1. **实质性条款**

|  |  |
| --- | --- |
| 序号 | 具体内容 |
| 1 | 完全满足本项目服务期限的要求。 |

注：上表所列内容为不可负偏离条款

1. **项目背景**

密码是保障网络安全的核心技术和基础支撑，是解决网络与信息安全问题最有效、最可靠、最经济的手段。近年来密码在维护国家安全、促进经济社会发展、保护人民群众利益方面发挥了越来越重要的作用，国家对重要领域商用密码的应用、基础支撑能力的提升以及安全性评估、审查制度等不断提出明确要求。《中华人民共和国密码法》第二十七条明确要求：“法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。”。2020年8月20日国家密码管理局发布《商用密码管理条例（修订草案征求意见稿）》第三十八条明确要求：“非涉密的关键信息基础设施、网络安全等级保护第三级以上网络、国家政务信息系统等网络与信息系统，运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，自行或者委托商用密码检测机构开展商用密码应用安全性评估”。

1. **项目目标**

 依据相关法律法规的要求，我单位需要对多个系统各进行壹次商用密码应用安全性评估（下称“系统密评”），切实保障我单位信息系统的安全，现面向社会选取合格的供应商提供评估服务。

|  |  |  |
| --- | --- | --- |
| **序号** | **系统名称** | **等保等级** |
| 1 | 深圳市金融风险监测预警系统 | 三级 |
| 2 | 深圳市地方金融监管信息系统 | 三级 |
| 3 | 深圳市绿色金融公共服务平台 | 二级 |
| 4 | 深圳金融行业统计数据库 | 二级 |

1. **项目服务要求**
2. **服务内容**

 根据《中华人民共和国密码法》、《商用密码管理条例》、《商用密码应用安全性评估管理办法（试行）》、《网络安全等级保护条例》、《国家政务信息化项目建设管理办法的通知（国办发〔2019〕57号）》等有关要求，依据GB/T39786-2021《信息系统密码应用基本要求》对信息系统的密码应用合规性、正确性与有效性进行评估，评估内容主要包含总体要求（密码算法、密码技术、密码产品、密码服务）、密码技术应用（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）、密码应用管理要求（制度、人员、实施、应急）与密钥管理（密钥生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等）。通过单元评估、整体评估、量化评估和风险分析等方法，评估信息系统密码应用的安全保护现状与相应等级的密码应用要求之间的差距，并分析这些差距可能导致的被评估信息系统所面临的风险，最终评出“符合”、“基本符合”与“不符合”的评估结论，并出具正式的《XXXXX系统商用密码应用安全性评估报告》。

1. **依据标准与规范**

GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》

GM/T 0115-2021《信息系统密码应用测评要求》

GM/T 0116-2021《信息系统密码应用测评过程指南》

信息系统密码应用高风险判定指引

商用密码应用安全性评估量化评估规则

商用密码应用安全性评估FAQ（第二版）

1. **服务成果**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **系统名称** | **等保等级** | **报告类型** | **报告数量** |
| 1 | 深圳市金融风险监测预警系统 | 三级 | 深圳市金融风险监测预警系统商用密码应用安全性评估报告 | 纸质版报告壹式叁份、电子版报告壹式壹份。 |
| 2 | 深圳市地方金融监管信息系统 | 三级 | 深圳市地方金融监管信息系统商用密码应用安全性评估报告 | 纸质版报告壹式叁份、电子版报告壹式壹份。 |
| 3 | 深圳市绿色金融公共服务平台 | 二级 | 深圳市绿色金融公共服务平台系统商用密码应用安全性评估报告 | 纸质版报告壹式叁份、电子版报告壹式壹份。 |
| 4 | 深圳金融行业统计数据库 | 二级 | 深圳金融行业统计数据库系统商用密码应用安全性评估报告 | 纸质版报告壹式叁份、电子版报告壹式壹份。 |

1. **服务完成期限**

合同签订之日起至2023年11月30日止。

1. **服务响应要求**

在服务期内，投标人应根据项目需要到指定现场处理问题或交流情况，出现紧急情况时能派出本单位人员在2小时内到达采购人办公地点提供现场支撑服务。

1. **评估要求**

商用密码应用安全性评估主要工作内容包括：通用要求评估、密码应用技术评估、密码应用管理评估与密钥生存周期管理评估等内容。

1. **通用要求评估**

具体要求如下：

|  |  |  |
| --- | --- | --- |
| **评估层面** | **评估内容** | **评估目的** |
| 密码算法 | 1. 核查系统使用的算法名称、用途、何处使用、执行设备及其实现方式；
2. 核查是否由经商用密码检测认证通过的密码产品提供；
3. 核查是否经国密局认可用在特定行业的专用算法。
 | 1. 确保系统中使用的密码算法符合法律、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 | 1. 核查密码技术是否由经商用密码检测认证通过的密码产品提供；
2. 核查密码技术是否以成果鉴定方式经国密局认可。
 | 1. 确保信息系统中使用的密码技术遵循密码相关国家标准和行业标准。
 |
| 密码产品 | 1. 核查密码产品/密码模块是否获得商用密码认证证书。
 | 1. 确保信息系统中使用的密码产品与密码模块符合法律法规和密码相关国家标准和行业标准 的要求
 |
| 密码服务 | 1. 核查是否具有国家密码管理部门同意使用的证明文件，例如行政审批、成果鉴定。
 | 1. 确保方案所涉及的密码服务符合法律法规和密码相关国家标准和行业标准 的要求
 |

1. **密码应用技术评估**

主要从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全4个层面对信息系统中应用的密码技术进行分析与评估。具体要求如下：

| **评估层面** | **评估内容** | **评估目的** |
| --- | --- | --- |
| 物理和环境安全 | 从下列维度，对物理与环境方面的密码应用内容进行合规、正确、有效性评估：1. 物理访问身份鉴别；
2. 电子门禁系统；
3. 访问记录完整性；
4. 视频监控记录完整性等。
 | 1. 确保密码应用满足对应级别的密码防护需求
2. 确保影响信息系统物理和环境层面的安全因素能得到有效控制，且没有高风险项。
 |
| 网络和通信安全 | 从下列维度，对网络和通信方面的密码应用内容进行合规、正确、有效性评估：1. 身份鉴别；
2. 通信数据完整性；
3. 通信过程中重要数据机密性；
4. 网络边界控制信息完整性；
5. 安全接入认证。
 | 1. 确保密码应用满足对应级别的密码防护需求
2. 确保影响信息系统网络和通信层面的安全因素能得到有效控制，且没有高风险项。
 |
| 设备和计算安全 | 从下列维度，对设备和计算方面的密码应用内容进行合规、正确、有效性评估：1. 身份鉴别；
2. 远程管理通道安全；
3. 系统资源访问控制完整性；
4. 重要信息资源安全标记完整性；
5. 日志记录完整性；
6. 重要可执行程序完整性及真实性。
 | 1. 确保密码应用满足对应级别的密码防护需求；
2. 确保影响信息系统设备和计算层面的安全因素能得到有效控制，且没有高风险项。
 |
| 应用和数据安全 | 从下列维度，对设备和计算方面的密码应用内容进行合规、正确、有效性评估：1. 身份鉴别；
2. 访问控制完整性；
3. 重要信息资源安全标记完整性；
4. 重要数据传输完整性和机密性；
5. 重要数据存储机密性和完整性；
6. 行为不可否认性。
 | 1. 确保密码应用满足对应级别的密码防护需求；
2. 确保影响信息系统应用和数据层面的安全因素能得到有效控制，且没有高风险项。
 |

1. **密码应用管理评估**

主要是对影响商用密码防护效能的管理制度与措施进行分析与评估。管理制度与措施主要包括：安全管理制度，人员管控，信息系统实施，应急预案。具体要求如下：

|  |  |  |
| --- | --- | --- |
| **评估层面** | **评估内容** | **评估目的** |
| 管理制度 | 1. 是否建立密码应用安全管理制度，管理制度是否涵盖人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理；
2. 是否建立相应密钥管理规则；
3. 是否建立密码操作规程；
4. 是否定期修订安全管理制度；
5. 是否明确管理制度发布流程；
6. 是否留存制度执行过程记录。
 | 确保管理制度符合信息系统密码应用管理实际，满足密码应用安全性评估对管理制度的要求。 |
| 人员管理 | 1. 人员是否了解并遵守密码相关法律法规和密码管理制度；
2. 是否建立密码应用岗位责任制度并明确职责和权限；
3. 是否建立上岗培训制度；
4. 是否定期对密码应用安全岗位人员进行考核；
5. 是否建立关键岗位人员保密制度和调离制度。
 | 确保人员管理符合信息系统密码应用人员管理工作实际，满足密码应用安全性评估对人员管理的要求。 |
| 建设运行 | 1. 是否制定密码应用方案；
2. 是否根据密码应用方案制定密钥安全管理制度；
3. 是否制定实施方案；
4. 是否在系统投入运行前开展密码应用安全性评估；
5. 是否定期开展密码应用安全性评估及攻防对抗演习。
 | 确保建设运行要求符合信息系统密码应用建设运行工作实际，满足密码应用安全性评估对建设运行管理的要求。 |
| 应急处置 | 1. 是否制定密码应用应急策略和应急预案；
2. 通过何种方式保证事件发生后及时向信息系统主管部门报告；
3. 事件处置后，是否向有关主管部门上报处置情况。
 | 确保应急处置要求符合信息系统密码应用应急处置工作实际，满足密码应用安全性评估对应急处置工作的要求。 |

1. **密钥生存周期管理评估**

| **生命周期** | **评估内容** | **评估目的** |
| --- | --- | --- |
| 产生 | 1. 确认密钥是否在符合 GB/T 37092 的密码产品中产生；
2. 确认密钥协商算法是否符合法律、法规的规定和密码相关国家标准、行业标准的有关要求；
3. 核实密钥产生功能的正确性和有效性，如随机数发生器的运行状态、密钥关联信息包括密钥种类、长度、拥有者、使用起始时间、使用终止时间等。
 | 1. 密钥产生所使用的随机数发生器或密钥协商算法经国家密码管理部门核准的。
 |
| 分发 | 1. 确认系统内部采用何种密钥分发方式：离线分发方式、在线分发方式、混合分发方式；
2. 确认信息系统使用了哪些密码技术对密钥进行处理以保护其机密性、完整性与真实性，并核实保护措施使用的正确性和有效性。
 | 1. 确保密钥的机密性、完整性以及分发者、接收者身份的真实性等。
 |
| 存储 | 1. 确认系统内部所有密钥（除公钥）是否均以密文形式进行存储，或者位于受保护的安全区域；
2. 确认信息系统使用了哪些密码技术对密钥进行处理以保护其机密性（除公钥）、完整性，并核实保护措施使用的正确性和有效性。
 | 1. 确保密钥（除公钥）存储过程是不被非授权的访问或篡改；
2. 确保公钥存储过程不被非授权的篡改。
 |
| 使用 | 1. 确认信息系统内部是否具有严格的密钥使用管理机制，以及所有密钥是否有明确的用途并按用途被正确使用；
2. 确认信息系统是否具有公钥认证机制，以鉴别公钥的真实性与完整性；
3. 确认信息系统采用了何种安全措施来防止密钥泄露或替换，是否使用了密码算法以及算法是否符合相关法规和标准的要求；
4. 确认当发生密钥泄漏时，系统是否具备应急处理和响应措施；
5. 确认信息系统是否定期更换密钥，并核实密钥更换处理流程中是否采取有效措施保证密钥更换时的安全性。
 | 1. 确保密钥有明确的用途；
2. 确保各类密钥均被正确地使用、管理。
 |
| 更新 | 1. 确认信息系统内部是否具有密钥更新策略；
2. 并核实当密钥超过使用期限、已泄露或存在泄露风险时，是否会根据相应的更新策略进行密钥更新。
 | 1. 确保密钥会根据相应的更新策略进行更新。
 |
| 归档 | 1. 确认信息系统是否采取有效的安全措施，以保证归档密钥的安全性和正确 性；
2. 核实归档密钥是否仅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；
3. 确认密钥归档的审计信息是否包括归档的密钥、归档的时间等信息。
 | 1. 确保密钥归档过程保证了密钥的安全性和正确性，并生成了审计信息。
 |
| 撤销 | 1. 若信息系统内部使用公钥证书，则确认是否有公钥证书撤销机制和撤销机制的触发条件， 并确认是否有效执行；
2. 核实撤销后的密钥是否已不具备使用效力。
 | 1. 确保公钥证书具备撤销机制。
 |
| 备份 | 1. 若信息系统内部存在需要归档的密钥，则确认是否具有密钥备份机制并有效执行；
2. 确认密钥备份过程中系统使用了哪些密码技术对密钥进行处理以保护其机密性、完整性；
3. 确认密钥备份的审计信息是否包括备份的主体、时间等信息。
 | 1. 确保密钥备份过程保证了密钥的机密性和完整性，并生成了审计信息。
 |
| 恢复 | 1. 确认系统内部是否具有密钥的恢复机制并有效执行；
2. 确认密钥恢复的审计信息是否包括恢复的主体、时间等信息。
 | 1. 确保密钥具备恢复机制，并生成审计信息。
 |
| 销毁 | 1. 确认系统内部是否具有密钥的销毁机制并有效执行；
2. 核实密钥销毁过程和销毁方式，确认是否密钥销毁后无法被恢复。
 | 1. 确保密钥具备销毁机制，且销毁过程具备不可逆性。
 |

1. **服务人员**

投标人应指派一名项目经理（仅限一人），须是投标人在职员工，具备3年及以上从事商用密码应用安全性评估服务项目管理工作经验且具有硕士研究生及以上学历。

投标人应指派固定的团队为本项目提供专业服务，应指定1名技术负责人（不与项目经理为同一人），并派驻不少于2人（可包含技术负责人）驻现场开展工作，须均是投标人在职员工，须应具有1年及以上从事商用密码应用安全性评估工作经验且具有本科及以上学历。

如须调整服务团队成员，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。

1. **评分标准**

本次采购采用综合评分法，是指投标文件满足招标文件全部资格性要求，且按照评审因素的量化指标评审得分最高的投标人为中标候选人的评标方法。

评标总得分＝F1×A1＋F2×A2＋……＋Fn×An

F1、F2……Fn分别为各项评审因素的得分；

A1、A2、……An 分别为各项评审因素所占的权重(A1＋A2＋……＋An＝1)。

评标过程中，不得去掉报价中的最高报价和最低报价。

总得分（总分100分）=价格+技术部分+综合实力+诚信情况，分值及评分标准详见下表。

|  |  |  |
| --- | --- | --- |
| **序号** | **价格** | **权重（%）** |
| 1 | **价格部分** | **10** |
| **序号** | **评分因素** | **权重** | **评分准则** |
| 1 | 投标总价 | 10 | 1. **价格分计算方法：**

采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算：投标报价得分=(评标基准价／投标报价)×1001. **价格评审优惠政策：**

中小型企业、微型企业、监狱企业、残疾人福利性单位承接服务，对其价格给予10%的扣除，用扣除后的价格参与评审。满足多项优惠政策的企业，不重复享受多项价格扣除政策。优惠主体资格的认定资料为《中小企业声明函》《残疾人福利性单位声明函》《监狱企业声明函》等承诺性质的资料（声明函样式见“附件一”）；监狱企业如需享受优惠政策，除上述资料外，还须提供省级以上监狱管理局、戒毒管理局出具的监狱企业证明文件。 |
| 2 | 技术部分 | 55 |
| **序号** | **评分因素** | **权重** | **评分准则** |
| 1 | 总体服务方案 | 15 | 1. **评审内容：**

投标人应按照招标文件的要求提供本项目特点的总体服务方案，内容应至少包含项目需求理解、评估依据、评估内容、评估过程、进度管控、评估方法、重点难点分析、质量控制、服务团队、风险管理、保密管理与售后服务等。1. **评分依据：**
2. 优：方案内容全面具体、针对性强、可操作性强且科学合理；
3. 良：方案内容较为全面具体、针对性较强、可操作性较强且较为科学合理；
4. 中：方案内容较为简单、针对性、可操作性及科学合理性基本符合要求；
5. 差：未按采购文件要求提供针对本项目的总体服务方案。

评价为优得100%的分数；评价为良得70%的分数；评价为中得40%的分数；评价为差不得分。如果评审为差，要求专家书面说明理由，并记录在档。 |
| 2 | 项目重点难点分析、应对措施及相关的合理化建议 | 10 | 1. **评审内容：**

投标人应按照招标文件的要求提供本项目可能的重点难点分析、应对措施及相关的合理化建议等。1. **评分依据：**
2. 优：内容全面具体、针对性强、可操作性强且科学合理；
3. 良：内容比较全面具体、针对性较强、可操作性较强且较为科学合理；
4. 中：内容比较简单、针对性、可操作性及科学合理性基本符合要求；
5. 差：未按采购文件要求提供针对本项目的相关内容

评价为优得100%的分数；评价为良得70%的分数；评价为中得40%的分数；评价为差不得分。如果评审为差，要求专家书面说明理由，并记录在档。以上累计得分，最高得100分。如果评审为差，要求专家书面说明理由，并记录在档。 |
| 3 | 质量（完成事件、安全、环保）保障措施及方案 | 8 | 1. **评审内容：**

投标人应按照招标文件的要求提供质量保障措施与质量保障方案、质量体系建设等。1. **评分依据：**
2. 优：方案内容全面具体、针对性强、可操作性强并且科学合理；
3. 良：方案内容比较全面具体、针对性较强、可操作性较强并且较为科学合理；
4. 中：方案内容比较简单、针对性、可操作性及科学合理性基本符合要求；
5. 差：未按采购文件要求提供针对本项目的质量保障措施与方案。

评价为优得100%的分数；评价为良得70%的分数；评价为中得40%的分数；评价为差不得分。如果评审为差，要求专家书面说明理由，并记录在档。 |
| 4 | 服务承诺 | 2 | 1. **评审内容：**

投标人应按照招标文件的要求提供全面具体的实质性承诺，内容至少包括：1. 承诺将严格按照相关法律法规与标准开展评估工作，按时按质完成项目内容；
2. 承诺严格按照招标文件要求进行人员配置与更换；
3. 承诺无条件配合采购人完成本次项目的结项工作；
4. 提供违约承诺，说明未达到承诺内容时的处理办法。
5. **评分依据：**

承诺以上全部四项的得100%的分数，否则不得分。 |
| 5 | 拟安排的项目负责人（仅限一人）情况 | 10 | 1. **评分内容：**

投标人应指派一名项目团队负责人（仅限一人），须是投标人在职员工，具备3年及以上从事商用密码应用安全性评估服务项目管理工作经验且具有硕士研究生及以上学历，不满足以上条件本项不得分。在此基础上进行以下评审：1. 全日制硕士毕业的，得10%的分数；全日制博士毕业的，得20%的分数，其他学历不得分；
2. 具有中华人民共和国人力资源和社会保障部或各省市区级人力资源和社会保障部门颁发的副高级职称的，得10%的分数；具备中华人民共和国人力资源和社会保障部或各省市区级人力资源和社会保障部门颁发的正高级职称的，得20%的分数；
3. 具有由省级及以上人力资源和社会保障部门颁发的持有信息系统项目管理师证书的，得20%的分数；
4. 国家认证认可监督管理委员会与国家密码管理局的商用密码认证技术委员会委员的，得40%的分数。
5. 以上四项累计得分，最多得100%的分数。
6. **评分依据：**
7. 要求提供通过投标人缴纳的近三月的社保证明作为本单位员工的证明依据（由于社保部门原因最近一个月的社保证明无法提供的可往前顺延一个月）；
8. 要求提供投标人相关证明资料作为得分依据；
9. 学历、学位证书，须同时提供证书复印件以及学信网查询记录复印件加盖公章，原件备查。如学历学位证明颁发较早，学信网无法查询，可提供毕业院校、人社部门等颁发机构或监管机构等单位出具的证明（如开标前无法获得，可提供承诺函（格式自拟），承诺证书真实性，并在中标后提供相关证明材料供采购方核验）；
10. 未按要求提供或提供不清晰导致专家无法有效判断的不得分；以上资料均要求提供复印件（或官方网站截图），原件备查。评分中出现无证明资料或专家无法凭所提供资料判断是否得分的情况，一律作不得分处理。
 |
| 6 | 拟安排的项目团队成员（项目负责人除外）情况 | 10 | 1. **评分内容：**

投标人应指派固定的团队为本项目提供专业服务，应指定1名技术负责人（不与项目经理为同一人），并派驻不少于2人（可包含技术负责人）驻现场开展工作，须均是投标人在职员工，须应具有1年及以上从事商用密码应用安全性评估工作经验且具有本科及以上学历，不满足以上条件本项不得分。在此基础上进行以下评审：1. 技术负责人
2. 全日制硕士毕业的，得10%的分数；全日制博士毕业的，得20%的分数，其他学历不得分；
3. 具有由中国信息安全产品测评认证中心颁发的CISP证书（注册信息安全专业人员）或由国际信息系统安全认证机构（International Information Systems Security Certification Consortiurm，Inc(ISC)）颁发的CISSP证书（信息系统安全专业认证）或由中国信息安全认证中心颁发的CISAW证书（信息安全保障人员认证），得20%的分数；
4. 具有国际软件测试资质认证委员会颁发的ISTQB证书（国际软件测试工程师认证），得20%的分数。
5. 团队其他成员
6. 全日制本科及以上学历的，有1人得10%的分数，最多得20%的分数；
7. 具有由中国信息安全产品测评认证中心颁发的CISP证书（注册信息安全专业人员）或由国际信息系统安全认证机构（International Information Systems Security Certification Consortiurm，Inc(ISC)）颁发的CISSP证书（信息系统安全专业认证）或由中国信息安全认证中心颁发的CISAW证书（信息安全保障人员认证），有1人得10%的分数，最多得20%的分数。

以上五项累计得分，最多得100%的分数。1. **评分依据：**
2. 要求提供通过投标人缴纳的近三月的社保证明作为本单位员工的证明依据（由于社保部门原因最近一个月的社保证明无法提供的可往前顺延一个月）；
3. 要求提供投标人相关证明资料作为得分依据；
4. 学历、学位证书，须同时提供证书复印件以及学信网查询记录复印件加盖公章，原件备查。如学历学位证明颁发较早，学信网无法查询，可提供毕业院校、人社部门等颁发机构或监管机构等单位出具的证明（如开标前无法获得，可提供承诺函（格式自拟），承诺证书真实性，并在中标后提供相关证明材料供采购方核验）；
5. 未按要求提供或提供不清晰导致专家无法有效判断的不得分；以上资料均要求提供复印件（或官方网站截图），原件备查。评分中出现无证明资料或专家无法凭所提供资料判断是否得分的情况，一律作不得分处理。
 |
| 3 | 综合实力 | 30 |
| **序号** | **评分因素** | **分值** | **评分准则** |
| 1 | 投标人资格（资质、认证）情况 | 10 | 1. **评分内容：**
2. 投标人具备检验检测机构资质认定证书（许可使用CMA标志），提供证书扫描件，每一项为10%的分数，最多得10%的分数；
3. 投标人具备中国合格评定国家认可委员会认可证书（CNAS），提供证书扫描件，每一项为10%的分数，最多得20%的分数；
4. 投标人具备国家密码管理局授权的商用密码产品检测资质，提供证书扫描件，得30%的分数；
5. 投标人具备省级及以上政府部门颁发的密码及系统测评类工程技术中心，提供证书扫描件，得40%的分数。

以上四项累计得分，最多得100%的分数。1. **评分依据：**
2. 要求提供有效的认证证书作为得分依据；
3. 以上资料均要求提供复印件（或官方网站截图），原件备查。评分中出现无证明资料或专家无法凭所提供资料判断是否得分的情况，一律作不得分处理。
 |
| 2 | 投标人同类项目业绩情况 | 5 | 1. **评分内容：**

投标人提供至本项目招标之日前三年内承担过市级及以上商用密码应用安全性评估项目案例，提供一个案例得30%的分数，提供三个及以上得100%的分数。投标人应提供至少2个案例的业绩清单与相关证明，否则本项不得分。1. **评分依据：**
2. 要求同时提供合同关键信息作为得分依据；
3. 通过合同关键信息无法判断是否得分的，还须同时提供能证明得分的其它证明资料，如项目报告或合同甲方出具的证明文件等；
4. 以上资料均要求提供复印件，原件备查。评分中出现无证明资料或专家无法凭所提供资料判断是否得分的情况，一律作不得分处理。
 |
| 3 | 投标人自主知识产权产品（创新、设计）情况 | 10 | 1. **评分内容：**
2. 投标人于本招标书发布之日近三年获得的商用密码技术类项目相关专利和软件著作权，每提供1个专利或著作权得10%的分数，最多得30%的分数；
3. 投标人曾参与省部级及以上的密码或信息编码相关课题研究，提供课题研究合同扫描件（至少包含合同双方盖章、合同服务内容）或课题研究委托书扫描件（至少包含委托方盖章，委托内容），得30%的分数，否则不得分；
4. 投标人作为牵头单位起草信息系统密码应用相关的国家标准，提供证明文件（国家标准尚未发布的，可提交立项证明文件），得40%的分数。
5. **评分依据：**
6. 要求提供有效的证明文件为得分依据；
7. 以上资料均要求提供复印件（或官方网站截图），原件备查。评分中出现无证明资料或专家无法凭所提供资料判断是否得分的情况，一律作不得分处理。
 |
| 4 | 服务网点 | 5 | 1. 深圳投标人或非深圳投标人但在深圳有合法注册的分公司（或售后机构）（分公司的必须提供分公司营业执照扫描件，售后机构必须同时提供售后服务合作合同及售后机构营业执照扫描件作为得分依据，原件备查）的，得100%的分数；
2. 外地投标人承诺：中标后一个月内在深圳设立经营（服务）网点，提供承诺文件（格式自定）的，得50%的分数。
 |
| **4** | **诚信情况** | **5** |
| **序号** | **评分因素** | **分值** | **评分准则** |
| 1 | 诚信情况 | 5 | 投标人在参与政府采购活动中存在诚信相关问题且在主管部门相关处理措施实施期限内的，本项不得分，否则得满分。投标人无需提供任何证明材料，由工作人员向评审委员会提供相关信息。 |