Global Computing Consortium
全 球 计 算 联 盟

机密计算标准体系研究报告

全球计算联盟

机密计算专业委员会

编写单位

中国电子技术标准化研究院
华为技术有限公司
中国电信集团有限公司
天翼云科技有限公司
北京国家金融科技认证中心
安谋科技（中国）有限公司
超聚变数字技术有限公司
南湖实验室
飞腾信息技术有限公司
麒麟软件有限公司
中科院软件所
工商银行

编写组成员

王惠莅、羡喻杰、金意儿、庞婷、于攀、严敏瑞、惠静、聂乐乐、李想、赵宇航、王骏超、谢秋华、张磊、谭琳、张大朋、秦宇、张敏、刘静、冉佳欣、黄司辉、李博文、黄江

版权声明

序

数据是数字时代的基础性战略资源与关键性生产要素，数据安全问题，尤其是使用中的数据安全问题需求非常迫切，数据使用安全问题的本质是安全计算问题，这就要求 CPU、GPU、DPU 等能够支撑安全计算功能。机密计算是目前为止最为现实的一种数据使用安全技术，相比隐私计算范畴内的同态加密、安全多方计算、联邦学习等技术，机密计算兼具高安全性和高性能，但产业化进程中面临众多挑战，例如技术路线多样、互操作与业务迁移难度大、开发成本偏高等、亟需通过标准化破解瓶颈，推动产业生态走向成熟。

机密计算标准体系研究报告从机密计算产业发展的视角，阐述了机密计算技术的发展现状和演进路径；介绍了机密计算的五种典型应用模式，为行业用户落地应用提供了重要参考。

机密计算标准体系研究报告系统性梳理了机密计算标准体系框架，对标准进行分类，详细解析了机密计算领域内已发布的标准，待制定的标准及优先制定标准清单，为产学研界掌握机密计算标准发展动态提供了优质参考。

GCC 机密计算专业委员会将团结机密计算产业链上下游伙伴，以产学研用融合模式制定产业界急需标准，通过标准符合性测评、标准应用案例推广等活动，推动标准落地，进而解决生态碎片化问题，降低机密计算应用成本。

全球计算联盟

机密计算专业委员会

2025 年 11 月

目　录

第一章 机密计算发展现状 3

第二章 机密计算标准体系 4

第三章 总结与展望 12

参　考　文　献 17

机密计算标准体系研究报告

第一章 机密计算发展现状

在数字经济时代背景下，数据作为新型生产要素的战略价值日益凸显，机密计算作为保护使用中数据安全的关键技术迎来突破性发展。该技术通过构建硬件级可信执行环境（TEE），结合密码学与安全协议，实现了数据使用过程中的机密性和完整性保护，有效实现了云计算、边缘计算及人工智能等场景中"数据可用不可见"的核心诉求，现已成为全球数字安全领域的重要技术方向。在 Gartner 发布的《2026 年十大技术趋势》中，机密计算赫然在列，Gartner 预测，到 2029 年，75%以上在非可信基础设施中处理的业务将通过机密计算保障使用安全。

机密计算技术演进呈现显著代际特征：

- 第一代技术（2010-2018）以 ARM TrustZone 和 Intel SGX 为代表，通过 CPU 指令集扩展实现系统级/进程级隔离，需深度定制开发支持；
- 第二代技术（2019-2022）包括 AMD SEV、Intel TDX 和 ARM CCA 等，基于硬件虚拟化构建机密容器/虚拟机，支持应用无缝迁移；
- 第三代技术（2023-今）聚焦异构协同与集群化部署，通过可信计算基扩展实现跨架构设备互联，重点支撑大模型训练推理等复杂场景。

当前机密计算使用方业务场景复杂，主要有包含以下应用模式：

- 构建机密计算一体化应用：机密计算应用方合作企业多，数据量大，业务场景复杂，实时性处理要求高，需要各合作方统一配合，基于机密计算技术构建一体化应用，达成软硬件解耦、高可用、灵活部署等能力；
- 构建统一的机密计算管理能力：规范通信接口，进行统一部署和管理，支持对机密计算业务监控和高可用保障；
- 支持小模型场景下的数据安全：小模型场景下，通过 CPU 进行微调与推理，需要使用私有数据集，能够对数据安全保护；
- 支持大模型场景下异构安全：在大模型场景下，需要结合 GPU、NPU 等设备，需要保障机密计算场景下异构设备互联互通安全；

- 支持云场景应用安全：当前云客户通过专属云的硬件资源隔离来确保客户数据安全，希望可以通过机密计算能力，提供客户更加灵活和低成本的部署方案。

第二章 机密计算标准体系

2.1 整体框架

通过梳理业界机密计算的发展现状与趋势，整合国内外各组织联盟对机密计算的标准化成果，深度分析机密计算标准体系。机密计算标准体系主要有基础共性、关键技术、产品应用和测试评价四个部分组成，完整的标准体系框架见图 1。

1) 基础共性类标准：定义清楚机密计算是什么，统一术语，明确机密计算核心组件、核心功能、如何与上层应用对接，形成统一行业认识；
2) 关键技术类标准：为广泛推广机密计算应用落地，规范主流应用模式中涉及的基础关键技术架构、核心流程和服务接口等；
3) 产品与应用类标准：指导行业怎么用，规范基于机密计算研发的产品中应具备的安全功能，并为行业应用提供技术指南，指导客户选型；
4) 测试评价类标准：为机密计算相关产品、平台等提供安全性、性能、兼容性等测试评价方法，牵引产业进步，为用户方提供选型参考。

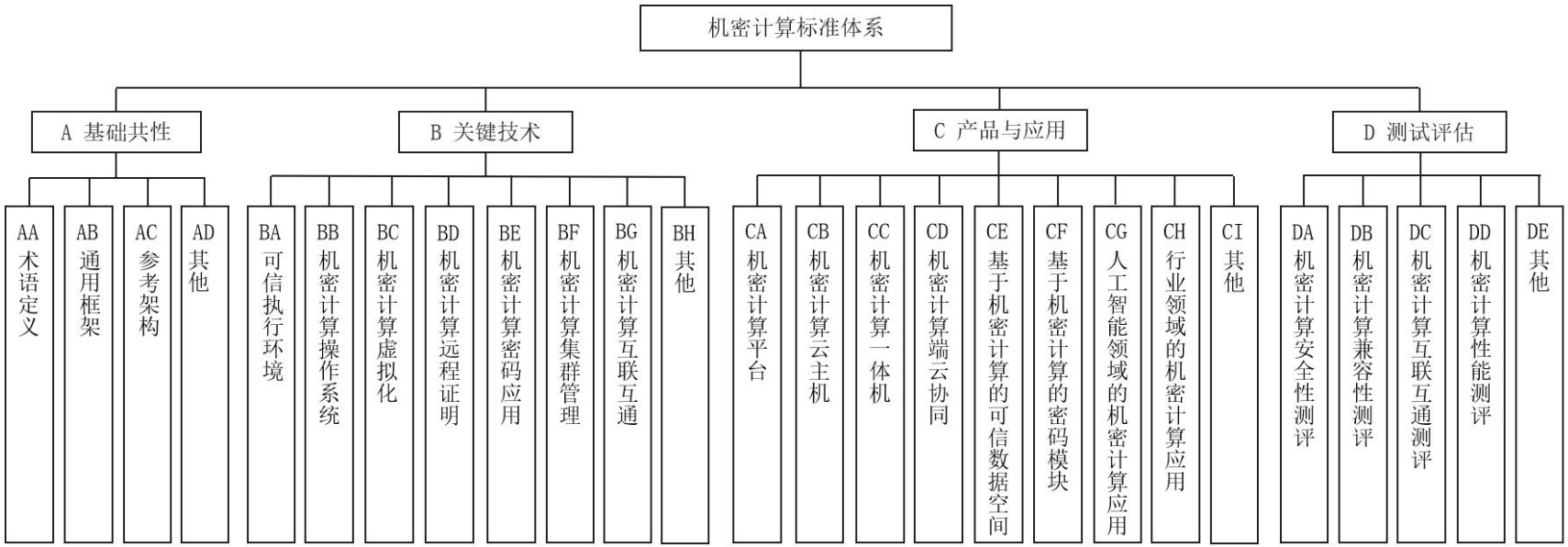
机密计算标准体系
A 基础共性
B 关键技术
C 产品与应用
D 测试评估
AA 术语定义
AB 通用框架
AC 参考架构
AD 其他
BA 可信执行环境
BB 机密计算操作系统
BC 机密计算虚拟化
BD 机密计算远程证明
BE 机密计算密码应用
BF 机密计算集群管理
BG 机密计算互联互通
BH 其他
CA 机密计算平台
CB 机密计算云主机
CC 机密计算一体机
CD 机密计算端云协同
CE 基于机密计算的可信数据空间
CF 基于机密计算的密码模块
CG 人工智能领域的机密计算应用
CH 行业领域的机密计算应用
CI 其他
DA 机密计算安全性测评
DB 机密计算兼容性测评
DC 机密计算互联互通测评
DD 机密计算性能测评
DE 其他

图 1 机密计算标准体系

2.2 分类介绍

2.2.1 基础共性类

基础共性类标准是推动机密计算标准体系建设、落实《机密计算标准体系框架》各项措施的重要保障，是机密计算的基础性、总体性标准，包括机密计算的定义、核心组件、核心功能等，与上层应用对接，形成统一行业认识。

基础共性类标准设计见表 1，给出了各个标准的名称、状态和标准主旨。

表 1 基础共性类标准简介

类别	标准名称	状态	标准主旨
AA 术语定义	机密计算 术语	待制定	• 定义核心概念：可信执行环境、硬件隔离、内存加密、机密计算平台、远程证明、信任根（RoT）、密封存储等； • 区分相关技术：与可信计算、隐私计算、同态加密等的区分； • 定义参与角色：机密计算数据提供方、机密计算平台提供方、机密计算服务提供方、证明者(Attester)/验证者(Verifier)/依赖方(Relying Party)等角色标准化命名。
AB 通用框架	GB/T 45230-2025 数据安全技术 机密计算通用框架	已发布	确立了机密计算通用框架,描述了框架的核心组件和基础功能,并提供了机密计算服务及实现机制。
	ISO/IEC JTC1/SC27	征求意	给出机密计算的概念、基本属性、核心机制及调度

	25093《cybersecurity-confidential computing-part1:overview and concept》（CD阶段）	见稿	模型等。
AC 参考架构	T/CESA 1229-2022《服务器机密计算参考架构及通用要求》	已发布	标准旨在从最终产品和开发过程的角度出发，建立系统化的机密计算定义和统一框架，清晰地描述机密计算服务中各种参与角色的安全责任，提出机密计算角色、角色安全职责、安全功能组件以及他们之间的关系，指导机密计算参与者进行机密计算服务规划时的安全评估与设计。

2.2.2 关键技术类

技术支撑类标准紧扣机密计算相关技术发展及应用情况，明确各项关键技术的安全保障要求，为机密计算健康发展保障护航。

关键技术类标准设计见表 2，给出了各个标准的名称、状态和标准主旨。

表 2 关键技术类标准简介

类别	标准名称	状态	标准主旨
BA 可信执行环境	GB/T 41388-2022《信息安全技术 可信执行环境 基本安全规范》	已发布	给出了 TEE 系统整体技术架构、硬件要求、安全启动过程基本要求、可信虚拟化、可信操作系统、可信应用与服务管理基本要求、可信服务基本功能及要求、跨平台应用中间件、可信应用架构及

			安全要求、测试评价方法的相关技术要求，标准适用于指导 TEE 系统的设计、生产及测试。
	GB/T 42572-2023《信息安全技术 可信执行环境服务规范》	已发布	提出了 TEE 服务的技术框架及主要功能构成，规定了相关安全技术要求及测试评价方法，适用于 TEE 服务的设计、开发、测试等。设备制造商、系统软件提供商、检测机构和科研机构等 TEE 服务参与方可参照执行。
	YD/T 4234-2023 《基于可信执行环境的安全计算系统技术框架》	已发布	定义了基于可信执行环境的安全计算系统的技术框架，对基于可信执行环境的安全计算系统的概述、技术架构、技术特性、安全要求等进行规范。适用于基于可信执行环境的安全计算系统的设计、开发、测试、运维等。
	YD/T 4947-2024《隐私计算可信执行环境产品安全要求》	已发布	规定了基于 TEE 产品的安全要求，适用于基于可信执行环境的隐私计算产品的研发、测试、评估和验收等。
	GP TEE System Architecture v1.3 | GPD_SPE_009	已发布	阐述了符合 Global Platform Protection Profiles 和功能规范定义的 TEE 安全认证和功能合规性。本文档总结了这两个领域的各个方面，为读者提供了 Global Platform TEE 的安全性和潜在功能的概述。

	GP 《TEE Management Framework: Open Trust Protocol (OTrP) Profile Version 1.1》（OTrP，Open Trust Protocol Profile）	已发布	OTrP 仅针对于 Global Platform 定义下的 TEE，对于非 GP 的 TEE，可参考 TEEP 协议。采用 Global Platform TEE 架构的机密计算技术可参考此标准对可信应用进行管理与配置。
BB 机密计算操作系统	机密计算操作系统安全技术要求	待制定	规范为支持机密计算，操作系统应具备的安全功能，利用机密计算硬件资源，实现机密计算环境，完成对机密计算环境内的资源调度。
BC 机密计算虚拟化	机密计算虚拟化安全技术要求	待制定	给出机密计算虚拟化的典型技术架构、主流形态等，规范机密计算虚拟化安全功能要求，包括虚拟化层安全加固、虚拟化环境可信验证和虚拟资源防逃逸等。
BD 机密计算远程证明	机密计算统一远程证明框架	待制定	• 抽象通用证明流程：度量启动->报告生成→报告收集→验证→结果传递的标准化交互模型； • 定义度量报告格式：为不同机密计算平台提供统一的度量报告格式，便于远程证明服务器统一解析； • 定义统一的报告收集、结果传递等交互接口。
	GCC-1006-2025《机密计算远程认证服务技术要求》	已发布	规范机密计算远程认证服务具备的能力及接口，支撑不同架构和实现的机密计算环境的安全认

			证。
BE 机密计算密码应用	GCC 《机密计算密码应用技术要求》	草案	给出了机密计算平台密码应用技术架构、安全目标，以及机密计算各系统层次和安全功能的密码应用技术指南。适用于机密计算平台相关方设计、开发、使用时参考，也可为开展机密计算平台检测、评估提供技术参考。
BF 机密计算集群管理	机密计算集群管理安全要求	待制定	包括机密计算集群架构组成、安全基线要求、集群管理规范和集群节点互信机制等方面，同时考虑在集群模式下，大规模节点互信互通的安全与性能折中优化。
BG 机密计算互联互通	异构机密计算安全框架和接口规范	待制定	• 定义统一的异构机密计算安全通信流程：如机密计算通信实体创建、通信实体的安全通信机制、通信实体的交互报文处理流程等； • 定义统一的异构机密计算安全通信接口。
	TDISP（TEE Device Interface Security Protocol）协议	已发布	定义了一种用于可信 I/O 虚拟化的架构，规范了 TVM 和 Device 之间如何建立信任关系，Host 和 Device 之间的互联安全以及如何以可信的方式将 TDI 与 TVM 绑定或分离。
	跨 TEE 技术互操作性规范	待制定	为应用开发者提供一套相对统一的、屏蔽底层 TEE差异的基础编程接口（如关键管理、密封存储、安全通道等基础服务）。降低开发门槛，提

			升应用的可移植性，加速产业生态繁荣。可参考CCC API、GP TEE Internal Core API等，但需考虑国内主流技术路线。

2.2.3 产品与应用类

产品与应用类标准旨在助力机密计算在各产业、领域和行业的应用推广。

产品应用类标准设计见表 3，给出了各个标准的名称、状态和标准主旨。

表 3 产品应用类标准简介

类别	标准名称	状态	标准主旨
CA 机密计算平台	GCC-1005-2025《机密计算平台技术要求与测评方法》	已发布	规定了机密计算平台在可信硬件层、系统软件层和系统服务层的安全要求，和相应的测评方法。
	机密计算平台接口设计规范	待制定	按照机密计算平台的核心功能，抽象定义服务接口为上层应用与使用方提供标准化接口。上层应用依据此接口，完成机密计算能力扩展与生态扩展，使用方可通过此接口直接使用机密计算的原生能力。
CB 机密计算云主机	机密计算云主机技术规范	待制定	结合云场景，定义机密计算云主机技术规范，包括机密虚拟机镜像格式等，明确机密计算云主机厂商应具备的能力，以及机密计算云主机使用方应注意的要求。
CC 机密计算一体机	机密计算一体机技术规范	待制定	结合一体机场景，定义机密计算一体机技术规范，明确机密计算一体机厂商应具备的能力，以及机密

			计算一体机使用方应注意的要求。
CD 机密计算端云协同	机密计算端云协同技术规范	待制定	规范端云协同机密计算的架构组成、安全要求和协同计算机制等，确保用户数据从端侧到云侧的全链路安全。
CE 基于机密计算的可信数据空间	基于机密计算的可信数据空间技术要求	草案	规定了基于机密计算的可信数据空间的技术要求。适用于基于机密计算的可信数据空间相关方设计、开发、使用时参考，也可为开展基于机密计算的可信数据空间能力评估活动提供参考。
CF 基于机密计算的密码模块	基于机密计算的商用密码模块技术规范	待制定	给出基于机密计算环境构建内生商密模块的架构组成，必要的服务接口等。
CG 人工智能领域的机密计算应用	生成式人工智能领域机密计算应用指南	待制定	识别机密计算在生成式人工智能领域的应用场景，并给出技术实现参考等，例如如何采用机密计算保护 AIGC 水印、如何采用机密计算保护模型和提示词等敏感数据。
CH 行业领域的机密计算应用	互联网行业机密计算应用指南	待制定	结合互联网行业机密计算的应用场景，给出互联网行业的机密计算应用指南，包括各场景中的技术实现参考等。
	金融行业机密计算应用指南	待制定	结合金融行业机密计算的应用场景，给出金融行业的机密计算应用指南，包括各场景中的技术实现参

			考等。
	T/BFIA 054—2025 《基于可信执行环境的安全计算金融应用技术要求》	已发布	规定了基于可信执行环境的安全计算金融应用的技术要求，包括功能要求、安全要求、集群管理要求等。
	电信行业机密计算应用指南	待制定	结合电信行业机密计算的应用场景，给出电信行业的机密计算应用指南，包括各场景中的技术实现参考等。

2.2.4 测试评价类

测试评价类标准旨在规范机密计算应用过程中的测试评价方法。

测试评价类标准设计见表 4，给出了各个标准的名称、状态和标准主旨。

表 4 测试评价类标准简介

类别	标准名称	状态	标准主旨
DA 机密计算安全性测评	GCC-1005-2025 《机密计算平台技术要求与测评方法》	已发布	规定了机密计算平台的技术要求和测试评价方法，适用于机密计算平台相关方设计、开发、运维和测评参考。
DB 机密计算兼容性测评	机密计算兼容性测试规范	待制定	明确测试范围与对象，包括机密计算平台、中间件和应用软件等，并为各测试对象制定测试指标和测试方法。
DC 机密计算互联互通测评	机密计算互联互通测试规范	待制定	明确测试范围与对象，包括机密计算平台、中间件和应用软件等，并为各测试对象制定测试指标

			和测试方法。
DD 机密计算性能测评	机密计算性能测试规范	待制定	分别面向机密计算平台、中间件和应用软件等，规范各测评对象的核心工作环节，例如，机密计算环境初始化、可信验证、数据封装、密码运算、异构设备互联等的性能测试评价方法。
	YD/T 4948-2024《隐私计算 可信执行环境产品性能测试要求》	已发布	规定了基于 TEE 的产品性能相应的测试方法，包括技术要求、测试维度、测试场景等内容，适用于基于 TEE 的隐私计算产品的研发、测试、评估和验收等。该标准为机密计算相关产品的性能测试提供了相应的参考。

第三章 总结与展望

3.1 研究总结

本报告系统性地梳理了国内外机密计算标准化现状，深入调研了国内核心标准组织（TC260 全国信息安全标准化技术委员会、CCSA 中国通信标准化协会、GCC 全球计算联盟联盟）以及国际主要标准组织（ISO/IEC JTC 1/SC 27/WG 3、IETF、Confidential Computing Consortium (CCC)/GlobalPlatform (GP)等）在机密计算领域的工作成果、标准规范和路线图。研究范围覆盖了机密计算的核心技术要素（如可信执行环境 TEE、内存加密、远程证明、安全服务等）、安全要求、参考架构、测评方法以及特定应用场景的支撑需求。

研究表明：

- 标准化生态正在形成： 国际层面，ISO/IEC、IETF、CCC/GP 等组织在基础框架、核心协议（如远程证明、TEE 接口）方面已取得初步进展，国内 TC260、CCSA、GCC 等

组织积极跟进并启动相关标准研制，但完整的标准体系尚未完全建立。

- 产业需求迫切且多元： 云计算、大数据、人工智能、金融科技、医疗健康、政务数据共享等关键领域对数据要素在流转、处理过程中的机密性与完整性保护需求激增，亟需统一、可信、高效的机密计算技术标准作为支撑，以解决数据流通的信任瓶颈，释放数据价值。
- 技术挑战与标准缺口并存： 现有标准主要集中在基础框架和核心组件层面，在跨平台/跨 TEE 技术的互操作性、统一的远程证明框架与协议、细粒度的安全分级与测评、特定应用场景的集成规范以及隐私保护技术与机密计算的融合等方面存在显著空白或深度不足。

基于上述调研和深入的产业需求分析，本报告规划了一个层次清晰、覆盖全面、面向未来的机密计算标准体系框架，旨在为国内机密计算产业的健康、有序、安全发展提供标准化指引。

3.2 未来展望

机密计算作为保障数据要素安全流通的核心技术，其标准化工作对于构建数字经济时代的新型信任基础设施至关重要。未来标准体系建设应重点关注以下方向：

- 技术演进驱动标准创新：紧密跟踪硬件 TEE（如 Intel SGX, AMD SEV, ARM CCA, RISC-V Keystone 等）、基于硬件的内存加密、同态加密等隐私增强技术与机密计算的融合等前沿技术发展，及时将成熟、安全的技术方案纳入标准。
- 深化应用场景牵引：标准研制应更加聚焦云边端协同中的敏感数据处理、AI 模型训练与推理保护、可信数据空间、内生密码等典型应用场景，制定更具针对性的实现指南和接口规范。
- 强化互操作性与生态构建：推动不同 TEE 实现、不同云平台、不同应用之间基于标准的无缝协作是产业落地的关键。标准应着力解决接口统一、协议兼容、证书互认等问题。
- 加强国内协同与国际合作：深化国内 TC260、CCSA、GCC 等组织间的协同，避免重复建设，形成合力。积极参与 ISO、IETF、CCC 等国际标准组织的活动，贡献中国方案，

推动形成全球互认的标准体系。

基于当前标准缺口、产业落地紧迫性和技术成熟度，建议优先启动以下关键标准的研制工作：

表 2 优先研制标准

标准	原因
机密计算 术语	统一机密计算概念、范围、核心组件（TEE、远程证明、内存加密等）的理解和定义，理清机密计算、可信计算和隐私保护计算等不同技术路线区别和关联，为整个标准体系奠定共同语言基础。
机密计算统一远程证明框架	远程证明是建立TEE实例可信性的核心机制。当前不同TEE技术（SGX, SEV, CCA等）的证明流程和数据格式各异，严重阻碍互操作性和应用推广。亟需制定（或主导/深度参与国际）统一的、技术中立的远程证明模型、协议（如基于IETF RATS架构）、证据格式和验证接口标准。这是实现跨平台信任的“钥匙”。
异构机密计算安全框架和接口规范	随着数据可信流通、大模型推理等业务场景快速发展，客户对机密计算的需求已经不局限于CPU，需要突破CPU边界，将机密计算环境延伸到GPU、NPU和DPU等异构处理器侧，因此，亟需制定异构机密计算的安全通信流程和接口规范标准。
跨TEE技术互操作规范（基础API/服务接口）	为加速机密计算推广应用，亟需为应用开发者提供一套相对统一的、屏蔽底层TEE差异的基础编程接口（如关键管理、密封存储、安全通道等基础服务）。降低开发门槛，提升应用的可移植性，加速产业生态繁荣。可参考CCC API、GP TEE Internal Core API等，但需考虑与国内主流技术路线兼容。

参 考 文 献

[1]GCC 《机密计算白皮书（2024）》

Global Computing Consortium

全 球 计 算 联 盟