**CA电子签名更新改造项目（一期）**

**技术需求**

1. **项目建设背景**

中国医学科学院肿瘤医院结合自身医疗信息系统业务情况，于2011年采购了电子认证系统，包括签名验签专用设备和时间戳专用设备，目前主要面向HIS、电子病历、互联网诊疗等业务系统提供电子认证服务，用于解决医技护工作人员基于证书的身份认证及电子签名。但由于密码产品采购时间较早，存在设备老化，算法有待替换、实体Key应用不广等问题，本次项目将依据《密码法》等相关法律法规，开展电子认证系统升级改造工作，实现“可信身份、可信数据、可信行为、可信时间”的目标，保证电子病历的真实可信和合法有效性。

1. **项目建设依据**
* 《中华人民共和国电子签名法》（主席令第十八号）
* 《中华人民共和国网络安全法》（2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过）
* 《中华人民共和国密码法》（中华人民共和国主席令 第三十五号）
* 《中华人民共和国数据保护法》（2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过）
* 《关键信息基础设施安全保护条例》（国令第745号）
* 《电子认证服务管理办法》（中华人民共和国信息产业部令第35号）
* 《信息安全技术 公钥基础设施数字证书格式》（GB/T 20518-2018）
* 《信息安全技术 公钥基础设施时间戳规范》（GB/T 20520-2006）
* 《信息安全技术 证书认证系统密码及其相关安全技术规范》（GB/T 25056-2018）
* 《信息安全技术 智能密码钥匙应用接口规范》（GB/T35291-2017）
* 《基于SM2密码算法的数字证书格式规范》（GM/T 0015-2012）
* 《SM2椭圆曲线公钥密码算法》（GM/T 0003.3-2012）
* 《SM2密码算法加密签名消息语法规范》（GM/T 0010-2012）
* 《时间戳接口规范》（GM/T 0033-2014）
* 《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）
1. **项目建设目标**

为保障我院HIS系统、电子病历系统、LIS系统、HRP、OA、互联网诊疗等业务的信息安全，为实现电子病历的可信归档管理，以及全院无纸化建设，依据《卫生系统电子认证服务管理办法（试行）》、《电子病历应用管理规范（试行）》及相关标准规范要求，需要建立全院统一的合法有效的、高可用性的电子认证服务体系、业务应用安全支撑体系，作为可信电子病历归档管理搭建的前期系统准备，同时保证电子病历从生成过程的真实可信和合法有效性。

**项目建设目标：**

1.本次项目建设须符合《密码法》相关要求，使用的密码技术及算法符合国家密码主管部门要求；

2.建立我院统一的电子认证服务体系，面向我院临床人员、行政人员，统一发放与管理数字证书，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；

3.建立我院HIS系统、电子病历系统、LIS系统、OA系统等医院信息系统统一的业务应用电子认证安全支撑体系，提供合理的、实用的、可信的医疗业务建设方案，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，实现在PC端、手机端、移动PDA等设备上的电子认证服务的使用，有效提升医院信息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，从而保证医院电子化病历数据的真实性、有效性、完整性。

4.为我院开展《电子病历应用水平分级评价》、《国家医疗健康信息互联互通标准化成熟度测评》等评价工作的相关系统建设，落实信息安全等级保护要求，提供安全技术支撑。

1. **项目建设内容和要求**

**4.1 数字证书服务体系建设要求**

建立我院的数字证书服务体系，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) 提供证书全在线服务模式，支持证书在线更新、在线解锁等服务；

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、SDKey等；

7) 提供管理员管理、系统管理等日常服务；

**4.2 电子认证应用支撑体系建设要求**

根据我院HIS系统、电子病历系统、LIS、PACS、OA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的应用，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。投标产品应提供详实的电子认证体系搭建方案，方案应满足以下要求：

1. 全面分析我院HIS系统、电子病历系统等信息系统的电子认证服务需求，提出有针对性的、完善的应用安全支撑体系整体框架，并提供具体的证书、证书应用产品或证书应用技术构成；体系应包括签名验签产品、时间戳产品、证书管理产品等，体系架构合理。
2. 改电子认证体系，应保证与我院HIS系统、电子病历系统、LIS系统、PACS系统、HRP系统、Portal系统、OA系统、移动护理等系统的集成，实现系统登录认证、医疗文书电子签名、行政文书电子签名等功能。请分别阐述电子认证体系与前述系统（包括不限于）的应用集成方案，详细说明集成的业务环节和业务流程等，应支持在B/S、C/S等各类系统架构下的应用进行集成，并满足医院对业务安全、应急处理和业务连续性的要求。
3. 详细分析提供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VC/VB/.Net、Java、JavaScrpit等各类开发平台和技术的实际集成需要。

**4.3 电子认证移动应用建设要求**

根据我院对移动医疗环境电子认证应用需求，设计满足移动查房、移动护理、移动OA等移动场景的解决方案,并设计满足HIS、电子病历、LIS等系统在不使用实体USBKEY条件下、使用手机端进行电子签名认证的解决方案，方案应满足以下要求：

1. 提供的产品或解决方案能够满足合法性、便捷性、多人共用、多场景使用。
2. 通过移动设备可直接对移动设备上的文书做签署，无需回传到PC端进行签署。
3. 提供手机端（支持安卓、IOS、鸿蒙等主流操作系统），对HIS、电子病历、LIS、OA等系统PC端的操作及文书进行扫码签名认证。
4. 提供的产品或解决方案支持数据签名、文档签名，满足签章文书多样性。文档签名展示时支持手写体。
5. 投标方应提供安全、高效的网络部署方案，保证内网到外网的单向传输，保证内网设备的安全性，保证部署在内网、外网不同网络中的系统，均能使用手机扫码签名功能，同时保证电子签名系统顺畅、高效运行。

**4.4 系统继承**

我院现在在用的CA产品厂家为北京CA（BJCA），所投产品应能与我院现有电子认证体系无缝对接，数字证书在不适配的情况下复用，证书客户端无需重复安装，请投标人提供所投产品与北京CA的详细衔接方案、详细的案例名单以及相关证明材料。

1. **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. 售后服务体系：投标人应当具有良好的服务理念和完善的售后服务体系，能够按照投标技术方案提供系统集成技术支持服务；配备1名专职项目经理，保障项目全周期对接，以及项目的运维支持对接。
2. 质保期：所投软、硬件产品质保期不低于三年，质保期内应用软件和硬件的升级、维护均免费；在实施与质保期内，免费提供与医院相关信息系统的对接服务和技术支持。
3. 证书key的质量保证期为1年，自证书交付之日起计算。质保期内证书key非人为因素损坏的，供应商负责免费更换或修复；此后的损坏，供应商应负责维修。
4. 数字证书的有效期为1年，自证书签发之日起计算。供应商对发放的数字证书在证书有效期内提供免费售后服务，包括证书使用指导、证书损坏修复、证书挂失等，确保用户安全、正常地使用数字证书。运维支持：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。
5. 日常技术支持：提供7x24小时热线电话、远程网络、现场等技术支持服务，对于系统故障，要求提供快速响应机制，满足我院业务连续性要求；
6. 培训方案：根据医院的业务特点和用户认知程度不同，提出系统而有效的培训方案。
7. **投标人资质要求**
8. #投标人具备可证明投标数字证书产品（个人证书、设备证书）原厂商符合《中华人民共和国电子签名法》、《卫生系统电子认证服务管理办法（试行）》等法规文件相关要求，具有电子认证服务许可证及入围国家卫健委（原卫生部）电子认证服务接入测试证明文件（须提供证明文件复印件，并加盖投标人公章）
9. 投标人具备中华人民共和国增值电信业务经营许可证（业务种类包含：信息服务业），（须提供有效的证书复印件并加盖投标人公章）；
10. 投标人具备有效的信息安全管理体系认证证书（须提供有效的证书复印件并加盖投标人公章）。
11. #投标人具备所投数字证书产品（个人证书、单位证书、设备证书）原厂商的电子认证服务系统支持国产密码算法，且通过国家密码管理局安全性审查及互联互通测试的相关证明文件（需提供国家密码管理局相关证明文件复印件，并加盖投标人公章）
12. 投标人需提供不少于5家大型三甲医院同等规模项目验收证明材料。（须提供合同及验收报告并加盖投标人公章）
13. **产品采购一览表**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品名称** | **单位** | **数量** |
|  | 签名验签专用设备 | 台 | 2 |
|  | 时间戳专用设备 | 台 | 1 |
|  | 证书管理专用设备 | 台 | 1 |
|  | 协同签名系统 | 台 | 2 |
|  | 个人证书（已有1100张证书，扩充500张） | 张 | 500 |
|  | 设备证书 | 张 | 6 |
|  | 智USBKey数字证书介质（已有1100张USBKey，扩充500枚） | 枚 | 500 |

1. **产品选型要求**

**8.1签名验签专用设备：2 台**

|  |  |
| --- | --- |
| **序号** | **功能指标要求** |
| 1 | 实现基于数字证书的身份认证，支持不同CA的证书验证，提供CRL/OCSP等多种方式的证书有效性验证 |
| 2 | 提供PKCS1/ PKCS7 attach/PKCS7 detach/XML Sign 等多种格式的数字签名和数字签名验证功能(PKCS1签名支持记录签名日志功能) |
| 3 | 对数据进行加密传输，只有指定的信封接收者可以解密数据 |
| 4 | 对文件提供数字签名和数字签名验证功能 |
| 5 | 提供 CRL/OCSP 等多种方式的证书有效性验证 |
| 6 | 信任源管理：可同时配置多条证书链，验证不同 CA 系统签发的数字证书 |
| 7 | 提供证书解析功能， 获取证书中的任意主题信息以及扩展项信息 |
| 8 | 实现对客户端证书的存储，管理员可以通过页面进行证书导入和查找，业务系统可以通过接口获取已存储的证书 |
| 9 | 可以自动更新黑名单，采用动态更新方式，无需重启服务 |
| 10 | 提供应用系统访问策略配置，包括所使用服务器证书、所使用根证书链、验证CRL策略等配置 |
| 11 | 可以开关时间源同步状态，配置时间源服务器地址，保证数字签名验证服务器时间的准确性，另外支持手工设定服务器时间 |
| #12  | 支持PDF格式的版式文件验章和批量验证 |
| **序号** | **非功能指标要求** |
| 1 | 将服务器配置信息备份到PC端，也可以将PC端的备份文件恢复到系统，方便出问题时的尽快恢复 |
| 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 | 签名能力：4300次/秒，签名验证：3200次/秒 |
| 6 | 适用环境：千兆环境，并发用户多 |
| 7 | 支持算法：SM1、SM2、SM3、SM4 |
| 8 | 须满足卫生部卫生系统电子认证服务相关技术规范 |
| **序号** | **产品规格要求** |
| 1 | 设备高度 | 2U |
| 2 | 网络接口 | 2个千兆网口 |
| 3 | 电源指标 | 1个工控电源 |
| **序号** | **资质要求** |
| #1 | 产品须具备《计算机信息系统安全专用产品销售许可证》 |
| #2 | 产品具备国家密码管理局颁发的《商用密码产品型号证书》符合GM/T 0028-2014《密码模块安全技术要求》、GM/T 0039-2015《密码模块安全检查要求》安全等级第二级相关要求 |
| #3 | 产品符合《计算机信息系统安全产品部件第1部分：安全功能检测GA216.1-1999》（中完整鉴别类）《信息安全技术通用渗透测试检测条件 JCTJ 005-2016》（6.2.1、6.2.2）中相关条款所述要求 |
| #4 | 产品须具备国家密码管理局颁发的《商用密码产品认证证书》 |
| #5 | 可兼容多应用场景的适配：公安一所CTID、移民局出入境、财政非税票据 |
| #6 | 支持IPv6 Ready Logo认证 |
| #7 | 投标人需提供不少于5家大型三甲医院同等规模项目验收证明材料。（须提供合同及验收报告并加盖投标人公章） |

8.2时间戳专用设备：1台

|  |  |
| --- | --- |
| **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 | 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 |
| 4 | 可配置IP、网关、端口、连接数、超时时间 |
| 5 | 将服务器配置信息备份到PC端，也可以将PC端的备份文件恢复到系统，方便出问题时的尽快恢复 |
| 6 | 提供对于外部导入时间戳服务器证书的上传、查询、导出等功能 |
| 7 | 可以测试时间戳服务器到其他网络地址的互通状态 |
| 8 | 可以让某个IP或者IP段端访问服务，而不在白名单内的IP或者IP段不能访问服务器的服务 |
| 9 | 授时精度：0.5-3ms(毫秒)，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 | 时间戳签发性能≥2000次/秒 验证性能≥1000次/秒 |
| 6 | 时间同步协议：NTP、SNTP |
| 7 | 满足算法标准：SM2、SM3 |
| 8 | 满足应用接口：Java、C、COM、WebService |
| 9 | 满足应用平台：Windows Server；Linux；AIX；Solaris；Unix |
| **序号** | **产品规格要求** |
| 1 | 设备高度 | 2U |
| 2 | 网络接口 | 2个千兆网口 |
| 3 | 电源指标 | 1个工控电源 |
| **序号** | **产品资质要求** |
| #1 | 产品须具备《中国科学院国家授时中心检测证书》 |
| #2 | 产品制造厂商须具有该产品完全自主知识产权，提供软件著作权证书 |
| #3 | 产品符合《信息安全技术 公钥基础设施 时间戳规范 GB/T 20520-2006》、《信息安全技术 通用渗透测试检测条件 JCTJ 005-2016》（6.2.1、6.2.2）中相关条款所述的有关要求 |
| #4 | 产品须具备国家密码管理局《商用密码产品认证证书》 |
| #5 | 支持IPv6 Ready Logo认证 |
| #6 | 投标人需提供不少于5家大型三甲医院同等规模项目验收证明材料。（须提供合同及验收报告并加盖投标人公章） |

8.3证书管理专用设备：1台

|  |  |
| --- | --- |
| **序号** | **功能指标要求** |
| 1 | 实现证书自动静默更新 |
| 2 | 实现证书应用客户端环境自动更新 |
| 3 | 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 |
| 4 | 提供查看系统状态、配置系统IP/端口、管理员管理、设备编号管理、日志管理、服务管理、备份恢复等管理功能 |
| **序号** | **非功能指标要求** |
| 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 | 须满足国家卫生健康委（原卫生部）卫生系统电子认证服务相关技术规范 |
| 4 | 支持Windows、Linux、AIX等主流应用平台 |
| 5 | 支持Java、COM、C等应用集成接口 |
| **序号** | **产品规格要求** |
| 1 | 设备高度 | 2U |
| 2 | 网络接口 | 2个千兆网口 |
| 3 | 电源指标 | 1个工控电源 |
| **序号** | **产品资质要求** |
| #1 | 产品须具备软件著作权登记证书 |

**8.4 协同签名系统：2套**

|  |  |  |
| --- | --- | --- |
| **产品/服务** | **技术指标项** | **详细技术要求** |
| 协同签名系统 | 证书服务 | 支持连接第三方CA，为用户申请签发数字证书 |
| 身份认证 | 提供认证服务接口，支持基于数字证书的身份认证方式 |
| 数据签名 | 提供数据签名服务接口，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。 |
| 签名验证 | 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 |
| PDF电子签章 | 对PDF文档进行电子签章，并且在电子文档上显示签章图片 |
| PDF电子签章验证 | 验证PDF签名文档有效性、完整性 |
| 应用管理 | 管理接入的业务应用，支持对业务应用的添加、编辑、冻结、解冻、注销等 |
| 用户管理 | 管理证书用户，支持用户变更手机号、冻结、解冻、注销等操作 |
| 设备管理 | 支持用户在多个移动终端设备上使用同一个用户身份，支持对用户终端设备的绑定、解绑等 |
| 密钥管理 | 提供密钥生成、存储、销毁、归档、统计产销等功能，支持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 |
| #授权管理 | 产品支持一人多设备、一设备多人的应用场景；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 |
| #统计分析 | 产品支持用户量、签名量、证数量的统计分析，提供截图证明 |
| 日志审计 | 提供业务操作日志、管理员操作日志等审计功能 |
| 协同签名APP | 证书下载 | 支持用户在移动端下载个人证书 |
| 数据签名 | 支持用户在移动端签署业务数据 |
| 文档签章 | 支持用户在移动端签署PDF文档 |
| 批量签名 | 支持用户在移动端批量签署业务数据 |
| 设置签名图片 | 支持用户在移动端设置手写签名图片 |
| 指纹签名 | 支持用户在移动端使用指纹代替证书口令进行签名 |
| 接口服务 | 提供手机端证书下载、数据签名、文档签章、扫码签名等接口 |
| #应用获取 | 移动端APP要能够在Android应用市场和苹果AppStore中已经发布,提供应用市场截图 |
| 产品资质 | #产品须具备国家密码管理局颁发的《商用密码产品认证证书》 |
| #产品须具有《计算机软件著作权登记证书》 |
|  | #产品基于协同密钥技术来实现移动端用户私钥的生成和使用，具备专利证明复印件 |
|  | #产品须具备《计算机信息系统安全专用产品销售许可证》 |
|  | #产品须具备公安部产品检验检测报告 |
|  | 投标人需提供不少于5家大型三甲医院同等规模项目验收证明材料。（须提供合同及验收报告并加盖投标人公章） |

**8.5个人证书：500张**

|  |  |
| --- | --- |
| **序号** | **功能指标要求** |
| 1 | 标识个人用户网络身份 |
| 2 | 符合国家卫生健康委（原卫生部）《卫生系统数字证书格式规范（试行）》 |
| 3 | 符合国家卫生健康委（原卫生部）《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 |
| **序号**  | **资质要求**  |
| #1 | 产品制造商须符合北京市卫生健康委员会原（北京市卫生局）《北京市卫生系统电子认证服务管理办法（试行）》文件要求 |
| 2 | 产品制造厂商须具有电子认证服务许可证，须符合国家卫生健康委（原卫生部）《卫生系统电子认证服务管理办法（试行）》文件要求 |
| #3 | 所投产品可与我院现有电子认证体系无缝对接，数字证书在不适配的情况下复用，证书客户端无需重复安装，需提供所投产品制造商与我院现电子认证提供商（BJCA）的合作证明 |
| #4 | 所投产品制造商具备中华人民共和国增值电信业务经营许可证（业务种类包含：信息服务业），（须提供有效的证书复印件并加盖投标人公章） |
| #5 | 所投产品制造商具备有效的信息安全管理体系认证证书（须提供有效的证书复印件并加盖投标人公章） |

**8.6设备证书：6张**

|  |  |
| --- | --- |
| **序号** | **功能指标要求** |
| 1 | 标识设备网络身份 |
| 2 | 符合国家卫生健康委（原卫生部）《卫生系统数字证书格式规范（试行）》 |
| 3 | 符合国家卫生健康委（原卫生部）《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 |

**8.7 USBKey数字证书介质：500枚**

|  |  |
| --- | --- |
| **序号**  | **功能指标**  |
| 1  | 符合国家卫健委《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 容量不小于 32K 字节  |
| 4  | USB Key 自身的安全要求：具备完善的 PIN 校验保护功能  |
| 5  | 支持标准的 RSA 和国产商用密码算法  |
| **序号** | **产品资质要求** |
| 产品资质 | #产品须具备国家密码管理局颁发的《商用密码产品认证证书》 |