一、说明

**1 总则**

1.1 投标人应具备国家或行业管理部门规定的，在本市实施本项目所需的资格（资质）和相关手续（如果有），由此引起的所有有关事宜及费用由投标人自行负责。

1.2 投标人对所提供的系统应当享有合法的所有权，没有侵犯任何第三方的知识产权、技术秘密等权利，而且不存在任何抵押、留置、查封等产权瑕疵。

1.3 投标人提供的服务应当符合招标文件的要求，并且其质量完全符合国家标准、行业标准或地方标准。

1.4 投标人应如实准确地填写投标服务的规格、技术参数等相关信息，因上述信息内容填写不完整、不准确，而导致投标文件被误读、漏读，由投标人自行负责，为此投标人需承担其投标文件在评标时被扣分甚至被认定为无效投标的风险。

★1.5若本项目涉及国家强制认证产品（信息安全产品、3C认证产品、强制节能产品、电信设备进网许可证等），则根据国家有关规定，投标人提供的产品必须满足强制认证要求。（详见第一章投标人须知及前附表21.3（9））

★1.6投标人提供的产品和服务必须符合国家强制性标准。

1.7采购人的技术需求参数仅起说明作用，并没有任何限制性和排他性，投标人在投标中可以选用其他替代标准、技术规格或型号，但这些替代要在不影响整体平台功能实现的前提下，并在可接受范围内接受偏离。

1.8投标人在投标前应认真了解采购人的使用需求、使用条件和其他相关条件，一旦中标，应按照招标文件和合同规定的要求提供服务。

1.9投标人应根据本章节中详细技术规格要求，采用市场主流技术服务能力或按照要求提供定制化产品参加竞标。同时，**请投标人务必注意：无论是正偏离还是负偏离，都不得与招标要求相差太大，否则将可能影响投标人的得分**。一旦中标，投标人应按投标文件的承诺签订合同并提供相应的产品和服务。

1.10本项目如涉及软件开发，则开发软件（包括软件、源程序、数据文件、文档、记录、工作日志、或其它和该合同有关的资料的）的全部知识产权归采购人所有。投标人向采购人交付使用的软件系统已享有知识产权的，采购人可在合同文件明确的范围内自主使用。支撑该系统开发和运行的第三方编制的软件的知识产权仍属于第三方。如采购人使用该软件系统构成上述侵权的，则由投标人承担全部责任。

1.11投标人认为招标文件（包括招标补充文件）存在排他性或歧视性条款，自收到招标文件之日或者招标文件公告期限届满之日起10日内，以书面形式提出，并附相关证据。

二、项目概况

**2 项目名称**

上海东方枢纽国际商务合作区综合信息管理服务平台市政务云资源服务

**3 项目地点**

上海东方枢纽国际商务合作区。

**4 招标范围与内容**

**4.1 项目背景及现状**

为贯彻落实党中央、国务院的决策部署，支持上海“五个中心”建设，海关总署、上海市人民政府会同相关部门，积极探索建设上海东方枢纽国际商务合作区，研究编制了《上海东方枢纽国际商务合作区建设总体方案》，经国务院批复于2024年2月28日正式发布。

商务合作区定位为便利国际商务交流的新平台、服务资源要素汇聚的新载体、推动长三角一体化发展的新节点，主要打造便利国际商务交流、服务高端国际会展活动、提升国际培训服务质量三个核心功能。区域紧邻浦东国际机场和上海东站，规划面积约0.88平方公里，其中先行启动区0.43平方公里，分为两个区块，通过封闭通道联接，以实现区域跨境交往便利、国际商务活动活跃、创新要素资源集聚、专业服务能力领先、配套设施完备的功能目标。商务合作区的规划和建设工作将坚持一体化原则，聚焦功能定位，通过数字化手段优化流程，实现便利化和风险防控，满足制度创新和风险防范要求，实现安全与便利的统一。

2024年3月，市政府批准成立上海东方枢纽国际商务合作区管理局筹备工作组，全面统筹协调商务合作区管理局正式成立前区内各项行政管理工作。2025年2月17日，经中央编委、市编办批准，上海东方枢纽国际商务合作区管理局正式成立，在中国（上海）自由贸易试验区管理委员会保税区管理局加挂一块上海东方枢纽国际商务合作区管理局牌子。

综合服务平台的实施，将遵循“统筹规划、分步实施、能快则快”的原则，确保到2025年完成先行启动区的封闭验收和基本功能落地运行，进而为2028年实现全域封闭运作，并在2030年全面建成商务合作区打下扎实基础。

**4.2 项目招标范围及内容**

为满足东方枢纽商务区系统建设，计划采购配套的私有云底座资源（IaaS+PaaS）、算力服务器资源和配套的技术服务。

**4.3服务期**

本项目服务期为自合同签订之日起12个月。

**5 承包方式**

5.1 依据本项目的招标范围和内容，中标人以包云平台服务、包部署集成测试、包安全的方式实施总承包。

5.2本项目不允许分包。

**6 合同的签订**

6.1 本项目合同的标的、价格、质量及验收标准、考核管理、履约期限等主要条款应当与招标文件和中标人投标文件的内容一致，并互相补充和解释。

**7 结算原则和支付方式**

7.1 结算原则

7.1.1本项目合同结算价以审计价为准，中标人的中标单价不变，实际工作量以采购人或第三方按照招标文件规定的验收标准核定为准。

7.1.2发生设备维修的，如该设备尚在服务期内的，采购人不另行支付相关费用；如在服务期外的，单价按照投标文件中明确的备品备件单价（含维修人工费）计取，数量按实结算。如投标文件中没有类似备品备件单价可参照的，则由合同双方协商确定维修单价。

7.2 支付方式

7.2.1 本项目合同金额采用**分期付款**方式，在采购人和中标人合同签订，且财政资金到位后，按下款要求支付相应的合同款项。

7.2.2分期付款的时间进度要求和支付比例具体如下：

（1）第一笔付款-预付款(30%)：合同签订且财政资金下达后，采购人收到合法有效的发票后30日内，完成支付预付款；

（2）第二笔付款-进度款(40%)：主体项目通过中期评估检查且财政资金下达后，采购人收到合法有效的发票后30日内，完成支付第二笔合同款；

（3）第三笔付款-验收款(30%)：主体项目完成审价及审计并取得相应报告，且通过项目验收，在财政资金下达后，采购人收到合法有效的发票后30日内，依据审计金额完成支付剩余合同款。

7.3采购人不得以法定代表人或者主要负责人变更，履行内部付款流程，或者在合同未作约定的情况下以等待竣工验收批复、决算审计等为由，拒绝或者延迟支付中小企业款项。如发生延迟支付情况，应当支付逾期利息，且利率不行低于合同订立时1年期贷款市场报价利率。

三、技术质量要求

**8 适用技术规范和规范性文件**

各投标人应充分注意，凡涉及国家或行业管理部门颁发的相关规范、规程和标准，无论其是否在本招标文件中列明，中标人应无条件执行。标准、规范等不一致的，以要求高者为准。

**9 招标内容与质量要求**

**服务资源清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **具体内容** | **数量** | **服务期** | **备注** |
| 1 | CPU | 2090核 | 12个月 |  |
| 2 | 内存 | 4616GB | 12个月 |  |
| 3 | 高性能存储 | 115.9TB | 12个月 |  |
| 4 | GPU算力 | 24卡 | 12个月 | ●核心工作内容每卡算力不小于280TFlops |
| 5 | 应用负载均衡服务 | 2套 | 12个月 |  |
| 6 | 安全隐患感知服务 | 4节点 | 12个月 |  |
| 7 | 数据库审计服务 | 2实例 | 12个月 |  |
| 8 | 常规安全漏洞扫描 | 120次 | 12个月 |  |
| 9 | 系统上线漏洞扫描 | 91实例 | 12个月 |  |
| 10 | VPN接入 | 4套 | 12个月 |  |
| 11 | 在线防护WAF | 4套 | 12个月 |  |
| 12 | 网页防篡服务 | 4套 | 12个月 |  |
| 13 | 公有IP服务 | 2个 | 12个月 |  |
| 14 | 互联网带宽（骨干级） | 1Gbps | 12个月 |  |
| 15 | 数据备份服务 | 65TB | 12个月 |  |
| 16 | 网络访问控制服务 | 4套 | 12个月 |  |
| 17 | 入侵防御服务 | 4套 | 12个月 |  |
| 18 | 用户管理服务 | 4套 | 12个月 |  |
| 19 | 用户身份认证服务 | 4套 | 12个月 |  |
| 20 | 应用入云部署服务 | 1次 | 12个月 |  |
| 21 | 数据归档服务 | 91套 | 12个月 |  |
| 22 | 文字识别服务（OCR） | 3QPS | 12个月 |  |
| 23 | 安全防病毒(服务器端) | 91套 | 12个月 |  |
| 24 | 密码服务/安全认证网关服务 | 2套 | 12个月 |  |
| 25 | 密码服务/时间戳服务 | 2套 | 12个月 |  |
| 26 | 密码服务/签名验签服务 | 2套 | 12个月 |  |
| 27 | 密码服务/可信密码服务 | 2套 | 12个月 |  |
| 28 | 公务人员证书（key） | 50套 | 12个月 |  |
| 29 | 证书介质（key） | 50套 | 12个月 |  |
| 30 | 短信服务 | 400万条 | 12个月 |  |
| 31 | 日志审计服务 | 50实例 | 12个月 |  |
| 32 | 邮件服务 | 50实例 | 12个月 |  |

**说明：上表中所列为本次招标的主要服务内容，投标人不得减少主要内容数量。**

**10 技术指标要求**

**10.1基础设施层技术要求**

1.

**10.1.1基础设施层整体要求**

（1）总体架构要求：满足本次国际商务合作云平台总体架构，中标人提供的私有云平台需要与市私有云平台进行无缝对接。

（2）IaaS资源池：基线资源池规模满足至少虚拟2090CPU，内存4616GB，高性能存储规模达到115.9TB。

（3）算力服务器：提供支撑系统运行的训练服务器，算力不低于8969TFlops（FP16）

（4）在各项资源发放水位高于70%时及时报告采购人。中标人应按照采购人的要求，根据实际需求进行扩容。

（5）云运维管理平台服务：云服务商应使用自主的、开放的、适应国际标准的商业化虚拟化软件，并搭建统一的个性化云运维管理平台提供服务。云运维管理平台能够基于OpenStack架构的虚拟化软件，提供云运营管理服务和云运维管理服务，能够对IT基础设施进行统一管理。云运维管理平台支持主流虚拟化软件。

（6）安全服务：需符合网络安全等级保护基本要求第三级安全通用要求和云计算安全扩展要求，满足《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）第三级安全测评通用要求和云计算安全扩展要求、满足《信息安全技术云计算服务安全能力要求》（GB/T 31168-2014）增强级。中标人所提供的服务及提供服务所需的软/硬件设备符合《网络安全审查办法》要求及国家网信办的相关要求，所提供的服务及提供服务所需的软/硬件设备符合《中华人民共和国密码法》及国家密码管理部门的相关要求。

（7）出口性能：私有云机房的所有网络出口应具备流量监控能力，支持历史流量回放，各出口的监控能力不低于出口实际配置的上联物理带宽。

**10.2软件技术要求**

**10.2.1云业务管理平台要求**

中标人须提供一套能够针对商务合作区系统私有云上承载的业务进行综合管理的商业化云业务管理平台软件，提供云业务管理和业务云上资源监控等相关个性化服务，能够对云上业务进行有效管理。云业务管理平台软件需支持与中标人所提供的云运维监控平台对接的能力、以及在基础设施层各类服务器及其虚拟化环境中部署的能力。

|  |  |
| --- | --- |
| **规格** | **指标要求** |
| 服务接入管理 | 提供对各项云服务的接入验证审查管理能力，将各项云服务纳入统一的监管体系，包括云资源服务、云软件服务、云安全服务等。 |
| 服务申请管理 | 支持各项云服务申请的统一管理，包括上云、下云、优化、扩容等申请。 |
| 服务交付管理 | 支持各项云服务交付的统一管理，包括服务工单发放、服务交付跟踪、服务交付验证等。 |
| 服务监控管理 | 支持对各类云服务的监控及分级告警管理。 |
| 服务响应管理 | 支持统一的云服务响应管理，包括登记、分发、跟踪、验证、回访等。 |
| 服务故障管理 | 支持各类云服务故障的全流程管理，涵盖故障的发现、定位、诊断、修复、核实等环节。 |
| 服务计量管理 | 支持针对各类云服务的计量管理，并以数据、日志、报告等形式提供相应的计量依据。 |
| 服务计费管理 | 支持各类云服务的计费管理，并以使用单位、云服务商的维度生成月度、季度、年度账单。 |
| 服务评估管理 | 支持各项云服务的周期性评估，包括云服务质量、满意度、安全、用量、使用情况等。 |
| 服务结算管理 | 支持服务周期内的结算管理，基于平台数据，为服务结算提供依据和参考。 |

**10.2.2云运维管理平台要求**

中标人须提供统一云运维管理系统，提供高效的运维管理手段，提升问题处理效率，缩减问题处理时间，在问题发生时可快速自动通知到维护人员，提供分析工具，方便研判故障。提供健康分析功能，能够实时监控并分析数据中心的资源使用状态，评估健康度和风险，协助客户主动运维。提供日常的运维报表，后台运维支持，用户发现问题后应快速分级响应。

|  |  |
| --- | --- |
| **规格** | **指标要求** |
| **告警及性能管理** | 支持多维度告警/事件展现。提供按监控对象、按物理位置、按虚拟逻辑、按来源系统、按服务分组、按VDC等维度查看告警，保证云场景下告警管理的灵活性； |
| 提供告警导出，按指定字段模糊查询告警，按指定字段排序告警以及配置告警列表展示字段的能力； |
| 提供告警处理功能，包括确认、清除等，对选择的告警进行处理。支持用户进行告警确认、取消确认、清除告警、标识误告警、更新告警级别、编辑告警备注、编辑告警经验、查看告警关联帮助，协助管理员更好的处理告警事件； |
| 提供重复告警的归并功能，即多条同源告警合并成一条告警呈现，提供告警的首次发生时间、最后发生时间、发生次数等信息； |
| 提供告警通知功能。通过设置通知规则，当收到符合条件的告警时，自动通过邮件、短信通知用户。支持按设置的规则，当收到符合规则告警后，通过邮件、短信方式，通知用户，支持逾期升级通知。支持告警声音，不同级别可设置不同的声音； |
| 支持告警自定义筛选。支持按多个维度的条件组合进行筛选，包括但是不限于按告警名称、状态、级别、来源、告警对象位置（如数据中心、机房、集群）、告警对象条件（比如VDC、用户）等筛选条件，并支持告警导出功能； |
| 支持设置告警级别、以及告警阈值能力，支持设置告警规则，有符合规则的告警，自动按照预置的告警级别进行告警； |
| 支持告警统计报表，可以对已经发生的告警进行分类统计，并输出报表，便于整体的分析数据中心告警事件； |
| 提供数据中心所有虚拟机利用率分布概览图查看，支持搜索查看单个虚拟机信息，支持数据中心、虚拟化平台、集群三个不同粒度查看虚拟机概况，支持按照资源使用率过滤显示。 |
| 支持把用户查看的性能指标、设备参数保存成视图，后续查看直接选择视图即可，不需要重新选择参数，提升操作效率。 |
| **报表管理** | 支持周期性生成报表，立即生成报表，周期类型包括：天、周、月、季度。只需要设置一次报表参数，即可周期提供报表数据。提供界面截图； |
| 支持自动将报表发送到指定的Email地址。 |
| **设备管理** | 一、统一设备管理： |
| 1、提供统一设备管理能力，统一管理包括数据中心存储、服务器、应用、网络设备（路由器、交换机、防火墙），提供全网资源信息的Dashboard（分类总数、资源利用情况、关键指标Top，如CPU、内存等）； |
| 2、支持管理主机设备、网络设备、存储设备等第三方主流厂商设备的管理； |
| 3、设备规模应满足私有云未来设备增长的要求。 |
| 4、设备分组：提供设备分组能力，支持将多台设备划入一个分组，以简化后续对这些设备的批量操作。分组在拓扑中不显示。 |
| 二、服务器管理： |
| 1、基本信息管理：通过机架图等可视化方式，提供服务器以及各部件基本信息、健康状态的展示功能，并可通过远程KVM和虚拟媒体远程操作服务器； |
| 2、性能分析：提供网口性能、服务器功耗、CPU占用率/内存占用率、创建分析任务和时间段性能等多个指标分析； |
| 3、无状态计算：通过抽象服务器硬件配置文件，使服务器的配置灵活的变更，以提高服务器故障更换和服务器扩容的效率； |
| 4、配置部署：提供对服务器设备的批量配置及部署，包括服务器BIOS配置、网络配置、RAID卡配置、OS部署等功能。 |
| 三、存储管理 |
|
| 1、提供存储容量利用率预测能力，支持查看和统计存储空间使用情况，包括磁盘空间分配、存储池利用率；支持主机实际存储、虚拟机存储空间使用率查看；提供容量预测的功能，可作为扩容的依据，比如从主机角度预测硬盘容量、文件系统容量等； |
| 2、提供系统内部物理和逻辑组件间的关联关系可视化展示，以便故障发生时能够精确定位。 |
| 四、安全管理 |
| 1、用户管理：提供用户创建、删除、查看、修改等功能，缺省提供admin用户作为超级用户。其中，用户密码使用不可逆算法PBKDF2加密存储保障安全性； |
| 2、角色管理：提供角色创建、修改、删除及查看等功能； |
| 3、鉴权管理：提供多种种鉴权方式。包括不限于STS 和 URL 鉴权； |
| 4、本地认证：提供用户管理、登录鉴权、安全策略等功能； |
| 5、RADIUS认证：由RADIUS服务器对登录请求进行认证，根据用户在RADIUS服务器上的所属用户组，映射到管理系统中所属角色为用户授权； |
| 6、LDAP认证：由LDAP服务器对登录请求进行认证；并根据LDAP服务器上用户所属用户组，映射到管理系统中所属角色来为用户授权。 |
| 五、网络管理： |
| 1、支持通过流量分析了解流量的构成和分布。根据接收到的Flow报文自动添加设备，并且自动分析设备接口流量，提供各种纬度的报表展现；用户也可以灵活调整哪些设备接口监控、哪些不监控； |
| 2、支持可订制的dashboard操控板、图形化界面能反馈全网流量状况，并且面板流量数据支持实时动态局部刷新； |
| 3、提供接口、应用、来源主机、目的主机、DSCP、会话、接口组、应用组等多个维度的流量数据；  |
| 4、支持下钻式的数据获取方式； |
| 5、支持原始流量数据的流量审计； |
| 六、安全性要求：前后台采用https协议，数据传输加密，涉及密码等敏感信息采用加密存储方式，防止泄露。 |
| **流程管理** | 包括：服务台、事件管理、问题管理、变更管理、配置管理、发布管理等。 |

**10.2.3云虚拟化平台要求**

|  |  |
| --- | --- |
| **规格** | **指标要求** |
| 基础要求 | 为了保证云平台的开放性及先进性，虚拟化管理平台基于业界主流OpenStack架构。 |
| Openstack增强 | 支持物理裸机统一管理。基于OpenStack Ironic开放框架，支持对标准X86服务器、ARM服务器、GPU服务器的接入和自动化管理。 |
| 支持物理裸机资源管理和业务发放，可以基于管理系统在物理裸机上自动加载业务部署所需的主流操作系统。 |
| 支持物理裸机资源CPU、内存、磁盘、网络IO等各项资源使用情况的监控。 |
| 支持物理服务器网络自动化配置。 |
| 提供租户专属物理机集群功能，提供专属云服务，将若干台物理服务器组成的集群单独指定给某一特定租户，只允许该租户的虚拟机创建在该集群中。以此实现租户独占物理资源的能力。 |
| 支持基于WebUI的向导式系统升级工具，支持将OpenStack的手动、复杂升级过程简化为自动化、高可靠性的升级，提升升级效率、降低升级风险。降低对运维人员的技能要求。 |
| 相比社区OpenStack，提供可靠性功能增强，包括但不限于：提供黑匣子功能，Guest OS故障能自动保存内核黑匣子信息。针对系统关键进程，支持CPU、内存等资源占用阀值检测及告警上报关键进程资源风险，及时预防、规避系统潜在风险。虚拟机热迁移异常检测，支持热迁移超时取消，避免虚拟机迁移永久卡死，如对迁移时间给出限制。镜像下载支持MD5校验，保证镜像下载完整性。支持管理数据一致性审计，支持一致性审计功能，避免管理系统与计算节点数据不一致。 |
| 计算虚拟化 | 虚拟化软件架构须采用裸金属架构，支持标准X86服务器、ARM服务器，充分利用Intel VT和AMD-V的硬件虚拟化技术，支持Intel扩展页表技术。支持GPU虚拟化。虚拟化软件必须能直接安装在服务器硬件设备上，不能采用在服务器上先安装操作系统的方式，虚拟化软件要能直接管理硬件资源。 |
| 支持虚拟机基本的生命周期管理动作，包括创建、删除、启动、关闭、重启等。 |
| 支持容器基本的生命周期管理动作，包括创建、删除、启动、关闭、重启等。 |
| 支持虚拟机迁移，使用同一共享存储的主机之间将处于运行态的虚拟机由当前所在的主机迁移到另一台主机上，在迁移的过程中不影响用户对虚拟机的使用。 |
| 支持虚拟机HA(High Available)机制，提升虚拟机的可用度，允许虚拟机出现故障后能够重新在资源池中自动启动虚拟机。 |
| 支持高精度虚拟机，以满足虚拟机任务处理时，对性能和延迟抖动有严格要求的场景。虚拟机独占分配的VCPU、内存、I/O物理资源，其它虚拟机无法占用。 |
| 支持对虚拟机镜像的生命周期管理，支持镜像的创建、上传、删除、下载、查询等操作。 |
| 支持虚拟机NUMA亲和性调度，减少VM内存访问时延，提升VM性能。 |
| 支持虚拟机之间亲和性部署规则。虚拟机聚合规则，即多个虚拟机必须运行于同一主机。虚拟机互斥规则，即多个虚拟机必须运行于不同主机，不能同时运行同一主机。 |
| 网络虚拟化 | 支持SDN功能，提供自动化网络部署功能。 |
| 支持通过基于OpenStack的云管理平台实现计算、网络资源统一自动化发放。 |
| 支持物理机、虚拟机统一自动化发放功能，包括物理服务器网络自动化配置。 |
| 提供灵活的SNAT和VPC多子网能力，提供灵活的基于Subnet使能SNAT访问外网的能力，提供单个IPsec连接保护多个本地子网的能力。 |
| 存储虚拟化 | 支持存储多路径功能，通过自动优选路径和IO负载均衡选路算法优化，提升存储链路的可靠性和性能。 |
| 支持虚拟机运行时快照功能，虚拟机快照内容包括：虚拟机的电源状态(打开、关闭、挂机)、内存、硬盘、网卡以及CPU寄存器。 |
| 可靠性要求 | 管理节点配置负荷分担部署模式，在保障系统运行的可靠性的情况下，可以平滑扩容管理节点，以便管理更大规模的集群。 |
| 系统支持对OpenStack的管理节点的数据备份与恢复操作。支持每日备份、立即备份。备份介质支持第三方FTP或对象存储。 |
| 通过心跳检测机制，实时监控管理进程，及时检测管理进程进程故障或僵死，并支持自动重启状态异常的进程。 |
| 备份要求 | 支持无代理备份，不需要在虚拟机内安装备份代理软件。 |
| 支持LAN-free备份与恢复，减少对生产服务器的性能影响。 |
| 支持在线备份，在虚拟机是开机和关机状态下都可进行备份。 |
| 支持增量备份，每次只需备份变化数据块，减少备份数据量，降低备份成本。 |
| 支持虚拟机系统卷数据（如安装的软件）的恢复。 |
| 配置要求 | 配置提供本期项目实际所需的足够的授权 |

**10.2.4备份软件要求**

|  |  |
| --- | --- |
| **规格** | **指标要求** |
| 数据备份 | 数据库及应用保护 | 支持对主流数据库进行在线备份保护，备份任务配置过程全部图形化向导指引完成，无需编写脚本。 |
| 支持对达梦数据库、人大金仓、神舟通用等数据库在线数据备份保护 |
| 支持对GaussDB等国产数据库进行有效在线数据备份保护，并提供相关厂商产品兼容性互认证证书或可查询官网链接认证 |
| 支持对Hadoop文件系统进行在线备份保护，支持文件、目录、格式和日期过滤，支持永久增量备份。支持备份数据恢复至原环境和其他Hadoop集群，支持恢复至其他文件系统。 |
| 国产化支持 | 支持鲲鹏、龙芯、飞腾平台下的软件安装部署和数据保护。 |
| 卷级备份 | 支持文件系统的卷级备份功能，以整卷为单位进行数据备份，提升海量小文件环境下的备份效率。支持整卷恢复和单文件目录级别的细粒度恢复 |
| 虚拟化及云平台备份 | 支持对主流虚拟化应用的备份，支持单机和集群部署环境。以上虚拟化应用均支持以虚拟机、资源池和整个集群为单位进行备份保护保护，无需在虚拟机内部安装任何代理软件。支持针对FusionCloud的永久增量备份以及基于租户化对接及管理，备份数据流不会占用FusionCloud管理网络导致拥塞，需提供相关于FusionCloud备份对接的互认证兼容性证书及官网查询链接 |
| 虚拟机恢复时支持选择目标集群、资源池和存储资源，支持原位置恢复和恢复为新虚拟机，能够设置恢复后虚拟机的CPU、内存和网络配置。支持保留源虚拟机MAC地址恢复，支持恢复后自动打开虚拟机。 |
| 支持虚拟机分流备份功能，一个任务包含来自多个宿主主机的虚拟机时，会对虚拟机按宿主机进行归类，优先抽取不同宿主机上的虚拟机进行备份，提升备份速度和效率。 |
| 支持虚拟机并发备份和恢复功能，支持在WEB页面中设置单个备份和恢复任务中的虚拟机并发备份和恢复数量，可大幅提高备份恢复效率 |
| 源端重复数据删除技术 | 支持基于源端的可变长度切片的重复数据删除技术，多个备份任务可以共享同一个重复数据删除指纹池，也可以根据数据的不同单独设置专属指纹池，最大限度的提升重复数据删除效率，减轻带宽压力，降低传输数据量和备份数据存储成本。 |
| 支持并行重复数据删除，通过在多个不同的节点上构建指纹池，并将指纹并行分布于多个节点，有效解决单点性能和存储空间压力问题 |
| 采用内存级指纹池进行重删，所有指纹读写全部保存于内存中，从而提升指纹查询和处理效率，并且减少了因磁盘中指纹池增大所导致的随机IO压力。当指纹池不再需要进行备份时，将指纹同步到磁盘当中。指纹池构建在不同重删节点上，而生产数据可以基于多个不同的指纹池，执行并行重删。 |
| 采用内存进行重复数据删除加速，重复数据删除的计算和对比均在内存中进行。重删指纹池实现按需加载到内存，不使用时写入普通机械磁盘中，无须高性能的SSD。大幅提高重复数据删除速度和效率，降低投资成本。 |
| 数据安全性 | 支持对备份数据进行加密传输和存储，支持AES256和SM4两种加密算法，提升传输过程以及存储的安全性 |
|  | 备份数据存储 | 所有的定时备份任务，其备份数据存储在一个统一的存储介质管理系统中，无需针对不同类型的任务单独配置单独隔离无法空间共享的存储池，提高空间利用率的同事简化管理维护。 |
| 支持备份存储介质管理系统支持在线扩容，所有备份节点均可在线增加磁盘，新增磁盘空间自动添加进存储介质管理系统中，且即时可用，现有备份任务无需任何调整，备份数据可自动写入新增加的空间内。 |
| 永久增量备份 | 支持永久增量备份技术，初次备份对所有数据进行完全备份，之后只对新增加或改动过的数据做增量备份。每个增量备份的数据副本将自动合成为完全副本，但数据存储空间只占用一份完全副本大小及增量数据大小，能够大幅度减少备份时间的同时节省相比传统定期完全备份数据所需的存储空间 |
| 数据保留 | 以单个备份任务为单位设定备份数据的保留周期，支持基于时间范围和完全备份副本数量两种方式控制备份数据的保留周期，同时支持将备份数据直接从客户端D2C备份到对象存储中做长期保留 |
| 持续数据保护 | 数据库复制 | 支持数据库的逻辑复制，基于生产端日志解析方式的数据库同步。 |
| 支持数据库的物理复制，实时捕获生产数据库的所有操作引起的数据块变化，并实时传输至备用数据库中进行应用，保持备用数据库在物理结构上与生产数据库保持实时同步，备用数据库在复制阶段处于mount状态，生产库发生故障后可open并对外提供服务。 |
| 数据卷复制 | 支持对云服务器整机（所有磁盘分区，包括操作系统分区）和数据卷进行卷级别的实时复制功能，可将生产服务器上数据卷的数据变化实时复制到目标服务器上指定的数据卷上，保持生产服务器和目标服务器之间的指定数据卷的数据同步。采用整机复制策略时，目标服务器为未安装操作系统的裸机环境，生产服务器故障后直接启用目标服务器接管生产业务，无需重新安装配置操作系统和应用软件。支持备份客户端的内存占用控制，也可以按照自定义的频率间隔复制数据变化以降低对生产系统的影响。 |
| 支持差异数据智能识别功能，可自动识别生产服务器和目标服务器上的数据差异性，仅同步差异数据，提升复制效率。 |
| 实时备份 | 支持对云服务器的整机（所有磁盘分区，包括操作系统分区）和数据卷进行卷级别的实时备份，将生产服务器的数据变化实时备份到备份设备内部保存为日志数据，并同时将变化数据实时写入到备份设备内部与生产服务器一一对应的虚拟磁盘中。 |
| 支持实时备份数据的应急接管和容灾演练功能，基于虚拟磁盘快照和实时备份的日志数据，通过图形化界面快速生成生产服务器在历史某一时间完整状态的完整虚拟磁盘，时间选择精度为微秒（0.000001）级（提供该功能界面截图）。在时间精度选择时，系统界面提供对应时间状态的生产服务器的磁盘IO负载波形图，以辅助选择合适的IO状态。同时，通过图形化界面为该虚拟机磁盘配置相关的存储、计算和网络资源后形成一个完整的虚拟机，可使用备份设备内置的企业级虚拟化软件启动该虚拟机。 |
| 支持在应急接管模式下，管理界面提示对应生成服务器的MAC地址并默认为生成的虚拟机使用该MAC地址，以确保虚拟机启动后无需配置IP地址即可提供业务应急，且应急接管和容灾演练的虚拟机，均可通过备份设备的WEB页面直接进行图形化的管理，无需安装任何插件，包括开机、断电、重启、远程控制等功能。 |
| 支持在应容灾演模式下，生成的虚拟机默认与生产服务器网络隔离，避免虚拟机启动后与生产业务冲突。 |
| 支持应急接管虚拟机的在线回迁功能，在应急虚拟机持续提供业务访问的同时，实时实现操作系统、应用软件和业务数据回迁到目标裸机服务器环境中，回迁完毕后即可由目标服务器提供业务。 |

**10.3安全要求**

**10.3.1基本要求**

私有云平台应按网络安全等级保护基本要求第三级建设，满足《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）第三级安全测评通用要求和云计算安全扩展要求、《信息安全技术 云计算服务安全能力要求》（GB/T 31168-2014）增强级。

**10.3.2平台安全要求**

中标人建设的私有云平台需满足包括但不限于如下安全要求：物理安全、网络安全、主机安全、云管理平台安全等。

（1）物理安全：中标人用于建设私有云服务中心的机房需满足国家A级（GB50174-2008）的安全要求，具备防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应等能力。

（2）网络安全：中标人需针对私有云平台按照国家网络安全等级保护基本要求要求建立一套网络安全防护体系，对网络边界处提供访问控制、病毒过滤、防攻击、防入侵、防篡改、内外网数据安全隔离交换等立体安全防护，保护平台内部网络通信安全。

访问控制：私有云平台在各网络边界处均应部署安全访问控制设备，包括防火墙、IPS、VPN网关、安全网关等，能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。支持按用户和系统之间的允许访问规则，允许或拒绝用户对受控系统进行资源访。控制粒度为单个用户，同时应通过VPN网关及软件系统应用功能实现对远程拨号访问权限的用户数量进行限制。支持云服务客户自行对网络访问控制规则进行配置。

安全审计：中标人需对私有云平台使用网络设备运行状况、网络流量、用户行为、特权命令等进行日志记录，能够根据记录数据进行分析并生成审计报表，同时对系统审计的记录进行有效安全保护，避免受到未预期的删除、修改或覆盖等不安全操作。

边界完整性检查：中标人通过部署网络行为管理系统、安全审计系统应能够对非授权设备私自连到内部网络的行为及内部网络用户私自连到外部网络的行为进行检查，能根据用户信息、主机信息、IP信息等准确定出非法互联位置，并对其进行有效的网络阻断控制。

入侵防范：配备有IDS或IPS入侵防范、检测系统或安全网关系统，实现的实时防范功能应包括：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等非法网络攻击行为，当检测到攻击行为时，系统将详细记录相关信息，同时在发生严重入侵事件时具备报警、记录功能。

恶意代码防范：中标人在网络的边界处对各种恶意代码进行检测和清除功能，系统应支持自动及手工方式对恶意代码库的升级和检测系统的更新功能。

网络设备防护：中标人所使用的网络设备均应支持对登录用户的身份鉴别功能，支持采用加密用户口令鉴、RADIUS身份认证等方式，可通过命令行、Web、中文图形化配置软件等方式进行配置和管理，并可通过ACL访问控制列表的方式实现对网络设备的管理员登录地址进行限制，所有网络设备用户均应具备唯一标识。

（3）主机安全：对主机的物理安全摆放位置，主机访问控制方面进行保护。

主机访问控制：主机系统应启用主机系统的访问控制功能，依据安全策略控制用户对资源的访问权限，通过系统的技术维护措施严格限制默认账户的访问权限，对重要信息资源设置敏感标记，并依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

（4）云管理平台安全：包括虚拟化及云运维管理平台的安全保护，支持物理资源与虚拟资源统一管理。

虚拟化安全：支持有代理或者无代理安全方式进行虚拟环境的整体防护；整体的虚拟化安全措施应避免“病毒风暴”。

私有云平台安全：如果云运维管理平台需要数据库的支持，应保护好云运维管理平台的数据库安全，设置强壮复杂的密码策略、备份数据库和配置相关的网络安全服务；云运维管理平台的访问许可应加强管理，删除不需要的用户账号；安装云运维管理平台软件的操作系统需设置安全策略。

私有云平台访问控制安全：用户在访问私有云平台资源过程中支持使用数字证书进行身份认证，包括但不限于中标人维护人员、用户授权操作人员、管理单位监管人员，且数字证书的介质购买和服务费由中标人提供。

（5）日志审计：包括日志采集、日志传输与存储转发、日志检索、日志分析和资产管理功能。

日志采集：支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于720种日志对象的日志数据采集；支持主动、被动相结合的数据采集方式，支持通过Agent采集日志数据，支持通过syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Kafka等多种方式完成日志收集；内置大量日志处理模型，自动解析主流网络设备、安全设备和中间件的日志数据，标准化自动识别系统类型至少达到200种；支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射。（需提供截图证明）

日志传输与存储转发：支持对单个/多个日志源批量转发，支持定时转发，可通过syslog和kafka方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志；支持TLS加密方式进行日志传输，支持日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量。

日志检索：支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP地址、特征ID、URL进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件。

日志分析：支持网站攻击、漏洞利用、C&C通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到350条以上，支持自定义关联分析规则（需提供截图证明）

资产管理功能：支持资产全生命周期管理，资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等，支持自定义资产标签、属性。

（6）部署在私有云平台中的应用系统若发现重大安全事故或者安全隐患时，中标人需要配合进行安全整改。

**10.4国密技术要求**

**10.4.1国密服务要求**

中标人需提供密码应用、物理和环境安全、网络和通信安全、设备和计算安全、密钥管理及密码安全管理体系制度等方面的建设和咨询服务。

**10.4.2国密软件要求**

|  |
| --- |
| **用途：签名验签服务系统** |
| **要求** | **具体要求** |
| 部署要求 | 签名验签服务能够部署在云端虚拟机中，并且能与CA、云密码机进行联动，与CA配合完成证书的验证，与云密码机配合完成签名和验签功能； |
| 功能要求 | 支持配置信任多个CA根证书，可验证不同CA机构签发的符合SM2证书标准的签名结果。 |
| 支持制作数字签名，支持对数据原文制作数字签名，签名结构符合SM2证书国家标准。 |
| 支持配置记录日志的类型，如业务日志、管理员日志、Debug日志、错误日志，并可根据需求开启或关闭，支持错误和故障日志完整保留，并可进行下载。 |
| 监管要求 | 支持签名验签服务运行状态监控，包括服务正常运行情况、业务连接数、CPU、内存占用率、磁盘使用率等业务状态，提供信息提取接口便于第三方网络管理软件进行信息提取； |
| 支持故障定位功能，错误签名或验签信息必须有详细的日志，譬如验签的原文、验签的时间等。 |
| 密评要求 | 签名验签服务应用程序与服务申请应用、云密码机之间的数据传输应采用基于商用密码算法的机密性和完整性保护； |
| 签名验签服务的访问控制信息、日志信息能够自主进行基于商用密码算法的完整性保护。 |

|  |
| --- |
| **用途：时间戳服系统** |
| **要求** | **具体要求** |
| 部署要求 | 时间戳服务能够部署在云端虚拟机中，并且能与CA/RA系统、签名和验证签系统、云密码机进行联动，与签名和验签系统、CA/RA系统配合完成证书的验证与签名功能； |
| 功能要求 | 能够与第三方授时中心、卫星授权时间源进行时间同步，确保所签发时间戳时所获取的时间的有效性； |
| 监管要求 | 支持签名验签服务运行状态监控，包括服务正常运行情况、业务连接数、CPU、内存占用率、磁盘使用率等业务状态，提供信息提取接口便于第三方网络管理软件进行信息提取； |
| 安全要求 | 时间戳服务可采用分级权限管理，支持初始化管理员和操作员，负责管理员、操作员权限的判断。 |
| 可靠性要求 | 部署后可保证在当一台物理机器出现问题时，时间戳服务能够漂移至其他物理机，不影响业务系统的正常运行。 |
| 密评要求 | 承载时间戳服务的虚拟机，其运维管理支持集中的安全管理通道，身份认证基于商密证书的强身份认证或支持基于商用密码算法的信任链； |
| 时间戳服务的访问控制信息、日志信息能够进行基于商用密码算法的完整性保护。 |
| 时间戳服务应用程序与服务申请应用、云密码机之间的数据传输应采用基于商用密码算法的机密性和完整性保护； |

|  |
| --- |
| **用途：电子签章系统** |
| **要求** | **具体要求** |
| 部署要求 | 电子签章服务能够部署在云端虚拟机中，并且能与CA/RA系统、时间戳服务、云密码机进行联动；与CA/RA配合完成证书的验证；与时间戳服务配合获取可信时间；与签验签系统和云密码机配合完成签名和验签功能； |
| 功能要求 | 支持电子签章用章审计； |
| 通过证书/证书链导入CA信息，支持多CA证书验证。 |
| 通过设置不同的服务端口来添加多个电子签章服务，为不同的应用系统同时提供电子签章等服务。 |
| 监管要求 | 支持电子签章服务运行状态监控，包括服务正常运行情况、业务连接数、签章使用率等状态，提供信息提取接口便于第三方网络管理软件进行信息提取； |
| 可靠性要求 | 电子签章系统部署后能够漂移至其他物理机，不影响业务系统的正常运行。 |
| 密评要求 | 电子签章系统的访问控制信息、日志信息能够进行基于商用密码算法的完整性保护。 |
| 电子签章服务应用程序与服务申请应用、云密码机之间的数据传输应采用商用密码算法进行机密性和完整性保护； |

|  |
| --- |
| **用途：RA/CA系统** |
| **要求** | **具体要求** |
| 部署要求 | RA/CA系统能够部署在云端虚拟机中，并且能与应用系统配合完成基于证书的身份认证及相应证书管理功能； |
| 功能要求 | 访问控制：实现基于身份的访问控制，阻止对信息资源的非授权使用。 |
| 身份生命周期管理：包括对用户身份的赋予、变更、冻结、注销等全生命周期进行管理。 |
| 信息保密性功能：对身份数据和访问控制信息进行保护,非授权用户无法得到用户身份信息。 |
| 提供基于数字签名的日志记录和审计功能。 |
| 监管要求 | 支持RA/CA系统运行状态监控，包括服务正常运行情况、业务连接数、签章使用率等状态，提供信息提取接口便于第三方网络管理软件进行信息提取； |
| 可靠性要求 | 具备完善的多机并行能力及容错能力，支持负载均衡，可以保证在一台物理机器出现问题时，RA/CA服务能够漂移至其他物理机，不影响业务系统的正常运行。 |
| 密评要求 | RA/CA系统的访问控制信息、日志信息能够进行基于商用密码算法的完整性保护。 |
| RA/CA与其他应用程序之间的重要数据传输应采用商用密码算法进行机密性和完整性保护； |

|  |
| --- |
| **用途：密码服务管理平台系统** |
| **要求** | **具体要求** |
| 基本要求 | 产品具有国家密码管理局颁发的《商用密码产品型号证书》 |
| 部署要求 | 支持云环境部署，可集中部署和分布式部署； |
| 功能要求 | 支持虚拟密码机、签名验签服务、时间戳服务、电子签章服务的动态添加删除功能； |
| 支持加解密服务、认证服务和完整性保护等密码运算，并支持这些运算的统计功能，且能根据管理需求添加并显示相应统计功能； |
| 提供虚拟密码设备、密码资源配置、密码资源分组等进行统一管理。支持设备注册、注销、隔离、恢复。设备信息包含IP、端口、部署数据中心、厂商、设备型号、设备序列号、所属系统等 |
| 为业务系统提供底层的密码运算服务支撑，包括密钥访问处理、密码运算等。 |
| 提供密码设备监控功能，包括设备状态、CPU利用率、内存使用情况、磁盘空间、设备服务链接数等。 |
| 密钥管理要求 | 为业务系统及模块提供以密钥生命周期为主线的密钥管理功能，包含密钥的生成、存储、分发、备份、更新、撤销、归档和恢复等信息进行采集、存储、查询及分析等； |
| 持密钥同步服务功能，多个密钥管理系统之间具有密钥同步功能 |
| 所有密钥需按照国家采购人认可的密钥生成方法产生，不使用软件、人工等伪随机数方法产生；密钥生成装置需为硬件设备；能生成高质量随机数、对称密钥和非对称密钥；必须以加密方式导出密钥生成装置的密钥； |
| 支持密钥同步服务功能，多个密钥管理系统之间具有密钥同步功能 |
| 监管要求 | 支持云密码机集群管理，支持虚拟密码机、签名验签服务、时间戳服务、电子签章服务资源池管理和监控； |
| 可靠性要求 | 支持将密码服务协议转换处理完成后得到的服务请求分发到负载均衡模块，支持加密设备之间的业务负载功能，业务请求采用轮转调度算法实现负载均衡。 |
| 密评要求 | 承载密码管理服务平台的虚拟机，其运维管理支持集中的安全管理通道，其身份认证基于商密证书的强身份认证或支持基于商用密码算法的信任链； |
| 密码管理服务平台的访问控制信息、日志信息能够进行基于商用密码算法的完整性保护。 |
| 密码管理服务平台应用程序与服务申请应用、云密码机之间的数据传输应采用商用密码算法进行机密性和完整性保护； |

|  |
| --- |
| **用途：密码评估系统** |
| **规格** | **指标要求** |
| 根据密评要求和相关解答定义出对应的密码风险符合度报告，用户可自行进行密评符合度评估 | 总体要求评估功能 | 总体要求评估模块：对密码算法，密码技术，密码产品，密码服务进行安全符合度评估 |
| 密码功能要求评估 | 密码功能评估模块：能够对密码功能的机密性，完整性，真实性，不可否认性进行符合度评估 |
| 安全管理评估功能 | 1.制度评测模块：根据信息系统密码应用基本要求规定，对等级保护二级和三级的标准制定制度管理符合度评测功能 |
| 2.人员评测模块：根据信息系统密码应用基本要求规定，对等级保护二级和三级的标准制定人员管理评测功能 |
| 3.实施评测：根据信息系统密码应用基本要求规定，实现实施管理评测功能模块，涵盖规划，建设，运营三部分 |
| 4.应急评测：根据信息系统密码应用基本要求规定，对等级保护二级和三级的标准制定应急管理符合度评测功能 |
| 安全技术评测功能 | 1.物理和环境安全评估模块：根据信息系统密码应用基本要求规定，对等级保护二级和三级的标准进行物理和环境安全评估 |
| 2.网络和通信评估模块：根据信息系统密码应用基本要求规定，对等级保护二级和三级的标准进行网络和通信安全评估 |
| 3.设备和计算安全评估模块：根据信息系统密码应用基本要求规定，对等级保护二级和三级的标准进行设备和计算安全评估 |
| 4.应用和数据安全评估模块：根据信息系统密码应用基本要求规定，对等级保护二级和三级的标准进行应用和数据安全评估 |
| 5.密钥管理评估模块：根据信息系统密码应用基本要求规定，对等级保护二级和三级的标准进行密钥管理安全评估 |
| 分析功能 | 1.综合评分功能：能够对各个模块的评测结果进行打分和分析 |
| 2.建议功能：根据评测结果自动出具建议报告 |
| 3.能力矩阵图：根据系统各个模块收集到的信息制作能力矩阵分析图，能够清晰分析出系统的薄弱点和优势点 |

**10.5平台软件层技术要求**

1.

**10.5.1平台软件层整体要求**

（1）系统部署要求：中标人提供的平台软件层服务中涉及基础资源使用的（包括但不限于计算、存储、备份）应当使用本项目建设的私有云云基础设施服务资源。

（2）接口服务要求：中标人应当提供包括但不限于API发布、管理、流量控制、熔断、用户管理功能的API网关，中标人提供的平台软件层能力中涉及API方式提供的应当具备通过API网关服务的能力。

（3）安全隔离要求：中标人提供的服务涉及集中部署的应该符合网络安全等级保护三级的要求，开展安全加固工作，每个服务期开展不少于4次服务的安全策略配置、安全扫描和系统漏洞的加固，配合使用单位完成应用的等级保护工作。提供软件介质部署在使用单位资源上的，应当提供安全漏洞修复补丁并提供技术支持，配合使用单位完成应用的等级保护工作。中标人应当通过技术方式确保不同安全责任主体之间的隔离。

（4）服务交付要求：中标人提供的私有云平台软件层服务，应当面向使用单位提供每个服务项的服务接入方式，包括但不限于界面、API接口、文件等。

（5）管理能力要求：中标人应当具备与私有云基础设施监管服务平台（以下简称“云管平台”）进行数据对接和业务协调联动，包括但不限于实时接收使用单位在云管平台中发起的PaaS服务申请工单信息，并向云管平台反馈工单实时处理信息。

（6）监控能力要求：中标人应当对所提供的各项平台软件层能力提供实时动态的监控服务，并将监控数据同步到“云管平台”中，同步内容包括但不限于服务的使用情况统计、计量计费数据、告警数据、资源数据、运行性能数据、故障处置信息、安全相关信息以及其他日志数据。

（7）协同工作要求：中标人应当按照采购人的要求，配合本项目其他包件中标人开展平台软件层建设工作。

（8）中标人应当配合采购人完成服务考核评估工作，并负责对已经出现的服务问题进行整改。

**10.5.2软件技术要求**

**10.5.2.1管理平台**

|  |  |
| --- | --- |
| **规格** | **指标要求** |
| 功能要求 | 支持对部署在PaaS软件运行环境中的应用程序进行版本更新 |
| 提供开放的软件支撑应用程序查询、创建、更新、删除接口 |
| 提供PaaS应用程序版本更新主要内容说明的服务或接口； |
| 提供控制PaaS应用程序运行状态的接口或工具； |
| 提供获取PaaS应用程序当前运行状态的接口或工具； |
| 提供管理PaaS应用程序发布的接口或服务，支持PaaS应用程序的发布和撤回； |
| 提供PaaS应用程序发布的审核机制，支持将审核结果及意见反馈给用户，支持PaaS用户在线查询应用程序的审核状态； |
| 提供PaaS应用程序版本另生成规则及说明文档； |
| 提供图形化的PaaS应用程序版本管理界面； |
| 提供多版本PaaS应用程序的发布、同步及访问控制； |
| 提供批量控制PaaS应用程序运行状态的功能； |
| 提供管理PaaS应用程序运行状态的图形化界面 |
| 提供PaaS应用程序发布接人规范，并提供发布示例： |
| 提供图形化的申请PaaS应用程序发布和撤回的界面。 |
| 支持获取租户范围内PaaS软件运行环境的监控信息。 |
| 支持定义租户范围内PaaS应用程序的资源分配、安全性和可用性等方面的策略； |
| 支持PaaS应用程序的多个副本分散在不同的PaaS软件运行环境中进行部署，避免单一PaaS软件运行环境实例故障带来的可用性问题; |
| 支持将PaaS应用程序的或组件分布的部署在多个PaaS软件运行环境中，将应用程序的访问负载分散到不同的PaaS软件运行 环境实例中，以提升PaaS 应用程序的访问件能。 |

**10.5.2.2安全防病毒服务（主机端）**

|  |  |
| --- | --- |
| **规格** | **指标要求** |
| 服务描述 | 面向主机端提供多维度防御病毒传播和横向感染的服务能力，实时监控每个服务器端/客户端的运行状态、攻击日志、病毒状态，最大程度的减小病毒传播的可能，全面提升主机端安全管理能力。 |
| 部署模式 | 支持管理端+客户端组合部署，实现终端的集中管控和策略下发。同时支持单机部署以及级联部署。 |
| 功能要求 | 提供主机端安全防病毒服务，服务功能要求包括不限于：1.病毒防护：病毒查杀、病毒诱捕，如勒索病毒等；2.系统防护：系统加固防御、漏洞修复、入侵检测、系统加固、网络防御、病毒库升级（在线/离线）、文件实时监控、软件安装拦截等；3.终端集中管理：使用单位（多租户）管理、资产管理、服务管理、审计管理、风险态势展示等功能。 |
| 性能要求 | 1、在管理端（CPU：64核，内存：128GB 磁盘容量：8TB ）资源配置的场景下，支持管理的客户端数量应大于1万台。2、在客户端（CPU：4核，内存：8GB 磁盘容量：50GB ）的资源配置场景下： 1）病毒扫描时，主机内存资源占用≤50MB, CPU资源占用率≤15%； 2）病毒监控时，主机内存资源占用≤50MB, CPU资源占用率≤1%； 3）病毒检出率≥98%。（不具备测试验证场景时，提供相关软件产品检出率证明材料） |
| 兼容性要求 | 1、支持中标麒麟、银河麒麟、统信UOS、深度等多种主流国产操作系统，同时支持Linux、Windows、Unix等国外主流操作系统。2、支持达梦、人大金仓、神通等多种国产数据库，同时支持Oracle、DB2、SQL Server、MySql等国外主流数据库。 |
| 服务要求 | 提供包括不限于该服务的安装介质、版本升级介质、软件安全风险补丁、产品文档、培训咨询、管理端巡检服务、管理端性能调优、重要活动和重大节假日管理端保障等保障服务。 |
| 验收考核要求 | 1、提供服务对应软件产品的使用详情，以及提供按套授权的许可编号。2、服务结算按照实际授权开通套数计算。 |

**10.5.2.3安全防病毒服务（PC客户端）**

|  |  |
| --- | --- |
| **规格** | **指标要求** |
| 服务描述 | 面向PC终端提供多维度防御病毒传播和横向感染的服务能力，实时监控每个PC端的运行状态、攻击日志、病毒状态，最大程度的减小病毒传播的可能，全面提升PC终端安全管理能力。 |
| 部署模式 | 支持管理端+客户端组合部署，实现终端的集中管控和策略下发。同时支持单机部署以及级联部署。 |
| 功能要求 | 提供PC客户端安全防病毒服务，服务功能要求包括不限于：1.病毒防护：病毒查杀、病毒诱捕，如勒索病毒等；2.系统防护：系统加固防御、浏览器保护、漏洞修复、入侵检测、系统加固、网络防御、病毒库升级（在线/离线）、文件实时监控、软件安装拦截、弹窗拦截等；3.行为管理：移动存储介质管理、外部设备监控、非法外联监控、终端进程服务监控、文档检查与跟踪；4.终端集中管理：使用该客户端软件产品的集中管理、资产管理、服务管理、审计管理、风险态势展示等功能。 |
| 性能要求 | 1、在管理端（CPU：8核，内存：8GB 磁盘容量：1TB）的资源配置场景下，支持管理的客户端数量大于10万台，小于30万台；2、在客户端（CPU：4核，内存：8GB 磁盘容量：50GB ）的资源配置场景下： 1）病毒扫描时，主机内存资源占用≤50MB, CPU资源占用率≤15%; 2）病毒监控时，主机内存资源占用≤50MB, CPU资源占用率≤1%; 3）病毒检出率≥98%。（不具备测试验证场景时，提供相关软件产品检出率证明材料） |
| 兼容性要求 | 1、支持中标麒麟、银河麒麟、统信UOS、深度等多种主流国产操作系统，同时支持Linux、Windows、Unix等国外主流操作系统。2、支持红莲花等多种国产浏览器，同时支持IE、firefox等多种国外主流浏览器。 |
| 服务要求 | 提供包括不限于该服务的安装介质、版本升级介质、软件安全风险补丁、产品文档、培训咨询、管理端巡检服务、管理端性能调优、重要活动和重大节假日管理端保障等保障服务。 |
| 验收考核要求 | 1、提供服务对应软件产品的使用详情，以及提供按套授权的许可编号。2、服务结算按照实际授权开通套数计算。 |

**10.5.2.4实时语音转写服务**

|  |  |
| --- | --- |
| **规格** | **指标要求** |
| 服务描述 | 提供基于普通话将实时/离线音频流转换为文字的实时语音转写服务，不含方言和小语种。 |
| 部署模式 | 支持单机和集群部署模式 |
| 功能要求 | 提供基础普通话转写服务，不包含方言和外语，提供16K在线引擎的单声道识别服务，可以将音频流实时识别为文字，也可以支持上传音频文件进行识别；返回结果包含每句话的开始和结束时间，适用于音视频字幕、直播字幕、会议记录等场景。**一、语音接入要求**1.支持多音频格式接入，如支持raw、mp3、opus、vox、alaw、ulaw格式录音接入。支持8k16bit，16k16bit采样率音频接入。支持音频传输加密处理，并提供音频最佳压缩比和网络纠错能力。2.支持多渠道接入，语音识别需满足实时语音流的多种接入方式，支持Android/IOS/H5渠道接入；支持国际标准的媒体资源控制协议MRCP协议接入。**二、语音识别要求**1.数字字符串转写功能，支持电话号码识别，支持金额识别，支持日期识别2.端点检测，端点检测是对输入的音频流进行分析，确定人员说话的起始和终止的处理过程。一旦检测到人员开始说话，语音开始流向识别引擎，直到检测到人员说话结束。识别引擎需在人员说话的同时就开始进行识别处理，避免话务数据信息丢失。3.噪声消除，在实际应用中，针对电话场景，适应人员在千差万别的环境中的语音文件识别要求，提供软件噪声消除功能，满足噪音环境下的语音文件识别。4.中文连续转写，根据场景，定制包括专业术语连续语音文件识别功能，满足8小时以上的不间断识别要求，并支持识别结果实时反馈，输出响应时间应小于700ms。**三、语音识别结果展示要求**1.支持敏感词过滤，能够自动对语音文件识别结果中的敏感词进行自动过滤。2.支持语气词过滤，支持能将语气词和多余的词汇滤除，以保证录入文本的规整。3.数字字符串自动规整，能通过上下文语境分析，支持对语音文件识别结果中的数字串自动规整，可以识别日期、金额、单号等数字，文本输出为阿 拉 伯数字，并符合数字书面表达形式。4.标点智能预测，对语音识别文件的文本结果智能预测其对话语境，提供标点智能预测功能，自动生成标点符号，提高输出文本的可读性与规整性。5.针对识别结果能够进行二遍智能纠正，在实时语音文件识别过程中，能针对语音识别第一次识别错误的文本结果，能够根据语音内容对第一次的错误文本结果进行纠正，保障文本输出的正确性。6.识别文本词边界输出，语音文件识别服务返回文本识别结果时需携带识别结果的分词信息，并携带分词的起始和终止点，用于分析说话人语速变化，辅助情绪识别。 |
| 性能要求 | 1、语音识别准确率，中文普通话场景下，语音识别准确率应不低于90%（识别率：指中文汉字识别率）。2、支持大词汇量（≥5000）、非特定、噪声环境（40分贝左右）、多麦串音（两个人及以上）等情况下的汉语识别能力。3、人机交互60秒内短句在线平均子句响应时间在1秒内。4、实时语音转写：支持30路以上并发能力，平均子句响应时间在1秒内； 离线语音转写：支持30路以上并发能力，1小时完成不少于100小时语料转写能力。 |
| 兼容性要求 | 1.硬件兼容性X86环境；2.系统兼容性，支持CentOS、银河麒麟等操作系统；3.产品API接口支持Java、C++、C#、go、Python等多种编程语言； |
| 安全性要求 | 提供的软件产品通过第三方安全检测。 |
| 服务要求 | 提供包括不限于该服务的安装使用材料、产品使用介质、版本升级介质、产品API、适配改造、管理端安全问题修复、管理端应急保障、产品文档、培训咨询、巡检服务、管理端性能调优、重要活动和重大节假日管理端保障等保障服务。 |
| 验收考核要求 | 1、提供PaaS服务对应软件产品的使用详情。2、服务结算按照软件产品部署后支撑的“路数”进行结算。 |

**10.5.2.5在线语音合成服务**

|  |  |
| --- | --- |
| **规格** | **指标要求** |
| 服务描述 | 提供基于中文的普通文本合成为拟人的语音，“像人一样开口说话”的文章等文本转音频(TTS)在线语音合成服务，不包含方言和小语种。 |
| 部署模式 | 支持单机和集群部署模式 |
| 功能要求 | 1.提供基础普通话合成服务，不包含方言和小语种。基于海量文本语料的自然语言理解技术实现的语音合成功能。2.支持中文断词断句准确、普通话男声女声声库、普通话男声女声试听等功能。3.提供百万量级词条的词典，高精度的多音字处理能力。4.准确的韵律层级预测，使合成语音的使用者更易于理解句子的内容；5.语音合成服务，基于HTTP请求的REST API接口，将文本转换为可以播放的音频文件。合成的文件格式为 mp3，pcm（16k），wav（16k）等。6.支持语速和音量设置,支持合成音的音量、语速、音高（基频）等多种合成参数动态调整功能；7.多样化合成方式：支持数字读法判断，根据上下文和语境判断数字朗读方式，是朗读成数值还是号码；支持指定姓氏发音，通过[r1]标记强制人名中姓氏发音；支持预录音的模版音合成等功能。8.多种合成文本的编码：GB2312、GBK、UTF8等各种合成文本的编码；9.中文多音字发音预测：支持根据上下文和语境判断中文多音字发音，对于单字或者有歧义的多音字发音，可以通过强制拼音标记来指定发音。10.功能点包括：文本分析、韵律停顿预测、声学参数预测、语音合成等。 |
| 性能要求 | 1、在建议配置(CPU:72核 内存:256G)下语音合成可支持的并发路数为40路，实时率不低于1.52、语音合成自然度指标达MOS评分在4.5分及以上 |
| 兼容性要求 | 1.硬件兼容性X86环境；2.系统兼容性，支持CentOS、银河麒麟等操作系统；3.产品API接口支持Java、C++、C#、go、Python等多种编程语言； |
| 安全性要求 | 提供的软件产品通过第三方安全检测。 |
| 服务要求 | 提供包括不限于该服务的安装使用材料、产品使用介质、版本升级介质、产品API、适配改造、管理端安全问题修复、管理端应急保障、产品文档、培训咨询、巡检服务、管理端性能调优、重要活动和重大节假日管理端保障等保障服务。 |
| 验收考核要求 | 1、提供PaaS服务对应软件产品的使用详情。2、服务结算按照软件产品部署后支撑的“路数”进行结算。 |

**10.5.2.6文字识别服务（OCR）**

|  |  |
| --- | --- |
| **规格** | **指标要求** |
| 服务描述 | 提供纸质文档电子化文字识别服务，实现对纸质文档电子化文件的识别，包括不限于对身份证、户口簿、医疗票据、个人签名等在内的大量个人证件、企业证件、业务单据、凭证进行处理，以及支持中文、英文、中英文混合语种识别。 |
| 部署模式 | 支持单机和集群部署模式 |
| 功能要求 | 1、票证识别范围包括不限于： 1）增值税发票、增值税发票（卷票） 2）火车票 3）出租车发票 4）客运汽车票 5）定额发票 6）身份证、户口本、驾驶证、行驶证 7）营业执照、组织机构代码 8）航空行程单2、通用文字识别能力： 1）支持中文、英文、中英文混合语种识别。 2）支持表格识别：能够将表格识别信息进行格式化展示，并且可以搭配表格恢复引擎将识别的表格结果转换为Excel文件。 3）支持图片格式：支持PNG、JPG、JPEG、BMP格式图片识别。 4）单字位置显示：支持识别结果单字位置显示(默认识别结果为单行显示)，并且可以对单字位置功能进行开关处理 。 5）支持手写体识别 |
| 性能要求 | 1、在脱机离线文字中英文扫描识别场景下手写正确率高于95%2、在脱机离线印刷体扫描识别的正确率达97%3、识别速度：在(CPU:32核 内存:128G GPU: NVIDIA Tesla T4\*1 )的资源配置下，支持8路并发，平均响应时间2秒以内。4、单个文图像文件（图片大小4M以内，图片内容为50字左右）的识别速度在2秒以内。 |
| 兼容性要求 | 1.系统兼容性，支持CentOS、银河麒麟等操作系统；2.产品API接口支持Java、C++、C#、go、Python等多种编程语言； |
| 安全性要求 | 提供的软件产品通过第三方安全检测。 |
| 服务要求 | 提供包括不限于该服务的安装使用材料、产品使用介质、版本升级介质、产品API、适配改造、管理端安全问题修复、管理端应急保障、产品文档、培训咨询、巡检服务、管理端性能调优、重要活动和重大节假日管理端保障等保障服务。 |
| 验收考核要求 | 1、提供PaaS服务对应软件产品的使用详情。2、服务结算按照软件产品部署后支撑的“QPS（每秒查询率）”进行结算。 |

**10.5.2.7人像身份核验服务**

|  |  |
| --- | --- |
| **规格** | **指标要求** |
| 服务描述 | 提供“人脸核身场景、人证核验场景、人像活体检测”的人像身份核验服务。 |
| 部署模式 | 支持单机和集群部署模式 |
| 功能要求 | 1、人脸检测：检测图片中的人脸并分别标记出人脸框坐标点、人脸关键点,支持多人脸。2、人脸属性：对图片进行属性检测，返回性别、年龄、有无口罩等属性,支持多人脸和指定的人脸检测（默认检测当前图片中最大的脸）。3、人像质量检测：对图片进行质量检测，返回姿态、模糊、嘴部状态信息,支持多人脸人脸特征提取，提取图片中人脸的特征值，支持进行多人脸或指定人脸检测（默认检测图片中最大的一张人脸）。4、人脸特征比对：传入两个人脸特征值，检测特征值的比对相似度；特征值可由特征提取接口获取。5、两图比对：传入两张图片，检测图片的比对相似度；支持选择图片中的某个或多个人脸进行比对。6、单图防伪：基于单张图片，判断图片中的人脸是否为二次翻拍。7、视频交互活体：基于视频，对视频中的人像进行动作活体检测分析，判断视频中的人是否为活体，动作序列支持眨眼、张嘴、点头、摇头动作。8、视频静默活体 ：基于视频，对视频中的人像进行活体检测分析，用户无需配合作出相应指令。9、H5交互活体（含前端JS示例）：基于H5前后端连续帧传输方案，按要求实时完成一系列随机动作指令后，即可判断摄像头捕捉的对象是否为真人，支持质量检测，支持多人脸告警。10、H5静默活体（含前端JS示例）：基于H5前后端连续帧传输方案，无需依据提示进行脸部相应动作，保持直视屏幕即可判断摄像头捕捉的对象是否为真人，支持质量检测，支持多人脸告警。11、操作日志管理：对用户在管理后台的操作进行展示和查找，筛选条件包括用户名、姓名、操作时间等。12、提供软件产品基本功能管理功能，包括不限于：用户管理、角色管理、账户管理、监控管理、使用情况管理等能力。 |
| 性能要求 | 1.支持戴口罩人脸识别首位命中率不低于98%。2.在线人脸比对实人认证并发数支持50及以上，线下人脸1:1服务并发达1000及以上。3.人像特征库总容量：不小于5亿张人脸图片；4.“判断画面中的人脸是否为真实人脸，有效识别打印照片、显示屏上显示的照片及视频等”相关功能，活体检测精度（拒绝率≧99%，接受率≧99%）； |
| 兼容性要求 | 提供接入服务的 API 接口，支持微信、支付宝 H5、小程序、SDK 等多种场景接入。 |
| 安全性要求 | 提供的软件产品通过第三方安全检测。 |
| 服务要求 | 提供包括不限于该服务的安装使用材料、产品使用介质、版本升级介质、产品API、适配改造、管理端安全问题修复、管理端应急保障、产品文档、培训咨询、巡检服务、管理端性能调优、重要活动和重大节假日管理端保障等保障服务。 |
| 验收考核要求 | 1、提供PaaS服务对应软件产品的使用详情，包括不限于按照服务使用次数统计的详情。2、服务结算按照使用单位实际使用次数进行结算。 |

**10.6平台技术验证要求**

为保障中标人提供的私有云资源平台能承载招标人业务应用标要求，并能与现有业务应用环境相匹配，中标人须提供适量的资源供招标人进行技术验证测试，且测试结果基本符合招标人要求。

**11 质量标准及验收要求**

**11.1质量标准**

11.1.1 中标人所交付的云服务系统应满足本项目合同文件明确的功能性、使用性要求。信息系统的质量标准按照国家标准和招标需求确定，上述标准不一致的，以严格的标准为准。没有国家标准、行业标准和企业标准的，按照通常标准或者符合招标目的的特定标准确定。

11.1.2 中标人所交付的信息系统还应符合国家和上海市有关系统运行安全之规定。

**11.2系统测试及验收方案**

11.2.1 采购人应依据云平台服务的条件和性质，按照招标文件明确的要求向中标人提供业务系统的部署、安装和集成环境。如采购人未能在该时间内提供部署和安装环境，中标人可相应顺延交付日期。如对中标人造成经济损失，采购人还应依本合同规定承担违约责任。

11.2.2 中标人应在进行系统交付前5个工作日内，以书面方式通知采购人并向采购人提供完整的竣工资料和竣工验收报告。采购人应当在接到通知与资料的5个工作日内安排交付验收。中标人在交付前应当根据合同文件中的检测标准对本项目进行云平台功能和运行检测，以确认本项目初步达到符合本合同交付的规定。

11.2.3中标人应按照合同及其附件所约定的内容进行交付，如果约定采购人可以使用或拥有某软件源代码的，中标人应同时交付软件的源代码并不做任何的权利保留。所交付的文档与文件应当是可供人阅读的书面和电子文档。

11.2.4 采购人在本项目交付后，应当在5个工作日内向中标人出具书面文件，以确认其初步达到符合本合同所约定的任务、需求和功能。如有缺陷，应向中标人陈述需要改进的缺陷。中标人应立即改进此项缺陷，并再次进行检测和评估。期间中标人需承担由自身原因造成修改的费用。

11.2.5自云平台功能部署上线之日起，采购人拥有（90）天的试运行权利。云平台验收通过的日期为实际竣工日期。

11.2.6如果由于中标人原因，导致云平台在试运行期间出现故障或问题，中标人应及时排除该故障或问题。以上行为产生的费用均由中标人承担。

11.2.7如果由于采购人原因，导致云平台在试运行期间出现故障或问题，中标人应及时配合排除该方面的故障或问题。以上行为产生的相关费用均由采购人承担。

11.2.8云平台试运行完成后，采购人应及时进行系统验收。中标人应当以书面形式向采购人递交验收通知书，采购人在收到验收通知书后的5个工作日内，确定具体日期，由双方按照本合同的规定完成验收。采购人有权委托第三方检测机构进行验收，对此中标人应当配合。

11.2.9 如果属于中标人原因致使云平台未能通过验收，中标人应当排除故障，并自行承担相关费用，同时延长试运行期30日，直至其完全符合验收标准。

11.2.10 如果属于采购人原因致使云平台未能通过验收，采购人应在合理时间内排除故障，再次进行验收。

11.2.11 采购人根据信息系统的技术规格要求和质量标准，对云平台验收合格，签署验收意见。

**12 人员配备要求**

12.1 投标人应充分考虑满足本项目的建设要求，提出自身有足够能力实施的方案，根据对项目的理解提供项目实施详细进度计划和项目人员配置管理计划，包括组织结构、项目负责人、组成人员及分工职责，并提供人员简历、资质证书。

12.2 投标人应优先选派具备相关项目实施经验的项目经理和核心技术人员，组建本项目实施团队人员，确保项目按计划开发实施完成。

12.3 投标人针对本项目成立项目小组，在投标书中提供书面名单，人员一旦得到确认，无特殊理由不得随意变动，其中项目经理具有相当项目经验，项目经理未得到采购人同意的情况下不得随意更换。

12.4 采购人有权根据实施情况要求更换项目经理和实施人员。

**13 售后服务要求（包括延伸服务要求）**

13.1 免费质保期自本项目完工验收合格后开始计算，免费质保期为一年。在免费质保期内，由中标人免费承担招标文件提到的云平台运行维护工作，维护工作包括但不限于平台的故障修复、定期检查及调优等服务内容， 投标人须提供不少于一年的每周7天\*8小时技术服务（投标人可提供优于招标要求的技术服务)，服务内容及方式包括电话技术服务支持、远程故障修复、定期巡查巡检及调优及必要时现场支持服务。

13.2 对于在免费质保期内找到的系统缺陷，中标人无条件为采购人进行修复。

13.3 免费质保期内，中标人接到维护通知后应在半小时内响应并协助采购人处理问题，1 小时内赶赴采购人现场处理问题，除不可抗力因素外，费用全部由中标人承担。质保期内设备质量经权威机构鉴定不符合质量要求的，由此给采购人带来的一切损失由中标人承担。

13.4 免费质保期外，中标人接到维护通知后应在1小时内响应并协助采购人处理问题，3 小时内 赶赴采购人现场处理问题，费用按年计算，投标人需列明质量保证期外售后服务所需费用（不能超过中标合同）。

**14 项目的保密和知识产权**

14.1 中标人保证对其提供的服务及出售的标的物享有合法的权利，应保证在其出售的标的物上不存在任何未曾向采购人透露的担保物权，如抵押权、质押权、留置权等。

14.2采购人委托开发软件的知识产权归采购人所有。中标人向采购人交付使用的信息系统已享有知识产权的，采购人可在合同文件明确的范围内自主使用。

14.3在本合同项下的任何权利和义务不因中标人发生收购、兼并、重组、分立而发生变化。如果发生上述情形，则中标人的权利随之转移至收购、兼并、重组后的企业继续履行合同，分立后成立的企业共同对采购人承担连带责任。

14.4 中标人应遵守合同文件约定内容的保密要求。如果采购人提供的内容属于保密的，应签订保密协议，且双方均有保密义务。

14.5采购人具有源代码修改权和永久使用权。采购人对本次开发的软件拥有产权，具有软件开发平台的永久使用权，中标人在售后维护期内（包括续签的售后服务期）应提供软件开发平台的后续升级及因开发平台升级导致的应用软件升级服务。

14.6 如采购人使用该标的物构成上述侵权的，则中标人承担全部责任。

**15 技术培训**

15.1技术文件：

中标人应为所有被培训人员提供详细技术文件。

15.2技术服务：

云平台系统操作培训：对云平台服务的使用人员，进行具体功能模块使用培训。

云平台系统日常维护培训：对云平台管理人员进行系统的日常维护培训，保证系统运行的可靠性及持续性。在系统扩展时，也提供对系统管理人员的后继培训。

系统相关技术培训：对云平台管理人员进行系统相关关键技术的培训，有利于管理人员对系统的日常维护，避免管理操作不当引起的系统故障。

中标人负责提供培训资料，所有资料是中文书写，培训对象主要包括云平台管理员及业务人员。系统相关软硬件的日常管理及维护由云平台管理员负责，专业性较强，需要进行专门的培训，以备日常工作的需要。同时也要对业务人员进行必要的培训以确保其对业务系统能够正常、有效地使用。

四、投标报价须知

**16 投标报价依据**

16.1 投标报价计算依据包括本项目的招标文件（包括提供的附件）、招标文件答疑或修改的补充文书、工作量清单、项目现场条件等。

16.2招标文件明确的项目范围、实施内容、服务期限、质量要求、售后服务、管理要求与标准及考核要求等。

16.3服务清单说明

16.3.1 服务清单应与投标人须知、合同条件、项目质量标准和要求等文件结合起来理解或解释。

16.3.2采购人提供的服务清单是依照采购需求测算出的主要内容，允许投标人对服务清单内非核心工作内容进行优化设计，并依照优化后的方案进行报价。各投标人应认真了解招标需求，如发现核心工作内容和实际采购需求不一致时，应立即以书面形式通知采购人核查，除非采购人以答疑文件或补充文件予以更正，否则，应以工作量清单为准。

**1****7投标报价内容**

17.1 本项目报价为全费用报价，是履行合同的最终价格，除投标需求中另有说明外，投标报价（即投标总价）应包括项目前期调研、数据收集和分析、方案设计、项目研发、基础环境集成实施、智能化安装工程、硬件集成实施、软件开发和集成实施、安全集成实施、系统调试及试运行、验收和评估、操作培训、售后服务、投入使用这一系列过程中所包含的所有费用。

17.2 投标报价中投标人应考虑本项目可能存在的风险因素。投标报价应将所有工作内容考虑在内，如有漏项或缺项，均属于投标人的风险，其费用视作已分配在报价明细表内单价或总价之中。投标人应逐项计算并填写单价、合计价和总价。

17.3在项目实施期内，对于除不可抗力因素之外，人工价格上涨以及可能存在的其它任何风险因素，投标人应自行考虑，在合同履约期内中标价不作调整。

17.4 投标人按照投标文件格式中所附的表式完整地填写《开标一览表》及各类投标报价明细表，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

**18投标报价控制性条款**

18.1 投标报价不得超过公布的预算金额或最高限价，其中各分项报价（如有要求）均不得超过对应的预算金额或最高限价。

18.2 本项目只允许有一个报价，任何有选择的报价将不予接受。

18.3 投标人提供的服务应当符合国家和上海市有关法律、法规和标准规范，满足合同约定的服务内容和质量等要求。不得违反法规标准规定或合同约定，不得通过降低服务质量、减少服务内容等手段进行恶性低价竞争，扰乱正常市场秩序。

★18.4经评标委员会审定，投标报价存在下列情形之一的，该投标文件作无效标处理：

18.4.1减少服务清单中主要资源内容数量；

18.4.2 投标报价和技术方案明显不相符的。

五、政府采购政策

**19节能产品政府采购**

19.1 按照《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）的要求，采购人采购的产品属于“节能产品品目清单”中的，在技术、服务等指标同等条件下，应当优先采购节能产品。采购人需购买的材料产品属于政府强制采购节能产品品目的，投标人必须选用节能产品。

19.2投标人如选用节能产品的，则应在投标文件中提供国家确定的认证机构出具的、处于有效期之内的节能产品的认证证书；反之，该产品在评标时不被认定为节能产品。

**20环境标志产品政府采购**

20.1 按照《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）的要求，采购人采购的产品属于“环境标志产品品目清单”中的，在性能、技术、服务等指标同等条件下，应当优先采购环境标志产品。

20.2投标人如选用环境标志产品的，则应在投标文件中提供国家确定的认证机构出具的、处于有效期之内的环境标志产品的认证证书；反之，该产品在评标时不被认定为环境标志产品。

**21促进中小企业发展**

21.1 中小企业（含中型、小型、微型企业，下同）的划定按照《中小企业划型标准规定》（工信部联企业【2011】300号）执行，参加投标的中小企业应当提供《中小企业声明函》（具体格式见“投标文件格式”），反之，视作非中小企业，不享受相应的扶持政策。如项目允许联合体参与竞争的，则联合体中的中小企业均应按本款要求提供《中小企业声明函》。

21.2 依据市财政局2015年9月发布的《关于执行促进中小企业发展政策相关事宜的通知》，事业单位、团体组织等非企业性质的政府采购供应商，不属于中小企业划型标准确定的中小企业，不得按《关于印发中小企业划型标准规定的通知》规定声明为中小微企业，也不适用《政府采购促进中小企业发展管理办法》。

21.3 如项目允许联合体参与竞争的，组成联合体的大中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。

21.4对于小型、微型企业，按照《政府采购促进中小企业发展管理办法》（财库【2020】46号）和《关于进一步加大政府采购支持中小企业力度的通知》（财库【2022】19号）规定，其报价给予**10%**的扣除，用扣除后的价格参与评审。

21.5如项目允许联合体参与竞争的，且联合体各方均为小型、微型企业的，联合体视同为小型、微型企业，其报价给予**10%**的扣除，用扣除后的价格参与评审。反之，依照联合体协议约定，小型、微型企业的协议合同金额占到联合体协议合同总金额30%以上的，给予联合体**4%**的价格扣除，用扣除后的价格参与评审。

21.6供应商如提供虚假材料以谋取成交的，按照《政府采购法》有关条款处理，并记入供应商诚信档案。

**22****促进残疾人就业（注：仅残疾人福利单位适用）**

22.1 符合财库【2017】141号文中所示条件的残疾人福利性单位视同小型、微型企业，享受促进中小企业发展的政府采购政策。残疾人福利性单位属于小型、微型企业的，不重复享受政策。

22.2 残疾人福利性单位在参加政府采购活动时，应当按财库【2017】141号规定的《残疾人福利性单位声明函》（具体格式详见“投标文件格式”），并对声明的真实性负责。