信息系统密码评审服务

1.测评范围

密码应用安全性评估服务包括以下几个应用系统：

服务名称	系统名称	数量	备注	级别
湖南省卫生健康委应用系统密码应用安全性评估	湖南省新冠病毒区域（全员）核算检测信息平台	1	密码应用安全性评估	三级
	湖南省妇幼直报系统	1	密码应用安全性评估	三级
	湖南省干部保健系统	1	密码应用安全性评估	三级
	湖南省血液联网系统（血液综合管理平台）	1	密码应用安全性评估	三级

2.需求描述

（一）按照信息系统密码应用安全性评估相关要求，开展信息系统密码应用安全性，符合国家有关信息系统密码应用安全性评估工作要求。

（二）依据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）、《信息系统密码测评要求》、《信息系统密码应用测评过程指南》、《商用密码应用安全性评估量化评估规则》、《信息系统密码应用高风险判定指引》等标准对上述 4 个系统从密码算法、密码技术、密码产品、密码服务、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、密钥管理和安全管理（制度、人员、实施、应急）等方面进行密码应用安全性评估。通过评估检验各

信息系统密码应用是否合规、正确、有效，针对被测系统在密码应用安全方面存在的安全问题提出可行性完善建议，为进一步完善信息系统的密码应用安全管理体系、加强信息系统的密码应用安全防护措施提供依据

3.项目预算及服务期限

项目预算：20 万元。

服务期限自合同签订之日起至项目竣工验收之日止。

4.项目背景

为全面贯彻总体国家安全观和网络强国战略，深入贯彻落实习近平总书记关于核心技术自主可控重要批示精神和工作安排，2019 年 10 月 26 日国家颁布了《密码法》，于 2020 年 1 月 1 日正式实施，其中“第二十七条”明确了关键信息基础设施商用密码应用安全性评估的要求。根据国家、省、市密码管理部门在政务系统商密算法应用的相关监管要求，以及财政部印发《政务信息系统政府采购管理暂行办法》和国务院印发的《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知（国办发【2019】57 号）》， 以及《湖南省人民政府办公厅关于印发湖南省直单位政务信息系统项目建设管理办法的通知》（湘政办发[2020]34 号，以下简称《办法》）和《湘党政信发[2019]1 号》的要求，政务信息化项目建设的采购需求应当落实国家密码管理有关法律法规、政策和标准规范的要求,同步规划、同步建设、同步运行密码保障系统并定期进行密码应用安全性评估。

5.商用密码应用安全性评估内容

5.1 依据标准

信息系统密码安全服务全过程所有工作严格按照最新国家相关安全标准执行，以保证服务工作科学、规范地进行，具体参考的标准如下：

《中华人民共和国密码法》

《中华人民共和国网络安全法》

《商用密码应用安全性评估管理办法（试行）》

GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》

《信息系统密码测评要求（试行）》

《商用密码应用安全性评估测评过程指南（试行）》

《商用密码应用安全性评估测评作业指导书（试行）》

GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》

GB/T 35273-2020 《信息安全技术 个人信息安全规范》

GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》

GM/T 0025-2014《SSLVPN 网关产品规范》

GM/T 0027-2014《智能密码钥匙技术规范》

GM/T 0014-2012《数字证书认证系统密码协议规范》

GM/T 0026-2014《安全认证网关产品规范》

GM/T 0030-2014《服务器密码机技术规范》

GM/T 0031-2014《安全电子签章密码技术规范》

GM/T 0033-2014《时间戳接口规范》

GM/T 0029-2014《签名验签服务器技术规范》

GB/T 36968-2018《信息安全技术 IPSecVPN 技术规范》

GB/T 38636-2020 《信息安全技术 传输层密码协议（TLCP）》

GB/T 15843.3-2016 《信息技术 安全技术 实体鉴别 第 3 部分：采用数字签名技术的机制》

GB／T 37092-2018 《信息安全技术密码模块安全要求》

《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知

（国办发【2019】57 号）》

《国家密码管理局关于请进一步加强国家政务信息系统密码应用与安全性评估工作的函（国密局函【2020】119 号）》

《湖南省人民政府办公厅关于印发湖南省省直单位政务信息系统项目建设管理办法（湘政办[2020]34 号）》

5.2 评估内容

商用密码应用安全性评估时按照相关要求分别从系统技术和安全管理等方面全方位对信息系统的密码使用情况进行评估，评估范围主要包括：物理机房、服务器操作系统、数据库系统、交换机、路由器、防火墙、密码算法、密码技术、密码产品、密码服务、应用、安全管理相关文档等，主要具体内容如下表：

序号	评估内容		评估对象
1	通用要求	密码算法测评	密码算法
		密码技术测评	密码技术
		密码产品测评	密码产品
		密码服务测评	密码服务
2	物理和环境安全测评	身份鉴别	物理机房
		电子门禁记录数据完整性	物理机房
		视频记录数据完整性	物理机房
		密码服务	物理机房
		密码产品	物理机房
3	网络和通信安全测评	身份鉴别	交换机、路由器、防火墙等
		通信数据完整性	交换机、路由器、防火墙等
		通信数据机密性	交换机、路由器、防火墙等
		访问控制信息完整性	交换机、路由器、防火墙等
		接入设备的真实性	交换机、路由器、防火墙等
		密码服务	交换机、路由器、防火墙等
		密码产品	交换机、路由器、防火墙等
4	设备和计算安全测评	身份鉴别	操作系统、数据库、服务器
		远程管理通道安全	操作系统、数据库、服务器
		访问控制信息完整性	操作系统、数据库、服务器

序号	评估内容		评估对象
		重要信息资源安全标记完整性	操作系统、数据库、服务器
		日志记录完整性	操作系统、数据库、服务器
		重要可执行程序完整性	操作系统、数据库、服务器
		密码服务	操作系统、数据库、服务器
		密码产品	操作系统、数据库、服务器
5	应用和数据安全测评	身份鉴别	应用
		访问控制信息完整性	应用
		重要信息资源安全标记完整性	应用
		重要数据传输机密性	应用
		重要数据存储机密性	应用
		重要数据传输完整性	应用
		重要数据存储完整性	应用
		不可否认性	应用
		密码服务	应用
		密码产品	应用
6	安全管理测评	管理制度	安全管理相关文档
		人员管理	安全管理相关文档
		建设运行	安全管理相关文档
		应急处置	安全管理相关文档

5.3 通用要求评估

密码算法测评

测评单元	测评指标	测评方式
密码算法合规性检查	信息系统中使用的密码算法应当符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。	访谈、文档审查和实地查看或配置检查
		文档审查和实地查看或配置检查

密码技术测评

测评单元	测评指标	测评方式
密码技术合规性检查	信息系统中使用的密码技术应遵循密码相关国家标准和行业标准。	访谈、文档审查和实地查看或配置检查

密码产品测评

测评单元	测评指标	测评方式
密码产品合规性检查	信息系统中使用的密码产品与密码模块应通过国家密码管理部门核准。	访谈、文档审查和实地查看或配置检查

密码服务测评

测评单元	测评指标	测评方式
密码服务合规性检查	信息系统中使用的密码服务应通过国家密码管理部门许可。	访谈、文档审查和实地查看或配置检查

5.4 物理和环境安全测评

测评单元	测评指标	测评方式
身份鉴别	8.1 a）宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；	访谈和文档审查
		文档审查和实地查看或配置检查
		至少包括配置检查或工具测试中的一种
电子门禁记录数据完整性	8.1 b）宜采用密码技术保证电子门禁系统进出记录数据的存储完整性；	访谈和文档审查
		文档审查和实地查看或配置检查
		至少包括配置检查或工具测试中的一种
视频记录数据完整性	8.1 c）宜采用密码技术保证视频监控音像记录数据的存储完整性。	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		至少包括配置检查或工具测试中的一种
访问控制信息完整性	8.2 d）宜采用密码技术保证网络边界访问控制信息的完整性。	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		至少包括配置检查或工具测试中的一种
接入设备的真实性	8.2 e）可采用密码技术对从外部连接到内部网络设备进行接入认证，确保接入的设备身份真实性	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		至少包括配置检查或工具测试中的一种
密码服务	8.2 f）以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受	访谈和文档审查
		至少包括配置检查或工具测试中的

测评单元	测评指标	测评方式
	检测认证的，应经商用密码认证机构认证合格。	一种
		至少包括配置检查或工具测试中的一种
密码产品	8.2 g）以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。	访谈和文档审查
		访谈、文档审查和实地查看或配置检查
		访谈、文档审查和实地查看或配置检查

5.5 网络和通信安全测评

测评单元	测评指标	测评方式
身份鉴别	8.2 a）应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		访谈、文档审查和实地查看或配置检查
通信数据完整性	8.2 b) 宜采用密码技术保证通信过程中数据的完整性；	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
重要数据的机密性	8.2 c) 应采用密码技术保证通信过程中重要数据的机密性；	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
网络边界访问控制信息的完整性	8.2 d) 宜采用密码技术保证网络边界访问控制信息的完整性；	文档审查，同时，至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
安全接入认证	8.2 e) 可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
密码服务	8.2 f）以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
密码产品	8.2 g）以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。	访谈和文档审查
		至少包括配置检查或工具测试中的

测评单元	测评指标	测评方式
		一种
		文档审查和实地查看或配置检查

5.6 设备和计算安全测评

测评单元	测评指标	测评方式
身份鉴别	8.3 a) 应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
远程管理通道安全	8.3 b) 远程管理设备时，应采用密码技术建立安全的信息传输通道；	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
访问控制信息完整性	8.3 c) 宜采用密码技术保证系统资源访问控制信息的完整性；	文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
重要信息资源安全标记完整性	8.3 d) 宜采用密码技术保证设备中的重要信息资源安全标记的完整性；	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
日志记录完整性	8.3 e) 宜采用密码技术保证日志记录的完整性；	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
重要可执行程序完整性、重要可执行程序来源真实性	8.3 f) 宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
密码服务	8.3 g）以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
密码产品	8.3 h）以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。	访谈和文档审查
		至少包括配置检查或工具测试中的一种

测评单元	测评指标	测评方式
		文档审查和实地查看或配置检查

5.7 应用和数据安全测评

测评单元	测评指标	测评方式
身份鉴别	8.4 a) 应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；	访谈和文档审查 至少包括配置检查或工具测试中的一种，并结合文档审查
访问控制信息完整性	8.4 b) 宜采用密码技术保证信息系统应用的访问控制信息的完整性；	访谈和文档审查 至少包括配置检查或工具测试中的一种，并结合文档审查
重要信息资源安全标记完整性	8.4 c) 宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；	访谈和文档审查 至少包括配置检查或工具测试中的一种
重要数据传输机密性	8.4 d) 应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；	访谈和文档审查 至少包括配置检查或工具测试中的一种
重要数据存储机密性	8.4 e) 应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性；	访谈和文档审查 至少包括配置检查或工具测试中的一种
重要数据传输完整性	8.4 f) 宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性；	访谈和文档审查 至少包括配置检查或工具测试中的一种
重要数据存储完整性	8.4 g) 宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；	访谈、文档审查和现场查看 至少包括配置检查或工具测试中的一种，并结合文档审查
不可否认性	8.4 h) 在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。	访谈和文档审查 至少包括配置检查或工具测试中的一种
密码服务	8.4 i）以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。	访谈和文档审查 至少包括配置检查或工具测试中的一种
密码产品	8.4 j）以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。	访谈和文档审查 至少包括配置检查或工具测试中的一种

5.8 安全管理测评

测评单元		测评指标	测评方式
管理制度	具备密码应用安全管理制度	8.5 a）应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；	访谈、文档记录核查。
	密钥管理规则	8.5 b）应根据密码应用方案建立相应密钥管理规则；	访谈、文档记录核查。
	建立操作规程	8.5 c）应对管理人员或操作人员执行的日常管理操作建立操作规程；	访谈、文档记录核查。
	定期修订安全管理制度	8.5 d）应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订；	访谈、文档记录核查。
	明确管理制度发布流程	8.5 e）应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制；	访谈、文档记录核查。
	制度执行过程记录留存	8.5 f）应具有密码应用操作规程的相关执行记录并妥善保存。	访谈、文档记录核查。
人员管理	了解并遵守密码相关法律法规 和密码管理制度	8.6 a）相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；	访谈、文档记录核查。
	建立密码应用岗位责任制度	8.6 b) 应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限： 1) 根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位； 2) 对关键岗位建立多人共管机制； 3) 密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密钥管理员岗位不可与密码审计员、密码操作员等关键安全岗位兼任； 4) 相关设备与系统的管理和使用账号不得多人共用。	访谈、文档记录核查。
	建立上岗人员培训制度	8.6 c) 应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能；	访谈、文档记录核查。
	定期进行安全岗位人员考核	8.6 d) 应定期对密码应用安全岗位人员进行考核；	访谈、文档记录核查。
	建立关键岗位人员保密制度和调离制度	8.6 e) 应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。	访谈、文档记录核查。
建设运行	制定密码应用方案	8.7 a）应依据密码相关标准和密码应用需求，制定密码应用方案；	访谈、文档记录核查。

测评单元		测评指标	测评方式
	制定密钥安全管理策略	8.7 b）应根据密码应用方案，确定系统涉及的密钥种类、体系及其生命周期环节，各环节安全管理要求参照《信息安全技术 信息系统密码应用基本要求》附录 A；	访谈、文档记录核查。
	制定实施方案	8.7 c）应按照应用方案实施建设；	访谈、文档记录核查。
	投入运行前进行密码应用安全性评估	8.7 d）投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行；	访谈、文档记录核查。
	定期开展密码应用安全性评估及攻防对抗演习	8.7 e）在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。	访谈、文档记录核查。
应急处置	应急策略	8.8 a）应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置；	访谈、文档记录核查。
	事件处置	8.8 b）事件发生后，应及时向信息系统主管部门进行报告；	访谈、文档记录核查。
	向有关主管部门上报处置情况	8.8 c）事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。	访谈、文档记录核查。

6.商务要求

1、投标人提供 2 个及以上密码评估类似业绩，并提供相关证明材料。

2、投标人须列入国家密码管理局公告（第 42 号）明确的《商用密码应用安全性评估试点机构目录》，并提供相关证明材料。

3、投标人获得过国家级或省级密码行业相关科技奖项 2 个以上，提供相关证明材料。