## 项目概况

《电子病历应用管理规范（试行）》明确了有条件的医疗机构电子病历系统可以使用电子签名进行身份认证，可靠的电子签名与手写签名或盖章具有同等的法律效力，并且明确了电子病历的身份识别、操作痕迹、时间、人员信息等做到可追朔，医院通过全面部署可靠电子认证服务成为必然。

# 1、项目建设目标

南通市第三人民医院全面落实网络安全法、国家卫健委和地方卫健委的有关规范要求，全面实施本院无纸化为目的，结合本院实际情况，全面引入电子认证，面向本院医护人员解决身份认证、授权管理、责任认定等安全问题，具体而言包括：

1)数字证书服务体系：面向医院全体医护人员建立统一的、符合卫生行业规范的数字证书服务体系，为医院信息系统解决行为人的身份凭证及凭证认证问题。

2)基础应用安全支撑体系：建立基于数字证书的应用安全支撑体系，实现医护人员基于数字证书的身份认证、关键业务环节的电子签名和时间戳应用，实现医疗数据的完整性保护、可信时间、以及责任认定等安全需求。

3)实现移动终端的CA应用：使用无线应用CA技术，实现移动查房、协同办公过程中工作人员在使用移动终端操作时的强身份认证、安全传输及重要数据抗抵赖性安全需求，提升整个无线应用的信息安全防护能力。

# 2、项目建设实现功能

通过在医院部署电子认证管理体系和电子认证应用安全支撑体系，来满足全院信息系统对于用户身份真实性鉴别、数据完整性保护、业务抗抵赖、权威举证、隐私保护等需求。满足如下功能：

1)数字身份管理体系：数字身份管理体系支持对接第三方合法CA中心运行系统，为证书业务管理员提供本地化的数字证书生命周期管理和日常管理等电子认证管理功能。数字生命周期管理服务主要包括：证书申请、发放、更新、吊销、丢失补办、损坏重办、印章制作等服务内容。在系统初始化时，由证书管理员为医护人员和工作人员提供身份数字证书，并且提供对外接口可以嵌入人力资源管理、OA系统等，在管理人员登记医师等人员信息时进行数字证书同步申请发放。日常管理功能主要是提供管理员管理、系统管理、查询统计、升级监测等日常管理功能，其中证书模板配置功能可以由管理员自定义扩展项满足业务系统实际应用需求；提供并提供对证书发放情况、证书状态等情况进行查询、统计及报表输出功能，满足医疗卫生机构证书运营支撑和日常管理需要。

2)客户端认证体系：主要包括面向院内医护人员身份认证、电子签名，医护人员采用移动证书APP+数字证书方案。

3)应用安全支撑体系： 应用安全支撑体系主要是利用PKI/CA机制，为电子病历系统、护理病历系统、HIS系统、LIS系统、PACS系统等信息系统对于应用安全保障和可信医疗服务体系构建提供身份认证、授权管理、责任认定等功能服务，从而解决医疗卫生机构信息系统对于电子数据真实性、完整性、有效性、权威举证等问题。为了实现医护人员证书身份认证、数字签名&验证、可信时间戳、通用密码算法等基本功能以及可视化电子签章功能、医护人员手机证书应用等新兴场景下的CA应用，本期需建设数字签名验证服务、可信时间戳服务、电子签章系统服务、移动安全认证服务等数字证书应用安全支撑系统。

# 3、项目建设功能要求

1)数字身份管理系统(RA系统)采用运营模式建设，可以对接国内所有合法CA机构运营系统，医院后期可以合理选择不同CA机构证书服务。

2)数字身份管理系统(RA系统)提供接口可以嵌入医院OA系统、人事管理系统等，在人员信息登记时直接下发数字证书申请权限，签发符合医生资格的身份数字证书。

3)应用安全支撑体系统基于“设备虚拟化+分时多任务处理”机制，为接入业务系统提供独立的虚拟化的服务接入模式，分配单独的服务资源，各业务系统只需接入应用安全支撑体系统即可获取统一的电子认证服务。

4)移动证书APP/SDK/小程序方案应基于PKI/CA的应用安全防护和网络可信认证方案可以综合解决信息系统可信身份认证、可靠电子签名、可信时间戳、隐私数据保护等安全需求和医疗机构无纸化的需求。

## 一、项目需求产品清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 产品需求一览表 | | | | | |
| 序号 | 招标货物名称 | 数量 | 单位 | 功能描述 | 备注 |
| 1 | 数字签名验证服务器 | 1 | 台 | 含加密卡，部署在医院信息中心，为医院信息系统提供数字签名&签名验签、数据加解密以及通用密码服务功能。 | 软硬件一体机 |
| 2 | 时间戳服务器 | 1 | 台 | 含加密卡，部署在医院信息中心，通过GPS卫星或CDMA网络对接国家标准时间源为医院信息系统提供可信时间戳签名/验签服务功能。 | 软硬件一体机 |
| 3 | 证书管理系统 | 1 | 套 | 实现本地化的数字证书申请、审核、制作发放和管理，实现数字证书自动更新功能。 | 软件 |
| 4 | 电子签章系统 | 1 | 套 | 实现可视化的电子签名 | 软件 |
| 5 | 移动安全认证服务器、移动证书APP | 1 | 套 | 含硬件加密模块的软硬一体设备，部署在医院信息中心，实现移动端证书APP/SDK的私钥分割运算，实现移动端消息推送、移动证书发放管理、认证、扫码签名等功能。提供移动证书的申请、查阅、密码修改、证书更新等生命周期服务。 | 软硬件一体机 |
| 6 | 个人数字证书 | 500 | 张 | 标识医护人员网络实体身份。 |  |
| 7 | 单位证书 | 1 | 张 | 标识单位网络实体身份。 |  |
| 8 | 设备证书 | 4 | 张 | 标识设备网络实体身份。 |  |
| 9 | 应用软件改造 | 3 | 套 | LIS、PACS、互联网医院功能改造费用 |  |

## 二、技术要求

## 数字签名验签服务器

|  |  |
| --- | --- |
| 序号 | 功能指标要求 |
| 1 | 提供pkcs1/Pkcs7 attach/Pkcs7 detach/xml Sign 等对多种格式数据的数字签名和验证功能，提供对文件数字签名和验证功能，支持对文件进行MD2、MD5、SHA-1、SHA-256等方式的数字摘要签名；提供加解密PKCS7格式数字信封功能；提供证书解析功能，获取证书中的任意主题信息以及扩展项信息；  支持RSA算法及SM2算法 |
| 2 | 提供通用密码服务，包括摘要运算、随机数、对称加解密、非对称加解密、数字信封、base64编解码等功能，支持RSA、3DES、DES、AES、MD2、MD5、SHA1、SHA256等常见算法。设备支持国密最新算法； |
| 3 | 提供审计监测服务，包括应用日志采集，并与电子认证管理系统审计监测系统配合进行电子认证应用记录集中存储、管理等功能，用于监测电子认证应用情况、事后责任追溯等应用场景； |
| 4 | 证书本地验证服务，主要为业务系统提供局域网方式的证书有效性验证，提速证书认证和局域网运行效率； |
| 5 | 虚拟化服务功能：能支持将系统进行虚拟化分区处理，分别面向不同的接入单位提供独立的安全管理帐户和界面，各接入单位之间的密钥和数据相互逻辑隔离； |
| 6 | 提供证书验证功能，支持对X.509 Version 3、PKCS系列证书的DER和PEM格式的应用与验证 |
| 7 | 提供数据加密、解密功能，支持数字信封加密，支持DES、Tri-DES算法、以及国产密码算法 |
| 8 | 提供CRL的证书有效性验证，CRL更新配置可自动定时进行 |
| 9 | 服务器证书管理：实现对业务系统服务器端密码设备及服务器证书进行配置与管理，可生成服务器证书申请文件。 |
| 10 | 信任源管理：可同时配置多条证书链，验证不同CA的用户证书。 |
| 11 | 动态黑名单管理：可自动更新CRL黑名单、动态更新，不需要重新启动服务。 |
| 12 | 安全存储：基于密码技术构建安全存储区，用于对可信根证书及黑名单文件进行分类安全存储，防止非法操作。 |
| 13 | 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 |
| 序号 | 非功能指标要求 |
| 1 | 提供日志记录，可将日志以syslog的方式发送到指定服务器 |
| 2 | 支持双机、负载均衡 |
| 3 | 提供C、COM 、Java 等主流开发API |
| 4 | 签名能力：≥2000次/秒，签名验证：≥3500次/秒 |
| 5 | 适用环境：千兆环境，并发用户多 |
| 6 | 支持性能扩展，提供增加硬件加密引擎或并行负载扩展方式。 |
| 序号 | 产品规格要求 |
| 1 | 设备高度：≥2U |
| 2 | 网络接口: ≥ 4个千兆网口 |
| 3 | 电源指标：≥1个工控电源 |
| 4 | 硬件加密卡：有 |

## 时间戳服务器

|  |  |
| --- | --- |
| 序号 | 功能指标要求 |
| 1 | 提供时间戳签发功能，能实现基于硬件权威时间源的时间戳签发、验证、查询等功能； |
| 2 | 提供审计监测服务，包括应用日志采集，并与电子认证管理平台审计监测系统配合进行电子认证应用记录集中存储、管理等功能，用于监测电子认证应用情况、事后责任追溯等应用场景； |
| 3 | 虚拟化服务功能：能支持将系统进行虚拟化分区处理，分别面向不同的接入单位提供独立的安全管理帐户和界面，各接入单位之间的密钥和数据相互逻辑隔离； |
| 4 | 服务器证书管理：实现对业务系统服务器端密码设备及服务器证书进行配置与管理，可生成服务器证书申请文件。 |
| 5 | 签发时间戳：接收应用系统发来的时间戳签发请求，签发时间戳后将时间戳返回给应用系统，时间戳服务请求遵循国际通用的RFC3161标准 |
| 6 | 验证时间戳：处理应用系统发来的时间戳验证请求，将时间戳验证结果返回给应用系统 |
| 7 | 权威国家时间源：产品内置国家认可的时间源模块,可提供多种授时方式包括：CDMA、GPS等供用户选择使用 |
| 8 | 时间同步: 支持NPT、SNTP时间同步协议 |
| 9 | 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 |
| 序号 | 非功能指标要求 |
| 1 | 提供日志记录，可将日志以syslog的方式发送到指定服务器 |
| 2 | 支持双机、负载均衡 |
| 3 | 提供C、COM 、Java 等主流开发API |
| 5 | 时间戳签发性能≥1000次/秒 验证性能≥800次/秒 |
| 6 | 授时精度：0.5-3ms(毫秒) |
| 7 | 守时精度：<1ms（72小时），内置恒温晶振 |
| 8 | 适用环境：千兆环境，并发用户多 |
| 9 | 支持性能扩展，提供增加硬件加密引擎或并行负载扩展方式。 |
| 序号 | 产品规格要求 |
| 1 | 设备高度：≥2U |
| 2 | 网络接口: ≥4个千兆网口 |
| 3 | 电源指标：≥1个工控电源 |

## 移动安全认证服务器

|  |  |
| --- | --- |
| 序号 | 功能指标要求 |
| 1 | 软硬一体部署须采用带硬件密钥模块的设备，密码运算模块必须部署在医院内网，保证医院数据不离开医院内部网络。 |
| 2 | 具备RA中心模块，技术上可与所有国内第三方合法CA机构进行对接，满足医院后期对CA机构的选择需求。 |
| 3 | 提供用户管理功能，包括用户信息管理、用户实名认证管理、用户状态管理、用户证书管理，其中用户证书管理需要能够针对电子证照进行绑定，并维护多终端情况下的用户证书生命周期；支持白名单机制。 |
| 4 | 提供手机设备管理功能，包括密码设备标识、密码设备认证，通过移动设备管理，对移动客户端密码设备进行统一管理。 |
| 5 | 提供移动终端密码模块管理功能，对移动终端密码模块版本进行管理。 |
| 6 | 提供应用管理功能，对接入应用进行管理，包括应用的基本信息和接入状态。 |
| 7 | 提供与移动终端密码模块接口功能，通过与移动安全密码模块的接口实现移动安全密码模块的接入，完成对证书的申请、更新、补发、注销相关生命周期管理，同时基于分割密钥算法来保障移动证书私钥的安全。 |
| 8 | 提供与数字证书认证系统接口，与数字证书认证系统对接，提供签发证书的能力。 |
| 9 | 提供与应用系统接口，通过与应用系统接口实现移动安全认证服务系统与应用系统的对接。 |
| 10 | 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。 |
| 11 | 提供系统管理功能，包括系统配置、操作员管理、CA接入配置、统计查询等功能。 |
|  | 具有使用日志查看功能，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。 |
| 12 | 支持面向应用提供数字证书二维码扫码认证登录服务功能。 |
| 14 | 支持批量签名推送功能，面向应用提供批量数据签名操作服务功能。 |
| 15 | 支持推送认证和推送签名功能，能够接收手机后台移动安全认证服务器的推送认证和推送签名消息，利用手机数字证书实现证书认证和证书签名功能 |
| 16 | 采用后台消息推送机制，解决医院多终端类型数字签名兼容性问题，支持PC、专业PAD/PDA或其他专业终端的数字签名。 |
| 序号 | 产品规格要求 |
| 1 | 设备高度：≥2U |
| 2 | 网络接口: ≥4个千兆网口 |
| 3 | 电源指标：≥1个工控电源 |
| 4 | 硬件加密卡：有 |

## 移动证书APP/SDK/小程序（移动端软件）

|  |  |
| --- | --- |
| 序号 | 功能指标要求 |
| 1 | 提供移动客户端的密钥生成、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，负责与移动安全认证服务系统进行安全通信，以协作产生签名密钥对、执行签名等任务。与移动安全认证服务系统共同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。 |
| 2 | 提供证书申请、下载、证书查看、口令修改、用户管理、日志管理等功能，（提供系统截图）移动客户端签名必须与本地部署的移动安全认证服务系统通讯实现安全的数字签名，不在第三方机构进行业务数据落地，防止用户隐私泄密。 |
| 3 | 提供数字签名、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，并能够针对终端获取对应的特征值与证书进行绑定 |
| 4 | 提供二维码扫码认证、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。 |
| 5 | 手机APP端可以设置支持安全可靠的免密签名功能。（提供系统截图） |
| 6 | 提供应用管理功能，对接入应用进行管理，包括应用的基本信息和接入状态。 |
| 7 | 可以灵活配置手机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。 |
| 8 | 支持手写签名信息添加和更新功能，手写签名方式支持直接通过手机屏幕手写签名、通过线下纸质签名后拍照和从相册中选择手写签名方式。 |
| 9 | 手机证书可以选择手势密码、口令密码、人脸识别等多种手段对数字证书和密钥运算因子进行安全保护。 |
| 10 | 支持密码管理功能，支持验证当前使用密码，修改证书密码和找回密码功能。找回密码支持短信找回密码和授权码找回密码方式。 |
| 11 | 能够基于现有常见的开发框架平台，以小程序方式提供移动端证书管理和应用服务，要求支持微信小程序、钉钉小程序和支付宝小程序。 |
| 12 | 手机端签名必须与医院本地部署的手机端后台系统通讯实现安全的数字签名，不在第三方机构进行业务数据落地，防止患者隐私泄密。 |
| 13 | 密码管理功能支持设置指纹密码签名，推送免密签名和扫码免密设置功能。设置指纹密码签名后即直接验证手机指纹即可完成签名；设置免密签名后，即可实现用户无操作状态下的自动签名功能。 |
| 14 | 支持环境IOS 9.0以上，Android 4.2以上 |
| 15 | 支持算法：  非对称算法：RSA1024、RSA2048、SM2  对称算法：DES、3DES、AES128、AES192、AES256、SM4  哈希算法：SHA1、SHA256、SHA512、MD5、SM3 |
| 16 | 算法性能  密钥对生成时间（ms）：  RSA1024 小于300ms/次，RSA2048 小于900ms/次，SM2 小于60ms/次  签名时间（ms）：  RSA1024 小于50ms/次，RSA2048 小于100ms/次，SM2 小于60ms/次  验签时间（ms）：  RSA1024 小于5ms/次，RSA2048 小于10ms/次，SM2 小于60ms/次 |

## 证书管理系统

|  |  |
| --- | --- |
| 序号 | 功能指标要求 |
| 1 | 能够实现与合法第三方CA机构运营系统对接，实现第三方权威数字证书的注册、受理、发放、状态变更等业务功能； 可与对接国内任意合法第三方CA机构对接，方便医院按需选择CA机构。 |
| 2 | 提供开发接口可以嵌入医院OA系统、人事管理系统等，在人员信息登记时直接下发数字证书申请权限，签发符合医生资格的身份数字证书。 |
| 3 | 签发的数字证书遵循x．509v3标准证书格式、符合《卫生系统数字证书格式规范（试行）》、《卫生系统电子认证服务规范（试行）》，支持自定义证书扩展域管理； |
| 4 | 证书业务办理（申请、更新）要求能同时支持三种模式的证书办理方式：一种是面对面由管理员代为进行系统资料填写、提交、证书业务办理的模式；第二种是由业务系统的用户的申请信息，由业务系统、用户身份管理系统或虚拟身份所在系统提供身份信息并进行审核。申请信息提交后审核由后台系统接口自动完成；第三种是要求RA系统面向应用系统提供证书申请、证书下载、证书更新、证书查询和验证等接口服务，即用户或管理员可以直接通过应用系统侧完成证书发放和状态管理功能； |
| 5 | 能够面向医院提供统一的数字证书服务，实现医护人员证书信息查询和管理；提供证书批量制作功能，支持用户信息的批量导入； |
| 6 | 系统管理功能：系统管理，包括对CA机构管理（可多CA机构接入）、用户管理、业务系统管理、系统证书管理、权限角色管理。能够实现对业务系统电子认证应用记录进行采集、管理、审计，提供电子认证应用信息监测、事后分析功能； |
| 7 | 能够提供详尽的查询、统计、报表功能，能统计用户、证书、机构、时间段内、应用领域等不同维度的证书发放和使用情况； |
| 8 | 能支持证书备案信息同步功能，同步的证书信息包括用户信息、证书信息、机构信息、时间信息、应用领域信息等； |
| 9 | 能够支持完整的权限管理功能，支持业务管理员、操作员、审计员多级管理机制； |
| 10 | 能够提供业务日志管理功能，能记录系统所有的业务操作日志，包括系统登录、权限变更、业务办理、系统维护等记录； |
| 11 | 能够提供数据备份、恢复功能，为管理员提供基于web页面的操作界面实现数据备份、恢复，降低系统维护复杂度； |
| 12 | 系统以及数字证书必须符合国家、行业、省市级以及《商用密码管理条例》、《中华人民共和国电子签名法》和《电子认证服务管理办法》等相关法规标准，能满足实际的业务环境要求，具备扩展性以满足定制化改造需求；应提供标准的、通用的、多样化的接口形态，并满足与各类应用系统的集成需求； |
| 13 | 支持SSL通道加密：提供通道加密功能，保障数据传输安全。 |
| 序号 | 非功能指标要求 |
| 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 |

## 电子签章系统

|  |  |
| --- | --- |
| 序号 | 功能指标 |
| 1 | 基于数字图像和数字签名技术，提供电子文档的电子签章功能，实现电子文档的数据真实性保护、完整性保护和抗抵赖保护。数字签名技术要求基于权威第三方CA认证服务，符合《中华人民共和国电子签名法》的要求。 |
| 2 | 提供控件支持医护人员个人USBKEY证书签章及手机APP证书签章。 |
| 3 | 电子签章信息可直接包含在文档中，打开文档即可实现完整性验证，当签章后的数据文档内容被篡改，系统要能校验出来并提示被篡改。 |
| 4 | 电子签章系统支持丰富的二次开发接口供集成，电子签章支持嵌入应用系统控制的各个流程，对各个审批环节进行电子签章；用户直接在应用系统的业务流程中打开文档，通过在应用系统中集成的电子印章功能，用户直接点击该按钮，由应用系统调用对应数字证书+电子印章，通过电子印章接口功能实现在应用系统中的电子签章功能。 |
| 5 | 电子签章系统支持后台的自动批量电子签章功能，面向应用提供标准接口，可以调用签名验签服务器上的数字证书和时间戳服务器签署时间戳，完成PDF格式文档的自动批量签章，签章包含权威时间戳信息。 |
| 6 | 电子签章系统支持后台的证书管理和印章管理，支持印章状态管理功能 |
| 7 | 系统管理功能：主要包括对电子印章、用户、证书、日志信息、统计查询和系统配置功能。 |
| 8 | 电子印章数据结构：电子印章数据结构符合《GM/T 0031-2014 安全电子签章密码技术规范》 |
| 9 | 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 |
| 10 | 提供独立的维护子系统，方便管理员通过web页面进行当前系统资源包括（CPU、内存、存储空间、应用运行状态等）监控，可以通过web页面实现版本更新和升级 |
| 11 | 支持双机、负载均衡 |
| 12 | 提供C、COM 、Java 等主流开发API |

## 数字证书

|  |  |
| --- | --- |
| 序号 | **功能指标要求** |
| 1 | 标识个人、单位、服务器等网络身份 |
| 2 | 符合卫生部《卫生系统数字证书格式规范（试行）》 |
| 3 | 符合卫生部《卫生系统电子认证服务规范（试行）》 |
| 4 | 证书格式标准遵循x．509v3标准 |
| 5 | 支持存放介质：智能USBKey、智能手机、PAD、PDA等智能移动设备 |
| 6 | 支持自定义证书扩展域管理 |

## 三、供应商资格要求

1、供应商须具有具有ISO20000信息技术服务管理体系证书

2、供应商须具有ISO27001信息安全管理体系证书

3、供应商须具有CCRC信息安全服务资质证书（信息系统安全集成）

4、供应商须具有ITSS信息技术服务标准符合性资质证书

5、参于本次项目的电子认证服务提供商须通过国家卫健委（原卫生部）测试、复审通过的电子认证服务机构，并提供公告复印件或网页公告截图；电子认证服务提供商须具备工信部颁发的有效期内的电子认证服务许可证以及国家密码管理局颁发的有效期内的电子认证服务使用密码许可证。

6、供应商为代理商参与投标的需出具电子认证服务商出具的针对本项目的原厂授权函及售后服务承诺函；