | **产品具备《软件著作权证书》** |  |
| 2 | **具备电子签章系统商用密码产品认证证书及电子签章系统信息技术产品安全测试证书。** |  |

* 1. **手写数字签名系统**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 申请和获取签名数字证书。根据签名业务及签名主体鉴证信息，向电子认证服务机构证书服务平台申请颁发数字证书； |  |
| 2 | 通过手写数字签名终端，获取签名人手写签字笔迹，作为数字签名可视化展现效果图示； |  |
| 3 | 使用数字签名密码算法，对知情同意书进行密码运算，保护知情同意书的有效性； |  |
| 4 | 提供知情同意书的存储、归档、展现、验证举证服务。支持知情同意书共享、同步到电子病历系统； |  |
| 5 | 系统兼容性良好，提供版本接口，方便与各种应用系统结合； |  |
| 6 | 提供web管理平台，具备设备信息、签名业务等数据展示；具备设备信息管理、证书申请、日志记录等功能； |  |
| 7 | 系统支持维护医院科室信息，支持设备绑定科室信息，支持设备、科室状态修改； |  |
| 8 | 支持对签名数据加盖时间戳，保障签名数据的时间权威可靠； |  |
| 9 | 系统支持多院区信息维护，支持院区签名数据统计、查询；支持签名数据分科室、院区、时间段折线图展示； |  |
| 10 | 支持设备使用状态、科室/病区数量以及签名业务数据总览； |  |
| 11 | 通过手写输入设备，获取签名人手写签字，作为数字签名可视化展现效果图示。支持手写板、智能手机、PAD、PDA等终端手持设备人证比对认证服务。 |  |
| 12 | 能够支持个人多源身份认证平台实现患者手写签字时的身份实名认证，包括基于公安部人口库的人脸识别认证、银行三要素、四要素认证、电信运营商认证、微信、支付宝等多源认证需求，满足不同患者认证方式便利性。 |  |
| 13 | 系统具备证书过期提醒功能； |  |
| **序号** | **产品资质要求** |  |
| 1 | **★具备数字签名管理软件产品著作权证书及签名验签服务器信息技术产品安全测试证书** |  |
| 2 | **★为保证可举证性，须提供个人多源身份认证系列软件、个人网上身份统一认证平台软件、手持专用设备人证比对认证 APP软件、人脸识别服务端软件、IOS/Android 端人脸识别中间件软件著作权证书。** |  |
| 3 | **产品具有计算机软件著作权登记证书** |  |

* 1. **统一电子认证系统（含服务器）**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标** | **备注** |
| 1 | 提供用户信息管理功能：至少支持查看详情、停用用户、编辑用户信息和同步用户信息的操作，支持同步选中用户的信息，支持导出用户信息，支持添加单个用户和批量用户功能；提供通过选择认证级别、用户状态、同步状态查询对应范围用户信息，通过输入用户名称、身份证号码和手机号查询指定用户信息。**（提供产品截图证明)** |  |
| 2 | 提供基本配置信息：至少包括接口证书、免密签名有效期配置、token模式配置、用户登录状态有效期配置等。**（提供产品截图证明)** |  |
| 3 | 具有数据可信保全和责任认定功能，能够查看每笔扫码登录、扫码签名、推送签名信息的使用记录详情，包括签名类型、应用系统、签名时间、签名摘要描述等信息。使用日志支持通过日志类型、初始时间、截止时间进行日志筛选，保证每笔签名业务的数据保全及责任认定；（**提供产品截图证明）** |  |
| 4 | 提供管理员管理功能：支持停用管理员账号、编辑管理员信息和权限以及注销管理员账号；提供添加管理员及配置管理员权限的功能，包括用户权限、应用权限、管理员权限、证书权限、配置权限、日志权限及统计权限 |  |
| 5 | 提供用户证书管理功能：支持查看证书详情的操作；支持通过输入用户姓名、身份证号码、电话号码、证书序列号及UUID查看证书信息 |  |
| **序号** | **非功能指标要求** |  |
| 1 | 标准机架式服务器设备支持≥4个千兆网口；具备≥1个RJ45串口管理；具有LCD或LED液晶显示模块，支持显示CPU、内存、IP等实时信息。 |  |
| **序号** | **产品资质要求** |  |
| 1 | **★具备数据可信保全与责任认定软件著作权证书提供证明文件** |  |
| 2 | **★为保证用户数据安全，生产厂商数据管理能力需成熟且稳健，生产厂商需提供3级及以上的数据管理能力成熟度等级证书。** |  |
| 3 | **★统一认证系统具备商用密码产品认证证书、网络安全专用产品安全检测证书。** |  |

* 1. **个人数字证书**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 标识医护人员用户网络身份； |  |
| 2 | 由权威合法的第三方CA机构签发，符合《x.509C的国内数字证书格式规范》。证书标准遵循 X.509 V3格式标准； |  |
| 3 | 支持存储于智能USBKEY、IC卡等多类型介质； |  |
| 4 | 数字证书支持RSA、SM2算法； |  |
| 5 | 支持自定义证书扩展域管理。 |  |
| **序号** | **产品资质要求** |  |
| 1 | **具备国家权威机构颁发的电子认证服务系统密码使用安全合规性证明并提供证明文件** |  |
| 2 | **具备CCRC信息系统安全集成二级或以上资质及CCRC信息系统安全运维二级或以上资质并提供证明文件。** |  |

* 1. **移动数字证书（医护）**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 标识医护用户网络身份； |  |
| 2 | 由权威合法的第三方CA机构签发，符合《x.509C的国内数字证书格式规范》。证书标准遵循 X.509 V3格式标准； |  |
| 3 | 支持存储于智能USBKEY、IC卡、移动APP客户端等多类型介质； |  |
| 4 | 数字证书支持RSA、SM2算法； |  |
| 5 | 支持自定义证书扩展域管理。 |  |
| **序号** | **产品资质要求** |  |
| 1 | **具备国家权威机构颁发的电子认证服务系统密码使用安全合规性证明并提供证明文件** |  |
| 2 | **具备CCRC信息系统安全集成二级或以上资质及CCRC信息系统安全运维二级或以上资质并提供证明文件。** |  |

* 1. **单位数字证书**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 标识单位用户网络身份； |  |
| 2 | 由权威合法的第三方CA机构签发，符合《x.509C的国内数字证书格式规范》。证书标准遵循 X.509 V3格式标准； |  |
| 3 | 支持存储于智能USBKEY、IC卡、移动APP客户端等多类型介质； |  |
| 4 | 数字证书支持RSA、SM2算法； |  |
| 5 | 支持自定义证书扩展域管理。 |  |
| **序号** | **产品资质要求** |  |
| 1 | **具备国家权威机构颁发的电子认证服务系统密码使用安全合规性证明并提供证明文件** |  |
| 2 | **具备CCRC信息系统安全集成二级或以上资质及CCRC信息系统安全运维二级或以上资质并提供证明文件。** |  |

* 1. **设备数字证书**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 标识设备网络身份； |  |
| 2 | 由权威合法的第三方CA机构签发，符合《x.509C的国内数字证书格式规范》。证书标准遵循 X.509 V3格式标准； |  |
| 3 | 数字证书支持RSA、SM2算法； |  |
| 4 | 支持自定义证书扩展域管理。 |  |
| **序号** | **产品资质要求** |  |
| 1 | **具备国家权威机构颁发的电子认证服务系统密码使用安全合规性证明并提供证明文件** |  |
| 2 | **具备CCRC信息系统安全集成二级或以上资质及CCRC信息系统安全运维二级或以上资质并提供证明文件。** |  |

* 1. **证书存储介质**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | USBKey智能密码钥匙，实现数字证书的安全存储与使用； |  |
| 2 | 标准USB2.0规范，兼容USB1.1，兼容3.0规范接口； |  |
| 3 | 提供标准安全中间件 CSP 及 PKCS#11 v2.11 接口，硬件实现数字签名，支持X.509 v3标准证书格式； |  |
| 4 | 支持Window2000/2003/2008/XP/Vista/Win7/Win8等32位和64位中文、英文、繁体操作系统； |  |
| 5 | 硬件支持1024/2048位RSA和SM2非对称算法，支持SSF33、SM1、SM3、SM4等国密算法。支持DES、3DES等对称算法和SHA-1、SHA256摘要算法； |  |
| 6 | 智能卡芯片CPU至少32位，用户可用空间（Byte）不低于64K，可存放多张证书； |  |
| 7 | USBKey自身的安全要求：具备完善的PIN校验保护功能； |  |
| 8 | 支持标准的RSA和国产商用密码算法； |  |
| 9 | 数据存储时间不小于10年，可读写次数(次)不小于10万次。 |  |
| **序号** | **非功能性指标要求** |  |
| 1 | RSA（2048）密钥对生成时间<12秒；SM2密钥对平均生成时间<2秒； |  |
| 2 | RSA（2048）签名速度≥5次/s，RSA（2048）验签速度≥20次/s，SM2私钥签名≥4次/s，SM2公钥验证≥2次/s； |  |
| 3 | RSA（2048）加密速度≥20次/s，RSA（2048）解密速度≥5次/s，SM2公钥加密≥2次/s，SM2私钥解密≥4次/s。 |  |
| **序号** | **产品资质要求** |  |
| 1 | **具备智能密码钥匙商用密码产品认证证书** |  |

* 1. **患者签名终端（有线）**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 电磁屏技术类型：无线无源；电磁笔：无电池无源笔；压感：≥8192级；≥10.1寸高清显示屏；分辨率≥1280\*800； |  |
| 2 | 能记录客户在签名设备上的完整轨迹，无断点； |  |
| 3 | 签名时轨迹同步在屏幕上展示，延迟小于0.5秒； |  |
| 4 | 平均无故障时间：大于18000小时； |  |
| 5 | 能以原始轨迹数据、矢量图片方式保存签名数据 |  |
| 6 | 支持图像加签验签技术:可以对签字图像指纹图像，进行原RGB级别SM3+SM2加密封装，确保图像原始RGB不被篡改，并可F5隐写如RGB中形成不可变水印，并且数据链条可加时间戳确保时间的可溯源性。 |  |
| 7 | 支持原笔迹签名及手书功能，可进行原笔迹签名功能及手写输入指定文字；笔迹图像存储及原笔迹数据存储；手写输入数据可以保存为图片，矢量图片及原笔迹数据； |  |
| 8 | 具备同屏显示功能，上位机可将当前显示内容推送到签批设备上，并且上位机也能实施查看签批设备显示操作状态；文件合成功能；设备可根据功能规则（如XYP数据，关键字数据）进行签字名图片的对指定格式的文件进行插入操作。 |  |
| 9 | 系统：Linux（支持Windows、安卓、国产麒麟、统信等系统平台交互） |  |

* 1. **患者签名终端（无线）**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 显示模块：≥10.1寸高清显示屏；分辨率≥1280\*800；亮度：≥250cd/m²；摄像头：≥前置200万像素，后置≥500万像素；  |  |
| 2 | 数字证书申请功能，支持与第三方CA机构对接，下发合规的数字证书； |  |
| 3 | 支持用户在多个移动终端设备上使用同一个用户身份； |  |
| 4 | 数据签名功能，提供数据签名服务接口，与业务系统对接，支持业务系统发起签名请求，并调用签名接口对患者签名信息、指纹信息进行数字签名，并加盖时间戳； |  |
| 5 | 支持按照科室维度登录应用，查看该科室有待签文件的患者、待签文件数量； |  |
| 6 | 支持缓存机制，支持网络不佳状态下，缓存患者已提交签署的文件。待网络稳定后文件状态自动更新； |  |
| 7 | 支持记录当前已签署的文件数量，可查看已签署文件详情； |  |
| 8 | 提供身份认证服务，支持对患者进行可靠身份认证，并基于可信身份实现可靠签署； |  |
| 9 | PIN重置功能，支持忘记证书PIN码向管理端发起重置PIN码申请； |  |
| 10 | 支持对终端移动终端进行管理：包括设备的查看、挂起、停用； |  |
| 11 | 文件推送交互和全屏签署功能：可在交互终端上进行PDF等板式文件的推送和信息交互，能在浏览后进行签署； |  |
| 12 | 具备数字证书登录功能； |  |
| **序号** | **非功能指标要求** |  |
| 1 | 指纹模块：传感器类型：半导体电容式，传感器尺寸：≥23.0\*35.0mm，有效图像尺寸；≥12.8\*18mm，图像大小；≥256\*360pixel,图像分辨率：≥508dpi，比对方式：1：1/1：N，认假率（FAR）；<0.0001%; |  |
| 2 | CPU：高性能CPU，处理器核心数量≥6核，主频≥1.8G；系统：安卓（支持Windows、安卓、国产麒麟、统信等系统平台交互）；内存：≥4GB；存储：≥64GB； |  |
| 3 | 电池：电池类型：聚合物高密度安全电池；电池容量：标配≥8000mAH；待机时长：≥12h；工作时长：≥7.5h； |  |

* 1. **事件性数字证书**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 标识患者网络身份； |  |
| 2 | 由权威合法的第三方CA机构签发，符合《x.509C的国内数字证书格式规范》。证书标准遵循 X.509 V3格式标准； |  |
| 3 | 数字证书支持RSA、SM2算法； |  |
| 4 | 支持自定义证书扩展域管理。 |  |
| **序号** | **产品资质要求** |  |
| 1 | **具备国家权威机构颁发的电子认证服务系统密码使用安全合规性证明并提供证明文件。** |  |
| 2 | **具备CCRC信息系统安全集成二级或以上资质及CCRC信息系统安全运维二级或以上资质并提供证明文件。** |  |

* 1. **系统可靠性方案**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | ★系统需具备高度可靠性，并提供在紧急情况下的系统可靠性切换方案，紧急情况涵盖但不限于断网、服务器故障等情形。  |  |

* 1. **院内业务系统接口**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能指标要求** | **备注** |
| 1 | 对接院内业务系统，HIS、LIS、PACS、EMR、手麻、重症、互联网医院系统等所有需要电子签名的系统； |  |

* 1. **合作研发要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **名称** | **功能指标要求** | **备注** |
| 1 | 电子签名系统合作研发需求 | 投标人应具有与目标医院合作研发电子签名系统条件与能力，根据目标医院现有的业务流程，提出相应的电子签名系统研发方案及合作办法 |  |
| 2 | 电子签名系统合作研发需求 | 1. 研发目的

国家卫生健康委办公厅2017年印发《电子病历系统应用水平分级评价管理办法（试行）》中，明确要求医疗机构积极做好卫生系统电子认证服务体系建设，实现身份认证、授权管理和责任认定；《中华人民共和国电子签名法》明确可靠的电子签名与手写签名或盖章具有同等的法律效力。为满足《中华人民共和国电子签名法》、《电子病历系统应用水平分级评价管理办法（试行）》、《卫生健康领域电子签名应用规范》等法律法规要求，实现医疗文书、处方、检验报告等全流程电子化签名合法性。覆盖门诊/住院电子病历、知情同意书、医嘱、护理记录、互联网医院等业务场景，降低纸质文件流转，缩短患者等待时间。构建符合等保三级标准的可信认证体系，确保签名数据存储、传输、验证全过程防篡改、防抵赖。 |  |
| 3 | 电子签名系统合作研发需求 | 1. 研发办法

采用本地化私有部署，国产商用密码算法（SM2/SM3/SM4）实现数字证书签发；支持与医院现有信息系统（HIS/LIS/PACS/EMR）无缝集成，提供标准化API接口。构建“可信身份、可信行为、可信数据和可信时间”电子认证体系，合作研发支持USBKey/扫码/指纹/人脸多模态生物识别签名；同步国家授时中心可信时间源，签名时间戳误差≤0.1秒；兼容iOS/Android/HarmonyOS系统的移动端签署设备；确保医疗文书的合法性和可追溯性。 |  |
| 4 | 电子签名系统合作研发需求 | 1. 时间周期

中标人需提出合理的时间周期，提出详细的进度安排，有具体的时间保障措施，以确保项目按时、高质量完成。 |  |
| 5 | 电子签名系统合作研发需求 | 1. 双方责权利划分

合作研发项目费用由中标人承担；中标人不得将本合作研发项目委托给任何第三方：中标人保证合作研发过程不侵犯第三人的知识产权；在完成合作研发项目后，中标人交付给目标医院可运行的软件，包括系统技术文档、数据等；中标人需协助目标医院进行软件调试，直至目标医院验收合格；中标人负责为目标医院培训人员；中标人不得将该研发项目的信息资源（包括源代码、系统技术文档、软件、数据等）泄露或许可第三方阅读、使用或复制。目标医院提供合理的建议；完成研发后，目标医院在7天内组织验收，并提出验收意见。该研发项目整个研发产品由目标医院独享专利、著作权等申请权；利用本合作研发项目成果申报的各类奖项，目标医院有作为第一人及第一单位的优先权；中标人作为第二人及第二单位。以上为研发协议签订时的基本内容，未尽事宜待投标人中标后签订研发协议时与目标医院协商确定。 |  |

**八、其他内容不变。**

**九、请潜在投标人及时在河南省公共资源交易系统下载更正后的采购文件。**