**数字证书年费项目**

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第三方电子认证服务机构的数字证书年费，为医护人员提供权威第三方电子认证服务，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。

1. 服务/运维对象及地点

1）服务/运维对象为医护人员，本项目主要采购医护人员数字证书服务，用于医护人员业务操作过程中的数字证书认证服务。

2）服务/运维对象为医院单位主体，本项目采购单位数字证书，用于单位主体电子签名时的数字证书认证服务。

1. 周期：2024年度一年。
2. 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 | 数字证书服务 | 个人数字证书 | 个人数字证书 | 5000 | 25元/个/年 |
| 2 | 数字证书服务 | 单位数字证书 | 单位数字证书 |  |  |

1. 日常服务/维护内容
2. 数字证书的签发、更新、注销、变更、查询、验证服务。
	* 数字证书格式符合卫生部《卫生系统电子认证服务规范（试行）》，符合卫生部《卫生系统数字证书格式规范（试行）》；服务提供商须通过卫生部电子认证服务接入测试，并具有相关证明文件。
	* 数字证书服务的提供方能够实现与上海市卫生健康行业市级电子认证平台对接，实现数字证书的注册、发放、备案等业务功能。
	* 数字证书支持现有医院基于智能手机移动终端的签发、管理、扫码认证/签名、推送认证/签名应用场景。
3. 数字证书发放使用过程的客户服务支持、使用指导培训、使用故障处理、应急措施处置服务。
	* ☆需要有本地化的客户服务团队提供日常的证书发放、使用服务支持。
	* ☆需要有本地化的技术支持团队提供日常的使用故障处理和应急处置服务。

3）☆权威第三方电子认证签名举证服务：当医护人员使用数字证书服务完成电子签名后，如发生需要举证数据完整性和业务不可抵赖性场景时，可以提供权威第三方举证服务。

1. 功能完善及扩展性服务/维护

#能扩展提供SSL站点证书，包括国际RSA证书和国密SM2证书，证书兼容性及安全性要求：RSA算法兼容目前主流的浏览器和平台，Firefox 6.0及以上、Android 4.0及以上、IOS 5及以上、java 6u45及以上、Windows XP及以上、OS X 10.9及以上，要求证书为国产自主品牌（提供商标注册证），具备自主管理、审核、签发证书的能力，审核数据不能出境，提供签发界面截图。以上两点必须同时具备。SM2算法兼容360安全浏览器、奇安信可信浏览器、海泰安全浏览器、赢达信安全浏览器。

#提供SSL证书申请、审核、签发、安装、备份、故障处理的全程一对一VIP人工服务。

#签发SSL证书的关键信息基础设施均应在国内有机房、数据库支持，保证整体证书签发业务可用性需大于99.95%。

#SSL证书后台有OCSP\CRL不间断服务，支持国内的OCSP\CRL查询，服务均受国内网络优化，可用性需大于99.99%。

1. 服务/维护要求及方式

△为本项目提供7\*24小时的售后服务，建立一整套完善的签发部署备份的规范流程，集中一批高水准的业务支持团队，提供自签发、部署、技术咨询等全方位的技术支持服务。

服务形式主要有以下两种：

△远程支持服务：通过远程接入的方式与客户的技术人员实现网络联接，远程对问题进行检查、排故、和分析。所指派固定服务技术人员仅在得到甲方许可并确保对所访问的网页安全、数据完整性的情况下才可进行相关操作。

☆现场服务：在特殊情况下，按照甲方的需要进驻场地提供支持服务，解决故障等突发性问题。

投入人员：驻场0人，实施2人等

1. 服务/运维价格是否一次谈判三年有效，□是 ■否
2. 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