**云南大学附属医院全院数字认证系统功能需求**

# 基础应用安全支撑功能

针对医院内部业务系统运行环境、架构复杂，经过在各大医院的项目实施经验，针对应用模式和方案设计进行深度优化，能够满足医院B/S、C/S、C/DB等各类系统架构；Windows、Linux、AIX、Solaris、Unix等各类系统运行环境下的应用。

## 身份认证

用户（如医生等）使用数字证书USBKey登录电子病历客户端，电子病历客户端通过调用客户端控件和数字签名验证服务器实现对存储于USBKey内数字证书的读取、解析、验证和展现，实现基于数字证书的安全登录。

## 数字签名和验证

数字签名验证服务器实现基于数字证书的身份认证、数字签名、数据加密等功能，核心是将提交的医疗数据进行数字签名，以保证数据的不可抵赖性、完整性需求，并在查询相关数据时，实现用户对于所查询的数据的有效性验证。通过部署数字签名验证服务器实现电子病历生成等医院内部重要业务环节中的数字签名及验证。

## 可信时间戳

通过集成部署时间戳服务系统，可以有效证明电子数据的有效性及产生时间，将经签名的一个可信赖的日期和时间与特定电子数据绑定在一起，为服务器端应用提供可信的时间证明，为医院提供可信时间服务。

## 电子签章

在电子信息世界，数字签名是隐藏在电子文档中的一串字符，不能像现实世界的电子签名一样直接展现给用户，通过依托成熟产品—电子签章系统，在医嘱单、检验单等医疗过程中实现电子签章功能，实现了电子病历中数字签名的可视化、图形化，使可靠电子签名在电子病历中可形象展现，并提供方便的签章验证辨伪操作界面。

# 2.知情文书患者电子签名功能（患者签名）

病人或家属知情文书的无纸化签署，采用手写数字签名模式，由信手书手写签名系统根据当事人个人身份信息、手写签名笔迹数据、当前可靠时间信息以及部分辅助证据（例如指纹采集或签署时摄像头采集的的照片的数据）为当事人签发数字证书，并完成对电子文档的数字签名。

# 3.移动端电子签名应用功能

结合医院移动查房的实际情况，为解决医护人员的电子签名问题，并生成与纸质文档同等法律依据效力的电子化文档，实现全院查房“无纸化”工程，应用安全产品需与移动医疗系统进行集成开发。

# 4.互联网医院电子签名功能

互联网医疗网域内部署“移动协同签名系统”，为医院互联网医疗应用提供移动签名服务，包括身份认证、数据签名等；

业务系统通过服务端SDK进行集成对接，实现身份认证、电子签名、时间戳、电子签章等功能；

“移动协同签名系统”本地化部署，以患者为中心的所有诊疗数据全部保存在医院内部，保证所有数据不出医院，从而保障患者数据的安全性、保密性。

# 5.产品详细功能

## 签名验签专用设备

**功能指标：**

1. 支持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，支持国产密码算法
2. 支持证书验证功能，支持对X.509 Version 3、PKCS系列证书的DER和PEM格式的应用与验证
3. 支持数据加密、解密功能，支持数字信封加密，支持国产密码算法
4. 支持CRL的证书有效性验证，CRL更新配置可自动定时进行
5. 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。
6. 支持备份恢复功能，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
7. 支持日志记录，可将日志以syslog的方式发送到指定服务器
8. 支持双机、负载均衡
9. 支持C、COM、Java等主流开发API
10. SM2签名不小于2000次/秒。

## 时间戳专用设备

**功能指标：**

1. 支持时间戳的签发及验证功能
2. 支持多种时间戳服务接口，满足各类应用开发平台调用
3. 支持可信时间发布功能
4. 支持时间同步机制
5. 支持时间源签名服务加密设备的配置管理
6. 支持第三方CA证书导入、导出、备份和恢复等管理功能
7. 支持应用平台：Windows server; Linux；AIX；Solaris；Unix
8. 支持应用接口：Java、C、COM
9. 支持算法标准：SM2、SM3
10. 支持时间源管理：支持GPS或北斗或4G授时方式
11. SM2签名不小于1000次/秒。

## 电子签章系统

### 电子签章系统软件

**功能指标：**

1. 支持第三方CA机构签发的数字证书
2. 支持基于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. 支持电子印章图片写入证书存储介质中，并与证书绑定
4. 支持自动生成电子印章图片，或支持采集的手写签名
5. 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

### 电子印章制作服务

**功能指标：**

1. 提供基于手写签名采集的制章服务。

## 证书管理专用设备

**功能指标：**

1. 收集证书应用环境发起的证书更新请求，再统一由证书管理服务器管理员批量更新证书并由证书应用环境自动更新证书，证书更新支持移动端和PC端在线和离线更新。
2. 系统提供网页版证书在线帮助、证书应用环境下载页、更新包导入。
3. 系统提供机构管理功能，实现在多机构共用证书管理服务器时的信息分类；系统管理员可以按照机构名称查询证书更新状态信息。
4. 系统支持查看系统状态、配置系统IP/端口，管理员管理、时间源管理、设备编号管理、日志管理、服务管理、备份恢复等功能。
5. 系统支持配置网络时间同步服务器及同步策略，实现与时间源的时间同步校对。
6. 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
7. 提供日志记录，可将日志以syslog的方式发送到指定服务器
	1. **移动签名专用设备**

**功能指标：**

1. 支持同步用户接口，支持注册应用用户
2. 支持认证服务接口，支持基于数字证书的身份认证方式
3. 支持数据签名服务接口，支持业务系统发起签名请求，服务器与用户手机完成协同签名。
4. 基于标准PKI验证过程，支持验证PKCS1/PKCS7标准格式的电子签名，包括验证签名及证书有效性等
5. 支持扫码签名、推送签名功能
6. 支持单个签名、批量签名和自动签名功能
7. 支持原生APP（Android和IOS），在应用市场中可以直接下载
8. 支持SDK开发包，供第三方APP集成。
9. 移动客户端运行环境：Android 4.2及以上、iOS8及以上版本
10. 支持Java、C、COM、WebService应用接口
	1. **患者手写数字签名系统**

### 手写数字签名专用设备

**功能指标要求：**

1. 申请和获取签名数字证书。根据签名业务及签名人鉴证信息，向电子认证服务机构证书服务平台申请颁发用于手写签名的一次性数字证书。
2. 通过手写数字签名终端，获取签名人手写签字笔迹，作为数字签名可视化展现效果图示。
3. 使用数字签名密码算法，对知情同意书进行密码运算，保护知情同意书的有效性。
4. 提供知情同意书的存储、归档、展现、验证举证服务。支持知情同意书共享、同步到电子病历系统。
5. 支持的应用环境Windows server2000/2003/2008;Linux;Unix
6. 提供C、 Java 等主流开发API
7. 业务处理能力不小于100000笔/小时；

### 手写数字签名板

**功能指标：**

1. 手写签名采集：通过显示屏签名板采集签名笔迹
2. 指纹采集：集成指纹采集模块
3. 电源：USB总线供电
4. 扩展：支持USB扩展，如二代身份证读取
5. 内置密码芯片，支持国产密码算法
6. 兼容性：windows XP/vista/win7/win8/win10
7. 显示屏尺寸：手写屏显示效果流畅，屏幕显示不小于10.1寸
8. 屏幕比率：手写屏须提供支持将PC界面在手写签名屏的屏幕上扩展显示，屏幕显示比例不小于16:10；
9. 有效显示区：手写签名屏根据签名需要能够最大化显示签名区域，要求有效显示区域不少于216.96 (W)X135.6 (H)mm规格要求；

## 数字证书

### 个人数字证书

**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

### 设备证书

**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

## 证书存储介质USBKEY

**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. USB Key为标准USB 1.1设备，支持USB2.0接口
3. USB Key支持PC/SC驱动，支持智能卡登录
4. USBKey容量>=64K字节
5. USB Key自身的安全要求：具备完善的PIN校验保护功能
6. 支持国产密码算法、支持第三方算法下载
7. 公钥私钥对生成时间<=30秒
8. 数字签名和验证时间<1秒/次
9. 支持硬件真随机数发生器

# 6.产品清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **产品描述** | **单位** | **数量** |
| **1** | **医护技人员软硬件产品部分** |
| 1.1 | 签名验签专用设备 | 实现基于数字证书的身份认证、数字签名、数据加密等功能本产品对外提供基于数字证书的身份认证服务、数据签名与签名验证服务、加解密服务和数字信封服务；支持Windows、Linux、AIX等主流应用平台；支持Java、COM、C等应用集成接口；支持SM2等签名算法。 | 台 | 1 |
| 1.2 | 时间戳专用设备 | 完成可信时间戳功能包含时间源，2U；2个1000M网口；支持Windows、Linux、AIX等主流应用平台；支持Java、COM、C等应用集成接口；支持SM2等签名算法。 | 台 | 1 |
| 1.3 | 电子签章系统 | 提供基于数字证书的数字签名和签章功能 | 套 | 1 |
| 2 | **医护技人员证书部分** |
| 2.1 | 个人数字证书 | 标识医护人员网络身份 | 张/年 | 2000 |
| 2.2 | 设备证书 | 标识各类设备的网上身份 | 张/年 | 5 |
| 2.3 | 智能密码钥匙 | 数字证书存储介质 | 枚 | 2000 |
| 2.4 | 电子印章制作费 | 供基于印章模板的制章服务。（按印章个数） | 枚 | 2000 |
| 3 | **证书管理部分** |
| 3.1 | 证书管理服务器 | 提供证书更新、客户端更新、证书环境在线帮助、机构管理、系统管理、时间同步管理、系统备份恢复、移动证书下载和证书申请&签章信息收集等功能；硬件规格：1U；2个100/1000M自适应网口；300w单服务器电源；支持RSA、SM2等算法 | 台 | 1 |
| 4 |  | **患者签名部分** |  |  |
| 4.1 | 手写信息数字签名专用设备 | 用于实现患者知情文书的文件的无纸化签署，手写数字签名系统软件，用于实现数据采集、数据格式处理、手写数字签名、签名验证、数据交付等功能，业务处理能力：108000笔/小时； | 台 | 1 |
| 4.2 | 指纹手写签名屏 | 10.1寸液晶电磁压感手写屏，内置指纹模块，支持手写签名同时采集签名人指纹数据。 | 台 | 90 |
| 5 | **移动签名部分** |
| 5.1 | 移动签名专用设备 | 移动签名服务器面向医护技人员的移动终端设备，实现移动端的数字证书的可靠电子签名功能,移动客户端运行环境：Android 4.2及以上、iOS8及以上版本 | 台 | 1 |
| 6 |  |  数字认证系统集成 |  |  |
|  |  | HIS、EMR、LIS、PACS等系统数字认证集成 | 套 | 1 |