**采购项目概况**

# 1、背景及现状

南阳市口腔医院将以电子病历的无纸化为最终目标，在我院电子病历系统、HIS、LIS、PACS等医院信息系统中引入电子认证服务，建立基于数字证书的电子认证服务体系和基于数字证书的应用安全支撑体系，切实保障本院信息系统的信息安全，也能提供本院网络医院的信息安全保障。

# 2、项目建设目标

为实现全院医、护、技电子签名为目标，保障我院电子病历系统等的业务信息安全，需依据《卫生系统电子认证服务管理办法（试行）》、《医疗机构病历管理规定(2013 年版）、《电子病历应用管理规范（试行）》及相关标准规范要求，建立全院统一的电子认证服务体系和业务应用安全支撑体系，实现“可信身份、可信数据、可信行为、可信时间”的目标，保证电子病历、网络医院平台的真实可信和合法有效性。

项目建设目标有：

1）建立我院统一的电子认证服务体系，面向我院医、护、技工作人员，统一数字证书发放与管理，提供优质的、符合卫生行业规范的数字证书生命周期服务，满足医院的实际需要。

2）建立我院电子病历系统等医院信息系统统一的业务应用安全支撑体系，设计合理的、实用的医院可信医疗业务建设方案，实现电子认证服务和相关技术与医院信息系统的有机集成结合，有效提升医院电子病历等系统的业务信息安全保障水平，构建安全可信的医院医疗业务环境，保证电子病历数据的真实性、完整性、有效性。

# 3、项目建设内容和要求

3.1电子认证服务体系建设要求

总体要求：满足卫计委对电子认证服务体系的要求；满足医院等级评审对电子认证服务体系的要求；满足河南省卫生厅数字化医院对电子认证服务体系的要求。建立我院的电子认证服务体系，从服务内容、服务模式、服务流程、服务保障等方面，设计符合我院特点的服务模式和流程等，方便证书发放和管理，满足我院实际业务需要。

具体满足以下要求：

1）提供证书全生命周期服务，包括证书申请、发放、更新、吊销、介质解锁、丢失补办、损坏重办等服务内容，方便医院用户获取证书服务；

2）提供证书的静默更新模式，确保在医院内网环境下不影响数字证书应用系统自身的业务连续性，不影响医护人员工作。

3）提供证书快速应急服务，满足医院对业务连续性的要求；

4）支持按照医院实际应用需要，灵活定制服务交付的业务流程；

5）提供灵活配置证书模版功能，支持自定义扩展项；

6）支持多种证书存储介质包括智能USBKey、智能射频卡等，满足医院对一证多用、一卡多用的特殊需求；

7）提供管理员管理、系统管理等日常服务；

8）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，满足我院日常管理需要。

3.2可信医疗服务建设要求

根据我院电子病历系统等医院信息系统的实际安全需求，设计基于数字证书的应用安全支撑体系，通过证书及证书应用相关产品和技术，实现电子认证服务与医院业务应用的有机结合，解决医院电子病历系统等系统的身份认证、授权管理、责任认定等安全问题，解决电子病历的真实性、完整性、有效性等问题，建立安全可信的医院医疗业务环境。

具体满足以下要求：

1）全面分析我院电子病历系统等信息系统的应用安全需求，提出针对的、完善的应用安全支撑体系整体框架，并阐述具体的证书、证书应用产品或证书应用技术构成；

2）分别阐述应用安全支撑体系在医院电子病历系统、HIS系统等的应用集成方案，详细说明集成的业务环节和业务流程等，详细阐述在B/S、C/S、C/DB等各类系统架构下的应用集成方式，并满足医院对业务安全、应急处理和业务连续性的要求；

3）详细分析阐述电子签名值的存储方式，并提供能够优化存储、减少空间占用的实用技术方案，有效降低电子签名值的存储占用空间；

4）选用的证书应用产品或应用技术应满足医院信息系统的业务环境以及性能的要求，具备扩展性以满足医院定制化改造需求；应提供标准的、通用的、多样化的接口形态，并满足医院PB、Delphi、VC/VB/.Net、Java、Flash等各类开发平台和技术的实际集成需要；

# 4、售后服务和技术支持要求

提供完善的售后服务和技术支持方案，包括但不限于以下内容：

1）按照投标技术方案，提供应用安全支撑体系医院信息系统中的集成技术支持服务；

2）所投标软件产品质保期不低于一年，硬件服务器产品不低于一年（软硬件产品质保期以系统上线验收完成日起算），证书介质质保一年，证书服务一年；并说明质保期后的售后服务内容和收费标准；

3）在系统建设、使用、运维等过程中遇到问题时，都能够得到投标人相应的技术支持与帮助；

4）提供全面、灵活的服务支持方式和手段，包括不限于网站服务、热线支持、邮件支持、现场支持等。

# 5、供货清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1.医、护、技签名产品清单如下： | | | | |
| 应用支撑产品部分 | | | | |
| 编号 | 设备名称 | 分类 | 产品功能 | 数量/单位 |
| 1 | 数字签名验证服务器 | 硬件 | 基于数字证书实现用户可信身份认证、可靠电子签名 | 1台 |
| 2 | 时间戳服务器 | 硬件 | 实现可信时间戳功能 | 1台 |
| 3 | 电子签章系统 | 软件 | 与电子病历系统集成，实现数字签名可视化 | 1套 |
| 4 | USBKey | 硬件 | 32位CPU，64K证书/密钥存储 | 300个 |
| 5 | 个人证书 | 证书服务 | 标识个人的网上身份 | 300张/年 |
| 6 | 服务器证书 | 证书服务 | 标识各类设备的网上身份 | 2张/年 |
| 7 | 单位数字证书 | 证书服务 | 标识各单位内部部门等机构的网上身份 | 1张/年 |
| 8 | 签名应用系统 | 应用软件 | 实现医院信息系统软件与CA签名服务器对接 | 1套 |

# 6、产品选型要求

投标人所投产品须满足国家卫计委卫生系统电子认证服务相关技术规范，符合国家密码管理局对商用密码产品的规范要求。

投标人所投产品至少应包括下述产品，产品具体指标上应满足如下要求：

（1）、医、护、技签名

1. 数字签名验证服务器：

|  |  |  |
| --- | --- | --- |
| 序号 | 功能指标 | |
| 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，支持RSA算法 | |
| 2 | 提供文件数字签名和验证功能, 支持对文件进行MD5、SHA-1等方式的数字摘要后在进行签名 | |
| 3 | 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。 提供证书更新功能 | |
| 4 | 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 | |
| 5 | 提供CRL的证书有效性验证，CRL更新配置可自动定时进行。 | |
| 6 | 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。 | |
| 7 | 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。 | |
| 8 | 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。 | |
| 9 | 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。 | |
| 序号 | 非功能指标 | |
| 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 | 支持双机、负载均衡 | |
| 4 | 提供C、COM 、Java 等主流开发API | |
| 5 | SM2算法签名能力850次/秒 | |
| 6 | 适用环境：千兆环境，并发用户多 | |
| 7 | 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 | ≥1U |
| 2 | 网络接口 | ≥2个千兆网口 |
| 3 | 电源指标 | ≥1个工控电源 |

1. 时间戳服务器

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | | 功能指标 | |
| 1 | | 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 | |
| 2 | | 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 | |
| 3 | | 支持算法：RSA、SHA1、SM2、SM3 | |
| 4 | | 权威国家时间源：产品内置国家授时中心时间源,提供多种授时方式，包括：CDMA、北斗2、GPS | |
| 5 | | 时间同步: 支持NPT、SNTP时间同步协议 | |
| 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 | |
| 序号 | | 非功能指标 | |
| 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 | | 支持双机、负载均衡 | |
| 3 | | 提供C、COM 、Java 等主流开发API | |
| 4 | | 时间戳签发效率(SM2) 1000次/秒;验证效率(SM2) 500次/秒. | |
| 序号 | | 产品规格要求 | |
| 1 | 设备高度 | | ≥1U |
| 2 | 网络接口 | | ≥2个千兆网口 |
| 3 | 电源指标 | | ≥1个工控电源 |

1. 电子签章系统：

|  |  |
| --- | --- |
| 序号 | 功能指标 |
| 1 | 支持第三方CA机构签发的数字证书。支持电子印章图片写入证书存储介质中，并与证书绑定。 |
| 2 | 提供基于Web界面的电子印章的制作和管理功能，提供日志审计功能。 |
| 3 | 支持自动生成电子印章图片，或支持采集的手写签名。 |
| 4 | 支持对多种文档格式如word\excel\html等的电子签章，实现数据完整性保护，确认签章者身份 |
| 5 | 支持原文、印章图片、数字签名的绑定，能够防止篡改。 |
| 6 | 提供电子签章中间件，满足C/S环境的电子签章集成 |

1. 证书存储介质：USBKey

|  |  |  |
| --- | --- | --- |
| 序号 | 功能指标 | |
| 1 | 符合卫生部《卫生系统数字证书介质规范（试行）》 | |
| 2 | USBKey容量<=64K Bytes | |
| 3 | USB Key为标准USB 1.1设备，支持USB2.0接口 | |
| 4 | 功耗<400毫瓦 | |
| 5 | 支持的证书X.509 V3规范标准 | |
| 6 | 数据存储时间不小于10年，可擦写50万次以上；平均故障间隔时间（MTBF）≥4000小时；工作温度：0℃ - 40℃，工作湿度：25%-80%，贮存温度：-10℃ - 55℃，贮存湿度：≦95%（40℃） | |
| 7 | 支持遵循国家相关规定的非对称、对称、摘要等加密算法， | |
| 8 | USB Key自身的安全要求：具备完善的PIN校验保护功能;USB Key内应至少支持建立三级应用；支持多应用，各应用间相互独立；支持多种文件类型（二进制、定长记录、变长记录、循环记录）; 能无缝挂接Microsoft Internet Explorer、Mozilla等主流浏览器，并完全支持HTTPS协议的应用 | |
| 序号 | 非功能性指标 | |
| 1 | 公钥私钥对生成时间<=30秒 | |
| 2 | 数字签名和验证时间<1秒/次 | |
| 3 | RSA加密速度>50kbps，RSA解密速度>30kbps | |
| 4 | | 支持硬件真随机数发生器  存储要求a) 公私钥对>=2个，b)必须在提供保护口令前提下才能访问密钥 |

1. 数字证书：个人证书

|  |  |
| --- | --- |
| 序号 | 功能指标 |
| 1 | 标识个人用户网络身份 |
| 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 |
| 6 | 支持自定义证书扩展域管理 |

1. 数字证书：服务器证书

|  |  |
| --- | --- |
| 序号 | 功能指标 |
| 1 | 标识设备网络身份 |
| 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 | 支持自定义证书扩展域管理 |

1. 数字证书：单位证书

|  |  |
| --- | --- |
| 序号 | 功能指标要求 |
| 1 | 标识单位用户网络身份 |
| 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 |
| 6 | 支持自定义证书扩展域管理 |

# 签名应用系统

实现医院信息系统软件与CA签名服务器对接。