采购需求文件

第一部分 供应商资格要求

1、满足《中华人民共和国政府采购法》第二十二条规定，即：

（1）具有独立承担民事责任的能力；

（2）具有良好的商业信誉和健全的财务会计制度；

（3）具有履行合同所必需的设备和专业技术能力；

（4）有依法缴纳税收和社会保障资金的良好记录；

（5）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）法律、行政法规规定的其他条件。

2、应未被列入失信被执行人、重大税收违法案件当事人名单，未被列入政府采购严重违法失信行为记录名单；

3、本项目不接受联合体。

第二部分 技术服务要求

一、采购清单

序号	服务内容	数量	单位
1	传输加密服务	1	项
2	数据加密服务、完整性保护服务、文件加密服务、密钥管理服务	1	项
3	终端密码服务	1	项
4	视频监控管理服务	1	项
5	密码应用咨询服务	1	项
6	方案设计与规划服务	1	项
7	系统集成与改造服务	1	项
8	培训服务	1	项
9	巡检服务	1	项

二、服务保障期限

一年

三、技术服务要求

3.1 需求概况

为满足《网络安全法》《密码法》及《信息系统密码应用基本要求》（GB/T 39786-2021）等政策标准的要求，提升医院信息系统的密码合规水平，保障核心业务系统的通信安全、数据安全与时间一致性，医院拟开展密码应用安全性评估配套支撑服务建设，采购密码安全服务，并包含密码建设实施方案编写、湖北省密码管理局备案咨询等服务。通过本项目，将为医院提供覆盖“传输加密、数据加密、时间同步”等方面的技术服务，支撑后续密评工作的开展。

医院目前已部署了签名验签服务器（签名验签服务）及电子签章等密码设备用于医技人员电子签名，并由第三方 CA 机构配发了相应数量的个人数字证书，相关签名设备具备商用密码产品认证证书，并在业务系统登录环节和电子签名环节实现了合规应用。本次需要在该环境基础上采购信息技术服务，完成合规改造，并要求尽可能减少对现有业务系统运行的干扰。

3.2 传输加密服务

3.2.1 服务内容

为医院指定的业务系统的数据通信链路提供基于国家密码算法的加密保护，确保传输过程中数据的机密性与完整性。提供基于国家密码算法的安全传输加密服务，支持对医院核心业务系统与终端访问链路进行 SSL VPN 加密保护，并保障国密算法的兼容性与可用性；服务提供方应配置具备国密算法支持能力的终端接入组件，保障加密访问环境的一致性。

3.2.2 服务要求

1、 服务提供方需负责完成医院对应系统的传输加密环境的接入部署，建立基于SSL VPN 协议的国密传输加密链路；

2、 提供贯穿部署、运行、策略管理和问题响应全过程的运维保障服务，包括加密策略制定、证书管理、异常处理与技术支持；

3、 结合信息安全管理要求，协助制定并实施加密通道使用规范，完善通信加密审计与管理制度，确保服务的可控、可管、可追溯；

4、 提供传输加密服务运行期间的状态监控、策略调整、日志审计及定期优化建议报告。

3.2.3 服务工具

2 台综合安全网关

序号	指标	技术要求
1	性能指标	≥1U 机架式设备，采用国产 CPU，国产操作系统，内置密码卡，≥4 个千兆电口，冗余电源。
2	资质证书	具备商用密码检测认证中心颁发的商用密码产品认证证书
3	负载功能	传输机密服务组件支持负载均衡，支持轮询、随机、IP 哈希和最小连接数多种负载算法
4	管理界面	支持管理界面 Web 代理数、CS 代理数、SSL 新建连接数、SSL 并发连接数、IPSec 隧道数、证书数量、CPU 使用率、内存使用率、存储使用率，实时网络吞吐量
5	正确性检测	支持包括 SM2 算法、SM3 算法、SM4 算法正确性检测，密钥完整性检测，随机数可靠性检测，服务状态检测，运行文件校验，关键配置信息校验
6	设备管理	支持 SSL 协议、IPSec 协议、登录管理、网络管理、日志管理、系统信息、网关管理以外，还应支持防火墙管理、密码卡管理、CA 中心管理、网络工具功能

7	协议加速	支持 SSL、IPsec 两种安全协议，通过内置的符合 GM/T0028《密码模块安全技术要求》安全等级二级的 PCI-E 密码卡实现 SSL 和 IPSec 协议加速功能
8	Web 认证	支持 Web 认证和客户端 SDK 方式访问传输加密服务
9	身份认证	客户端支持用户通过智能密码钥匙进行登录，实现运维人员身份鉴别

3.3 数据加密服务、完整性保护服务、文件加密服务、密钥管理服务

3.3.1 数据加密服务

3.3.1.1 服务内容

为医院指定的业务系统数据库提供符合国家密码标准的数据加密服务，保障数据在存储过程中的保密性与不可篡改性。提供对医院指定数据库的静态数据加密与密钥保护服务，确保敏感数据在存储层的保密性。服务过程中应使用符合国家密码算法标准的加密机制，支持透明加密与审计追踪能力。

3.3.1.2 服务要求

1、 服务提供方需完成医院相关业务数据库的加密接入部署，实现对存储数据的加密保护，确保在不影响系统性能和应用逻辑的前提下实现数据安全防护；

2、 提供全面的加密策略设计、密钥管理、访问控制和密钥生命周期服务，确保密钥生成、分发、更新、注销等过程的安全合规；

3、 服务期间应提供操作日志记录与行为审计功能，支持医院信息安全制度对操作可追溯性的要求；

4、 协助医院完善数据加密制度与合规流程，保障静态数据加密与访问控制机制与密评要求一致；

5、 提供运行期间的加密服务监控、配置优化、例行巡检与问题处置支持，确保加密服务长期稳定运行。

3.3.2 完整性保护服务

3.3.2.1 服务内容

为医院指定的业务系统数据库提供符合国家密码标准的完整性保护服务，保障数据在存储过程中的完整性。提供对医院指定数据库的静态数据完整性保护服务，确保敏感数据在存储层的完整性。服务过程中应使用符合国家密码算法标准的完整性保护机制，支持透明完整性与审计追踪能力。

3.3.2.2 服务要求

1、 服务提供方需完成医院相关业务数据库的完整性接入部署，实现对存储数据的完整性保护，确保在不影响系统性能和应用逻辑的前提下实现数据安全防护；
2、 提供全面的完整性保护策略设计、访问控制；
3、 服务期间应提供操作日志记录与行为审计功能，支持医院信息安全制度对操作可追溯性的要求；
4、 协助医院完善数据完整性制度与合规流程，保障访问控制机制与密评要求一致；
5、 提供运行期间的完整性保护服务监控、配置优化、例行巡检与问题处置支持，确保完整性保护服务长期稳定运行。

3.3.3 文件加密服务

3.3.3.1 服务内容

为医院的指定的业务系统文件数据提供符合国家密码标准的文件加密服务，保障文件在存储过程中的保密性与不可篡改性。提供对医院指定的文件加密服务，确保敏感文件在存储层的保密性。服务过程中应使用符合国家密码算法标准的加密机制，支持文件加密与审计追踪能力。

3.3.3.2 服务要求

1、 服务提供方需完成医院相关业务文件的加密接入部署，实现对存储文件的加密保护，确保在不影响系统性能和应用逻辑的前提下实现数据安全防护；
2、 提供全面的加密策略设计、访问控制服务；
3、 服务期间应提供操作日志记录与行为审计功能，支持医院信息安全制度对操作可追溯性的要求；
4、 协助医院完善文件加密制度与合规流程，保障文件加密与访问控制机制与密评要求一致；
5、 提供运行期间的加密服务监控、配置优化、例行巡检与问题处置支持，确保文件加密服务长期稳定运行。

3.3.4 密钥管理服务

3.3.4.1 服务内容

为医院指定的业务系统的加密密钥提供符合国家密码标准的密钥管理服务，保障密钥的全生命周期管理。提供对医院指定密钥管理服务，支持对 SM3 密钥、SM4 密钥进行全生命周期管理，支持审计追踪能力。

3.3.4.2 服务要求

1、 服务提供方需完成医院相关密钥管理服务的部署，实现对密钥的安全管理，防止医院内相关加密密钥泄露；
2、 提供密钥生命周期服务，确保密钥生成、分发等过程的安全合规；
3、 服务期间应提供操作日志记录与行为审计功能，支持医院信息安全制度对密钥可追溯性的要求；
4、 协助医院完善密钥管理制度与合规流程，保障密钥管理与密评要求一致；
5、 提供运行期间的密钥管理服务配置优化、例行巡检与问题处置支持，确保密

钥管理服务的长期稳定运行。

3.3.5 服务工具

2 台数据库加密机

序号	指标	技术要求
1	性能指标	≥2U 机架式设备，采用国产 CPU、国产操作系统，1+1 冗余电源，≥2 个千兆电口，设备支持光纤网口扩展，采用 SM4 算法对存量数据进行处理时，列加密速率≥14000 行/秒，列解密速率≥13000 行/秒,采用 SM4 算法对增量数据进行处理时，加密速率≥40 行/秒
2	国密算法	支持 SM4 对称密码算法，支持 SM3 摘要算法
3	数据库	支持 Oracle、Mysql、SQL Server、达梦、人大金仓、瀚高、Gauss 等主流数据库透明加密
4	字段级加密	支持字段级加密，确保数据的机密性
5	完整性	支持字段级完整性保护和校验，确保数据的完整性
6	自动识别	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
7	非关系型数据库	支持非关系型数据库透明加密
8	密钥管理	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
9	双因子认证	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
10	三权分立	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

3.4 终端密码服务

3.4.1 服务内容

为医院的客户端数据通信链路提供基于国家密码算法的加密保护，确保传输过程中数据的机密性与完整性。提供基于国家密码算法的安全传输加密服务，支持对终端访问服务端链路进行 https 加密保护，并保障国密算法的兼容性与可用性。

3.4.2 服务要求

1、 服务提供方需负责完成医院对应的客户端传输加密环境的接入部署，建立基于 SSL 等协议的国密传输加密链路；

2、 提供终端接入侧的安全访问能力，包括院内终端国密浏览器的兼容性调优，确保终端访问体验与加密能力并存；

3、 提供贯穿部署、运行、策略管理和问题响应全过程的运维保障服务，包括加密策略制定、证书管理、异常处理与技术支持；

4、 结合医院信息安全管理要求，协助制定并实施加密通道使用规范，完善通信加密审计与管理制度，确保服务的可控、可管、可追溯；

5、 提供传输加密服务运行期间的状态监控、策略调整、日志审计及定期优化建议报告；

3.4.3 服务工具

国密浏览器

序号	指标	技术要求
1	证书管理	支持证书管理，支持证书的导入导出
2	国密算法	支持基于 SM2 算法的 HTTPS/SSL 传输协议、支持支持 SM4 对称算法；支持 SM2 非对称算法
3	资质证书	具备商用密码检测认证中心颁发的商用密码产品认证证书

3.5 视频监控管理服务

3.5.1 服务内容

提供基于商用密码体系的视频监控管理服务，涵盖视频监控、门禁管理等核心模块。服务支持医院已部署的商密摄像头、商密存储及门禁设备的统一接入与运行状态实时监测，保障系统高效、安全运行。服务需保障门禁事件日志的完整性和视频记录文件的完整性。通过符合国家密码标准的技术手段，对门禁日志进行实时审计和篡改检测，对视频文件进行完整性校验与播放验证，确保所有监控与门禁记录的安全、真实、可追溯，为医院的安全管理提供有力支撑。

3.5.2 服务要求

1、服务提供方应保障医院现有商密视频监控设备、门禁设备的兼容接入，确保系统运行状态实时可视、故障快速预警、运维统一管理；

2、服务需实现视频监控与门禁系统的统一事件告警管理，支持对异常事件进行分级分类响应，满足医院信息安全管理制度对事件可追溯、操作可审计的要求；

3、服务主机系统应内置日志审计系统与视频播放器，日志审计系统须支持对门禁事件日志进行实时记录、校验与审计，具备检测日志是否被非法篡改的能力；

4、服务包含的视频播放器应支持视频记录文件的完整性校验功能，播放前自动检测视频数据是否存在异常篡改行为，如发现篡改应及时告警并提供明确提示信息，确保视频资料的取证有效性；

5、上述日志与视频完整性保障功能应基于国家密码算法标准进行实现，确保在数据采集、传输、存储及访问全流程中的安全合规性；

6、提供系统运行期间的巡检维护、策略优化、日志归档、问题处置及技术支持服务，保障门禁与视频监控系统长期稳定运行并满足等级保护及密码合规相关要求。

3.5.3 服务工具

1 台视频门禁监控管理系统

序号	指标	技术要求
1	性能参数	推荐视频接入路数：32 推荐门禁接入路数：16 推荐视频并发调阅：4 路（1080P@25 帧 4M 码流） 4 个 10/100/1000 MpbsI211 网口、1 个 COM 口+1 个 VGA 口+1 个 HDMI 口
2	视频导出加密	支持对客户端下载/导出的视频文件进行加密和完整性保护，通过专用播放器解密及完整性校验通过后才可正常播放
3	视频外发管控	支持视频图像下载后使用有效期和播放次数限制，仅允许授权用户在有效范围内查看使用
4	水印灵活配置	支持对水印文字大小、颜色、旋转角度等属性灵活配置，并能够适应监控画面窗口的移动
5	门禁记录完整性	支持对门禁事件（开/关门）进行完整性保护，完整性算法支持 SM2、HMAC-SM3 灵活配置
6	操作日志审计	支持对客户端登录、视频预览/回放/下载/导出、门禁进出等进行详细日志记录，支持日志完整性保护及有效审计
7	设备接入管理	支持商密摄像机、商密存储、商密门禁设备管理，并实时监控设备运行状态
8	事件告警管理	支持实时接收事件/告警信息，可根据事件级别筛选显示；支持门禁事件一键导出

3.6 密码应用咨询服务

3.6.1 服务内容

提供密码应用相关法律法规、技术标准等咨询，协助了解密评要求和密码应用规范。针对业务系统特点，进行现状与差距化分析及需求分析，给出商用密码

建设建议，业务系统密码应用对接改造指导，针对测评整改意见进行应答指导。

3.6.2 服务要求

1、 完成密码建设方案制定与测评过程指导，提升密评应对能力；

2、 提供咨询过程中的资料、文件及制度模板支持，提升医院整体密码合规水平。

3.7 方案设计与规划服务

3.7.1 服务内容

根据医院需求和密评标准，进行系统调研编制密码应用方案，包括密码技术选型、部署方式、密钥管理策略等。满足专家评审及湖北省密码管理局备案咨询要求。

3.7.2 服务要求

1、 开展密码应用系统的调研与需求梳理，明确系统改造目标；

2、 提供完整的密码应用方案，包括技术选型、部署结构、密钥管理、接口对接等内容；

3、 依据《GB/T 39786-2021》编制密码应用建设方案，涵盖物理和环境安全，网络和通信安全，设备和计算安全，应用和数据安全，管理制度，人员管理，建设运行，应急处置等层面；

4、 协助组织专家评审，提供评审意见修改及备案材料准备；

5、 协助对接湖北省密码管理局，完成商用密码应用安全性评估（密评）备案流程。

3.7.3 服务交付物

《医院商用密码应用建设实施方案》（含密评整改建议）

3.8 系统集成与改造服务

3.8.1 服务内容

负责将符合国家密码标准的商用密码产品集成至医院现有各类业务系统流程中，确保产品与原有信息系统在接口协议、业务流程、数据结构等方面的兼容性，实现密码功能在数据存储、传输、认证、访问控制等环节的有效应用。

对于不符合密码应用安全评估（密评）要求的系统，应提供现状调研、差距分析、整改建议、业务改造等服务，并协助完成改造过程中的开发、测试、上线及效果验证工作，尽可能减少对业务系统的影响，实现密码功能的平滑集成和合规落地。

3.8.2 服务要求

1、 完成密码产品与各业务系统的集成适配，实现密码功能全流程对接；

2、 提供改造全流程的技术支撑，确保实施可审计、可追踪；

3、 服务商须完成商用密码产品与医院现有系统的集成适配，确保密码功能实现全流程无缝衔接；

4、 服务商应提供系统改造全过程的技术支持，涵盖密码对接、系统配置调整、联调测试及部署上线等，确保改造过程可审计、可追溯；

5、 对于无法直接集成的业务系统，服务商应提供最小影响的改造建议或兼容适配方案，保障业务连续性与合规性的平衡；

6、 服务商须提供完整的技术文档交付，包括集成方案设计说明书、接口文档、改造说明、部署手册及测试报告等，供医院存档及审计使用；

7、 密码功能上线后应提供运行保障期服务，在保障期内负责处理集成过程中发现的功能缺陷及性能问题，确保系统稳定、安全运行并满足密评要求。

3.9 培训服务

3.9.1 服务内容

提供密码应用安全培训，提高人员安全意识和技能水平，深入了解密码应用的重要性、使用方法和相关操作规范，更好地配合密评工作和保障系统安全运行。服务商应提供针对医院管理人员、技术人员、安全运维人员的密码应用安全培训服务，培训内容应包括密码应用基本概念、国家法律法规与政策标准、典型产品使用方法、密评工作要求及整改案例分析等。

培训应结合实际部署系统开展操作演示与场景讲解，帮助参训人员理解密码技术在医院场景下的应用方式与安全要求，提升其密码应用意识和操作能力，为系统安全运行与密评合规提供人员保障。

3.9.2 服务要求

1、服务商应提供多种形式的培训服务，包括但不限于线下集中授课、远程视频讲解、线上培训资料包等，满足不同人员的培训需求与时间安排；

2、服务商应提供完整的培训归档资料，包括培训课件（PPT）、培训计划、签到表、现场照片、测试题与答卷、培训总结等，满足医院制度建设与审计要求；

3、服务商应根据参训对象分层设计培训内容，确保管理人员理解政策合规方向，技术人员掌握密码系统使用与运维技能；

4、根据医院要求，服务商应在系统上线、密评准备等关键节点提供专题培训，确保相关人员具备应对密评工作的能力；

5、培训应提供现场答疑与问题反馈机制，确保培训效果可评估、问题可闭环。

3.10 巡检服务

3.10.1 服务内容

服务商应提供季度例行的密码系统巡检服务，内容涵盖已部署商用密码产品及其运行环境的运行状态检查、配置合规性核查、密钥生命周期管理情况、密码策略执行情况、日志记录与访问控制等关键安全指标的综合检查。

巡检服务应以制度化、标准化的流程执行，形成闭环管理机制，对发现的问题应提出合理化优化建议，并进行跟踪整改，确保密码系统运行状态持续合规、

稳定、安全。

3.10.2 服务要求

1、服务商须按季度定期开展密码系统巡检工作，确保覆盖全部已部署商用密码产品及相关应用系统，并按要求提交标准化巡检报告；

2、巡检内容应包括但不限于：密码服务运行状态、密钥生命周期完整性、配置策略与国家标准一致性、日志完整性、访问控制策略等；

3、对于巡检中发现的系统隐患、配置问题或策略偏差，服务商应提出可行的整改建议，并协助医院制定整改方案，跟踪整改进度直至问题闭环；

4、服务商须提供完整的巡检支撑文档，包括巡检计划、现场检查记录、问题汇总表、优化建议报告、后续改进方向等材料，满足医院安全管理及评估需要；

5、医院可根据项目实施阶段或测评工作安排，要求服务商提供专项巡检与突发问题排查服务，服务商应及时响应并提供技术支持。