附件1

用户需求

“★”号条款

《用户需求》中标注有“★”号的条款必须实质性响应，负偏离（不满足要求）将导致投标无效。

1. **项目建设内容**

对省工业和信息化厅2021年拟立项项目信息系统，提供密码应用建设方案评估服务。在系统规划立项阶段，按照GM/T0054-2018《信息系统密码应用基本要求》及国家有关商用密码应用有关法律法规、政策标准的要求，对信息系统的密码应用建设方案（包括《密码应用解决方案》、《实施方案》与《应急处置方案》）进行评估。主要是对方案的完整性和合理性、密码应用的正确性、密码技术对信息系统安全保护的有效性、密码产品选取的合规性等方面进行评估，并出具《密码应用建设方案评估报告》。

针对信息系统密码应用建设方案开展评估，从总体要求、物理和环境、网络和通信、设备和计算、应用和数据、密钥管理、安全管理等方面开展测评，具体测评指标如下（以等级保护第三级信息系统为例）：

|  |  |  |
| --- | --- | --- |
| **技术/管理** | **安全分类** | **指标要求** |
| 总体要求 | 密码算法 | 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； |
| 密码技术 | 使用的密码技术应遵循密码相关国家标准和行业标准； |
| 密码产品 | 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； |
| 密码服务 | 使用的密码服务应通过国家密码管理部门许可。 |
| 技术要求 | 物理和环境安全 | a) 应使用密码技术的真实性功能来保护物理访问控制身份鉴别信息，保证重要区域进入人员身份的真实性； |
| b) 应使用密码技术的完整性功能来保证电子门禁系统进出记录的完整性； |
| c) 应使用密码技术的完整性功能来保证视频监控音像记录的完整性； |
| d) 宜采用符合GM/T 0028的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。 |
| 网络和通信安全 | a) 应在通信前基于密码技术对通信双方进行身份认证，使用密码技术的机密性和真实性功能来实现防截获、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性；  |
| b) 应使用密码技术的完整性功能来保证网络边界和系统资源访问控制信息的完整性； |
| c) 应采用密码技术保证通信过程中数据的完整性； |
| d) 应采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性； |
| e) 应采用密码技术建立一条安全的信息传输通道，对网络中的安全设备或安全组件进行集中管理； |
| f) 宜采用符合GM/T 0028的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。 |
| 设备和计算安全 | a) 应使用密码技术对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； |
| b) 在远程管理时，应使用密码技术的机密性功能来实现鉴别信息的防窃听；  |
| c) 应使用密码技术的完整性功能来保证系统资源访问控制信息的完整性； |
| d) 应使用密码技术的完整性功能来保证重要信息资源敏感标记的完整性；  |
| e) 应采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性保护； |
| f) 应使用密码技术的完整性功能来对日志记录进行完整性保护； |
| g) 宜采用符合GM/T 0028的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。 |
| 应用和数据安全 | a) 应使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性； |
| b) 应使用密码技术的完整性功能来保证业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等信息的完整性；  |
| c) 应采用密码技术保证重要数据在传输过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；  |
| d) 应采用密码技术保证重要数据在存储过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等； |
| e) 应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息等；  |
| f) 应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息、重要可执行程序等；  |
| g) 应使用密码技术的完整性功能来实现对日志记录完整性的保护；  |
| h) 应采用密码技术对重要应用程序的加载和卸载进行安全控制；  |
| i) 宜采用符合GM/T 0028的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。 |
| 密钥管理 | 密钥生成 | a)密钥生成使用的随机数应符合GM/T 0005要求，密钥应在符合GM/T 0028的密码模块中产生；密钥应在密码模块内部产生，不得以明文方式出现在密码模块之外；应具备检查和剔除弱密钥的能力。  |
| 密钥存储 | a)密钥应加密存储，并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥应存储在符合GM/T 0028的二级及以上密码模块中。  |
| 密钥使用 | a)密钥应明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前应对其进行验证；应有安全措施防止密钥的泄露和替换；密钥泄露时，应停止使用，并启动相应的应急处理和响应措施。应按照密钥更换周期要求更换密钥；应采取有效的安全措施，保证密钥更换时的安全性。  |
| 密钥分发 | a)应采取安全措施，防止密钥导入导出时被非法获取或篡改，并保证密钥的正确性。  |
| 密钥导入与导出 | a)应采取安全措施，防止密钥导入导出时被非法获取或篡改，并保证密钥的正确性。 |
| 密钥备份与恢复 | a)应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复应进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。 |
| 密钥归档 | a)应采取有效的安全措施，保证归档密钥的安全性和正确性；归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档应进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等；归档密钥应进行数据备份，并采用有效的安全保护措施。 |
| 密钥销毁 | a)应具有在紧急情况下销毁密钥的措施。 |
| 安全管理 | 制度管理 | a) 应制定密码安全管理制度及操作规范、安全操作规范。密码安全管理制度应包括密码建设、运维、人员、设备、密钥等密码管理相关内容；  |
| b) 应定期对密码安全管理制度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的安全管理制度进行修订；  |
| c) 应明确相关管理制度发布流程。  |
| 人员管理 | a) 应了解并遵守密码相关法律法规；  |
| b) 应能够正确使用密码产品；  |
| c) 应根据相关密码管理政策、数据安全保密政策，结合组织实际情况，设置密钥管理人员、安全审计人员、密码操作人员等关键岗位；建立相应岗位责任制度，明确相关人员在安全系统中的职责和权限，对关键岗位建立多人共管机制；密钥管理、安全审计、密码操作人员职责，互相制约互相监督，相关设备与系统的管理和使用账号不得多人共用； |
| d) 应建立人员考核制度，定期进行岗位人员考核，建立健全奖惩制度； |
| e) 应建立人员培训制度，对于涉及密码的操作和管理以及密钥管理人员进行专门培训；  |
| f) 应建立关键岗位人员保密制度和调离制度，签订保密合同，承担保密义务。  |
| 实施管理 | 规划 | a)信息系统规划阶段，责任单位应依据密码相关标准，制定密码应用建设方案，组织专家进行评审，评审意见作为项目规划立项的重要材料。通过专家审定后的方案应作为建设、验收和测评的重要依据。 |
| 建设 | a) 应按照国家相关标准，制定实施方案，方案内容应包括但不少于信息系统概述、安全需求分析、密码系统设计方案、密码产品清单（包括产品资质、功能及性能列表和产品生产单位等）、密码系统安全管理与维护策略、密码系统实施计划等； |
| b) 应选用的经国家密码管理部门核准的密码产品、许可的密码服务。 |
| 运行 | a) 信息系统投入运行前，应经密码测评机构进行安全性评估，评估通过方可投入正式运行； |
| b) 信息系统投入运行后，责任单位每年应委托密码测评机构开展密码应用安全性评估，并根据评估意见进行整改；有重大安全隐患的，应停止系统运行，制定整改方案，整改完成并通过评估后方可投入运行。 |
| 应急管理 | a) 制定应急预案，做好应急资源准备，当事件发生时，按照应急预案结合实际情况及时处置；  |
| b) 事件发生后，应及时向信息系统的上级主管部门进行报告； |
| c) 事件处置完成后，应及时向同级的密码主管部门报告事件发生情况及处置情况。 |

1. **服务人员要求**

在项目负责人员方面，应设立一名专职负责的项目经理，在服务期内，项目经理应根据项目需要到指定现场处理问题或交流情况。测评团队人员须具备所从事测评的专业技术和类似工作经验，并需具有通过国家密码管理局商用密码检测中心或国家商用密码应用安全性评估人员测评能力考核小组组织的商用密码应用安全性评估人员测评能力考核（分数在60分以上）。

投标人须书面承诺，如在项目实际执行过程中发生服务团队人员不能按采购文件要求胜任相关工作的，采购人有权要求更换，投标人须在两周内调整为符合采购文件要求且能胜任相关工作的人员并到位开展工作，否则采购人有权终止合同并报相关管理部门进行处理。 服务商应指派固定的团队为本项目提供专业服务，整个团队成员不得少于 12 人。 如须调整服务团队人员，须书面向采购人提出申请，说明申请理由，经采购人书面同意方可调整团队人员，调入人员的资历和从业经验不低于调出人员，否则视为违约行为，采购人有权终止服务合同。 应提供以上人员相关证明资料复印件并加盖公章，并提供以上人员在本公司任职的有效外部证明材料（如加盖政府有关部门印章的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单等）复印件。

1. **文档管理要求**

中标人应在项目完成时，将本项目所有成果文件汇集成册交付给采购人，所有文件要求用中文书写或有完整的中文注释。验收后，中标人按国家、省以及采购人档案管理要求，向采购人提供装订成册的纸质文档至少 1套。

1. **验收标准要求**

中标人应根据整体工作计划要求，包含但不限于以下要求：

（1）完成所有评估工作。

（2）项目交付物齐全，符合项目要求及有关标准的规定。

（3）评估报告详实、客观、有法律效力，为信息系统立项和验收提供准确指导，使系统达到立项和验收要求。

 （4）所编制商用密码应用建设方案评估报告需通过省密码管理局审批备案。

1. **服务响应要求**

项目服务响应要求如下：

（1）7\*24 电话支持：提供 7\*24 的技术支持电话服务，由专职技术工程师负责解答相关技术问题并给出解决方法。

（2）如果技术支持服务电话或远程支持服务解决不了的问题，技术支持服务人员可以在8小时内到达客户现场提供技术支持，24 小时内处理完问题；重大问题 48 小时内处理完。

1. **资产权属**

投标人为实施项目提供的所有资料及工作成果归采购人所有。

1. **保密要求**

中标人应同意：

1.未经采购人事前书面批准，不论服务期间或以后，中标人及其工作人员不得以任何方式泄漏采购人的保密信息。

2.不私自复制、下载、拷贝、携带和留存保密信息。

3.一旦服务工作终止，中标人及其工作人员将退还保存的属于采购人的所有保密信息及资料，如方案、制度、报告、合同等。

保密期限：从获知采购人保密信息时起，至保密信息已由采购人通过合法途径让普通公众知悉时止。

中标人违反本保密协议约定，要承担违约责任，采购人有权通过任何合理方式追究乙方的责任并终止服务合同。

1. **项目服务地点**

广东省工业和信息化厅

**九、项目服务期限及其它约定**

自签订合同之日起至本项目各系统完成立项申报并通过验收。

合同款需在合同签订及各项目建设资金到位后十个工作日内，才开始按合同约定进度予以支付。

附件2

**遴选申报文件格式**

## 遴选申报文件封面

正本（或副本）

项目名称：广东省工业和信息化厅商用密码应用建设方案评估服务

**遴**

**选**

**申**

**报**

**文**

**件**

遴选申请人：（全称并加盖单位公章）

年 月 日

## 遴选报价表

|  |  |  |  |
| --- | --- | --- | --- |
| **服务名称** | **服务内容** | **预算（元）** | **申请人报价（元）** |
| 广东省工业和信息化厅商用密码应用建设方案评估服务 | 密码应用建设方案评估服务 |  |  |
| 合计 |  |  |

注：遴选申请人需对每项服务内容逐一报价，报价超过总预算或分项预算的，属于无效报价。

遴选申请人：（全称并加盖单位公章）

年 月 日

## 遴选申请人概况（格式自拟）

## 拟投入本项目的人员情况汇总表（可扩充）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 姓名 | 拟任职务 | 专业 | 职称 | 联系电话 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |

## 遴选申请人服务经验（可扩充）

|  |  |  |  |
| --- | --- | --- | --- |
| 起止时间 | 项目名称 | 单位名称 | 服务金额 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

注：遴选文件中的同类服务经验是指2017年1月1日至今服务的项目。

## 服务方案（格式自拟）