**一、项目名称**

上海交通大学医学院附属新华医院信创密评改造项目

**二、项目参数**

**（一）名称**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 产品 | 数量 | 单位 |
| 1 | 签名验签服务器升级（利旧升级增加完整性保护工具模块） | 1 | 套 |
| 2 | 服务器密码机 | 2 | 台 |
| 3 | 数据库密码机 | 2 | 台 |
| 4 | 身份认证服务器 | 2 | 台 |
| 5 | 安全认证网关 | 2 | 台 |
| 6 | 个人身份数字证书（扩容）（卫生部标准格式） | 100 | 张 |
| 7 | SSL证书 | 2 | 张 |

**（二）最高限价**

人民币175.00万元万元

**（三）资格条件**

（1）投标人须具有独立承担民事责任的能力；

（2）投标人须具有良好的商业信誉和健全的财务会计制度；

（3）投标人须具有履行合同所必需的设备和专业技术能力；

（4）投标人须有依法缴纳税收和社会保障资金的良好记录；

（5） 投标人参加政府采购活动前三年内，在经营活动中没有重大违法记录；

（6）投标人在近三年内未被国家财政部指定的“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信名单；

（7）单位负责人为同一人或者存在直接控股、管理关系的不同单位，不得参加同一包件的竞争或者未划分包件的同一采购项目的竞争；

（8）本项目不接受联合体投标。

（9）法律、行政法规规定的其他条件。

**（四）功能及技术参数**

**一、采购标的需实现目标（项目概况）**

针对现阶段密码应用不广泛、不规范、不安全的严峻现实，为了贯彻落实《网络安全法》、《密码法》、《保守国家秘密法（修订）》、《关键信息基础设施安全保护条例》、《数据安全法》、《电子签名法》、《商用密码应用安全性评估管理办法》（试行）等法律法规对于密码安全应用的要求，以及国家2021年发布的《商用密码应用安全评估制度》，数字化医院商用密码安全应用及管理项目首先定位为数字医院密码安全基础设施建设。目标是从密码能力设备、服务保障和管理监督角度，不仅点对点地满足当前密评改造合规的需求，而且长期系统性地满足“以评促改、以评促建、以评促管，一评三同步”四位一体的密评合规常态化需求，全方位满足全院网络与信息系统广泛、正确、安全使用密码的需求，数字化医院商用密码安全应用及管理项目的目标不仅是满足当下点对点密评合规的需求，更是要满足密评长期化、常态化、系统化的需求。

落实GB/T 39786-2021要求：对标密评量化规则，点对点落实密评合规改造，并至少完成4个系统的商用密码安全应用测评需求。

升级密码应用安全基础能力：医院前期已部署数字身份管理系统、移动安全认证系统、数字签名验签系统、可信时间戳系统、电子签章系统、手写数字签名系统、医护人员数字证书等商用密码产品，基本可以解决数据安全的真实性、完整性和不可否认性需求，本期通过新增部署安全认证网关、服务器加密机、数据库加密机、SSL数字证书、身份认证服务器等基础密码产品满足数据安全机密性需求，完善密码应用安全基础服务能力。

通过密码安全服务体系解决医院信息系统的物理与环境安全、网络与通信安全、设备与计算安全以及为应用与数据安全提供真实性、机密性、完整性和不可否认性的密码服务支撑。

**二、采购清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 产品 | 数量 | 单位 | 质保期 | 是否核心产品 |
| 1 | 签名验签服务器升级（利旧升级增加完整性保护工具模块） | 1 | 套 | 1年 | 否 |
| 2 | 服务器密码机 | 2 | 台 | 3年 | 否 |
| 3 | 数据库密码机 | 2 | 台 | 3年 | 是 |
| 4 | 身份认证服务器 | 2 | 台 | 3年 | 是 |
| 5 | 安全认证网关 | 2 | 台 | 3年 | 是 |
| 6 | 个人身份数字证书（扩容）（卫生部标准格式） | 100 | 张 | 1年 | 否 |
| 7 | SSL证书 | 2 | 张 | 1年 | 否 |

**三、本项目需与现有系统进行对接,现有系统情况、接口情况介绍**

密评改造逐步逐年推进，和现有重症监护临床信息软件应用系统做安全加密。

重症监护临床信息系统，以重症监护病区电子病历及远程监护、会诊、探视和示教等软件的升级改造与实施应用为重点建设内容，并与医联中心端系统的对接改造，包括重症ICU电子病历系统、ICU远程监护系统、ICU远程智能会诊系统、ICU远程探视系统、ICU示教系统和ICU智慧管理等重症监护临床医疗业务，以及重症监护标准床单元的监护仪、呼吸机、输液泵、CRRT、ECMO等床旁监测设备生命体征参数的实时采集和感知。利用物联网、5G、人工智能、虚拟现实、增强现实等数字孪生及元宇宙技术，夯实建立重症ICU数字孪生底座系统，支持三维模型数据、物联感知数据和患者体征数据，支撑患者多标签管理、一床一档管理、病房环境监测、重要医疗监测设备管理等应用场景开发，打造“三层多域全周期”的数智临床服务新模式，形成儿童重症医学临床业务的“数字感知”、“数智决策”、“数字孪生”层次性发展，以推动重症ICU临床人机融生，提升重症ICU精准救治能力，实现以患者为中心的全流程、全周期可视化、人人享有同质化和高效的重症救治服务目标，赋能重症ICU数字化、精细化管理，引领数字孪生、元宇宙等新型技术在医疗领域的创新应用。

**四、产品参数**

**1.签名验签服务器**

甲方现有签名验签服务器制造商是上海神兵信息安全有限公司，并部署上海市数字证书认证中心有限公司的电子签名服务，本项目需在现有的签名验签服务器上升级一套完整性保护工具模块。

|  |  |
| --- | --- |
| 序号 | 功能参数要求 |
| 1 | 对医院已部署数字签名验签服务器进行升级，集成部署在签名验签服务器内。 |
| 2 | 支持SM3-HMAC算法，以满足业务系统数据完整性保护需求中密码应用对SM3-HMAC算法使用需求。 |
| 3 | 支持步骤流程：1.应用系统服务节后增加MAC字段；2.要求尾部关联系统调用接口时传输MAC值；3.应用系统接口接收数据后有限计算比对MAC一致后再继续后续业务流程，否则认为改请求的数据部完整而拒绝处理。 |
| 4 | 集成接口：/Hmac/sign |
| 5 | 提供HMAC-SM3算法完整性保护模块接口说明。 |
| 6 | ★兼容现有的ca签名验签服务器系统（需提供上海市数字证书认证中心有限公司的原厂证明） |
| 7 | ★须提供所投产品的厂家针对本项目的授权书。 |

**2.服务器密码机**

|  |  |
| --- | --- |
| 序号 | 设备参数要求 |
| 1 | 尺寸：小于等于2U  网口：10/100/1000M x2  电源：大于等于350W 工控电源  主板：满足信创要求  CPU ：满足信创要求，大于等于8核, 主频大于等于2.7GHz  内存：大于等于DDR4 8G  硬盘：大于等于500G固态硬盘 |
| 序号 | 功能参数要求 |
| 1 | 支持算法：支持 SM2 国密标准非对称算法；RSA 国际标准非对称算法；支持 SM1、SM4、SM7、ZUC 等国密标准对称算法；DES/3DES、AES 等国际标准对称算法；支持 SM3 国密标准杂凑算法；SHA1/SHA2 等国际标准杂凑算法。 |
| 2 | 支持双 WNG8 物理随机源生成真随机数。 |
| 3 | 国产化硬件：CPU、内存、主板、电源、密码卡等核心部件均采用国产化硬件。 |
| 4 | 安全合规：符合《GM/T0028-2014 密码模块安全技术要求》安全二级要求。 |
| 5 | 具有完善的权限控制：具有完善的分级权限控制机制，分为管理员、审计员、操作员等不同的管理角色，密码机不同的管理操作需要相应的管理角色登陆；管理角色载体为 USBKEY（智能密码钥匙）；管理角色认证方式支持基于身份的认证。 |
| 6 | 高可用性：支持采用集群负载的方式保证业务冗余，保证应用系统业务的可靠性。多机负载由接口层实现，对上层应用透明。支持多机负载提高密码运算性能。 |
| 7 | 冗余电源：保证设备运行的持续稳定。 |
| 8 | 网口支持主备模式绑定，保证网络冗余。 |
| 9 | 高可维护性支持：具备日志审计、状态监控、NTP 时间同步等扩展功能。 |
| 10 | 支持安全的密钥存储：密钥结构支持采用“系统保护密钥-用户密钥（内部密钥对或 KEK）-会话密钥”的三层密钥保护结构，保证关键密钥在任何时候不以明文形式出现在设备外，密钥备份文件受备份密钥加密保护。 |
| 11 | 支持安全的访问控制：具备 IP 白名单、连接口令等访问控制方式，授权接入的应用客户端请求；支持基于 RSA、SM2 的安全通道接入，确保数据传输的安全性。 |
| 12 | 支持安全的密钥存储功能：密码机内可安全存储各种类型的非对称密钥对、对称密钥。 |
| 13 | 支持安全的密钥生成功能：密码机可提供各类型密钥对的生成功能。 |
| 14 | 非对称密码运算：密码机可提供基于 SM2、RSA 等算法的签名/验签、加密/解密、密钥协商等功能。 |
| 15 | 对称密码运算：密码机可提供基于 SM1、SM4、SM7、DES/3DES、AES 等算法的加解密功能，算法模式支持ECB/CBC/OFB/CFB/CTR/XTS/GCM/CCM 等。 |
| 16 | 支持消息鉴别码的产生及验证：支持提供基于 SM1、SM4、DES/3DES、AES 等算法的 CBCMAC、CMAC 的产生及验证。 |
| 17 | 支持密钥管理功能：支持提供各类型密钥的生成、删除、查看、备份和恢复等功能。 |
| 18 | 标准接口：密码机提供 GM/T 0018、JCE、PKCS#11 等国密、国际标准规范接口。 |
| 19 | 网络协议：支持 IPV4/IPV6 双栈协议。 |
| 20 | ★须提供所投产品的厂家针对本项目的授权书。 |
| 21 | ▲服务器密码机具备《商用密码产品认证证书》 |

**3.数据库密码机**

|  |  |
| --- | --- |
| 序号 | 设备参数要求 |
| 1 | 尺寸：小于等于2U  网口：板载6\*GE  电源：300W 工控冗余电源  CPU ：4核4线程  内存：大于等于16G  硬盘：大于等于2T |
| 序号 | 功能参数要求 |
| 1 | 支持国密算法SM4对称密码算法，支持国密算法SM3摘要算法。 |
| 2 | 支持Oracle、MySQL、SQL Server、达梦、人大金仓、OpenGauss、GaussDB等主流数据库透明加密 |
| 3 | 支持字段级加密，确保数据的机密性，支持国密算法； |
| 4 | 支持字段级完整性保护和校验，确保数据的完整性，支持国密算法； |
| 5 | 支持varchar2、char、number等常见的字段类型； |
| 6 | 支持保留格式加密。 |
| 7 | 支持自动识别数据库内敏感数据，支持识别常见的身份证号、手机号等敏感数据；提供产品截图 |
| 8 | 支持用户自定义敏感数据识别规则； |
| 9 | 支持对加密字段制定独立于数据库的权限控制策略； |
| 10 | 独立权限控制策略支持控制库、表、字段三级对象； |
| 11 | 独立权限控制策略至少支持用户/应用 对数据库对象的增删改查四种权限； |
| 12 | 支持密文索引，支持以密文列的原始值为条件进行查询，支持精确查询； |
| 13 | 支持加密插件和加密网关两种数据库加密模式 |
| 14 | 加密和完整性保护对应用无影响，应用无需改造代码即可实现加密和完整性保护 |
| 15 | 支持本地密钥管理和连接第三方密钥管理系统两种密钥管理模式 |
| 16 | 本地密钥管理，密钥生成时采用由内部的密码卡的物理噪声源芯片生成的随机数，密钥生成后由加密卡中的保护密钥加密后存储。 |
| 17 | 本地密钥管理，支持密钥安全管理，通过管理控制台集中管理所有加密密钥。 |
| 18 | 支持连接密钥管理系统，由密钥管理系统进行密钥生命周期管理。 |
| 19 | 支持对密钥及系统配置等重要数据的备份/恢复机制，系统管理员可方便的在管理控制台完成系统备份操作，可下载到本地进行妥善保存。 |
| 20 | 支持基于HTTPS实现远程管理和配置 |
| 21 | 支持采用基于数字证书的硬件密码钥匙（USBKEY）“双因子”认证方式实现管理人员的身份鉴别 |
| 22 | 支持双主或集群等高可用机制部署； |
| 23 | 支持系统用户管理，支持根据三权分立原则划分用户角色及权限，包括管理员、审计员、操作员 |
| 24 | 支持所有的关键操作均记录日志，可对系统中所有的日志进行查询和审计。 |
| 25 | 支持配置系统网络、系统时间等系统配置。 |
| 26 | 加密插件模式：数据库加密表实时查询速率为200000条/秒， |
| 27 | 加密插件模式：数据库加密表实时插入速率5000条/秒 |
| 28 | 网关加密模式：数据库加密表实时查询速率50000条/秒 |
| 29 | 网关加密模式：数据库加密表实时插入速率3000条/秒 |
| 30 | ★须提供所投产品的厂家针对本项目的授权书。 |
| 31 | ▲数据库密码机具备《商用密码产品认证证书》 |

**4.身份认证服务器**

|  |  |
| --- | --- |
| 序号 | 设备参数要求 |
| 1 | 尺寸：小于等于2U  网口：10/100/1000M x2  电源：大于等于350W 工控电源  主板：满足信创要求  CPU ：满足信创要求，大于等于8核, 主频大于等于2.7GHz  内存：大于等于DDR4 8G  硬盘：大于等于500G固态硬盘 |
| 序号 | 功能参数要求 |
| 1 | 支持需要使用多因素认证服务的用户信息管理功能，用户信息至少包括用户名称、用户唯一标识、证件类型、证件号、手机号等基本信息配置管理。敏感信息加密保存，隐藏关键字段显示。 |
| 2 | 支持用户分组管理，能够针对不同的用户类型进行分组管理后，可以通过分组进行统一授权。 |
| 3 | 支持终端设备、服务器设备等数字资产管理，至少包括资产名称、资产IP地址、资产操作系统、操作系统版本、资产类型等基本信息配置管理，支持通过接口同步方式、或者客户端采集终端信息自动注册方式实现资产信息的采集。 |
| 4 | 支持同一类型资产的分组管理，可以针对资产组的统一授权访问管理。 |
| 5 | 支持基于用户或用户组访问资产或者资产组的访问控制权限管理，授权配置至少包括设置授权有效期，用户或用户组，资产或资产组等基本信息 |
| 6 | 多因素认证客户端插件信息监控和管理功能：能够实时监控资产安装的多因素认证客户端的认证访问状态、关键配置信息的更改情况、认证连接和访问情况的监控和功能功能，支持配置策略采用数据完整性保护技术处理后的配置下发同步。支持通过在本地直接进行各类算法（SHA256、国密算法SM3）的摘要计算，签名，验签，对称加密，非对称加密等计算，实现本地文件、数据、程序的完整性保护。 |
| 7 | 多因素认证客户端插件工作状态监控，至少包括是否处于在线或者离线状态、是否有效或者失效状态等。 |
| 8 | 支持资产数字证书申请管理功能，至少能够查询统计资产名称、资产IP、对应的设备证书序列号、证书状态、证书起始时间、证书结束时间、证书操作（申请、更新、注销等）信息 |
| 9 | 详细的认证安全策略配置管理和监控，至少包括安全策略名称、安全策略标识、安全策略类型、策略响应措施、策略优先级、违规次数配置、违规时长、封禁时长等基本需求配置功能。 |
| 10 | 详细的认证日志记录，用于事后审计，至少包括认证记录、数字证书申请记录、服务器配置操作记录和异常认证记录等基本日志记录要求。 |
| 11 | 认证日志至少需要记录资产名称、资产IP地址、用户访问账户、用户访问认证方式、认证访问结果，如果认证失败，失败原因描述、认证访问时间等基本审计信息。 |
| 12 | 数字证书日志至少需要记录资产名称、资产IP地址、证书申请类型、数字证书序列号、数字证书申请时间、申请结果、如果失败，失败原因描述、 |
| 13 | 操作日志和审计功能主要是针对登录访问多因素认证系统的管理用户，进行平台配置管理日志信息记录和审计功能，至少包括管理账户、操作类型（增加、删除、修改）、操作功能、操作资产对象的IP地址、操作状态、操作时间等进行查询管理，支持针对每条记录进行单独审计操作和审计管理。 |
| 14 | 异常认证记录主要针对违规账户、违规IP地址对于资产IP地址发起的违法安全策略的访问请求，进行统一的记录，作为对平台发起认证攻击的记录和预警。 |
| 15 | CA认证源配置管理和对接：能够支持CA机构的配置和CA服务的对接，至少包括CA机构的名称、CA机构接口地址、与CA机构通讯数字证书配置，配置完成后，可以直接通过接口调用，为多因素认证体系提供数字证书管理和应用服务。需要支持对接上海市卫生健康行业市区两级电子认证平台的证书接口，实现符合卫生行业格式的数字证书发放使用。 |
| 16 | 支持将用户登录访问windows操作系统、linux操作系统的认证请求推送或者扫码方式通过手机数字证书进行统一证书认证后实现合法登录访问。 |
| 17 | 多因素认证客户端和服务端通讯均采用国密数字证书进行双向身份认证和国密算法加密传输通讯，关键敏感配置信息采用国密算法进行完整性保护和验证。 |
| 18 | ★须提供所投产品的厂家针对本项目的授权书。 |
| 19 | ▲具备身份认证系统商用密码产品认证证书 |
| 20 | ▲安全认证网关具备《信息技术产品安全测试证书》 |

**5.安全认证网关**

|  |  |
| --- | --- |
| 序号 | 设备参数要求 |
| 1 | 尺寸：小于等于2U  网口：10/100/1000M x2  电源：大于等于350W 工控电源  主板：满足信创要求  CPU ：满足信创要求,大于等于8核, 主频大于等于2.7GHz  内存：大于等于DDR4 8G  硬盘：大于等于500G固态硬盘 |
| 序号 | 功能参数要求 |
| 1 | 采用SM2、SM3、SM4等国产密码算法，实现网络传输双向身份鉴别，通过建立基于国密算法的加密通道，终端用户数字证书身份验证支持当前的移动终端手机数字证书验证方式。 |
| 2 | 具有证书及校验文件管理模块，主要实现证书的导入及管理，负责CRL校验和证书链校验的配置管理。 |
| 3 | 具有隧道管理和代理配置模块，主要包含隧道添加和管理配置功能（包括隧道证书选择、客户端校验、加密协议及算法等配置），代理配置文件生成功能（支持ssh/sftp/telnet配置），链路启停相关操作等业务功能。 |
| 4 | 具有日志管理审计模块，主要面向用户提供管理员登录和操作日志的查询、审计以及用户访问日志记录等功能。 |
| 5 | 具有系统相关模块，主要是对系统资源、内存使用、流量网速的监控以及管理员的管理等。 |
| 6 | 链路加密证书管理功能：系统可实现链路加密证书的管理功能，支持RSA和SM2证书的外部直接导入和内部生成文件用户自签导入。 |
| 7 | CRL和证书链配置功能：支持对客户端证书、服务端证书吊销列表CRL和校验证书链的导入和管理。 |
| 8 | 代理配置功能：系统提供代理配置页面，可实现根据页面填写的配置生成对应链路的四层和七层代理配置文件，通过访问链路配置监听的代理路径地址访问目的地址的功能，支持对代理地址的轮询、ip\_hash负载配置。 |
| 9 | 链路操作功能：能提供通过管理页面操作链路的功能，包括启用、停用、重启访问链路以及配置文件的格式化。 |
| 10 | 隧道管理功能：提供隧道管理添加、展示的界面和功能。可通过添加隧道，整合转发链路中对应的吊销列表CRL、证书链校验、加密证书、加密算法、加密协议、转发代理等配置。生成的隧道链路支持在标准的SSL/TLS协议下实现数据加密传输。 |
| 11 | 系统监控功能：能提供实时显示服务器系统资源使用量和访问流量的面板，主要展示CPU使用率、磁盘空间状态以及实时的上传、下载流量秒速和总流量数据等。 |
| 12 | 日志管理功能：提供详尽的管理员日志和访问日志管理功能。管理员日志能记录系统管理员所有的业务操作日志，包括系统登录、配置修改、服务操作等记录。访问日志能记录具体用户访问对应资源时的相关信息。 |
| 13 | 日志审计功能：能提供管理员操作日志的验证审计，保证日志记录的可靠性。 |
| 14 | 具备完善的三级管理员权限配置体系和管理审计分离管理体系。支持系统初始化人员管理、管理员管理、操作员管理等分级管理配置，支持系统和业务管理与审计分离管理原则。 |
| 15 | 具备数据和配置备份恢复功能：提供数据备份、恢复功能，为管理员提供基于web页面的操作界面实现数据备份、恢复，降低系统维护复杂度。 |
| 16 | 提供基于web页面操作方式的系统升级和版本更新功能 |
| 17 | ★须提供所投产品的厂家针对本项目的授权书。 |
| 18 | 安全认证网关具备国家密码管理局商用密码检测中心颁发的《商用密码产品认证证书》。 |
| 19 | ▲安全认证网关具备《网络安全专用产品安全检测证书》 |
| 20 | ▲安全认证网关具备《信息技术产品安全测试证书》 |

**6.个人身份数字证书**

|  |  |
| --- | --- |
| 序号 | 功能指标要求 |
| 1 | 要求能实现第三方CA的本地发放和管理，要求能实现数字证书的申请、审核、发放、作废、更新等业务功能，并能提供批量证书信息录入方便管理员进行证书制作，发放。 |
| 2 | 要求证书应用能实现跨浏览器支持，能支持现有主流浏览器。 |
| 3 | 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）》 |
| 5 | 证书格式标准遵循X509 v3标准 |
| 6 | 支持存放介质：智能USBKey、蓝牙KEY、 SDKEY、及移动端终端文件证书安全存储。 |
| 7 | 支持自定义证书扩展域管理。 |
| 8 | 本次ca个人身份数字证书扩容100张 |
| 9 | ★须提供所投产品的厂家针对本项目的授权书。 |
| 10 | ▲产品制造厂商须具有《电子认证服务许可证》、《电子认证服务使用密码许可证》（需提供相关证明文件） |
| 11 | ▲产品制造厂商的CA系统已完成国产商用密码算法升级改造，提供国家密码管理局出具的相关证明文件复印件。 |
| 12 | ▲产品制造厂商须通过卫生部电子认证服务接入测试（需提供相关证明文件） |

**7.SSL证书**

|  |  |
| --- | --- |
| 序号 | 功能参数要求 |
| 1 | 确保网络服务在部署SSL证书后，可启用https协议，保证网络通讯的安全（防止数据在传输过程中被窃听、篡改和仿冒）和服务端身份有效识别。 |
| 2 | ▲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。 |
| 3 | ▲SM2算法数字证书兼容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。提供证明材料 |
| 4 | 符合国内、国际双标准，并支持国际RSA、国密SM2密码算法。客户信息和审核数据不出境、严格保护，全网信任。 |
| 5 | 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。 |
| 6 | 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%。 |
| 7 | 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%。 |
| 8 | SSL证书扩容2张 |
| 9 | ★须提供所投产品的厂家针对本项目的授权书。 |
| 10 | 证书签发机构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。 |
| 11 | ▲为保障用户数据隐私安全，证书签发机构需具备《ISO27701隐私信息管理体系认证证书》和《ISO27018个人可识别信息信息安全管理体系认证证书》（需提供相关证明文件） |

**五、实施要求**

为实现本系统在物理和环境、网络和通信、设备和计算、应用和数据等层面的密码应用功能，需开发适配若干密码应用功能模块。

1）用户身份认证模块

开发用户身份认证模块，对接移动智能终端签名验签系统登录认证接口，绑定应用系统的用户数字证书和用户ID，实现应用系统对用户的安全身份鉴别。

2）业务重要数据安全传输模块

通过安全认证网关客户端和安全认证网关设备建立SSL加密信道，实现应用系统通信数据的机密性和完整性保护。

3）服务器设备日志/访问控制信息完整性模块

开发服务器设备日志/访问控制信息完整性模块，调用服务器密码机提供的HMAC-SM3功能接口，或调用签名验签服务器提供的签名接口，实现应用服务器、数据库服务器等设备日志/访问控制信息的完整性保护。

4）重要可执行程序签名验签模块

开发重要可执行程序签名验签模块，调用服务器密码机提供的SM2算法数字签名功能接口，实现重要可执行程序的完整性、来源真实性保护。

5）用户访问控制信息签名验签模块

开发用户访问控制信息签名验签模块，调用签名验签服务器提供的SM2算法数字签名功能接口，实现应用系统用户的访问控制列表完整性保护。

6）应用系统重要数据加解密模块

开发应用系统重要数据加解密模块，调用服务器密码机提供的SM4算法加解密功能接口，实现用户身份鉴别数据、重要数据的存储机密性保护。

7）应用系统重要数据签名验签模块

开发应用系统重要数据签名验签模块，调用服务器密码机提供的SM2算法数字签名验签功能接口，实现用户身份鉴别数据、重要数据的存储完整性保护。

8）应用系统电子签章模块

开发应用系统电子签章模块，调用电子签章服务器、时间戳服务器提供的数字签名和时间戳服务功能接口，实现系统内电子文档签批的不可否认性。

**（五）商务要求**

**一、售后服务**

本项目中硬件提供三年原厂维护服务，证书类需提供一年授权服务。

响应时间：7\*24小时电话及现场响应。

工作日，当系统出现严重故障时，乙方应5分钟内响应服务，1小时内派工程师到现场服务。

非工作日，当系统出现严重故障，乙方应10分钟内响应服务，2小时内派工程师到现场服务。

提供热线支持服务及远程故障诊断服务，并提供联系方式和联系人。

提供三年原厂备件支持服务。

项目交接提供培训：在项目实施完毕后，乙方应派出培训讲师对甲方相关人员进行相关培训，包括但不限于：产品功能培训、产品排错培训等

技术咨询：使用中遇到操作、工作流程不清晰、系统维护等技术上问题时，提供咨询服务，技术人员将负责详细解答。

系统定期优化：定期为甲方进行系统优化，对服务器端的系统性能进行例行检查和优化工作。

软件版本升级：有新版本软件推出时，进行现有模块功能的版本升级。

**二、验收要求**

到货一次性验收

**三、交货地点**

新华医院

**四、交货时间**

合同签订后一个月内

**五、付款方式：**

验收合格一次性付清