**全院医护电子签名认证信息系统**

**用户需求书**

# 项目背景

根据我院LIS、HIS、PACS、电子病历系统等医院信息系统及互联网医院的实际安全需求，设计基于数字证书的应用安全支撑体系，通过CA数字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，以满足PC端和移动端医院信息平台在身份认证、授权管理、责任认定等方面的信息安全需求。可对HIS、电子病历、LIS、PACS等系统实现电子签名和加盖时间戳，解决医院信息系统的身份认证、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，逐步确立数字证书认证技术在我院信息化进程中信息安全保障的基础地位，并逐步实现完全无纸化的全院安全认证平台。整个系统建设须满足《中华人民共和国电子签名法》、《中华人民共和国密码法》以及《电子病历应用管理规范（试行）》等相关法律法规要求。

# 项目建设清单

|  |  |  |
| --- | --- | --- |
| **序号** | **建设内容** | **详细技术要求** |
| 1 | 协同签名系统 | 1. 产品支持基于数字证书的安全认证登录管理功能，能实现多种角色管理，包括但不限于管理员、操作员、审计员等
2. 支持基于服务端的签名任务发起和签名结果获取
3. 基于协同密钥技术来实现移动端用户私钥的生成和使用
4. 支持在线、离线证书签发模式、日志及审计功能
5. 支持用户量、签名量、证数量的统计分析
6. 支持一人多设备、一设备多人的应用场景；
7. 支持个人限制单证书的开关，关闭时同一个用户可在多个设备下载证书
8. 支持授权签名：用户只需要使用手机在PC端完成一次授权即可多次签名，并可以关闭授权
9. 支持推送签名：用户以推送的方式发起签名，签名者在手机端收到推送后直接完成签名；支持在签名任务中添加签名描述信息
10. 支持通过管理页面设置签章图片
11. 支持通过系统唯一用户标识绑定用户身份
12. 支持批量离线签发数字证书
13. 支持通过页面批量导入用户基础信息，支持通过页面批量导入用户签章图片
14. 支持通过接口添加用户信息，支持CRL配置和根证书配置，支持标准签名验证，能够与USBKey签名互通，支持证书有效性验证
15. 持系统状态一键检测
16. 支持通过NTP进行时间同步
17. 支持双机和集群部署
18. 支持通过轮询或注册回调方式获取签名结果
19. 高度：≤2U，网络接口：≧2\*1000M
20. CPU≧3.5GHz 四核，内存≧1\*8G，硬盘≧2\*2T
21. 服务端签名性能≧300TPS，客户端签名性能≧5000TPS
22. 电源指标：工控电源，双电源
23. 所投协同签名系统具备《商用密码产品认证证书》,提供证书复印件并加盖投标人或制造厂商公章。
24. 所投协同签名系统具有IPv6 Ready Logo认证证书，提供证书复印件并加盖投标人或制造厂商公章。
25. 所投协同签名系统具有CMA、CNAS认证的第三方公证地位的检验机构出具的检验检测报告，提供报告复印件并加盖投标人或制造厂商公章。
 |
| 2 | 时间戳服务器 | 1. 提供时间戳签发和验证服务
2. 内置权威时间源模块，信号源4G/5G、GPS、北斗三合一，符合国家授时中心的时间精度标准，并且经国家授时中心的权威鉴定测试，时间误差＜2毫秒；
3. 授时精度0.5-3ms(毫秒)，守时精度<1ms（72小时）
4. 内置恒温晶振，日老化率5E-10，秒稳定度优于2E-11，日平均准确度优于1E-12
5. 输出标准时间信号包括公历（年、月、日、时、分、秒）
6. 对外可提供高稳定、高性能的服务，支持热备负载功能
7. 支持黑白名单访问策略，采用动态更新方式
8. 支持国密算法SM2、SM3
9. 系统支持可视化管理，包括时间戳签名统计、系统监控、设备硬件及软件的运行状态监测功能
10. 支持系统日志审计、业务日志保存、业务日志查询等功能；
11. 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
12. 时间戳签发效率：SM2签发不低于1000次/秒次/秒，SM2验证不低于500次/秒
13. 所投时间戳服务器具备国家密码管理局颁发的《商用密码产品型号证书》，提供证书复印件并加盖供应商或制造厂商公章。
14. 所投时间戳服务器通过国家网络与信息系统安全产品质量监督检验中心的漏洞覆盖测试，并获得《信息技术产品安全测试证书》，提供证书复印件并加盖供应商或制造厂商公章。
 |
| 3 | 移动端APP或SDK | 1. 移动端提供SDK和APP两种形态模块
2. 移动端支持基于激活码下载证书和扫码下载证书
3. 移动端支持基于签名任务id和扫码签名
4. 移动端APP支持扫码签名、推送签名
5. 移动端APP支持通过扫码或手动方式配置服务端
6. 移动端APP要能够在Android应用市场和苹果AppStore中已经发布
7. 移动端SDK支持批量拉取签名任务：支持批量拉去待签名任务
8. 移动端SDK支持传PIN码签名：支持通过传入PIN码的方式进行签名。
9. 移动端支持通过PIN码或指纹进行认证后签名；
10. 移动端SDK支持开启和关闭指纹。
11. 所投移动端APP或SDK具备移动智能终端安全密码模块《商用密码产品认证证书》,提供证书复印件并加盖供应商或制造厂商公章。
 |
| 4 | 个人数字证书 | 1. 标识用户人员用户网络身份
2. 数字证书应支持SM2等国产密码算法
3. 密钥由移动终端和服务器协商产生，采用密钥分割技术保存密钥
4. 支持自定义证书扩展域管理
 |