附件：

1、协同签名服务器

|  |  |
| --- | --- |
| **序号** | **功能指标要求** |
| 1 | 支持连接第三方CA，为用户申请签发数字证书 |
| 2 | 可提供认证服务接口，支持基于数字证书的身份认证方式 |
| 3 | 可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 |
| 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 | 可对PDF文档进行电子签章，并在电子文档上显示签章图片 |
| 6 | 可验证PDF签名文档有效性、完整性 |
| 7 | 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 |
| 8 | 管理证书用户，支持用户变更手机号、冻结、解冻、注销等操作 |
| 9 | 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 |
| 10 | 可提供密钥生成、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 |
| 11 | 支持对系统配置及对系统管理员进行管理 |
| 12 | 可提供对数据签名、PDF签章等数据的统计查询功能 |
| 13 | 可提供业务操作日志、管理员操作日志等审计功能 |
| 14 | 基于手机端可提供SDK开发包 |
| 15 | 支持用户在移动端下载个人证书； |
| 16 | 支持用户在移动端签署业务数据；支持用户在移动端签署PDF文档 |
| 17 | 支持手机扫描二维码登陆认证功能；支持用户在移动端批量签署业务数据 |
| 18 | 支持用户在移动端设置手写签名图片；支持用户在移动端使用指纹代替证书口令进行签名 |
| 19 | 可提供手机端证书下载、数据签名、文档签章、扫码签名等接口；支持Android4.4、iOS9及以上版本 |
| **序号** | **产品规格要求** |
| 1 | 设备 | 2U机架式 |
| 2 | 网络接口 | ≥2个千兆网口 |
| 3 | 电源 | 双电源，功率550W |
| **序号** | **产品资质要求** |
| 1 | ★国家密码管理局颁发的《商用密码产品认证证书》 |
| 2 | 产品须具有《计算机软件著作权登记证书》 |
| 3 | 产品使用的密钥分割技术技术有专利支撑或第三方检测报告 |
| 4 | 产品须具备《计算机信息系统安全专用产品销售许可证》 |
| 5 | 具备移动智能终端安全密码模块（二级）商用密码产品认证证书 |
| 6 | 具备中国质量认证中心颁发的《中国国家强制性产品认证证书》 |
| 7 | ★产品须具备IPv6 Ready Logo认证证书 |
| 8 | 产品须具备《公安部检测报告》 |

2、时间戳服务器

|  |  |
| --- | --- |
| **序号** | **功能指标要求** |
| 1 | 可签发可信时间戳、验证时间戳有效性 |
| 2 | 内置国家授时中心时间源，权威可靠 |
| 3 | 可配置IP、网关、端口、连接数、超时时间 |
| 4 | 可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 |
| 5 | 可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 |
| 6 | 可以测试时间戳服务器到其他网络地址的互通状态 |
| 7 | 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 |
| 8 | 可提供备份恢复功能，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 |
| 9 | 支持双机、负载均衡 |
| 10 | 提供C、COM 、Java 等主流开发API |
| 11 | 时间戳签发性能≥500次/秒  |
| 12 | 时间源模块：可同时支持CDMA，北斗，GPS |
| 13 | 授时精度：0.5-3ms(毫秒) |
| 14 | 时间同步协议：NTP、SNTP |
| 15 | 满足算法标准：RSA、SHA1、SM2、SM3 |
| 16 | 满足应用接口：Java、C、COM、WebService |
| 17 | 满足应用平台：Windows Server；Linux；AIX；Solaris；Unix |
| **序号** | **产品规格要求** |
| 1 | 设备 | 2U机架式 |
| 2 | 网络接口 | ≥2个千兆网口 |
| 3 | 电源 | 双电源，功率550W |
| **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》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 | 具备中国质量认证中心颁发的《中国国家强制性产品认证证书》 |
| 6 | ★产品须具备IPv6 Ready Logo认证证书 |

3、电子签章系统

|  |  |
| --- | --- |
| **序号** | **功能指标要求** |
| 1 | 支持第三方CA机构签发的数字证书 |
| 2 | 可提供基于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 |
| 6 | 可提供电子签章中间件，满足C/S环境的电子签章集成 |
| 7 | 支持原文、印章图片、数字签名的绑定，能够防止篡改 |
| 8 | 基于安全客户端，支持电子印章签署功能 |
| 9 | 支持在线签章和离线签章 |
| 10 | 可提供印章管理功能，包括印章模板管理、印章制作、授权、停用、启用等功能 |
| 11 | 系统管理支持拔出管理员 Key 系统自动退出，保证系统安全 |
| **序号** | **产品资质要求** |
| 1 | 投标产品须具备《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 | ★产品须具备国家密码管理局《商用密码产品认证证书》 |
| 4 | 产品符合《信息安全技术电子签章产品安全技术要求GA/T 1106-2013》、《信息安全技术通用渗透测试检测条件 JCTJ 005-2016》中的相应条款所述的有关要求 |

4、单位证书

|  |  |
| --- | --- |
| **序号** | **功能指标要求** |
| 1 | 标识单位用户网络身份 |
| 2 | 符合原卫生部《卫生系统数字证书格式规范（试行）》 |
| 3 | 符合原卫生部《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 |
| 7 | 个人证书的提供方须具备《电子认证服务许可证》和《电子认证服务使用密码许可证》 |

5、个人证书（1000张）

|  |  |
| --- | --- |
| **序号** | **功能指标要求** |
| 1 | 标识个人用户网络身份 |
| 2 | 符合原卫生部《卫生系统数字证书格式规范（试行）》 |
| 3 | 符合原卫生部《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 |
| 7 | ★个人证书的提供方须具备《电子认证服务许可证》和《电子认证服务使用密码许可证》 |

6、设备证书（3张）

|  |  |
| --- | --- |
| **序号** | **功能指标要求** |
| 1 | 标识设备网络身份 |
| 2 | 符合原卫生部《卫生系统数字证书格式规范（试行）》 |
| 3 | 符合原卫生部《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 |
| 7 | 个人证书的提供方须具备《电子认证服务许可证》和《电子认证服务使用密码许可证》 |

7、手写信息数字签名服务器

|  |  |
| --- | --- |
| **序号** | **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数字证书，也可在未连接互联网的医院内网环境使用 |
| 2 | 可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 | 可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 | 可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 | CA中心根据手写信息数字签名系统采集和固化的可靠签署内容与行为数据，签发事件型数字证书，实现手写签名建立可靠对应的数字签名的方法 |
| 6 | 支持手写板、平板电脑、手机等客户端设备对签名人身份采集并对签名事件的处理 |
| 7 | 支持在数字签名、电子签章时加盖时间戳，确保签名时间的真实有效 |
| 8 | 可提供C、 Java 等主流开发API |
| 9 | 业务处理能力不小于108000笔/小时 |
| 10 | 适用环境：千兆及以上环境，多并发用户 |
| 11 | 支持算法：SM2、SM3、SHA256、RSA |
| **序号** | **产品规格要求** |
| 1 | 设备 | 2U机架式 |
| 2 | 网络接口 | ≥2个千兆网口 |
| 3 | 电源 | 双电源，功率550W |
| **序号** | **产品资质要求** |
| 1 | ★产品须具备国家密码管理局《商用密码产品认证证书》 |
| 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 | 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》(完整性鉴别类）、《信息安全技术 通用渗透测试检测条件 JCTJ 005-2016》中相关条款所述的有关要求 |
| 4 | 投标产品须具备《计算机信息系统安全专用产品销售许可证》 |
| 5 | 产品具备国家级单位签发的合法性声明 |
| 6 | 投标产品须具备《计算机信息系统安全专用产品销售许可证》 |

8、电子病历移动签署系统

|  |  |
| --- | --- |
| 序号 | 功能指标 |
| 1 | 为医疗服务对象提供可靠的电子签名方案，保证其签署的电子医疗文书合法、安全 |
| 2 | 建立新型的大众用户（患者、家属）证书服务模式，CA中心基于电子病历等系统用户的实名信息，为其颁发数字证书 |
| 3 | 患者或患者家属使用数字证书对医疗文书签名，此过程中无需为患者颁发密码设备，降低应用成本 |
| 4 | 满足医院复杂的业务场景，尤其是手术室或住院患者无法下床等场景 |
| 5 | 无缝对接电子病历账户系统、实现访问权限控制 |
| 6 | 实现电子病历存储、索引、查询、下载功能 |
| 7 | 提供电子病历签署状态控制 |
| 8 | 无缝对接手写信息数字签名系统进行数字签名，支持数据、PDF双签名模式 |
| 9 | 支持系统配置管理和日志审计 |
| 10 | 移动签署APP，支持患者、家属两种角色的签名，支持PDF签名和数据签名，支持拍照证据采集、绑定，支持批注功能，支持网络不稳定情况下的缓存功能 |
| 11 | 能够无缝对接院内现有的手写数字签名服务系统 |

9、签名客户端维护费（3万出院患者/年）

面向患者或家属用户，通过手写数字签名服务器实现事件型证书的签名、签章服务。包含手写板事件型证书签发年服务包费用，不限次使用，保证患者签名的合法合规。