

泸州市中医医院

商用密码改造和测评工作（包一）

需求参数

一、商用密码建设产品清单

序号	产品名称	数量	单位	基本参数	备注
1	动态口令服务器	1	台	1、标准机架式设备 $\geq 2U$ ，双电源，国产 8 核 CPU，国产操作系统，SSD 硬盘 $\geq 480G$ ，内存 $\geq 8G$ ，千兆电口 ≥ 6 个、千兆光口 ≥ 4 个； 2、性能要求： 短信令牌(SM3)生成 ≥ 1000 次每秒， 短信口令(SM3)生成 ≥ 300 次每秒， 动态令牌(SM3)验证 ≥ 1000 次每秒； 3、支持丰富的令牌算法种类，同时支持以下算法生成动态口令：SM3 算法、SM4 算法、HMAC-SM3 国密算法；支持 RSA 算法，支持动态增加算法，以扩展系统对多种不同算法的支持，支持各种加密算法； 4、支持多种令牌类型，包括：时间型令牌，事件形令牌，多键令牌，移动令牌等； 5、具备商用密码检测认证中心颁发的有效期内的《商用密码产品认证证书》； 6、提供原厂三年软硬件质保。	解决登录业务系统的身份鉴别问题，实现基于动态口令的双因素登录。
2	应用安全网关	1	台	1、标准机架式设备 $\geq 2U$ ，双电源，国产 8 核 CPU，HDD 硬盘 $\geq 1T$ ，内存 $\geq 16G$ ，液晶屏，千兆电口 ≥ 6 个、千兆光口 ≥ 4 个，内置密码卡； 2、SSL 吞吐率 $\geq 4Gbps$ ，SSL 每秒新建连接数 ≥ 10000 ，四层吞吐率 $\geq 40Gbps$ ，4 层并发连接数 ≥ 15000000 ，七层吞吐率 $\geq 40Gbps$ ； 3、支持 SM2、SM3、SM4 和通用标准算法，提供 SSL 卸载服务；SSL 协议支持： TLS1.0/TLS1.1/TLS1.2/TLS1.3/SM2v1.1； 4、具备商用密码检测认证中心颁发的有效期内的《商用密码产品认证证书》； 5、提供原厂三年软硬件质保。	解决用户访问业务系统时的通信链路加密问题，基于国密算法对通信数据进行加密和哈希运算，实现通信数据的机密性和完整性保护。

3	数据加解密服务器	1	台	<p>1、标准机架式设备≥2U，双电源，国产 4 核 CPU，硬盘≥1T，内存≥8G。千兆电口≥4 个、万兆光口≥2 个；</p> <p>2、默认密钥容量≥10,000，最大在线加解密吞吐量（SM4）≥1Gbps，最大每秒在线加解密处理能力（SM4）≥5000；</p> <p>3、为业务系统提供密钥管理、通用加解密、数据库加解密等安全服务，能够对敏感数据、重信息进行加密保护；</p> <p>4、支持不同字段采用不同密钥进行加解密，支持 SM2、SM3、SM4 国密算法；</p> <p>5、具备商用密码检测认证中心颁发的有效期内的《商用密码产品认证证书》；</p> <p>6、提供原厂三年软硬件质保。</p>	基于国密算法对存储到数据库中的重要业务数据进行加密，实现重要业务数据存储机密性和存储完整性保护。
4	SSL VPN	1	台	<p>1、标准机架式设备≥2U，双电源，国产 8 核 CPU，硬盘≥1T，内存≥16G，液晶屏，千兆电口≥6 个、千兆光口≥4 个，同品牌密码卡。最大并发用户数：≥2000；</p> <p>2、支持 SSLv3、TLSv1、TLSv1.1、TLSv1.2、TLSv1.3、SM2v1.1 等多种国际、国密加密协议，满足不同的应用场景的需求；</p> <p>3、同时支持 SSL 协议和 IPsec 协议的 site2site VPN 模式，采用国密证书实现 IPsec VPN 身份鉴别，IKE SA 和 IPsec SA 采用国密算法 SM2\SM3\SM4 进行安全协商；</p> <p>4、支持多种身份鉴别认证方法支持 LDAP、RADIUS、AD、证书、本地数据库、SAML、OAuth 等，能够满足密评场景中多因素认证需求；</p> <p>5、具备商用密码检测认证中心颁发的有效期内的《商用密码产品认证证书》；</p> <p>6、提供原厂三年软硬件质保。</p>	解决运维人员对设备进行远程运维时安全问题，基于 UKEY 实现运维人员登录时的双因素身份鉴别，基于国密算法对运维通道进行加密保护，实现运维管理通道安全。
5	站点证书	1	张	<p>1、提供受信任的第三方 CA 签发的证书，用于 PC 端浏览器与应该安全网关建立安全传输通道；</p> <p>2、提供原厂三年升级维保。</p>	部署应用安全网关上，业务系统的身份标识，防止网站被仿冒。
6	国密电子门禁系统	1	套	<p>1、系统符合 GM/T 0036 标准要求，具备门禁系统类商用密码产品认证证书，所含国密 CPU 卡、安全读卡模块、PSAM 卡、PCI-E 密码卡等密码模块。支持门禁日志记录篡改报警提示；</p> <p>2、门禁管理：支持人员管理、设备管理、门禁管理、权限配置、实时查看、日志查询、反潜、互锁、多卡开门、远程开关门、电子地图、输入输出报警联动等通用门禁管理功能；</p>	解决人员进出机房的身份鉴别。

				3、提供原厂三年软硬件质保。	
7	移动 令牌 客户 端	2	套	1、提供 Android、IOS 移动令牌 APP，支持动态密码生成，用于实现用户身份鉴别； 2、提供原厂三年软硬件质保。	动态口令服务器的配套工具，用于显示动态口令。
8	国密 安全 浏览器	10	套	1、为 PC 端用户提供基于国密算法的 SSL 数据通道加密，保障数据传输的机密性； 2、提供原厂三年软硬件质保。	用于使用国密算法访问业务系统
9	国密 堡垒 机	1	台	<p>1. 标准机架式设备，采用国产处理器和国产操作系统，内存≥16GB，硬盘≥2TB，冗余电源，千兆电口≥4 个，千兆光口≥2 个，配置国密硬件加密卡，≥2 个硬件动态口令卡，支持手机令牌验证，配置本次所需的手机令牌，配置资产授权数≥200 个，并发连接≥200 个；</p> <p>2. 支持完整的口令安全策略配置，可自定义密码长度、复杂度、历史密码复用限制，禁止密码与用户名、用户名逆序相同，支持密码过期告警，支持依据密码错误次数、访问源 IP 锁定账号，长期未登录账号自动禁用，保障账号口令安全基线；</p> <p>3. 支持对运维操作会话、文件传输会话进行实时监控，支持配置审计豁免策略，可对指定业务会话关闭录像审计，保护高敏感业务信息，防止机密数据二次泄露；</p> <p>4. 运维客户端具备资产分组、资产连通性检测、批量运维操作能力，支持资产访问审批、高危命令审批、多级复核审批，实现运维访问全流程权限管控；</p> <p>5. 资产信息导出文件支持加密封装，导出文件需使用解密工具才能读取内容，保障资产台账导出的数据安全；</p> <p>6. 对 Web 资产实现黑白名单访问管控，拦截未经授权的手动跳转行为，限制运维侧访问范围，降低越权访问与非法外联风险；</p> <p>7. 支持主机名称、资产名称、资产来源、网络状态、操作系统等条件查询，检索框支持多关键字模糊检索，便于快速定位目标运维资产；</p> <p>8. 兼容主流数据库，支持账号代填自动登录，可调用本地数据库客户端工具，应用发布服务器兼容 Windows 和国产主流操作系统；</p> <p>9. 提供原厂三年软硬件质保及特征库持续更新服务。</p>	<p>实现国密强身份鉴别，通过集成国密数字证书、USBKey 等，替代传统弱口令，满足密评中“身份鉴别”必须采用密码技术的合规要求。保障运维通道安全，在运维端与目标设备之间建立国密 SSL 加密通道，确保远程运维数据的机密性和完整性。</p>

10	堡垒机	1	台	<p>1. 标准机架式设备，千兆电口≥ 4个，内存$\geq 8\text{GB}$，硬盘$\geq 2\text{TB}$，≥ 2个硬件动态口令卡，支持手机令牌验证，配置本次所需的手机令牌，配置资产授权数≥ 100个，并发连接≥ 100个；</p> <p>2. 支持完整的口令安全策略配置，可自定义密码长度、复杂度、历史密码复用限制，禁止密码与用户名、用户名逆序相同，支持密码过期告警，支持依据密码错误次数、访问源 IP 锁定账号，长期未登录账号自动禁用，保障账号口令安全基线；</p> <p>3. 支持对运维操作会话、文件传输会话进行实时监控，支持配置审计豁免策略，可对指定业务会话关闭录像审计，保护高敏感业务信息，防止机密数据二次泄露；</p> <p>4. 运维客户端具备资产分组、资产连通性检测、批量运维操作能力，支持资产访问审批、高危命令审批、多级复核审批，实现运维访问全流程权限管控；</p> <p>5. 资产信息导出文件支持加密封装，导出文件需使用解密工具才能读取内容，保障资产台账导出的数据安全；</p> <p>6. 对 Web 资产实现黑白名单访问管控，拦截未授权的手动跳转行为，限制运维侧访问范围，降低越权访问与非法外联风险；</p> <p>7. 支持主机名称、资产名称、资产来源、网络状态、操作系统等多维度条件查询，检索框支持多关键字模糊检索，便于快速定位目标运维资产；</p> <p>8. 兼容主流数据库，支持账号代填自动登录，可调用本地数据库客户端工具，应用发布服务器兼容 Windows 和国产主流操作系统；</p> <p>9. 提供原厂三年软硬件质保及特征库持续更新服务。</p>	提供集中管控、安全访问与全程审计，解决“运维身份不可信、操作不可控、行为无审计”的问题。
----	-----	---	---	---	--

11	日志审计系统	1	台	<p>1. 标准机架式设备，配置千兆电口≥ 6个，内存$\geq 16\text{GB}$，硬盘$\geq 8\text{TB}$，冗余电源，本次配置日志源≥ 100个，日志处理性能≥ 4000条/秒；</p> <p>2. 具备网络资产自动发现识别能力，可主动扫描识别网络内日志源资产并完成登记建档，减少人工维护成本，保障资产台账完整准确，适配常态化资产变更管理；</p> <p>3. 支持全品类异构设备日志采集，兼容路由器、交换机、防火墙、物理服务器、虚拟化平台等网络设备、安全设备、主机系统，可统一归集设备运行日志与操作审计日志；</p> <p>4. 内置安全评估分析模型，围绕设备故障、身份认证、攻击行为、业务可用性、系统脆弱性多维度加权计算整体安全指数，支持展示实时安全评分及历史变化趋势，各风险指标支持逐层下钻，可溯源定位到原始日志告警事件，便于安全事件分析处置；</p> <p>5. 配备可视化日志解析辅助工具，支持针对日志样本划词提取关键字段，快速生成正则解析规则，同时支持解析效果预览与在线校验，降低自定义解析规则编写难度，提升日志归一化处理效率；</p> <p>6. 支持 Agent 代理采集模式，可对业务主机的 CPU、内存、磁盘、网络流量等关键运行性能指标进行采集，主机监控指标统一在平台界面可视化呈现，实现日志审计与主机运行状态一体化监控；</p> <p>7. 支持原始日志以标准文本格式对外输出，提供标准化数据输出接口，可对接第三方安全运营平台、大数据分析平台，满足跨系统数据共享、联动分析的业务需求；</p> <p>8. 支持日志数据本地备份和远程备份，可灵活自定义日志存储保留周期，满足等保及行业合规对日志留存的管控要求；</p> <p>9. 日志接收、转发全链路支持加密传输，对传输中的日志数据进行保护，有效防范日志在传输过程中被窃听、篡改，保障审计日志传输环节的数据安全；</p> <p>10. 提供原厂三年软硬件质保。</p>	统一日志归集与存储、满足合规审计要求
12	系统改造费用	2	个	<p>1、集成平台系统和互联网医院系统基于动态口令与数据加解密接口的升级改造，符合密评要求；</p> <p>2、配合网络和通信层面数据安全传输升级改造，符合密评要求。</p>	系统的二次开发和改造

13	密码应用方案编写服务	2	项	1、集成平台系统和互联网医院系统密码应用方案编写； 2、符合商用密码相关要求，达到四川省密码局备案的标准。	密码应用方案编写并配合通过评审备案
----	------------	---	---	--	-------------------

二、具体服务内容

供应商须无条件免费为本项目清单内所有软、硬件设备提供部署所需的一切（网线、光模块等）配件，对本项目清单内所有软、硬件设备提供 3 年原厂维保、升级等服务，严格遵循国家、省市商用密码法律法规、行业规范及密码主管部门管理要求开展服务，具体服务内容如下：

1、产品系统软件升级及硬件免费维修

供应商需对本项目服务范围清单内的产品提供原厂完整质保服务，包含硬件免费维修、原厂正版软件升级授权等全部服务内容。服务范围不限于设备故障硬件检测、更换、维修，系统固件、商用密码专用软件版本迭代升级、漏洞修复、合规补丁更新等，全程免收配件费、人工费、升级服务费等所有费用，保障设备软硬件持续合规、稳定运行。

2、配置修改及优化

（1）供应商需严格依据国家商用密码测评标准、商用密码合规评估要求、密码管理部门日常监管及执法检查整改意见、医院业务运行需求，全程配合医院完成商用密码合规整改、自查整改、专项整改等各项工作。

（2）结合日常巡检、定期检测出具的设备运行报告、系统合规报告，排查设备配置隐患、密码策略漏洞、系统运行短板，定制专属、可落地的设备配置调整方案、密码策略优化方案及系统整改提升方案。针对性完成商用密码设备参数配置调整、密码算法策略优化、访问权限管控升级、安全防护策略迭代等工作，确保所有设备及系统完全符合商用密码合规标准，顺利通过各级密码管理部门测评、检查及执法核验，适配医院日常业务运行需求。

3、故障处理

负责本项目服务范围内所有商用密码设施设备的故障监测、远程及现场诊断、精准故障定位、故障修复、系统复原、运行核验等全流程服务。

针对一般故障，快速处置、即时修复，保障设备快速恢复正常运行；针对重大故障、系统性故障、合规性故障，完成故障处置、系统恢复、试运行核验全部工作后，3 个工作日内向医院提交正式书面故障分析报告。报告需详细载明故障发生时间、具体故障现象、影响范围、故障排查及完整处理经过、最终处理结果，深度剖析故障根本原因、合规隐患、运行风险，并结合商用密码规范要求、医院业务场景，提供长效整改、优化、预防的专项改进建议。

4、应急处理支持

全面负责本项目服务范围内商用密码设施设备突发故障、突发合规问题、突发运行异常的应急处置工作。根据故障等级、影响范围、风险级别划分应急处置等级，制定对应的应急处置预案和解决方案，报医院审核通过后立即落地执行。

三、服务期限

本项目所有商用密码设备维保服务期限统一为 3 年原厂维保服务，自本项目所有软硬件设备交付并验收合格之日起计算，全程按本项目清单约定服务年限、服务标准提供常态化维保及合规保障服务。