附件1

项目管理和服务要求

具体工作内容和要求如下：

|  |  |  |
| --- | --- | --- |
| 工作内容 | 工作列表 | 内容描述和要求 |
| 网络和通信安全密码应用集成服务 | 网络和通信安全密码应用集成服务 | 服务内容包括：1.提供SSL VPN安全传输通道密码应用改造服务。2.与市密码资源池对接，调用云SSL VPN网关服务。3.实现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。4.实现采用密码技术保证通信过程中重要数据的机密性。5.SSL VPN安全传输技术采用的密码算法符合国家密码行业的技术标准。 |
| 设备和计算安全密码应用集成服务 | 服务器设备维护安全升级集成服务 | 服务内容包括：实现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。 |
| 应用和数据安全密码应用集成服务 | 数字证书登录集成服务 | 服务内容包括：1.实现与深圳市档案馆数字档案馆（室）系统集成，提供USBKEY数字证书登录的身份鉴别认证服务。2.提供USBKEY智能密码钥匙数不少于15个，USBKEY智能密码钥匙支持SM2/SM3/SM4的密码算法。3. ▲提供数字证书不少于15个，数字证书的有效期至少为3年。4.提供手写签名系统密码模块一套，手写签名系统密码模块的密码服务要求如下：1）证书读取：获取证书主题、序列号、有效期、公钥信息等；2）签名验签：支持表单结构化数据、附件格式的电子签名、验签，符合PKCS#1标准、PKCS#7标准和GM/T 0010规范的数字签名和验证功能。3）加密与解密：支持对称算法和非对称算法的加密与解密服务。4）算法合规性：支持SM2/SM3/SM4国产密码算法。5）▲浏览器兼容性：PC电脑端支持X86架构、ARM架构等环境下的多种浏览器。6）跨平台扩展性：支持B/S、C/S架构模式下的客户端应用。7）▲提供手写签名系统密码模块取得商用密码产品认证证书。8）▲投标方具有手写签名系统密码模块产品的开发及集成能力，提供证明材料（如商用密码产品认证证书显示的制造商信息）5.提供签名验签服务集成，签名验签服务的集成要求如下：1）提供基于数字签名、验证签名技术，为政务信息系统提供应用级数字签名、验证签名等服务；2）密码算法支持非对称算法SM2、对称密码算法SM1、SSF33、SM4等算法、杂凑算法SM3；3）支持数字证书签名结果的验签密码服务。 |
| 敏感信息加解密集成服务 | 服务内容包括：1．实现与深圳市档案馆数字档案馆（室）系统集成，面向敏感信息或重要数据提供加解密服务，保障数据存储的机密性。2.提供数据加解密集成服务，加解密集成服务要求如下：1）▲其功能为政务信息系统提供应用级数据加解密、杂凑等密码运算服务，实现信息的机密性、完整性、真实性和不可否认性保护。2）密码算法为SM4。3）加解密集成成果符合商用密码应用安全性评估的技术要求。4）技术支持包括加解密服务需求引导、技术资源协调、接口对接、测试联调、上线运行监控等服务。3.提供密钥管理服务，根据密码接入规范和标准管理协议，为政务信息系统提供密钥生成、存储、更新、备份、恢复及归档等密钥全生命周期管理。 |
| 系统日志电子签名集成服务 | 服务内容包括：1．实现与深圳市档案馆数字档案馆（室）系统集成，面向系统日志数据提供电子签名集成服务，保障数据存储的完整性。2. ▲提供时间戳服务集成服务，时间戳服务要求如下：1）其功能为基于公钥密码基础设施应用技术，为政务信息系统提供精准、安全和可信时间认证服务。2）系统日志依托时间戳技术实现电子签名集成，其集成成果符合商用密码应用安全性评估的技术要求。3）技术支持包括加解密服务需求引导、技术资源协调、接口对接、测试联调、上线运行监控等服务。 |
| 访问控制信息电子签名集成服务以及关键信息电子签名集成服务 | 服务内容包括：1．实现与深圳市档案馆数字档案馆（室）系统集成，面向系统访问控制信息、关键信息提供电子签名集成服务，保障关键信息、访问控制信息的完整性。2. 提供签名验签服务集成服务，签名验签服务要求如下：1）其功能为基于数字签名、验证签名技术，为政务信息系统提供应用级数字签名、验证签名等服务。2）访问控制信息、关键信息电子签名集成成果符合商用密码应用安全性评估的技术要求。3）技术支持包括加解密服务需求引导、技术资源协调、接口对接、测试联调、上线运行监控等服务。 |
| 密码安全服务 | 密码方案编制服务 | 服务内容包括：▲包含客户现状需求调研分析、针对用户系统密码保障体系建设提供密码应用方案，密码应用方案的编制成果，需通过第三方密码测评机构的商用密码应用安全性评估，通过评估的结果作为完成该编制服务完成的验收标准。 |
| 密码应用技术服务 | 服务内容包括：1.密码应用保障体系建设服务：依据目前密码应用方案建设，成立项目建设团队，主导整体密码体系建设，协调系统应用厂商、网络安全厂商及系统使用方，完成用户系统密码应用保障体系建设，并通过第三方密评机构的安全性评估。2.密码安全运营服务：为用户、管理人员及系统运维工作人员提供密码产品、技术等专项培训，保障密码应用工作顺利开展；针对后期业务供对接方案设计、对接咨询、对接测试，对接培训服务等内容，保障业务系统通过商用密码应用安全评估；针对后期出现密码应用安全事件，协助使用单位进行排查及处理。保障用户系统密码体系安全、稳定运行。3. ▲业务系统密码应用服务：针对已有的业务系统接入密码应用服务提供对接方案设计、对接咨询、对接测试，对接培训服务，并为各业务系统提供定制相应的密码服务接口，保证密码服务的有效应用，满足商用密码应用安全性评估要求及项目备案、验收等国家政策要求。 |