

TC-AICC可信计算 常见问题



腾讯云

【 版权声明 】

©2013–2026 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或 95716。

文档目录

常见问题

产品与概念

数据与安全

接入与使用

常见问题

产品与概念

最近更新时间：2026-10-28 15:46:00

什么是 TC-AICC 可信计算（AICC）？

TC-AICC 可信计算（Artificial Intelligence Confidential Computing，AICC）是腾讯云提供的大模型机密推理服务。它基于可信执行环境（TEE），让您的业务数据和模型在计算过程中也保持加密状态，权限范围外都无法读取，实现“数据可用不可见”。

已完成传输加密和存储加密，为什么还需要 AICC？

数据加密通常覆盖两个状态：存储态，即数据写入磁盘时加密；传输态，即数据在网络传输过程中加密。数据进入内存与显存参与计算时，需要还原为明文，这一环节缺少对应的保护手段，通常称为使用态。

大模型推理将提示词、业务数据、检索命中的文档、多轮会话上下文以及模型权重等内容放在使用态参与计算。

AICC 覆盖的正是这一环节，在经验证的可信处理边界内解密和使用。

AICC 与自建私有化 GPU 集群有什么区别？

私有化部署需要自行建设机房或采购整套图形处理器（Graphics Processing Unit，GPU）集群，承担硬件折旧，自行完成运维与安全加固，并跟进模型迭代节奏。

AICC 在公有云的弹性、成本与模型迭代能力之上提供机密推理能力，适用于既需要使用新上线的模型、又需要对计算过程的数据加以保护的业务。

AICC 支持哪些大模型？

AICC 已覆盖主流开源与商业模型的多个版本，并支持上传自有模型部署。

由于模型迭代较快，完整的支持清单请以实际开通展示为准。AICC 作为可信推理底座能力，与模型本身解耦，新模型的适配随平台模型的上线节奏同步推进。如您有特定模型的适配需求，可通过商务渠道提出。

AICC 支持多卡异构算力吗？

支持。AICC 可覆盖国产算力与主流 GPU，业务侧无需关注底层卡型差异。具体可用的卡型与规格，以实际开通展示为准。

AICC 的算力集群是专有集群吗？

是。AICC 所使用的算力集群为专有集群，与公共云集群物理隔离，用户之间为租户级隔离。承载您推理任务的物理机不与普通公有云业务负载共用。

数据与安全

最近更新时间：2026-10-28 15:46:00

使用 AICC 后，腾讯云能否读取您的数据？

在使用 AICC 可信推理时，用户数据明文的可见范围限制在用户客户端（含本地安全代理）和经过验证的可信执行环境内。处于该可信边界之外的腾讯云平台组件、运维人员以及其他租户，无法直接访问这些明文内容。该保护由以下三层机制共同实现：

- **端到端加密**：客户端 SDK 或您部署的安全代理在敏感内容进入云端链路前完成加密。请求到达可信处理边界后才被解密，受保护的响应内容在离开该边界前重新加密，使边界外的网关、转发与调度组件无法直接读取业务明文。
- **可信执行与隔离**：数据在授权的可信处理环境内解密并参与计算，通过适用硬件的内存透明加密、隔离与访问控制机制，限制外部主体对明文的访问。
- **身份验证与密钥授权**：客户端验证服务身份及硬件证明后建立安全会话。数据密钥按会话、请求和通信方向分别派生，获取密钥时校验会话有效性、请求凭证和时间窗口，限制解密能力的使用范围。

AICC 的安全能力可以由您自行验证吗？

可以。AICC 通过远程证明（Remote Attestation），支持您核验服务身份、硬件证明及报告覆盖的运行环境状态。您可以使用客户端 SDK 完成证明与安全会话校验，也可以在获取原始证明材料和所需证书链后，在本地独立复验。具体包括：

- **验证证明来源与完整性**：以通过可信渠道预置的硬件厂商根证书为信任起点，校验证书链和硬件证明报告的签名，确认其来源及内容完整性。准备好完整验证材料后，相关密码学校验可离线完成。
- **核查环境是否符合预期**：将报告覆盖的硬件安全状态、软件度量值等信息，与您认可的基线和安全策略进行比对。具体可验证的内容取决于硬件类型、度量范围和部署方式。
- **确认与安全会话的关联**：客户端 SDK 验证硬件证明与服务身份的绑定关系，并校验本次会话的协商信息。相关校验通过后，才继续完成会话密钥派生或加密导入，用于后续业务请求的加密保护。

腾讯云仅按约提供服务，不会对数据进行任何未获授权的使用。远程证明将这些约定转化为可在生产环境中逐项核验的密码学证据，验证所依赖的信任起点是固化在芯片内、不可篡改的硬件信任根，校验过程由您独立完成。

AICC 的远程证明具体验证了哪些内容？

远程证明的度量范围覆盖 13 个以上维度，自底层硬件至业务运行时形成完整的信任链，主要包括：

- **运行环境信息**：硬件信任根凭证、固件与内核的完整性。
- **安全镜像信息**：推理集群镜像的完整性度量值。
- **进程信息**：运行中的进程清单。
- **网络端口信息**：运维接口、调试端口与日志外发通道的关闭状态。
- **模型信息**：所加载模型的完整性。

AICC 在运行过程中持续校验上述度量值，并非仅在启动时检查一次。

使用 AICC 推理，数据会被留存吗？

AICC 不留存推理数据。请求与响应在传输链路中以密文形式存在，仅在经远程证明的可信执行环境（TEE）内解密，并短时参与计算；处理完成后，明文随内存释放，不写入持久化存储。会话密钥按会话和方向分别派生，并设有有效期，过期后即失效。

- **多轮对话：**多轮上下文随每次请求加密提交，服务端为加速推理生成的上下文缓存（KV Cache）同样位于可信环境的保护范围内，按策略过期淘汰，不跨会话、不跨租户复用。
- **工具调用与外部服务：**工具调用、外部检索等场景需要将数据发往 AICC 可信边界之外的服务，这些数据离开可信边界后的处理与留存不在 AICC 的保护范围内，由相应工具或服务提供方另行承诺。建议您仅使用可信的工具提供方，并事先评估其数据处理情况。

AICC 保护的只是输入数据，还是也包括模型权重？

两者都包括。对于部分业务而言，自研模型的权重本身就是核心资产。

在 AICC 中，用户上传的模型权重，被保护在经安全验证的可信执行环境内，腾讯云无法获取用户模型权重。

使用国产 GPU 算力时，AICC 如何实现数据保护？

部分国产 GPU 尚未提供与主流 GPU 同等的 GPU 侧 TEE 能力。针对这一情况，AICC 以中央处理器（Central Processing Unit, CPU）侧的可信根为基础，通过以下方式叠加实现数据保护。

- **环境隔离：**部署于独立的私有网络（Virtual Private Cloud, VPC），推理环境与其他业务在网络层面相互隔离。
- **镜像加固：**推理集群镜像经过安全处理，屏蔽日志打印与运维访问接口，并监控登录状态。
- **通道加密：**通过可信推理节点与客户端 SDK 或安全代理构建加密通道，数据自客户端发出即为密文。
- **可验证：**通过远程证明向您说明容器内的运维接口与日志接口已关闭。

亦即，国产算力场景下的保护不依赖单一芯片特性，而是由隔离、加固、加密、证明多层叠加实现，同样支持您独立验证。

AICC 的 SDK 与推理节点 Agent 是否会过度采集数据？

不会过度采集，腾讯云支持对 AICC 软件开发工具包（Software Development Kit, SDK）与推理节点 Agent 的源代码开展定向审阅。您可以在腾讯云提供的受控设备上查看组件的源代码，核对其中的数据采集范围。具体审阅安排请通过商务或 [提交工单](#) 申请。

AICC 通过了哪些第三方认证？

AICC 已通过中国信息通信研究院《企业级大模型推理安全成熟度模型》评估，评估结果为五级（引领级）。该评估覆盖七个维度，分别为基础设施安全、数据安全、模型安全、身份认证与访问控制、网络安全、运维安全、弹性与可靠性安全。其中与 AICC 相关的条款包括：可信执行环境部署、硬件级安全隔离、基于硬件信任根的远程证明、与密钥管理系统的联动、推理缓存数据的保护与生命周期管理、数据销毁的不可恢复性验证。

需要说明的是，AICC 提供的是技术能力与验证材料，不替代您依据所属行业要求自行完成的合规评估与认证工作。

使用 AICC 后，是否还需要自行对数据加密与鉴权？

客户端与可信推理节点之间的传输加密与身份认证由 AICC 提供，您不需要为此另行建设。

但该保护仅覆盖 AICC 链路本身。客户端侧的业务逻辑、权限管理，以及业务系统自身的访问控制与鉴权，仍需由您自行按相关安全要求实施。

AICC 是否支持自带密钥（BYOK）与 KMS 托管？

支持。您可以使用自有的密钥材料，密钥由您自行管理。AICC 同时支持对接密钥管理系统（Key Management System，KMS）托管推理链路使用的密钥，密钥的生成、轮转与访问记录由 KMS 统一管理。

接入与使用

最近更新时间：2026-10-28 15:46:00

接入 AICC 需要改造现有业务系统吗？

多数情况下不需要。AICC 提供两种接入方式，您可以根据自身架构选择。

- **SDK 方式：**适用于业务侧已有 AI 网关、转发代理或可改造的 Agent 的场景。将 AICC SDK 集成到网关、代理或 Agent 中，实现端到端加密。
- **安全代理方式：**适用于业务使用闭源第三方系统、无法集成 SDK 的场景。在您的可信域内部署一台机器运行安全代理，配置网络转发策略即可，业务端无需改造。

安全代理的运行环境要求为可运行容器引擎（Docker）的服务器，最低规格为 2核4GB，推荐规格为 4核8GB。

接入 AICC 对前端应用或客户端有什么要求？

没有特殊要求。AICC 提供的是机密推理服务，调用方式与普通推理服务一致。差异仅在于需要建立加密通道，通过集成 AICC SDK 或部署安全代理完成，两种方式任选其一。

开启 AICC 机密推理后，性能会下降多少？

AICC 对首字延迟（Time To First Token, TTFT）与每字延迟（Time Per Output Token, TPOT）的影响一般不超过 5%（基于内测数据及部分客户实测数据验证）。实际数值会随输入输出长度、并发量与业务类型浮动。

建议在概念验证（Proof of Concept, POC）阶段以您的真实业务流量实测，腾讯云可提供开启前后的对比数据。

开启 AICC 后，会影响大模型的输出效果吗？

不会。AICC 保护的是运行环境，不改变模型本身与推理逻辑，也不对数据做脱敏或截断处理。同一个模型在 AICC 环境与普通环境下的输出结果一致。