零信任安全建设项目

采购需求书

珠海市珠港机场管理有限公司

2024 年 6 月

一、项目概述

为全面提高珠海机场信息系统的安全防护能力，确保数据的完整性和安全性，珠海机场已于2023年建设完成零信任VPN平台，本次项目旨在基于零信任安全理念，通过新增零信任控制代理网关和授权，组建成完善的零信任安全防护体系，对珠海机场信息系统内外网络的访问控制、身份验证、数据加密、实时监测等方面进行全面升级和完善，以解决当前网络安全威胁带来的挑战。依据国家《中华人民共和国网络安全法》和公安部对信息系统等级保护工作的要求，零信任安全建设项目将有效阻止潜在的内部和外部威胁，提升整体安全性。通过完善的身份验证机制和访问控制策略，只有经过严格验证的用户和设备才能访问敏感信息，从而有效防止未经授权的访问和数据泄露。此外，实时监测系统和数据加密技术的引入将加强对异常行为的检测和应对能力，以确保信息系统的连续性和稳定性。零信任安全建设项目将为珠海机场带来全方位的改善和升级，提升信息系统的安全性和可靠性，有力应对日益复杂的网络安全威胁，为机场的业务运作提供可靠保障。

二、建设目标

通过本项目建设，落实国家的网络信息安全等级保护政策、标准，提升信息系统的安全防御能力，内外部网络访问内部资源时基于最小权限原则进行动态访问控制，应对高级持续性威胁、内部人员泄露等复杂网络攻击时，零信任安全能够提供更加有效的防护手段，保证本场信息系统的安全稳定运行。

通过零信任安全策略，实现对用户、设备、应用程序的细粒度访问控制，降低安全风险，确保在网络安全事件发生时，业务能够迅速恢复并继续运行，保护重要数据不被非法访问、篡改或泄露，在保障安全的前提下，优化用户访问体验，提高工作效率。

三、项目建设内容

通过以上建设内容，珠海机场将建立起一套完善的零信任安全框架，提高网络安全水平，保障业务的持续稳定运行。

1.远程办公安全性提升：通过实施多因素身份验证、VPN接入控制、应用隔离等措施，确保远程办公员工的设备和数据安全。

3.应用控制和访问控制：实施应用白名单和黑名单策略，防止未经授权的应用访问公司业务、文件、数据。

4.数据隔离和加密：将业务数据与个人数据进行隔离，采用加密技术保护数据的

传输和存储安全。

5.网络安全强化：实施零信任网络访问控制，对所有设备、用户和应用进行严格的验证和授权，防止内部和外部威胁的侵入。

6.威胁检测与响应：整合UEBA、EDR等安全技术，及时发现并应对潜在的安全威胁，保障机场网络的安全稳定。

四、技术需求

1. 硬件要求

序号	设备类型	参数要求	数量	单位
1	深信服零信任安全代理网关	➢ 性能参数：加密流量速率不低于300Mbps，最大并发用户数不少于 3000 个，最大 https 并发连接数30000个， https新建连接数不少于400个/秒。 ➢ 硬件参数:CPU不低于4核心,内存大小不少于16G，硬盘容量不少于128G SSD，电源：双电源，接口不少于6千兆电口+2千兆光口SFP。	1	台

2. 功能需求

模块	功能项	具体参数要求
用户认证	认证方式支持	支持对接珠海机场统一身份认证平台，同时支持珠海机场统一身份认证平台客户端集成零信任SDK的方式实现安全接入功能，避免单独安装零信任客户端。
		支持并具备包括不限于以下认证方式：本地账号密码认证、LDAP/AD认证、OAuth2.0标准协议的票据认证、CAS标准协议的票据认证、Radius账号认证、HTTPS帐号认证、证书主辅认证、短信主辅认证、标准Radius令牌认证、第三方令牌认证、TOTP动态令牌认证等认证方式，并可与企业微信、阿里钉钉、飞书结合实现扫码认证； 支持飞书用户或个人微信企业号通过H5接入。支持通过票据共享的方式跟统一身份认证系统进行单点登录对接，以间接实现业务系统的单点登录对接，支持反向OAuth对接及票据注入等模式。
	增强认证	支持强化系统认证安全性，可配置在触发异常环境的条件时，需完成增强认证才可登录。可配置的异常环境包括但不

		限于：帐号首次登录、帐号在该终端首次登录、闲置帐号登录、弱密码登录、异常时间登录、非常用地点登录等。
	多因素认证	支持多因素认证，支持管理员结合已对接的主认证和辅认证类型进行设置，可自由选择采用首次认证+二次认证+终端认证+增强认证等方式。
权限及访问控制	支持动态访问控制	为满足组织灵活的管理要求，支持配置动态访问规则，可配置化的 ACL 规则引擎，可以灵活地将终端环境、用户身份、处置动作等进行配置，针对不同操作系统设定单独或多系统访问控制策略。
	动态上线准入控制	支持配置动态上线准入规则，动态上线准入策略可支持按需授权，支持用户或用户组直接关联到应用。动态访问控制策略支持“与”、“或”条件嵌套，并可通过单一条件或条件组的方式灵活组合嵌套，可支持多种条件变量设置，当检测到不符合安全条件时，支持如短信增强认证、告警等灵活的补救动作，实现灰度处置，有效平衡员工访问体验和安全保障。
资源发布能力	隧道资源发布	支持隧道模式资源发布，基于 TCP、UDP、ICMP 等协议代理访问业务资源，支持发布 IP、IP 范围、IP 段、具体域名及通配符域名等形式的服务器地址，满足常见办公业务的代理，收缩业务暴露面。支持以隧道模式发布 http/https 协议的资源，以增加在隧道模式下发布的资源的 URL 级别审计能力，同时支持为隧道资源添加 WEB 水印以及单点登录功能。
	WEB 资源发布	支持 WEB 模式资源发布，可以支持基于 http 或 https 协议代理访问业务资源，支持发布 IP 或域名形式的后端服务器地址，支持通过域名+URL 路径发布和授权应用。支持将 WEB 应用以免认证的形式发布。
	WEB 页面安全	支持针对发布的 WEB 应用开启 WEB 水印，水印内容包括不限于用户名+当前年月日，起到威慑与溯源作用。应支持对 WEB 应用禁止复制、禁止打印、禁止下载、禁止鼠标右键、禁止浏览器调试功能，以保护应用的数据安全与应用安全。
	DNS 解析	支持以私有 DNS 发布企业资源，无需额外购买 DNS 服务即可使用域名访问内网资源，支持管理员自主配置是否允许从具体网络区域（局域网/互联网）接入时使用此私有 DNS 解析地址。
终端接入能力	客户端国产终端兼容性	零信任客户端须兼容主流国产硬件 CPU 的国产操作系统终端，需提供国产操作系统与零信任厂商的兼容性证明，包括但不限于麒麟 V10×龙芯、麒麟 V10×龙芯 LoongArch、麒麟 V10×飞腾、麒麟 V10×鲲鹏、麒麟 V10×兆芯、麒麟 V10×海光、麒麟 V10×海思麒麟；统信 V20×龙芯（3A3000、3A4000）、统信 V20×龙芯（3A5000）、统信 V20×飞腾、统信 V20×鲲鹏、统信 V20×海光、统信 V20×兆芯等。
	CDN 支持	支持配置企业的 CDN 作为零信任客户端下载地址以降低带宽压力。当客户端通过 CDN 加速等代理方式接入访问业务系统时，支持获取 CDN 加速前的访问 IP，并在日志中记录此 IP 为客户端 IP。

	客户端自动选路	支持多线路接入单网关访问业务的场景，支持时延优先的选路模式，支持周期性探测线路时延和多次探测确认恶化后切换，支持最低时延+相对时延阈值随机选择策略。
	弱网访问加速	支持优化 TCP 协议，增强隧道抗丢包、抗抖动特性，实现弱网环境的访问加速。
	短隧道资源时延优化	支持将短隧道资源新建连接耗时优化至 0RTT，降低业务访问网络时延，实现同等网络环境下访问速度接近甚至达到直连访问。
	虚拟 IP	支持以虚拟 IP 方式，访问真实的业务系统，以配合其他对 IP 有要求的安全设备工作，以及便于流量分析类设备进行流量分析。 支持共享虚拟 IP 池与独享虚拟 IP 两种模式。共享虚拟 IP 池可根据 IP 资源的充裕情况配置用户注销后立即释放虚拟 IP 或注销后指定时间再释放；在独享 IP 池中为用户分配指定的虚拟 IP 地址，绑定的虚拟 IP 不会释放。
	授信终端	支持设置授信终端绑定，支持配置绑定授信终端的可信网络区域、增强认证条件；并可限定用户可绑定的授信终端数量；支持配置一个账号绑定一个终端或绑定多个终端；支持用户自主绑定授信终端并设定不限于短信认证、令牌认证等；
零信任安全特性	SPA 单包授权	零信任平台需提供单包授权能力（SPA），支持 UDP+TCP 组合的单包授权技术，未授权用户无法连接零信任设备，无法扫描到服务端口。安全码支持共享码和一人一码及一次一码三种模式，可通过短信分发安全码。一人一码模式下，当实际登录用户跟分发 SPA 安全码绑定的用户不一致时，零信任系统可以产生安全告警。一次一码模式下激活码被用户使用并正常登录零信任系统后转换为安全码加密存储，换码成功后激活码失效，控制台日志须体现用户首次登录后的换码过程。
	虚拟网络域	支持对用户 PC 终端的出站、入站网络规则划分虚拟网络域进行管控，零信任用户在特定的网络域下只能主动并被限定访问网络域对应的 IP、IP 范围、IP 段、域名；支持配置终端用户通过悬浮球的方式快速切换虚拟网络域；虚拟网络域能力应支持主流操作系统，包括但不限于 Windows、macOS、麒麟 kylin、统信 UOS 等；支持用户离线后网络隔离策略持续生效，规避用户离网逃逸情况；
联动特性	上网行为管理联动	支持与上网行为管理设备通过 OAuth2.0 协议对接，使用零信任作为上网行为管理的认证源登录上线。
	网络威胁及态势感知设备联动	支持为每个用户分配独立的虚拟 IP，并将虚拟 IP 分配日志通过第三方 syslog 的方式同步到网络威胁分析设备。支持将用户访问零信任系统的认证及策略类请求加密流量解密后镜像给外部系统，如态势感知等设备，以完善系统的用户行为审计溯源能力。
	终端检测响应联动	支持联动终端安全类产品如终端检测响应 EDR 的检测评分作为动态访问控制策略条件。
集群特性	本地集群及工作负载	支持和现有零信任系统打通集群统一管理，横向扩展性能的同时接入授权共享，避免重复投入

		支持本地集群部署，且最少 2 台设备即可组建集群，单集群的最大节点数量不得少于 4 台，集群内节点可不依赖外置设备提供工作负载功能；
	分布式集群	支持分布式集群部署，且最少 2 个节点即可组建分布式集群，分布式集群的最大节点数量不得少于 4 个；支持对分布式集群节点的线路进行健康检查。
	授权共享及授权漂移	支持本地集群与分布式集群下各节点的零信任授权数均可共享使用，集群的总接入授权数是各节点授权数的总和。集群节点故障后分布式集群及本地集群均需支持授权漂移机制，总授权数与故障前保持一致；
审计及运维能力	用户安全日志审计	支持将具有异常登录行为的用户日志自动打标签为用户安全日志，以便于管理员快速审计定位。用户安全日志包括但不限于：帐号安全、中间人攻击、SPA 安全、cookie 劫持等。
	WEB 业务审计	支持对 WEB 应用通过无客户端智能脚本技术实现业务访问审计，非录屏、非远程桌面、非堡垒机方式，并支持将审计数据传递至日志中心或分析中心，还原出页面内容、鼠标移动、用户操作等用户访问业务的操作过程视频；
	客户端快速诊断及日志收集	支持终端环境诊断排查，提供终端诊断工具，支持对当前终端的基本环境进行扫描和一键修复；支持客户端应用访问诊断，输入应用地址后自动检测应用连通性；支持客户端自助日志收集；
国家商用密码	商用密码加密算法	支持中国商用密码标准，支持加密算法 SM2、SM3、SM4。
	商用密码卡支持	支持使用商密密码卡进行加密；支持在控制台对密码卡进行管理（包括不限于：激活、取消激活、密钥备份/恢复、管理 KEY 口令）
零信任系统授权	客户端授权要求	深信服零信任系统客户端永久使用许可授权终端数 700 个；操作系统兼容性：零信任客户端兼容主流操作系统，包括但不限于：Windows7（32 位、64 位）、Windows10（32 位、64 位）、Windows11（32 位、64 位）、MacOS10、MacOS11、MacOS12、Ubuntu（16、18、20、22）x86、统信、麒麟等操作系统。硬件兼容性：零信任客户端兼容主流国产硬件 CPU 的国产操作系统终端包括但不限于麒麟 V10×龙芯、麒麟 V10×龙芯 LoongArch、麒麟 V10×飞腾、麒麟 V10×鲲鹏、麒麟 V10×兆芯、麒麟 V10×海光、麒麟 V10×海思麒麟；统信 V20×龙芯（3A3000、3A4000）、统信 V20×龙芯（3A5000）、统信 V20×飞腾、统信 V20×鲲鹏、统信 V20×海光、统信 V20×兆芯等。

3. **服务要求**

序号	设备类型	参数要求	数量	单位
1	部署及培训服务	包括设备部署安装、基础数据录入、系统监控接入和培训服务等	1	项

五、项目管理要求

1. **项目计划管理**

在总体计划指导与控制下，将实施中所有的工作内容进行分解，形成由主计划-〉阶段计划-〉周计划-〉滚动计划体系，对计划变更需要按照本方案的变更控制流程处理。

在平台实施开发前提交项目实施开发计划。该计划允许珠港公司在项目执行过程中对进度、管理和合同工作成效方面进行监督。项目计划包括开发内容、进度安排、组织构架、人员组成和风险管理等。

2. **项目方案管理**

组织项目管理专家团队编制审定实施主计划。该计划提交珠港公司方进行审核后才开展执行，在实施开发过程中对项目的进度、管理和合同工作成效方面进行监督。具体来讲分解为以下可执行的工作细节。

（1） 项目沟通策略；

（2） 每周的项目状态沟通会议；

（3） 每周工作计划沟通会议；

（4） 关键业务流程设计沟通会议；

（5） 项目里程碑阶段沟通：

- 本阶段工作总结与评审；
- 下阶段工作任务部署。

3. **项目进度管理**

（1） 项目进度控制管理应该遵循以下原则：

- 项目进度控制管理的依据是项目合同所约定的工期目标；
- 在确保项目质量和安全的原则下，控制项目进度。

（2） 项目进度控制管理应该至少包含以下内容：

在了解项目特点的前提下，根据工期目标，提交总体进度计划，以及定期提交阶段性工作计划；

制定详细的项目建设进度计划，按照合同的进度计划制定具体的实施计划，定期跟踪检查，对可能发生的工程延误提出相应对策；

定期或不定期地召开或参加项目例会、协调会议等，向甲方通报项目进展情况，提交进度报告，及时解决相关问题；

建立项目变更流程，记录项目变更。

4. **项目质量管理**

乙方应建立严格的质量保证体系，制定项目实施质量控制方案和实施措施，并督促落实各环节质量控制内容和目标，保证项目实施与验收各个阶段工作满足甲方对质量的要求。

乙方应根据整个系统开发、现场部署的工作计划，对阶段性工作成果进行审查和测试，并向甲方提交里程碑式工作成果。通过保证各阶段性成果的质量，最终保证整个项目实施的质量。

乙方应在系统开发完成后对系统进行测试（功能适应性测试、性能测试、安全测试等），并提供测试用例及样例数据、测试环境配置要求。

乙方应确保把相关的技术技能和知识技能有效地传递给甲方。

5. 项目风险管理

在项目实施过程中，乙方须对整个项目进行项目风险评估和管理。乙方须定期地对项目风险进行评估，并对风险应对计划进行审计和调整。

在项目实施过程中，出现的对项目影响重大的风险，乙方须提出风险应对措施，如实向最终用户汇报，应对风险并控制风险发生、控制风险的影响，保证项目符合项目总体要求和目标。

六、项目整体要求

1. 货物要求

供货时，软件许可名称须为项目使用人珠海市珠港机场管理有限公司，并能通过序列号、官方热线电话、email等方法进行查验。

2. 货物质量和合法来源保障

为了保障产品质量及售后服务，供应商提供的所有设备必须为原装、全新、未经开箱产品。成交供应商应在成交后 15 天内提供所投设备的合法来源证明（或原厂供货证明）原件和采购清单中所要求的相关证书原件，送至本单位签收（注明提交时间）。如提供的证明文件不全或存在虚假情况，我方将向有关部门举报虚假响应，成交方须承担因此造成的一切法律责任，包括但不限于税款、滞纳金、罚款等损失。

3. 项目部署调试要求

供应商应派经甲方确认的有经验和能力、熟悉本合同所述货物的规格、技术指标及安装工艺的技术人员，负责系统设备安装工作，在安装部署期间应充分了解安装进度要求，解决安装中出现的技术问题。前期安装实施阶段需安排至少一人驻点实施安装及培训服务。

供应商须完成现场所有终端安装部署，应根据现场实际情况，制定终端部署方案，供应商对项目的规划和实施步骤加以说明，应做出整个项目分阶段的详细进度计划，以及对进度完成的保证措施和补救方法，并列明本次项目分阶段完成的时间表。

项目部署期间，须保持珠海机场生产系统运行不可中断，供应商须对设备系统不间断运行提出安全的部署措施。若实际实施中必须停用或重新启动所需设备，供应商需得到现场管理人员审核确认方才可执行，若未经现场管理人员的审核确认而造成的一切损失，由供应商承担。

项目部署期间，珠海机场业务系统如遇因部署的原因导致的技术故障，供应商须联合厂商进行及时的功能性技术调整，以保证部署影响的系统/办公终端可安全、稳定运行。

供应商应提供完备的系统部署方案、功能测试方案及测试报告。

4. 项目团队要求

供应商需根据项目整体实施进度，明确项目实施的组织架构及人员配备方案，标识项目团队核心成员，并提供参与该项目人员的履历。

（1）为使项目按质、按量、按时及有序实施，在项目实施期间，供应商需要进行现场实施。

（2）供应商的项目团队应当具有与项目相适应的专业力量，如人员数量、专业分布、工作年限、技术职务、技术职称、工作资历、类似项目业绩等。

（3）供应商应提供项目团队组织方式及其人员构成，对参加本项目的团队成员在本项目中投入工作天数的测算及在本项目中所承担的具体角色和任务的说明。

（4）项目实施人员必须至少有 2 年本项目内容相关的建设实施案例经验。需详细列出参与本项目的技术人员的姓名、专业工龄、职务、职称、相关经验等。

供应商应保证项目实施团队的主要人员稳定，未经甲方同意不得私自更换项目经理、主要项目团队成员和项目实施及售后运维的专职人员。

珠海机场或供应商认为需要更换项目经理、主要项目团队成员和项目实施及售后运维的专职人员时，均应提前两周向对方申明原因，供应商应在同时提出新的符合合同要求的项目经理和项目团队成员人选，经珠海机场同意并办理交接手续后方可更换。在技术服务期间，专职技术人员必须遵守甲方的相关工作管理规定。

5. 技术培训要求

供应商须对甲方的技术人员进行技术培训。须提供符合本项目详细的技术培训，并出示培训方案，使机场方人员达到能独立进行管理、维护测试和故障处理等工作。项

目测试期内提供现场指导。供应商提供的负责培训的人员应具备同类项目五年以上的经验。技术培训费用应包含在总价中。

技术培训至少应包括下列内容：

- 原理、构成和功能的描述。
- 常见故障的处理或排除。
- 各系统部件的检查、调整和维护。
- 对使用者关于设备基本操作技能的培训。

6. 项目质保期

自验收合格之日起对本项目的项目质量保证期不少于 3 年（若国家和/或生产厂家对本项目所涉及产品的质量保证期的规定高于本项目要求的，应按国家和/或生产厂家的规定执行，若文件中承诺高于该期限，按照供应商承诺）。在保修期内提供免费上门升级维护服务。

7. 售后服务要求

（1）项目维保期：项目验收后提供三年免费包含但不限于原厂的（上门/远程故障处理、软件升级、技术电话咨询等）售后维保服务（提供原厂供货证明及原厂售后服务文件），包括不限于系统平台的版本更新等升级服务。

（2）项目维保期内现场支持，解决日常维护当中的问题，包括但不限于操作使用、技术讲解、问题排故、功能性需求调整、bug 修复、补丁安装等。

（3）项目维保期内，对影响生产的故障提供 7*24 小时服务，15 分钟内电话响应。

（4）故障处理的现场支持服务，到达现场时间：

故障级别	响应时间	技术人员 到场时间	解决时间
I 级：属于紧急问题；其具体现象为：系统崩溃导致业务停止、数据丢失等。（具体视现场故障情况协定）。	5 分钟	1 小时内	2 小时以内
II 级：属于严重问题；其具体现象为：出现部分部件失效、系统性能下降但能正常运行，不影响正常业务运作。	5 分钟	1 小时内	3 小时以内
III 级：属于较严重问题；其具体现象为：出现系统报错或警告，但系统能继续运行且性能不受影响。	5 分钟	2 小时内	6 小时以内

故障级别	响应时间	技术人员到场时间	解决时间
IV 级：属于普通问题；其具体现象为：系统技术功能、安装或配置咨询，或其他显然不影响业务的预约服务。	5 分钟	远程支持（电话、传真、邮件等）	即时

（5）项目维保期内，每天（包括周六周日）在维修响应时间内，我方可随时通过电话或 email 就有关技术问题向中选方的技术人员进行咨询；我方电话享有高度的优先级，优先处理我方电话求助，直至得到我方满意的结果；专业的技术工程师须保证能提供快速有效的支持。

8. 质保期后服务要求

从质保期结束之日起，乙方须为珠海机场提供运维服务的范围和内容如下：

（1）乙方须对平台继续提供相应技术支持，包括提供技术支持联系人与联系方法，方便系统维护人员进行技术咨询。

（2）乙方须因软件缺陷问题而导致的系统故障，或由产品设计生产缺陷造成的故障，提供终身免费维修。

（3）提供 7*24 小时电话故障处理服务，重大故障响应相应时间不超过 20 分钟，一般故障处理时间不超过 2 小时，如在此时间内解决不了，将派维修技术人员尽快到达珠海机场工作现场给以解决。

（4）故障处理时必须遵守珠海机场的有关故障处理流程和上报机制，故障处理完毕后应形成分析报告及记录，并且定期分析故障记录发现潜在的风险。

（5）须保证珠海机场使用的系统版本是最新、稳定、可靠的运行版本。乙方承诺本项目质保期后的运维服务内容、标准与质保期内的一致。

9. 原厂技术服务要求

本项需提供原厂技术支持：

序号	子项	内容描述
1	技术支持时间	24 小时/天，7 天/周，365 天/年
2	技术支持获取方式	客户可以通过电话、Web 访问厂家技术支持资源，反馈问题并获取支持
3	问题处理	售后电话响应并解决客户咨询问题或软件问题
4	问题升级管理	对于复杂问题，提供问题升级通道，推动问题快速解决
5	在线信息访问	客户可通过厂家网站获取最新产品、方案信息。同时通过服务代码，可以访问厂家知识案例库，查找产品相关案例；参与技

序号	子项	内容描述
		术论坛讨论，与其他用户进行技术交流
6	版本更新	厂家为客户提供了服务代码，客户可以根据服务代码从厂家官方网站获取最新的网络产品软件版本及相关文档，实现版本更新
7	实施部署	提供项目初始的原厂实施技术支持，与客户一起制定改造方案，结合可实施的作业窗口期完成项目的安装部署。
8	现场技术支持	重大问题(具体现象为：系统崩溃导致业务停止、数据丢失等。具体视现场故障情况协定）7*24 小时响应，2 小时内到达现场

10. 包装、保险及发运、保管要求

- 设备材料的包装均应有良好的防湿、防锈、防潮、防雨、防腐及防碰撞的措施。凡由于包装不良造成的损失和由此产生的费用均由供应商承担。
- 供应商须负责将设备材料运到现场过程中的全部运输，包括装卸车、货物现场的搬运。
- 各种设备，必须提供装箱清单，按装箱清单验收货物。
- 货物在现场的保管由供应商负责，直至项目安装、验收完毕。
- 货物在系统安装调试验收合格前的保险由供应商负责，供应商须负责其派出的现场服务人员人身意外保险。
- 设备至甲方指定的使用现场的包装、保险及发运等环节和费用均由供应商负责。
- 其他要求：
  - 供应商负责本项目所有货物的安装调试以及所有必须的线材与备件等。
  - 供应商应提交详细项目安装进度表。
  - 供应商应设安装负责人，负责安装协调管理工作。
  - 安装所需工具设施物料由中选方自备、自费运到现场，完工后自费搬走。
  - 调试：按国家相关施工验收规范进行，分阶段进行调试。
  - 供应商应派有经验的技术人员到施工现场进行货物的安装和调测，负责处理货物的质量和数量短缺等问题，并应对产品质量全面负责。

11. 货物检验要求

- 货物的拆箱、安装、调试等项工作由供应商负责，但必须在甲方指定人员的参与下进行。具体安装和测试方法，在实际实施前必须先经甲方同意方可进行。调试的原始记录须经各方签字后作为验收的文件之一。
- 所有货物在开箱时必须完好，无破损，配置与装箱单相符，数量、质量及性能不低于本次项目文件中提出的要求。供应商在货物安装过程中造成场地损坏的修复所产生的费用由供应商负责。
- 供应商应给出项目详细的验收方案，包括验收项目、验收标准，验收实施方法等。
- 验收由甲方、供应商及相关人员依国家有关标准、合同及有关附件要求进行。

12. 项目实施周期

项目实施期：合同签订后项目建设周期为日历日 150 天内（其中涵盖试运行阶段 30 天），具体开始实施的日期以合同签订的时间为准。

13. 试运行及验收要求

项目完工交付后一个月内，甲方根据系统试运行情况，乙方需提供详细的项目验收方案，并在验收前提交至甲方进行审核。审核完成后才可进行付款验收。

甲方根据供应商已提供本项目规定的全部货物、服务和项目相关资料等包括但不限于：

- 需求清单内所有软件产品相关许可证书（含相应模块）。
- 需求书内要求的相关证明文件。
- 初次部署及测试报告。
- 灾难应急演练验证。
- 相关产品应用培训。
- 安装实施过程中涉及到的相关资料文件等。

七、安全性要求

根据系统安全需求，须确保设计、实施和交付符合等保实施意见以及等保管理办法对本项目的安全要求，并确保本项目评级满足《信息系统安全等级保护基本要求》“等保二级”及以上标准。

信息安全主要目标之一是保护业务系统和应用程序的基础数据安全。依据数据安全生命周期，系统从数据创建、存储、使用、共享、归档至销毁，使用了数据分级、数

据加密等措施，保障了数据的保密性、完整性、可用性、真实性、授权、认证和不可抵赖性。

数据加密：系统通过数据分类分级、数据加密和密钥管理为敏感数据提供可持续的信息保护，实现数据的灵活性、可靠性和可管理性；借助密钥管理中心和加解密产品实现数据安全保护和控制，将安全技术嵌入至整个数据安全生命周期中，以保障数据安全属性。

为确保系统管理操作和数据操作的安全性，满足更为安全的系统管理和审计需求，需提供基于角色的权限体系，采用“多员体系”机制，将系统管理与备份业务操作分离，分化管理员的操作权限彼此隔离、相互制约，完善监管机制，实现各个角色用户的行为可监管。

系统的所有数据库均加密处理，保护数据安全，通过 https 双向认证的方式，数据传输过程中进行加密传输，确保信息在传输过程中的信息安全。

八、付款方式

1. 合同价款

乙方按照甲方设计要求完成工程的全部安装调试工作，提供验收资料（包括但不限于：项目清单、系统调试报告），双方签署验收文件，且乙方开具项目总价相等的增值税专用发票及其他必要文件后 60 个工作日，甲方向乙方支付 95%的合同款；

质保金为合同款的 5%，质保 3 年，在质保期满后 60 个工作日办理支付手续，无息支付给乙方。

2. 履约保证金

乙方于合同签订的开工日之前，向甲方提交履约保证金，金额为含税总价的 5%。若乙方未在规定时间内提交足额履约保证金，则按约定的项目款支付时间再顺延 60 个工作日，同时需以乙方补交足额履约保证金为前提。

履约保证金采用银行转账方式提交。

收款人：珠海市珠港机场管理有限公司

开户行：交行珠海分行

账　号：444000091018170039333

如无异议，履约保证金在支付约定的项目结算时一并无息退还。

因乙方原因导致合同无法按约定履行的，甲方有权将履约保证金作为违约金扣除。

九、项目交付文件要求

1. 交付文件清单

根据本项目的采购需求，结合我司的技术支持规范。针对本次项目，我司项目交付验收时将提供平台维护方案，包括各服务器（如数据库服务器、接口服务器等所有本系统涉及到的服务器）的日常维护方案、应急处理方案、故障恢复方案等。

提供平台软件的使用手册、维护手册、常见故障处理解决方案、应急处理手册及包括但不限于以下文档：

《整体设计方案》

《详细设计说明书》

与本项目有关的业务数据标准（规范）：

《需求变更记录手册》

《项目计划》

《工作周报》

系统安装程序和安装说明文档：

《系统测试报告》

《系统部署方案》

《系统安装手册》

《系统维护手册》

项目各阶段验收文档

2. 交付文档要求

为使平台能高效、可靠运行，乙方必须在平台实施及后续服务阶段向甲方进行技术转移。方案中应包含以下内容：

- 部署到测试环境和生产环境的程序的可执行版本必须有严格的版本控制方案。
- 提供的各种文档应与其提供的平台功能相一致，技术文档应该全面、详细、准确。
- 提供的文档应能够满足所提供的平台安装、使用、维护的需要。
- 在任何时候提供平台升级和客户化功能增加时，都应提供相应的技术文档。
- 提供的所有技术资料应使用中文。

提供的文档和资料的文件格式为 Word 文档或 PDF 文档或其他可视化文件。

十、项目清单

名称	模块	描述	单位	数量
硬件功能	零信任安全代理网关	性能参数：加密流量速率不低于 300Mbps，最大并发用户数不少于 3000 个，最大 https 并发连接数 30000 个， https 新建连接数不少于 400 个/秒。 硬件参数：CPU 不低于 4 核心，内存大小不少于 16G，硬盘容量不少于 128G SSD，电源：双电源，接口不少于 6 千兆电口+2 千兆光口 SFP。	台	1
软件功能	用户认证	认证方式支持、增强认证、多因素认证	套	1
	权限及访问控制	支持动态访问控制、动态上线准入控制	套	1
	资源发布能力	隧道资源发布、WEB 资源发布、WEB 页面安全、DNS 解析	套	1
	终端接入能力	客户端国产终端兼容性、CDN 支持、客户端自动选路、弱网访问加速、短隧道资源时延优化、虚拟 IP、授信终端	套	1
	零信任安全特性	SPA 单包授权、虚拟网络域	套	1
	联动特性	上网行为管理联动、网络威胁及态势感知设备联动、终端检测响应联动	套	1
	集群特性	本地集群及工作负载、分布式集群、授权共享及授权漂移	套	1
	审计及运维能力	用户安全日志审计、WEB 业务审计、客户端快速诊断及日志收集	套	1
	国家商用密码	商用密码加密算法、商用密码卡支持	套	1
	零信任系统授权	零信任系统客户端永久使用许可授权终端数 零信任客户端兼容主流操作系统，包括但不限于：Windows7（32 位、64 位）、Windows10（32 位、64 位）、Windows11（32 位、64 位）、MacOS10、MacOS11、MacOS12、Ubuntu（16、18、20、22）x86、统信、麒麟等操作系统的终端。 零信任客户端兼容主流国产硬件 CPU 的国产操作系统终端包括但不限于麒麟 V10×龙芯、麒麟 V10×龙芯 LoongArch、麒麟 V10×飞腾、麒麟 V10×鲲鹏、麒麟 V10×兆芯、麒麟 V10×海光、麒麟 V10×海思麒麟；统信 V20×龙芯（3A3000、3A4000）、统信 V20×龙芯（3A5000）、统信 V20×飞腾、统信 V20×鲲鹏、统信 V20×海光、统信 V20×兆芯等。	个	700

部署及培训服务	部署及培训	包括设备部署安装、基础数据录入、系统监控接入和培训服务等	项	1

十一、其它要求

项目清单及报价要求仅指本次项目的主要采购范围，是本次项目建设的必要组成部分，并非详细完整配置。乙方须根据自己的方案，在报价清单中列明本项目建设及服务范围内所有设备、附件、软件、工具、服务、互联网专线等的名称、品牌、型号、规格、数量、价格等详细内容，所需费用包含在项目报价中。项目清单应完整、准确，满足系统的业务需求、总体要求、技术需求及服务要求。如有缺项则由乙方无偿补充直到满足以上相关要求。项目报价应包含项目建设所需的需求调研、功能开发、部署实施、设备运输、保险、材料、办证、培训、利润、税金及与乙方现有系统集成等全部一切费用。另乙方不得因甲方未列明的具体要求而增加费用，不得事后再议价。

十二、供应商资质

1.供应商承诺**本项目所提供产品的客户端支持采用 SDK 集成方式，并确保满足包括数据加密、访问控制、安全更新、数据防泄漏等安全性要求。**提供《承诺函》加盖公章（见附件）

2.供应商具备中国网络安全审查技术与认证中心颁发的CCRC信息安全服务资质认证证书，以上资质出具证书复印件证明加盖单位公章。

十三、本项目设报价上限：490,000.00 元。

十四、采购方式：公开询价。

十五、附件

附件 1 《零信任安全建设项目报价清单》

附件 2 承诺函

附件一

《零信任安全建设项目报价清单》

序号	名称	模块	描述	单位	数量	所提供品牌型号/参数	备注
1	硬件功能	零信任安全代理网关	性能参数：加密流量速率不低于 300Mbps，最大并发用户数不少于 3000 个，最大 https 并发连接数 30000 个， https 新建连接数不少于 400 个/秒。 硬件参数：CPU 不低于 4 核心，内存大小不少于 16G，硬盘容量不少于 128G SSD，电源：双电源，接口不少于 6 千兆电口+2 千兆光口 SFP。	台	1	深信服	
2	软件功能	用户认证	认证方式支持、增强认证、多因素认证	套	1	深信服	
		权限及访问控制	支持动态访问控制、动态上线准入控制	套	1	深信服	
		资源发布能力	隧道资源发布、WEB 资源发布、WEB 页面安全、DNS 解析	套	1	深信服	
		终端接入能力	客户端国产终端兼容性、CDN 支持、客户端自动选路、弱网访问加速、短隧道资源时延优化、虚拟 IP、授信终端	套	1	深信服	
		零信任安全特性	SPA 单包授权、虚拟网络域	套	1	深信服	
		联动特性	上网行为管理联动、网络威胁及态势感知设备联动、终端检测响应联动	套	1	深信服	
		集群特性	本地集群及工作负载、分布式集群、授权共享及授权漂移	套	1	深信服	
		审计及运维能力	用户安全日志审计、WEB 业务审计、客户端快速诊断及日志收集	套	1	深信服	
		国家商用密码	商用密码加密算法、商用密码卡支持	套	1	深信服	
		客户端授权要求	零信任系统客户端永久使用许可授权终端数	个	700	深信服	
3	部署及培训服务	部署及培训	包括设备部署安装、基础数据录入、系统监控接入和培训服务等	项	1	/	
合计：							拦标价￥： ￥:490,000.00， 超出拦标价的做否决处理。

说明：清单数量为估量，结算以实际数量为准。