| **指标** | **指标项** | **技术规格要求** |
| --- | --- | --- |
| 总体要求 | **\*合规性要求** | **1.产品须符合 GM/T 0030《服务器密码机技术规范》、GM/T 0005 《随机性检测规范》、GM/T 0018 《密码设备应用接口规范》、《商用密码产品随机数检测要求》等密码设备相关标准要求****2.产品具备《商用密码产品认证证书》且达到GM/T0028《密码模块安全技术要求》第二级要求****3.服务器密码机内置核心密码模块安全等级**≥**二级4.产品具备《产品软件著作权登记证书》****5.已与电子营业执照前置系统或相关SDK完成适配。** |
| 操作系统 | 产品支持国产化操作系统 |
| 数量 | 8台 |
| 实施要求 | 提供实施方案设计、安装调试、集群化部署等服务 |
| **\*集成要求** | **支持内部及外部的公私钥运算** |
| **使用密码机连接库连接密码机时，支持采用TLS1.2及以上或同等级别的通讯保护** |
| **产品支持对接密钥管理系统、密码服务平台，支持与符合GM/T 0050 《密码设备管理 设备管理技术规范》的密码设备管理平台对接；** |
| 售后要求 | 提供5年7×24小时质保服务 |
| 外形 | 设备外形 | 2U机架式设备 |
| 硬件规格 | 管理接口 | 要求具备业务口、管理口，且必须为独立接口 |
| 网络接口 | 至少包括两个独立千兆网口，支持配置bond0和bond1配置，支持IPv4和IPv6协议 |
| 设备尺寸 | 必须为标准机架设备 |
| CPU | 产品采用国产化CPU |
| 内存 | ≥16GB |
| 硬盘 | ≥240G SSD |
| 电源规格 | 双冗余热插拔电源，至少包括两个独立电源模块 |
| 性能要求 | **\*国密算法支持及运算性能** | 支持主流国密算法对称算法：SM1、SM4非对称算法：SM2摘要算法：SM3MAC算法：HMAC、CMAC性能指标：SM4加解密≥600MbpsSM3杂凑运算≥600MbpsSM2签名≥15000次/秒SM2验签≥8000次/秒SM2加密≥8000次/秒SM2解密≥9000次/秒SM2密钥对生成≥15000次/秒 |
| 功能要求 | 数据加密功能 | 产品能向应用程序提供数据加密/解密功能，支持的算法包括国家密码管理局制定的SM1、SM2、SM4算法，也包括国际通用的RSA、AES、3DES等算法 |
| 数据杂凑功能 | 产品能向应用程序提供数据摘要计算功能，支持的算法包括国家密码管理局制定的SM3算法以及国际通用的SHA-1、SHA-256算法 |
| 数据签名功能 | 产品能向应用程序提供数据签名功能，签名采用板卡内部静态存储的签名密钥对计算，支持的算法包括国家密码管理局制定的SM2签名算法以及国际通用的RSA(1024)、RSA(2048)算法；在计算原文杂凑数值时，SM3算法必须加入签名私钥对应的公钥以及用户标识(ID)计算 |
| 签名验证功能 | 产品能向应用程序提供签名验证功能，验证时的公钥由应用程序提供，计算原文杂凑数值时，SM3算法必须加入签名私钥对应的公钥以及用户标识(ID)计算 |
| 消息认证功能 | 能向应用程序提供消息认证码计算功能，消息认证码，支持SM1、SM4计算模式；支持HMAC及CMAC |
| 密钥管理功能 | 产品能向加密机管理人员提供密钥管理功能，包括密钥生成、密钥删除、密钥备份、密钥恢复等功能。 |
| 用户管理功能 | 1.产品应设置管理员，支持三权分立，并且满足相应管理权限才能进行管理操作。在进行管理操作前应通过身份鉴别，不同的管理操作应有不同的操作权限。2.产品提供web页面远程管理方式供管理人员对系统进行管理，配置需要支持使用国密SSL进行访问，支持单向验证和双向验证。  |
| 状态监控功能 | 状态监控功能：产品能向管理人员提供状态监控功能，状态信息包括板卡支持的算法类型信息、存储空间信息、厂商信息、版本信息、CPU占有率，内存占有率等内容； |
| 辅助功能 | 能向管理人员提供详细的设备日志，日志中包涵详细的错误码，在业务报错时可根据错误码进行错误定位和排查。 |
| 登录方式 | 支持基于硬件的双因素登录，支持IC卡或USBkey等登录形式 |
| 非功能性要求 | **\*集群式部署** | **支持集群式部署模式，不需要增加负载均衡设备即可实现系统的集群式部署** |
| **\*易用性** | **1. 支持国密标准SDF接口，支持java（JCE）接口****2. 服务器密码机与内置核心密码模块须为同一厂商** |
| 安全要求 | 系统安全性 | 系统不存在设备口令开放下载窗口，所有口令文件加密保存，确保密码的安全性，管理员口令采用强口令模式；  |
| 系统漏洞 | 系统内核自身不存在高危级别的漏洞，厂商负责升级更新补漏 |
| 系统监控告警 | 系统监控告警：支持监控设备系统资源的实时状况，包括CPU占有率、内存占有率等指标 |
| SSH登录 | 可以通过SSH方式登录管理 |
| 帐号管理 | 支持管理、操作、审计三权分立帐号配置 |
| 维保服务需求 | 维保服务 | **原厂商免费（免上门费、备件费、人工费及相关费用）提供5年7×24工程师上门维修服务。在接到报修后，要求2小时内工程师到达现场，4小时内备件到达现场，8小时内修复故障。****原厂商免费提供5年硬盘不返还服务。****原厂商免费提供5年硬件微码、固件升级与维护服务。****原厂商免费提供5年重要时期现场值守服务。****维保服务不得转包、分包。****在每次解决故障后，在3个工作日内出具问题分析报告。** |

附件1.

法人授权书

中国农业发展银行：

（单位名称）法定代表人（法人姓名）授权我单位职工（职工姓名）为我单位本次项目授权代理人，全权处理（中国农业发展银行智能算力平台采购项目）一切事宜。委托期限自签署之日起至本项目有效期截止之日止。

代理人无转委托权。

特此授权。

附：（代理人身份证复印件或扫描件正反面）

代理人姓名： 职务：

联系方式： 邮箱：

法人签字/盖章

公章

日期

附件2.

廉 洁 承 诺 书

甲方： 中国农业发展银行智能算力平台采购项目组

乙方：

根据国家相关法律法规，为预防商务往来的违法违纪事件发生，甲方、乙方承诺在双方的商务合作中履行以下约定。

**一、甲、乙双方廉洁义务**

（一）严格遵守党规党纪、国家有关法律法规。

（二）双方业务活动坚持公平、公正、公开、诚信原则（法律认定的商业秘密和合同文件另有规定除外），不得为获取不正当利益，损害国家、集体和对方利益。

（三）建立健全自我约束制度，开展廉洁教育，监督、查处违规、违纪、违法行为。

（四）发现对方在商务活动中有违规、违纪、违法行为的，应及时纠正，情节严重的，应向有关纪检监察部门举报。

**二、甲方廉洁义务**

（一）甲方严格遵守中国农业发展银行党风廉政建设责任制及廉洁从业规定。

（二）甲方按照公平、公正、公开和诚实守信的原则开展各项业务活动，为乙方提供公平的竞争环境与平台。

（三）甲方有权了解乙方有关诚信经营及廉洁从业方面的各项制度和规定，并自觉配合乙方遵守执行。

**三、乙方廉洁义务**

（一）乙方承诺遵守甲方在诚信经营及廉洁从业方面的各项制度和规定，以及相关党纪党规、国家法律法规，并自觉配合甲方执行。

（二）乙方在与甲方商务合作中，严禁以下不廉洁的行为：

1.贿赂甲方人员或其亲属、特定关系人；

2.支付、报销应由甲方人员或其亲属个人支付的费用；

3.赠送回扣、红包、礼金、购物卡、有价证券、贵重物品和好处费、感谢费等；

4.为甲方人员购置或提供通讯工具、交通工具和高档办公用品；

5.与甲方人员或其亲属以借贷名义发生经济往来;

6.无偿、象征性收取钱物或以明显低于市场价格向甲方人员提供物品、服务及股份；

7.以明显高于市场价格购买甲方人员个人物品；

8.允许甲方人员或其亲属、特定关系人在乙方投资、担任重要职务及相关联业务职务；

9.利用资源为甲方人员或其亲友非法谋利；

10.接受甲方人员提供的有偿中介活动；

11.为甲方人员提供可能影响公正执行公务的宴请，安排甲方人员娱乐、旅游、度假或到私人会馆等娱乐场所活动；

12.参加甲方人员婚丧嫁娶等活动，提供不正当利益；

13.与甲方人员进行赌博；

14.向招标代理机构等受托方提供不正当利益；

15.违反国家法律法规、甲方相关规定等其他不廉洁行为；

16.违反不诚信行为等（详见附件《诚信承诺函》）。

（三）乙方发现甲方人员有不廉洁、不诚信行为，应及时向甲方相关纪检监察部门进行实名举报。

**四、违约责任**

（一）甲方人员违反上述廉洁从业义务，经调查属实，甲方依据党政纪规等对当事人进行处理。

（二）乙方及其人员违反上述廉洁从业义务，经调查属实，甲方有权依据相关法律法规，将乙方列入“黑名单”并进行相应处理。

（三）甲方给予乙方本条第（二）款处理时，甲方有权书面通知乙方解除甲方与乙方已签订但尚未履行完毕的全部或部分商务合同，此时，乙方应赔偿由此给甲方造成的经济损失。

**五、附则**

（一）本承诺经双方签字、盖章后生效，并长期有效。

（二）监督举报电话：中央纪委国家监委驻中国农业发展银行纪检监察组，010-68081725；中共中国农业发展银行总行机关纪委，010-68081400。

甲方项目经理（签字）： 乙方客户经理（签字）：

 年 月 日 年 月 日