**移动数字证书认证维护费项目**

1. 总体要求：

随着医院信息化建设日趋成熟，HIS、LIS、PACS、RIS、电子病历等信息系统得到充分的应用，医院正在向信息化、现代化、数字化方向不断迈进，信息化高效的工作效率为患者带来了方便，也为医院带来了更直接的经济效益，同时也减轻了医务人员的手工工作压力。

医院的日常工作会产生大量的文件，包括处方、医嘱、病史记录、健康档案等，每个文件都必须有责任医生的签名而产生法律效应。随着医院信息化管理系统的全面实施，每天要分类产生和存档的电子文件越来越多，如何利用电子签名技术，取代纸面文件签名的程序，保证电子文件的法律效力，保护医患双方的合法权益，已成为越来越多的医院管理层关注的问题。

《中华人民共和国电子签名法》于2005年4月1日起正式实施，令电子签名与手写签名和盖章具有同等法律效力。医疗机构的电子文书亦属于电子业务范畴。通俗地讲，电子签名就是在使用的电子文件中，能够识别交易人的身份，保证交易安全，起到与手写签名或者盖章同等作用的电子技术手段。我国《电子签名法》的立法重点是：确立电子签名的法律效力；规范电子签名的行为；明确认证机构的法律地位及认证程序；规定电子签名的安全保障措施。该法律的颁布实施，为医疗机构已经开展的电子病历和电子文书档案的研究和开发，创造了有利的法律环境。

2009年12月卫生部特制定颁布了《卫生系统电子认证服务管理办法》，该办法于2010年1月1日实施。《卫生系统电子认证服务管理办法》使得卫生系统中电子认证有法可依，有效保障卫生信息系统安全，规范卫生系统电子认证服务体系建设。

目前肿瘤医院已经结合本院实际情况，引入权威第三方电子认证，建设了较为全面的以移动数字证书认证PKI/CA为基础的应用安全防护和网络可信认证体系，设计了从服务内容、服务模式、服务流程、服务保障等方面符合全院特点的服务模式和流程等，为医院医护人员、就医患者和信息系统提供基于移动数字证书认证的身份认证、数字签名、签名验证、电子签章、手写数字签名、可信时间戳、数据加解密等电子认证服务和应用安全保障能力支撑，为医疗信息系统实现可靠身份认证、授权管理、责任认定以及隐私保护提供基础。

本项目需要采购权威移动数字证书认证系统维护服务，为医疗信息系统实现可靠身份认证、授权管理、责任认定以及隐私保护业务支撑提供技术维护服务。

2.服务/运维对象及地点

运维对象：

* 电子认证服务器 2套
* 签名验证服务器 2套
* 云医签（单机版） 2套
* 电子认证管理服务器 1套
* 手写签名服务器 1套
* 财政电子票据数字签名验签系统 2套

3.周期：周期一年。

4.服务及维护清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 一级 | 二级 | 描述/型号 | 数量 | 指标重要性 |
| 1 | 电子认证服务器 | 电子认证服务器 | 主要实现医院数字签名、签名验证、可信时间戳等服务，实现医护人员签名验证、单位主体数字签名和权威第三方时间戳签署权威认证 | 2 |  |
| 2 | 证书管理系统 | 证书管理系统 | 主要实现数字证书的申请、下载、更新、吊销、查询等证书生命周期管理功能 | 1 |  |
| 3 | 移动安全认证服务器 | 移动安全认证服务器 | 主要面向移动终端数字证书认证模块，基于密钥分散算法实现密钥的安全生成、保存、使用、销毁功能，同时面向移动终端实现数字证书发放管理、数字证书认证、签名功能，并面向应用提供扫码认证/签名、推送认证/签名功能 | 2 |  |
| 4 | 移动安全中间件 | Android和IOS手机证书软件 | 主要提供给医护人员使用，实现智能手机终端的密钥安全管理和使用，医护人员手机数字证书申请下载安装、更新、吊销、证书认证、扫码认证、扫码签名、推送签名等功能场景应用 | 2 |  |
| 5 | 电子签章服务器 | 电子签章服务器 | 主要实现医院电子印章管理和电子签章、签章验证功能，实现电子文档签署者身份认证、文档内容完整性保护和业务抗抵赖功能 | 1 |  |
| 6 | 手写数字签名服务器 | 手写数字签名服务器 | 主要面向患者提供手写数字签名服务，支持通过采集手写数字签名指纹屏上的手写数字签名、指纹、影像信息，实现电子文书的手写数字签名 | 1 |  |
| 7 | 财政电子票据数字签名验签系统 | 财政电子票据数字签名验签系统 | 主要面向电子票据系统，提供符合财政要求的数字签名、签名验证、电子印章功能 | 2 |  |
| 8 | 手写数字签名指纹屏 | 手写数字签名指纹屏 | 主要包含手写数字签名屏幕、指纹采集仪、摄像头等设备，提供给用户进行手写数字签名过程使用。 |  |  |

5.日常服务/维护内容

* + 1. 项目故障处理

1）硬件故障维修：

* + - * 当硬件服务器故障时，需要进行硬件维修，如果无法维修，则进行同配置硬件更换；
      * 如果更换配件或服务器导致软件和数据库工作异常，需要进行软件重新部署和数据迁移。

2）软件故障排查：

* + - * 软件重启，当软件运行故障停机后，需要配合实现软件服务的重新启动和必要的运行配置；
      * 软件运行环境故障排除，当软件运行环境出现故障时，需配合进行运行环境故障排除；
      * 软件BUG升级修复，当软件出现系统故障或者BUG时，需配合进行运维升级，修复故障或BUG。

1. 使用故障处理
   * + - 当管理员在进行后台配置管理或者参数设置出现故障时，需配合进行故障修复处理；
       - 当用户在使用CA认证服务过程中，出现故障无法使用的情况时，需配合进行故障修复处理，确保用户可以正常使用。

二、系统升级服务

1）系统运维升级

* + - * 因CA软件系统本身的故障，进行系统运维升级；
      * 因CA软件系统运行环境的变化，需要进行的必要的运维升级

2）系统漏洞修复

* + - * 因客户信息安全保护要求的必要的系统安全漏洞补丁服务

三系统日常运维

1）系统巡检

* + - * 系统的例行巡检，检测服务器运行状态。标准服务：每6个月巡检一次
      * 系统巡检时的数据备份操作

2）特殊应急保障

* + - * 应要求的节假日或者特殊时间应急保障服务

3）配置参数变更

* + - * 必要的系统运行参数配置变更

4）服务使用情况统计

* + - * 应用户要求的服务是情况数据统计

5）日常咨询服务

* + - * 日常的电话、微信、QQ、邮件等远程方式的客户技术、运维、使用咨询服务

6.功能完善及扩展性服务/维护

1）需求定制开发：当系统运行过程中，如需要优化系统功能或者进行特殊场景的支持，需供应商能够支持系统使用过程的客户化二次需求开发服务，双方可以针对定制开发工作量进行核算。

2）应用集成对接支持：当系统运行过程中，有新的应用系统需要使用CA认证接口，需要供应商可以进行接口集成培训、应用接口集成配合，应用接口集成过程中的故障排查配合，应用集成后上线过程的必要配合，双方可以根据实际投入进行工作量核算。

1. 服务/维护要求及方式

1）电话/电子邮件技术支持

用户在数字证书的申请、更新和解锁等环节中如遇到业务办理或证书产品使用问题，可以通过客服热线、电子邮件方式进行咨询。如在证书登录、电子签名、电子签章等环节中遇到的各类证书应用的技术性问题，可通过热线电话、电子邮件等寻求帮助。

服务时间：7\*24小时

2）现场技术支持

用户在数字证书的申请、更新和解锁等环节中如遇到业务办理问题以及用户在证书登录、电子签章等环节中遇到的各类证书应用问题或产品使用问题，可以派遣技术工程师至用户现场协助解决问题，支持次数不限，紧急情况下要求4小时内到达现场。

服务时间：7\*24小时

3）远程技术支持

用户在数字证书的申请、更新和解锁等环节中如遇到业务办理问题以及用户在证书登录、电子签名、电子签章等环节中遇到的各类证书应用问题或产品使用问题，通过用户提供的VPN、远程桌面等进行远程检查和修复。支持次数不限。

服务时间：7\*24小时

4）巡检服务

每年定期至客户现场进行巡检，巡检内容包括：产品硬件设备、软件服务、应用等方面的检查和备份记录，并提交用户确认。

1. 投入人员：驻场0人，实施4人等
2. 服务/运维价格是否一次谈判三年有效，是 □否
3. 其他要求（数据统计、巡检服务、培训要求、供应商资质等）

供应商须具备工信部颁发有效的电子认证服务许可证和国家密码局颁发的电子认证服务密码许可证、电子政务电子认证服务机构相关证明。

供应商须通过卫生部电子认证服务接入测试。

ISO/IEC27017:2015云服务信息安全管理体系认证证书

ISO/IEC27701:2019隐私信息管理体系认证证书

ISO/IEC27001:2013信息安全管理体系认证证书

ISO/IEC20000-1:2018信息技术服务管理体系认证证书

ISO45001职业健康安全管理体系认证证书

信息系统集成及服务资质证书三级

信息系统安全集成服务资质二级

信息系统安全运维服务资质二级

信息系统风险评估服务资质三级

\*指标按重要性分为“★”、“☆”、“#”和“△”。★代表实质性指标，不满足该指标项将导致投标被拒绝，☆代表优质优价指标，#代表重要指标，△则表示一般指标项。