上海市口腔医院深化信息技术应用创新工作改造项目

\_（商用密码平台一期建设）

技术参数要求

2025年12月

# 商用密码平台一期建设

## 项目概述

密码是网络安全的基石，是维护网络安全最有效、最可靠、最经济、最系统的技术手段。尤其是在网络日渐开放融合，信息孤岛日渐消弭、传统网络安全防御体系日渐削弱、信 创国产化 替代任重道远的大趋势下，密码作为信息安全最后一道防线以及开放融合网络环境下的底层安全技术框架，应该得到前所未有的重视。

近年来医院电子认证密码系统的广泛应用，为我院实现常态化的密评合规、重构数字空间网络信任体系和网络新安全框架奠定了较好的基础，也充分证明密码安全技术在数字医疗领域的体系化应用需求已经到来。

上海市口腔医院已形成了包括医院内部网络、外网和互联网的完整网络体系，以及HIS、LIS、PACS、 MEMS、EMR、MHS以及互联网医院等为代表的信息化应用体系。医院具有一院多区复杂网络架构，全院分为闵行院区、黄浦院区、徐汇院区、浦锦院区、永嘉路门诊部等5个院区，采用串并联结合的方式通过裸光纤进行互联，具备业务系统分散、网络架构复杂，对于数据安全和管理带来极大挑战。随着数字医疗快速发展，在产业互联、万物互联、数字生态成为趋势、信息孤岛逐渐消弭的态势下，对于密码保障的需求将会越来越凸显，合规、正确、有效地使用密码，使用自主、安全、可控的密码服务，以密评改造为契机，加快推动密码安全保障基础设施的建设，对于推动重构数字医疗信息安全新体系具有重要意义，对于医院数字化转型具有战略意义。

立足我院打造一流智慧医院的发展思路，以密评为契机，以CA电子认证系统为基础，统筹规划我院密评改造工作、电子认证服务体系整合升级以及数字安全新框架构建，三位一体，对标基础设施，专业建设全院统一的密码安全权威保障体系，全面推动监管重点网络和信息系统的密码应用，是当前我院数字化建设的首要任务之一。

## 建设目标

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。

1. 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。
2. 升级密码应用安全基础能力：医院前期已部署证书管理系统、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、文件加密网关、完整性保护工具、个人身份数字证书、SSL数字证书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。

利旧产品清单如下

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 产品型号 | 单位 | 数量 |
| 1 | 签名验签系统 | Unitrust SVS | 套 | 1 |
| 2 | 时间戳系统 | Unitrust TSS |
| 3 | 电子签章系统 | Unitrust ESS |
| 4 | 移动安全认证系统 | Unitrust MTSP |
| 5 | 证书管理系统 | Unitrust RAG |
| 6 | 手写数字签名系统 | Unitrust DIDMS |

1. 打造密码安全基础设施：通过实施部署密码服务管理平台实现对全域密码应用的综合治理、服务保障以及随需调整、扩展和演进，掌握密评主动权，满足常态化、系统性的密评合规需求，避免运动式密评改造；统筹满足密码安全保障和电子认证服务基础设施需求。
2. 通过密码安全服务体系解决一院多区下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。

## 项目清单

### 硬件及服务清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品 | 功能描述 | 数量 | 最高限价 |
|
| 1 | 完整性保护工具 | 与医院已部署数字签名验签系统升级集成部署支持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。（详细需求见技术参数要求章节） | 1套 | 56700 |
| 2 | 个人身份数字证书 | 标识医护人员/工作人员网络实体身份。（详细需求见技术参数要求章节） | 800张 | 37800 |
| 3 | SSL数字证书 | 符合国际标准的国产SSL证书，由国内CA机构基于纯国产的CA PKI体系推出的本土化品牌，证书自主研发运营、安全可控。（详细需求见技术参数要求章节） | 2张/年 | 18900 |
| 4 | 安全网关系统 | 支持在标准的 SSL/TLS 协议下，通过网络隧道模式实现数据加密传输。支持 SM4 对称算法，SM2 非对称算法，SM3 摘要算法等国产密码算法。含3年原厂维保。（详细需求见技术参数要求章节） | 4台 | 425500 |
| 5 | 服务器密码机 | 密码机内可生成和安全存储各种类型的非对称密钥对、对称密钥;提供基于 SM1、SM2、SM43、SM4 等算法的签名/验签、加密/解密、密钥协商等功能。含3年原厂维保。（详细需求见技术参数要求章节） | 2台 | 283700 |
| 6 | 数据库加密机 | 基于符合国密算法，无需对应用程序、基础设施、业务结构进行更改就能实现加密保护，部署和使用不需要考虑额外的因素。含3年原厂维保。（详细需求见技术参数要求章节） | 1台 | 217500 |
| 7 | 统一认证系统 | 身份认证服务器提供包括数字证书、动态口令、短信验证码、生物特征等主流认证方式在内的多因素认证服务及统一身份认证登录、统一身份管理、统一认证授权等服务。含3年原厂维保。（详细需求见技术参数要求章节） | 1台 | 283700 |
| 8 | 文件加密网关 | 支持基于国产算法的国密SSL通道与文件系统密码模块客户端通信。支持应用系统免改造实现数据存储加密，不存在也不需要加解密接口开发和适配环节。含3年原厂维保。（详细需求见技术参数要求章节） | 1台 | 245900 |
| 9 | 密码服务管理平台 | 实现对全域密码应用的综合治理、服务保障以及随需调整、扩展和演进，掌握密评主动权，满足常态化、系统性的密评合规需求，避免运动式密评改造；统筹满足密码安全保障和电子认证服务基础设施需求。（详细需求见技术参数要求章节） | 1套 | 1210300 |

本次项目最高限价：278 0000.00元

说明：上海市口腔医院深化信息技术应用创新工作改造项目\_（商用密码平台一期建设）涉及的咨询管理费、监理费、软件测评费、系统集成费、安全测评费、密码测评费另行采购，不包含在本项目预算中。

## 产品及服务技术参数要求

### 完整性保护工具

|  |  |
| --- | --- |
| 序号 | 技术要求 |
| 1 | 对医院已部署签名验签系统进行升级，集成部署在签名验签系统内。 |
| 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 | ▲兼容院内已部署签名验签服务器（详见1.2第2项利旧产品清单）。（提供兼容承诺函） |

### 个人身份数字证书

|  |  |
| --- | --- |
| 序号 | 功能指标要求 |
| 1 | 个人身份数字证书符合《上海市数字证书使用管理办法》，签发证书的CA机构为上海市电子政务电子认证服务机构。 |
| 2 | 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。 |
| 3 | 与医院HIS、LIS、PACS、EMR等业务系统已使用数字证书为同一根证书，可兼容互认。 |
| 5 | 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。 |
| 6 | 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）》 |
| 7 | 证书格式标准遵循X509 v3标准 |
| 8 | 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。 |
| 9 | 支持自定义证书扩展域管理。 |

### SSL数字证书

|  |  |
| --- | --- |
| 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包括Firefox、Android、IOS、java、Windows等，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。（提供兼容性证明文件） |
| 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。(提供证明及说明材料） |
| 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%。 |

### 安全认证网关

|  |  |
| --- | --- |
| 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。（提供产品功能截图） |
| 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。（提供产品功能截图） |
| 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。（提供产品功能截图） |
| 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 | 性能参数：  最大并发连接 SM4-SM3不小于30000 次连接  吞吐率 SM4-SM3 不小于 800 Mbps/秒  新建连接数 SM4-SM3不小于1000次连接/秒 |
| 18 | 国产化硬件：CPU、内存、主板、冗余双电源、密码卡等核心部件均采用国产化硬件。  ≥1块双端口万兆网卡及配套光模块和光纤跳线。 |
| 序号 | 资质要求 |
| 1 | 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》，（提供证书复印件）。 |
| 2 | 安全认证网关具备公安部计算机信息系统安全产品质量监督检测中心颁发的《网络安全专用产品安全检测证书》（提供证书复印件）。 |
| 3 | 安全认证网关具备国家网络与信息系统安全产品质量检验检测中心颁发的《信息技术产品安全测试证书》（提供证书复印件） |

### 服务器密码机

|  |  |
| --- | --- |
| 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；SHA256/SHA2 等国际标准杂凑算法。 |
| 2 | 采用由国家密码管理局批准使用的双物理噪声源生成随机数。 |
| 3 | 国产化硬件：CPU、内存、主板、冗余双电源、密码卡等核心部件均采用国产化硬件。  ≥1块双端口万兆网卡及配套光模块和光纤跳线。 |
| 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 | 支持基于RSA/ECC密码算法的数字信封功能，并支持由内部密钥保护到外部密钥保护的数字信封转换功能。 |
| 6 | 采用由国家密码管理局批准使用的双物理噪声源生成随机数，可生成各类对称密钥（SM1、SM4、AES等）和非对称密钥（SM2、RSA 2048/4096等）。 |
| 7 | 设备内部支持对称密钥和非对称密钥的安全存储。密码机的内部密钥都位于内置的加密硬件中，且必须与授权管理员的USBKey进行密码运算，才能够提供服务 |
| 8 | 支持通过管理界面删除指定的对称或非对称业务密钥，也支持销毁全部业务密钥。支持通过物理开关对设备内全部密钥进行销毁。具有防暴力拆盖密钥自毁机制，销毁后通过任何技术均无法恢复。 |
| 9 | 采用基于密钥分割的方式备份密钥和安全数据，保障备份数据的安全性。采取高强度的密钥分割算法，只有满足最少数量的管理员才能进行恢复操作，备份密钥可恢复到相同型号的其它加密机设备中。 |
| 10 | 支持多级密钥保护模式，可根据使用单位的安全性和性能扩展需求，选择不同的密钥管理体系。 |
| 11 | 提供符合《GM/T 0018-2012 密码设备应用接口规范》的标准化接口，接口支持C、Java等主流编程语言。 |
| 12 | 支持多进程、多线程调用密码服务接口。 |
| 13 | 管理用户采用三权分立的模式，保障设备的安全访问，划分为系统管理员、安全管理员、审计管理员、系统操作员员四种类型。管理员和操作员身份通过USBKEY进行双因子认证。 |
| 14 | 支持断链修复功能，支持多机并行及负载均衡。 |
| 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 | 支持断链修复功能，支持多机并行及负载均衡。 |
| 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 | 系统运行平均故障间隔时间(MTBF)：≥30000小时。 |
| 21 | 2048位RSA签名/验签≥15000/30000次/秒；SM2签名/验签≥200000/100000次/秒；SM2加密/解密≥50000/50000次/秒；SM1算法加解密≥1Gbps；SM4算法加解密≥1Gbps；SM3杂凑算法≥1Gbps；随机数生成≥1Gbps。 |
| 序号 | 资质要求 |
| 1 | 服务器密码机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》（提供证书扫描件）。 |

### 数据库密码机

|  |  |
| --- | --- |
| 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等主流数据库透明加密。 |
| 3 | 支持独立于数据库的细粒度权限控制，支持对库、表甚至列的操作权限控制，防止高权限用户或非法用户越权访问敏感数据。（需提供产品功能截图）。 |
| 4 | 支持应用无需改动代码即可实现对敏感数据的完整性保护。 |
| 5 | 支持数据库动态脱敏。 |
| 6 | 支持使用三方密钥管理系统中的密钥保护数据库数据安全。 |
| 7 | 支持网关模式通过网络接入，应用简单修改数据库IP 即可接入数据库加密机。 |
| 8 | 支持内置敏感数据识别规则，用户也可以根据业务需要，增加自定义敏感数据识别规则。（需提供产品功能截图）。 |
| 9 | 支持应用零改造集成（可提供截图证明）。 |
| 10 | 单节点支持配置多个不同的存储设备，支持为不同应用分配独立的存储设备。 |
| 11 | 支持国产主流CPU、操作系统、数据库、中间件兼容互认证；提供证明兼容互认证材料。 |
| 12 | 支持加密网关部署的数据库加密模式。 |
| 13 | 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。 |
| 14 | 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。 |
| 15 | 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。提供密码卡商用密码产品认证证书，为保障密码芯片、密码卡安全性推荐与设备厂商为同一家。 |
| 16 | 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。 |
| 17 | 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。 |
| 18 | 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。 |
| 19 | 支持基于HTTPS实现远程管理和配置 |
| 20 | 支持高可用配置，通过配置数据集群和 keepalived 集群，实现灾备功能。（需提供产品功能截图）。 |
| 21 | 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。 |
| 22 | 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。 |
| 23 | 支持配置系统网络、系统时间等系统配置。 |
| 24 | 数据库加密表实时查询速率≥52000 条/秒。 |
| 25 | 数据库加密表实时插入速率≥26000 条/秒。 |
| 26 | 数据库加密表实时更新速率≥25000 条/秒。 |
| 27 | 2U机架式，CPU、内存、密码卡等核心部件均采用国产化硬件；标准冗余电源；网络接口≥2\*千兆电口；≥2\*万兆光口及配套光模块和光纤跳线； 内存≥32G。 |
| 序号 | 资质要求 |
| 1 | 数据库密码机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》（提供证书扫描件） |

### 统一认证系统

|  |  |
| --- | --- |
| 序号 | 技术要求 |
| 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。（提供产品功能截图）  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。（提供产品功能截图） |
| 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。（提供产品功能截图）  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 | 国产化硬件：CPU、内存、主板、冗余双电源、密码卡等核心部件均采用国产化硬件。  ≥1块双端口万兆网卡及配套光模块和光纤跳线。 |
| 序号 | 产品资质要求 |
| 1 | 统一认证系统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（提供证书复印件） |
| 2 | 统一认证系统具备公安部计算机信息系统安全产品质量监督检测中心颁发的《网络安全专用产品安全检测证书》（提供证书复印件） |
| 3 | 统一认证系统具备国家网络与信息系统安全产品质量检验检测中心颁发的《信息技术产品安全测试证书》（提供证书复印件） |

### 文件加密网关

|  |  |
| --- | --- |
| 序号 | 参数要求 |
| 1 | 支持基于SM2/SM3/SM4算法的国密SSL通道与文件系统密码模块客户端通信。 |
| 2 | 支持可视化客户端集中管理功能。 |
| 3 | 支持查看所有已部署的免改造机密性保障模块和免改造完整性保障模块运行情况。 |
| 4 | 支持管理账号分权，安全策略管理及安全审计功能。 |
| 5 | 支持客户端日志记录、告警信息的归集、查询、统计功能。 |
| 6 | 支持在线自定义配置机密性保护对象、自定义配置完整性保护对象。 |
| 7 | 支持物理机/虚拟机部署。 |
| 8 | 支持在国产芯片和操作系统上安装部署。 |
| 9 | 单台文件系统密码模块服务端可以支持200台文件系统密码模块客户端。 |
| 10 | 能完成操作系统内置式本地加解密，无需对外发送业务数据。 |
| 11 | 支持应用系统免改造实现数据存储加密，不存在也不需要加解密接口开发和适配环节。不改变现有网络架构，不改变现有存储架构。 |
| 12 | 支持对文件数据进行基于SM4算法的加密存储，并且对数据存储机密性保护进行集中管理。 |
| 13 | 支持物理机/虚拟机部署。 |
| 14 | 支持windows/linux及国产操作系统。 |
| 15 | 嵌入操作系统内核，具备防杀进程、防卸载功能。 |
| 16 | 支持从服务端配置指定客户端所在服务器的指定数据库数据目录进行全库加密。 |
| 17 | 支持基于操作系统内核层的文件加解密，从而全面适用结构化/半结构化/非结构化数据类型。 |
| 18 | 支持全面的透明加解密，不影响数据库检索功能，不影响数据库模糊查询功能，不影响数据库存储过程功能，不影响NFS远程数据挂载功能，不影响Docker容器数据持久化功能，不影响大数据架构HDFS分布式存储的数据组织及检索功能。 |
| 19 | 支持一文一密，显著降低数据泄露风险。 |
| 20 | 加解密性能不低于1Gbps。 |
| 21 | 具备可靠的的密钥全生命周期管理功能。 |
| 22 | 国产化硬件：CPU、内存、主板、冗余双电源、密码卡等核心部件均采用国产化硬件。  ≥1块双端口万兆网卡及配套光模块和光纤跳线。 |
| 序号 | 资质要求 |
| 1 | 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 |

### 密码服务管理平台

|  |  |
| --- | --- |
| 序号 | 功能参数要求 |
| 1 | 满足以下全部功能并支持全院业务系统密码应用安全性评估服务和管理需求。 |
| 2 | 提供认证策略管理：用户首次接入认证的策略配置；访问策略配置：配置用户访问资源的策略，用户客户端策略配置；信任评估：实时评估用户访问行为，形成决策信息；策略联动：接入外部安全大脑，形成决策信息。 |
| 3 | 提供动态访问控制：基于上下文信息，对用户访问动作进行权限判定；挑战认证：用户访问敏感资源时，发起挑战认证；服务隐身：隐藏应用系统的对外端口，对外只提供传输网关和认证服务；单包敲门：利用SPA技术，打开服务隐藏端口，完成认证接入；传输加密：使用GM SSL协议，加密通讯数据；网络管控：根据网络访问规则，限制用户终端应用的网络接入能力。 |
| 4 | 支持算法自适应：根据客户端协议自动适配不同的算法证书；协议自适应：根据客户端协议自动选择不同的加密算法；用户认证：通过双向认证协议认证用户身份；多站点证书：可配置多个站点证书，不同的服务使用不同的站点证书。 |
| 5 | 支持动态路由：不重启服务的情况下，使修改的API路由规则的实时生效；服务治理：根据代理服务的健康状态，动态转发请求；负载均衡：每个代理服务可配置多个实例，自动实现负载均衡；熔断限流：根据实时访问流量，自动限制访问频率，降低服务压力；认证鉴权：实现代理服务的统一鉴权。 |
| 6 | 支持接口画像功能：以图表的形式展示某个接口的性能指标、调用频率等；服务画像：以图表的形式展示某个服务的性能指标、调用频率等 |
| 7 | 提供仿真测试环境为方便应用系统的加载测试、密码设备的调整测试、专项密码应用的定制开发测试、以及平台本身的升级维护测试等需要。 |
| 8 | 提供开发者指南统一提供开放的一体化开发仿真环境和开发指南。 |
| 9 | 配套基于密码安全认证的零信任客户端，支持Windows版、Linux版、Android版、IOS版。 |
| 10 | 提供密码评分数据展示：能够查看所有业务系统的评分结果，每个测评单元得分情况，并按照评测结果给出相应的整改意见。（提供产品功能截图） |
| 11 | 提供监控大屏展示：实时展示平台用户、设备、业务、评估结果等业务数据。 |
| 12 | ▲提供设备网络拓扑图，能够根据设备数据，实时构建网络拓扑图，能够查看数据流向，查看设备监控状态，硬件基本信息、设备基本信息等。（提供产品功能截图） |
| 13 | 提供密码设备管理，提供对设备数据增、删、改、查属性；提供按照产品方向，产品类型、硬件类型分类管理设备 |
| 14 | 提供密码设备监控，能够实时监控设备CPU、内存、Sys Load、网络、磁盘等数据，并以图表的形式展示出来；提供监控密码设备主机情况，状态异常时，主动下线。提供产品功能截图。 |
| 15 | 提供密码服务管理，提供对服务数据增、删、改、查属性、状态管理、与接口关联等； |
| 16 | 提供密码服务关联密码设备，能够实现不同设备间的负载均衡，也可根据权重配置负载方式，提供在不停机的情况下，实时添加负载设备，实现动态扩容 |
| 17 | ▲提供密码服务动态路由，能够在后台灵活配置服务监听路径，代理路径，灵活实现服务的动态路由。（提供产品功能截图）。 |
| 18 | 提供密码服务的远程部署，能够在管理平台上传部署包，实现服务的远程部署 |
| 19 | 提供密码接口管理，提供对服务数据增、删、改、查属性、状态管理、与密码服务关联等 |
| 20 | 提供密码接口画像，能够查看某个密码接口的调用情况，按照时间维度的调用曲线，调用耗时统计、调用结果统计等。（提供产品功能截图） |
| 21 | 提供服务分组管理，提供按照业务用途，服务类型将密码服务、密码接口灵活分组，便于权限管理。（提供产品功能截图） |
| 22 | 提供访问策略管理，能够按照IP黑白名单、访问频率（秒、分、小时、天多个细粒度）、访问时间、请求体大小、服务组等多个维度管控业务系统调用密码服务，实现灵活的访问控制配置。（提供产品功能截图） |
| 23 | 提供用户统一管理，提供按照机构、唯一标识、姓名、手机号、证件号、认证状态、用户状态查询用户数据；提供配置分类字段； |
| 24 | 提供用户同步，能够通过配置，将密码设备中的所有用户数据同步到平台，统一管理，密码设备中的用户数据修改时，平台的用户数据会同步修改 |
| 25 | 提供业务系统管理，提供对业务系统数据增、删、改、查属性、状态管理、关联访问策略等 |
| 26 | 提供多种鉴权方式，能够为不同的业务系统配置不同的鉴权方式，鉴权方式包括账号密码，数据签名，HMAC签名等 |
| 27 | 提供证书统一管理，提供按照机构，证书算法、证书类型，证书状态等条件查询证书数据，提供配置分类字段； |
| 28 | 提供证书同步，能够通过配置，将密码设备中的所有证书数据同步到平台，统一管理，密码设备中的证书数据修改时，平台的证书数据会同步修改。（提供产品功能截图） |
| 29 | 提供业务调用异常管理，提供以列表的形式展示异常数据，可查看单条异常数据的详情，调用时间、失败原因等 |
| 30 | 提供业务调用异常统计，提供以业务系统、调用时间、异常分类、异常占比不同维度展示业务调用的异常情况，能够以饼图、折线图、水波图，柱形图等不同形式展现 |
| 31 | 提供平台操作日志审计，提供基于操作模块、操作人、输入IP、操作内容关键词、时间周期等查询日志。 |
| 32 | 提供平台登录日志审计，可直观地查询某个账户的登录、退出日志。 |
| 33 | 提供业务系统调用日志管理，提供以机构、业务系统、业务序列号、服务名称、接口名称、操作结果，调用时间等条件查询日志 |
| 34 | 提供证书数据统计，能够按日期统计，并展示证书数量折线统计图、分类柱状图、状态饼状图以及算法占比图； |
| 35 | 提供用户数据统计，能够按日期统计，并展示用户数量折线统计图、状态饼状图以及认证状态占比图； |
| 36 | 提供业务数据统计，能够按日期统计，并展示业务折线统计图、服务柱状图、应用调用饼状图以及调用耗时1ms内占比图。 |
| 37 | ▲提供密码自评功能，能够以问卷的形式，对业务系统进行预评估，形成评估结果，自动提出修改意见。（提供产品功能截图） |
| 38 | ▲提供密码自测工具，能够以页面的形式提供密码自测工具，包括验证PDF有效性、验证数据签名有效性，验证证书有效性等。（提供产品功能截图） |
| 39 | 提供机构管理，提供对机构数据数据增、删、改、查属性、状态管理； |
| 40 | 提供数据分权分域管理，能够以机构的维度的所有的业务数据进行逻辑隔离。（提供产品功能截图） |
| 41 | 提供管理员权限管理，能够按照不同的角色给管理员分配权限，提供动态修改角色的权限，实现灵活的权限配置 |
| 42 | 提供平台菜单配置，能够在管理后台动态配置平台菜单目录，修改菜单顺序，菜单名称，状态等。提供产品功能截图。 |
| 43 | 提供告警配置，提供设置监控阈值、监控信息发送方式以及监控信息接收人；可分别设置CPU、内存、磁盘的告警值；提供钉钉、邮箱通知；提供记录告警日志。提供产品功能截图。 |
| 44 | 提供巡检报告管理，提供在管理后台统一管理运维巡检报告，也可通过配置实现自动生成巡检报告。（提供产品功能截图） |
| 45 | 提供统一服务管理，所有密码服务由平台API网关对外统一发布，业务系统只调用网关一个地址 |
| 46 | 提供统一服务鉴权，所有业务接口由平台API网关统一鉴权 |
| 47 | 提供统一配置管理，在平台可集中管理所有密码设备的系统配置 |
| 48 | 提供统一业务监控，在平台可集中查看所有密码设备的业务调用情况，可基于服务、接口的维度查看 |
| 49 | 提供统一设备监控，在平台中可集中查看所有密码设备的主机情况、实时监控设备运行数据。提供产品功能截图。 |
| 50 | 提供统一认证功能，具备高度可配置性和可扩展性，能够适应不同业务系统的统一认证需求；提供多种认证协议，如OAuth2.0、JWT、CAS等； |
| 51 | 支持微服务架构，并支持虚拟机、容器化部署。 |
| 52 | 支持分布式架构、水平扩展和负载均衡，以满足高并发认证请求的需求。 |
| 53 | 具备高可靠性和容错性，能够在硬件或软件故障的情况下保持系统稳定运行 |
| 54 | 具备数据安全保护机制，包括密码存储、传输和使用过程中的加密和防护措施 |
| 55 | 具备完善的开发文档、示例代码和SDK，以简化集成和定制开发过程 |
| 56 | 符合《GMT 0050-2016 密码设备管理 设备管理技术规范》要求，支持与医院已部署数字证书认证系统、签名验签服务器、时间戳服务器、电子签章系统、移动智能终端签名验签系统以及本次采购的服务器密码机、安全认证网关、数据库加密机、文件加密网关、统一认证系统等密码产品进行对接，实现现有设备的服务加载、状态监控、配置同步功能，能够通过安全通道协议，实现与密码设备的安全通信，提供对密码设备资源进行统一管理和监控。 |
| 57 | 国产化硬件：CPU、内存、主板、冗余双电源、密码卡等核心部件均采用国产化硬件。  ≥1块双端口万兆网卡及配套光模块和光纤跳线。 |
| 序号 | 资质要求 |
| 1 | 密码服务管理平台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》（提供证书复印件） |
| 2 | 密码服务管理平台支持信 创环境部署，须通过上海信 创公共服务平台适配，具备上海软协信 创工委会颁发的《信 创产品评估证书》。 |

### 密码应用服务

|  |  |
| --- | --- |
| 序号 | 功能参数要求 |
| 1 | 参考相关国标、行标、行业主管单位下发的指导文件，协助用户确定测评系统边界，并明确定级标准与测评定级。 |
| 2 | 以《GM/T39786-2021 信息系统密码应用基本要求》、《信息系统密码应用基本要求》等相关标准文件，通过工具扫描和人工核查等安全测试方法，对被测系统进行安全风险评估、排查，对信息系统进行密码应用的差距分析。结合测评标准提供差距分析报告与整改实施建议。 |
| 3 | 以《GM/T39786-2021 信息系统密码应用基本要求》、《信息系统密码应用基本要求》等相关标准文件，结合行业特性要求、监管单位要求和密码安全业务需求进行系统方案设计与撰写。 |
| 4 | 协助密测检测机构，对《信息系统密码应用解决方案》进行专家评审或机构评审，并依据评审结论，对方案进行修订，完成方案最终评审。 |
| 5 | 以《GM/T39786-2021 信息系统密码应用基本要求》、《信息系统密码应用基本要求》等相关标准文件，结合《信息系统密码应用解决方案》及密测标准，梳理整改要点和实施改造指南，辅助集成商进行系统对接及改造，并提供咨询服务。 |
| 6 | 辅助用户完成密测测评全流程资料准备，配合用户与测评机构完成系统现场测评的人员访谈、文档查阅、技术核查与测评配合等工作，配合用户通过密测，获取密测报告。 |
| 7 | 承诺协助用户开展现有密码体系利旧改造 |
| 8 | 具备相关产品备品备件能力，具备7\*24小时报障热线，隔日提供备件能力 |

## 维保期及服务要求

1. 维保期：项目验收合格之日起36个月。
2. 指定至少1名售后技术工程师，1名资深研发工程师长期为医院提供技术支持服务，充分确保项目成功实施的各种项目资源协调。
3. 维保期内派专职专业工程师负责服务跟踪，每半年对系统巡检一次，保证系统在最优化的状态下稳定运行。
4. 维保期内出现影响用户业务的故障时，根据故障等级，提出相应的故障解决方案；
5. 维保期内对应用软件提供免费升级服务、免费提供安装部署、初始化配置系统服务；保证维保期后，院方新增应用系统时，提供免费软件对接等技术服务；
6. 根据院方实际工作需要进行修改并满足工作要求，并维护期内，保证维保范围内功能模块满足客户化需求。
7. 保证免费按时完成因上级部门政策要求调整、业务管理模式改变、医院信息化测评要求等而进行业务应用系统的升级和维护；
8. 提供7\*24小时电话、网络技术支持服务，遇到系统故障15分钟内响应，能够2小时内远程解决，远程无法解决的4小时内到达现场服务直至问题妥善解决。
9. 如医院遇系统调整、机房搬迁、重大活动等需要现场保障的，需派技术工程师前往现场保障，直至保障任务结束；

10.进度要求：

本项目实施周期为6个月。

1）项目总体进度及阶段性节点如下：

（1）第1个月，完成密码应用方案设计，并通过评估；

（2）第2个月至第4个月，完成密码应用新建；

（3）第5个月至第6个月，完成系统运行效率、使用效果的后评价工作，并通过项目验收。

2）详细计划如下：

| 阶段 | 时间节点 | 工作内容 | 实施主体 | 阶段性节点 |
| --- | --- | --- | --- | --- |
| 商用密码平台一期建设方案设计 | 第1个月 | 密码应用方案沟通研讨，确定改造内容和范围。 | 系统建设单位 |  |
| 开展密码应用方案设计，确定项目总体整体架构，明确项目实施周期和关键时间节点。 |
| 开展详细的密码应用方案编制，完成系统现状分析、密码应用需求分析、技术方案、安全管理方案和实施保障方案等内容的编制。 |
| 根据密码应用的场景及方案设计内容。 |
| 对方案进行评估。 | 密评机构 | 密码应用方案通过评估 |
| 选择集成商密码应用建设 | 第2个月-第4个月 | 选择集成商，负责系统的商用密码平台一期建设 | 系统建设单位系统建设单位、系统集成商 | 选择密码应用新建集成商完成本项目密码保障体系中的技术体系建设 |
| 根据密码应用技术方案中的密码服务清单，使用对应的密码资源。 | 系统建设单位 | 完成本项目密码保障体系中的管理体系设计 |
| 根据密码应用技术方案，复用系统所在的云机房电子门禁系统、视频监控系统。 |
| 根据密码应用技术方案，对系统网络和通信层面的身份鉴别、网络传输通道、集中管理通道等方面的安全需求进行商用密码平台一期建设。 |
| 根据密码应用技术方案，对系统设备和计算层面的管理员登录身份鉴别、远程管理身份鉴别信息传输、访问控制信息、重要应用程序、日志记录等方面的安全需求进行商用密码平台一期建设。 |
| 根据密码应用技术方案，对系统应用和数据层面的访问用户身份鉴别数据、医疗数据、业务日志数据等方面的安全需求进行商用密码平台一期建设。 |
| 根据安全管理方案，设计密码安全管理制度、人员管理、设备管理、应急处置等方面的管理体系。 |
| 试运行 | 第5个月 | 开展系统试运行、收集试运行期间的性能，效率、安全状态等数据，根据试运行情况做进一步评估和优化。 | 系统建设单位 | 开始试运行 |
| 项目验收 | 第6个月 | 完成系统运行效率、使用效果的后评价工作，根据评价结果进行项目验收。 | 系统建设单位 | 通过项目验收 |

11.团队要求：

1）组织和人员保障

我单位将该项目作为重点任务，在项目组织上本着“统一领导、健全组织、合理分工、密切协作”的原则，明确项目组织形式，设置项目组织架构，按照职责分工开展工作，为顺利实施商用密码平台一期建设项目，高质量、高效率完成商用密码平台一期建设提供组织保障。

项目组织形式见下图，各组工作实行组长负责制。



各组人员组成及工作职责如下表所示。

|  |  |  |
| --- | --- | --- |
| 序号 | 名 称 | 工作职责 |
| 1 | 项目负责人 | 总体负责项目的技术、组织和财务等方面工作，宏观把握项目改造内容和建设目标。 |
| 2 | 项目技术组 | 由项目负责人及项目骨干组成，负责项目总体管理、各部分工作协调、项目进展情况和项目完成情况的监督检查、项目改造后的质量把关。 |
| 3 | 项目财务组 | 由我单位财务部门负责人和骨干组成，负责项目执行过程中的经费管理。 |
| 4 | 质量保障组 | 负责按照本项目制定的质量保障措施，落实质量监督和管理。 |

1. 经费保障

本项目执行过程中，将严格按照单位资金使用管理办法，进行经费使用，确保经费使用合规。

1. 质量保障

在项目建设实施过程中，通过组织项目定期会议，保障实施工作按计划进行；同时对于项目实施过程中出现的偏差或问题，及时沟通协调，必要时通过项目技术组向项目负责人进行汇报，并形成相应的决策意见和修订方案。

1、项目例会制度

项目通过定期例会和不定期会议来跟踪项目进度，反馈和讨论项目实施过程中的问题，对项目技术方案进行评审，对计划完成情况进行总结和说明，同时对后续计划进行确认。在遇到技术障碍或方案涉及重大变更时，通过不定期会议，由项目技术组或质量保障组讨论决策，针对出现的变更或重大问题进行及时修正，并制定相应的措施和方案。

2、项目周报机制

由项目技术组制定项目进展周报机制，每周五提交本周的项目进展、阶段成果、遗留问题和下周计划，质量保障组对项目进度进行统筹跟踪，协调相关人员和资源，保障项目如期完成。

3、风险管理机制

项目在实施过程中，建立完善的风险管理机制，包括项目风险的识别、评估和管理，从资金、成本控制、采购合规、技术、人才、管理等多个方面进行风险管控，包括确定风险发生时的备选方案、资金、设备和人员等；定期检查和评估风险消减措施是否有效；定期进行风险排查；制定风险应对的启动机制等措施。

1. 监督检查

监督检查是保证项目实施各阶段的活动顺利开展的重要措施，拟通过如下几类活动开展监督检查工作：

阶段评审：在系统实施过程中，定期地或阶段性地对系统和文档进行评审。在本项目中拟进行以下三次评审：第一次评审方案合理性、确认验收方法；第二次评审方案的实施计划，实施步骤、测试方法，试运行方案等，并对第一次评审结果复核；第三次评审功能和综合检查。阶段评审要组织专门的评审小组，评审小组原则上由实施小组成员、用户项目管理小组成员、我公司代表等构成。

日常检查：在本项目实施过程中，督促各子系统填写项目进展报告，即各个设备调试进展报告、软件安装部署阶段进度表、项目完成情况表等三张表格。项目管理人员可以通过项目进展报告发现有关项目实施过程中的问题

5）其他

项目负责人具有注册信息安全专业人员CISP资质（或同等）资质优先考虑。

12.其他要求

1）投标人具有近三年类似项目业绩的优先考虑；

2）投标人具有ISO27001信息安全体系认证证书、CS信息系统建设和服务能力评价等级证书、ITSS信息技术服务标准符合性证书证书的优先考虑。

3）投标人需提供的密码应用安全解决方案设计包括：密码应用技术框架设计、密码服务支撑体系设计、物理和环境安全设计、网络和通讯安全设计、设备和计算安全设计、应用和数据安全设计、密评高风险项控制设计、密钥管理安全设计、以安全管理方案设计及安全与合规性分析。