ICS 35.160
CCS C 39

团　体　标　准

T/GCC　1005—2025

机密计算平台技术要求与测评方法

Technical requirements and evaluation methods for confidential computing platform

2025-10-17 发布　　2025-10-17 实施

全球计算联盟　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由全球计算联盟机密计算专委会提出。

本文件由全球计算联盟归口。

本文件起草单位：中国电子技术标准化研究院、华为技术有限公司、安谋科技（中国）有限公司、南湖实验室、中国工商银行股份有限公司软件开发中心、北京国家金融科技认证中心、南方科技大学、超聚变数字技术有限公司、国家信息技术安全研究中心、武汉大学、飞腾信息技术有限公司、希奥端计算技术有线公司、麒麟软件有限公司、杭州安恒信息技术股份有限公司、杭州锘崴信息科技有限公司、河南昆仑技术有限公司。

本文件主要起草人：姚相振、王惠莅、羡喻杰、庞婷、于攀、金意儿、惠静、张瑞、胡科开、卢孝新、杨臻、王骏超、张殷乾、杨喜乐、何佳、张磊、严志超、陈凌潇、黄司辉、冉佳欣、李博文、黄江、严敏瑞、马浩诚、许祥益、赵宇航、姜柯、谢秋华、武海龙、王娟、王杰、姜德隆、颜秉泽、谭琳、肖军、吴涛、梁少峰、张大朋、于博、董靓、陶立峰、王吾冰、张振永、李帜、孙琪、李艳、张洵。

机密计算平台技术要求与测评方法

1 范围

本文件规定了机密计算平台的技术要求和测试评价方法。

本文件适用于机密计算平台相关方设计、开发、运维和测评参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 45230 数据安全技术 机密计算通用框架

GM/T 0005 随机性检测规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

机密计算 confidential computing

在可信的硬件基础上，通过隔离、加密、证明等机制，保护使用中数据安全的计算模式。

[来源：GB/T 45230—2025,3.3]

3.2

机密计算平台 confidential computing platform

执行机密计算任务的基础软硬件集合。

[来源：GB/T 45230—2025,3.5]

3.3

机密计算环境 confidential computing environment

基于机密计算平台,为支撑机密计算应用程序运行所构建的计算环境。

[来源：GB/T 45230—2025,3.6]

3.4

机密计算操作系统 confidential computing operator system

专用于支持机密计算技术的操作系统，通过与底层硬件安全功能紧密结合，如TEE，提供安全保障功能。

[来源：GB/T 41388-2022,3.2]

3.5

可信执行环境 trusted execution environment

基于硬件隔离及安全启动机制，为确保安全敏感应用相关数据和代码的机密性、完整性、真实性和不可否认性目标构建的一种软件运行环境。

注：硬件级隔离是指基于硬件安全扩展机制，通过对计算资源的固定划分或动态共性，保证隔离资源不被富执行环境访问的一种安全机制。

[来源：GB/T 41388—2022,3.3]

3.6

可信虚拟化 trusted virtualization

基于可信执行环境的虚拟化方法。

[来源：GB/T 41388-2022,3.2]

3.7

机密虚拟机 confidential virtual machine

一种基于机密计算环境保护运行过程中数据与应用程序安全的虚拟机。

注：机密虚拟机镜像中的代码和数据不受管理程序和主机操作系统影响。

3.8

硬件信任根 hardware root of trust

通常由硬件和固件组成，为可信环境提供完整性度量、安全存储、可信报告等功能的模块。

4 缩略语

下列缩略语适用本文件：

CPU：中央处理器（Central Processing Unit）
CVM：机密虚拟机（Confidential Virtual Machine）
DPU：数据处理器（Data Processing Unit）
GPU：图形处理器（Graphics Processing Unit）
I/O：输入/输出（Input/Output）
NIC：网络接口卡（Network Interface Card）
NPU：神经网络处理器 (Neural Network Processing Unit)
TCP：传输控制协议（Transmission Control Protocol）
TEE：可信执行环境（Trusted Execution Environment）
UDP：用户数据报文协议（User Datagram Protocol）
VM：虚拟机（Virtual Machine）

5 概述

机密计算平台框架应符合GB/T 45230的规定，见图1，包含以下三个层次：

a) 可信硬件层基于硬件隔离实现受保护的硬件资源不被非授权任务访问，并为机密计算环境提供可信的硬件资源，可采用硬件隔离或内存加密机制保护数据机密性；

b) 系统软件层为机密计算环境提供基于逻辑的隔离机制，必要的软件资源和调度机制，可支持用户方直接部署机密计算应用或基于可信虚拟化能力，在机密虚拟机或容器中部署机密计算应用；

c) 系统服务层基于可信硬件与系统软件，提供必要的机密计算服务，包括隔离计算、安全启动和可信度量等。

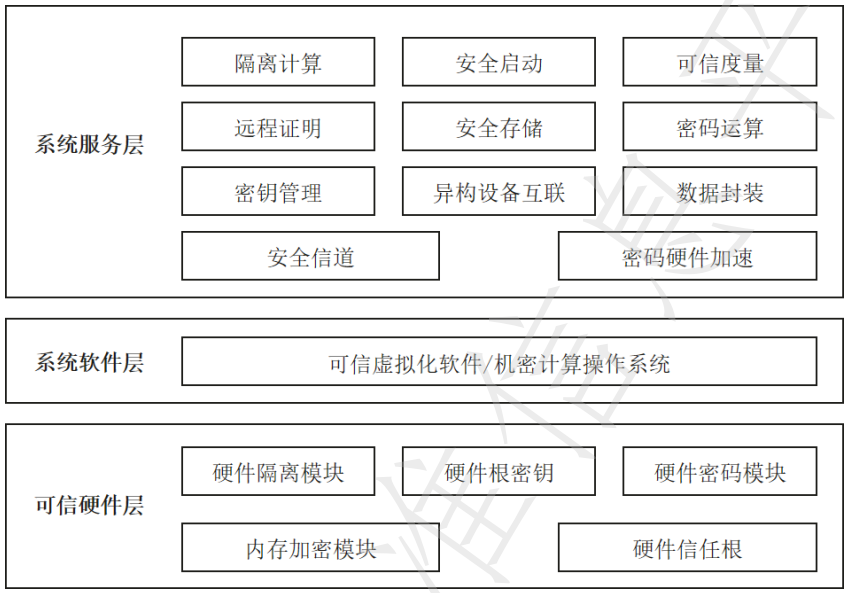

图1 机密计算平台参考架构

6 技术要求

6.1 可信硬件层

6.1.1 硬件隔离模块

硬件隔离模块包含可信执行控制单元和隔离内存空间，为机密计算环境提供硬件隔离的硬件基础。硬件隔离模块满足以下要求：

a) 应支持硬件隔离机制，将硬件资源隔离成安全资源和普通资源，并为上层软件提供安全状态和普通状态两种执行状态，硬件资源包含但不限于内存和芯片级 I/O 等；

b) 应保证机密计算环境使用的硬件资源不被其他环境访问；

c) 应保证普通状态无法访问安全状态下的硬件资源；

d) 应保证不同内存映射表间的相互隔离性，确保内存映射表不被非法篡改、破坏。

6.1.2 硬件根密钥

硬件根密钥是在可信硬件（如芯片）中固化的唯一密钥，用于密钥派生等场景。硬件根密钥满足以下要求：

a) 应保证硬件根密钥不被替换或篡改；

b) 应保证硬件根密钥禁止非授权访问。

6.1.3 硬件密码模块

硬件密码模块用于提供密钥派生、密码运算等功能，包含密码模块引擎与硬件随机数生成器等。硬件密码模块满足以下要求：

a) 生成的随机数质量应符合 GM/T 0005 的规定；
b) 派生出的密钥应保证机密性与完整性，禁止被非授权访问；
c) 密码算法应符合密码相关的国际标准、国家标准和行业标准等要求，算法应安全可靠。

6.1.4 内存加密模块

内存加密模块用于保证内存上的数据无法被直接获取。内存加密满足以下要求：

a) 应支持对机密计算环境使用的物理内存进行加密，确保物理内存上数据的机密性和完整性；
b) 应支持密钥无法被非授权软件访问；
c) 内存加密算法应采用符合密码相关的国际标准、国家标准、行业标准等要求的密码算法，算法应安全可靠；
d) 宜支持对机密计算环境中不同信任域间使用不同密钥加密。

6.1.5 硬件信任根

硬件信任根用于支撑机密计算环境启动过程信任链的建立，并用于实现安全启动、远程证明等功能，满足以下要求：

a) 应保证硬件信任根不被替换或篡改；
b) 应具备物理防护机制，如防故障注入；
c) 宜具有国家安全类权威机构签发的证书。

6.2 系统软件层

6.2.1 可信虚拟化软件

机密计算环境中可信虚拟化软件为CVM提供数据与应用程序保护的能力，提供资源管理和部署支撑，提供通信调度机制。机密计算平台支持可信虚拟化时，可信虚拟化软件满足以下要求：

a) 应支持创建多个 CVM，支持 CVM 生命周期管理；
b) 应具备管理 CVM 的 CPU、内存、外设等硬件资源能力；
c) 应支持 CVM 内存数据及应用不被管理程序窃取和篡改；
d) 宜支持 CVM 热迁移，确保 CVM 在运行不中断的条件，从一个机密计算环境安全地迁移至另一个经过验证的机密计算环境，CVM 相关的敏感数据再迁移过程中始终处于加密或隔离保护状态；
e) CVM 软硬件资源应具备访问控制能力，其他 VM 无法使用已被占用的资源。

6.2.2 机密计算操作系统

机密计算操作系统利用机密计算可信硬件资源，实现基于硬件隔离的系统执行环境，完成对机密计算环境内资源管理和调度。在机密计算平台支持机密计算操作系统时，机密计算操作系统满足以下要求：

a) 应提供机密计算环境和普通计算环境的通信机制；
b) 应提安全的隔离机制，保证普通计算环境中的应用软件和系统软件在非授权情况下无法访问机密计算环境；
c) 宜支持容器化部署；
d) 宜经过业界安全类权威测评机构的安全测评认证。

6.3 系统服务层

6.3.1 隔离计算

隔离计算基于硬件的隔离机制和软件的访问控制，区分普通计算环境与机密计算环境。提供计算应用程序的管理和调用功能。隔离计算应满足以下要求：

a) 应支持系统软件的隔离性，非机密计算环境的操作系统或其他特权软件在非授权下无法访问该机密计算环境；
b) 应确保 CVM 之间软硬件资源的隔离性，防止代码及数据的泄露；
c) 应支持机密计算应用程序的隔离性，不能越权访问其他机密计算应用程序。

6.3.2 安全启动

安全启动保证机密计算环境按照既定逻辑启动，通过公钥证书逐级验证待启动的固件或软件的签名，确保固件或软件不被篡改。安全启动满足以下要求：

a) 应支持基于硬件信任根，通过签名验签方法验证机密计算环境启动过程的每一个阶段，以确保机密计算应用程序按照预期行为执行计算任务，非法组件或签名应能被检测出，验证不通过应停止启动流程；
b) 应保证安全启动信任链按序逐级验证，不可被恶意绕过。

6.3.3 可信度量

可信度量能及时度量机密计算环境启动与运行过程是否按预期执行，可信度量满足以下要求：

a) 应基于硬件信任根建立机密计算环境启动过程中的信任链，对关键固件、操作系统或软件生成度量值；
b) 宜支持动态度量，包括但不限于应用程序代码段，动态库代码段，内核代码段等。

6.3.4 远程证明

远程证明提供对机密计算环境、CVM、机密容器等进行完整性与真实性验证功能。远程证明满足以下要求：

a) 应支持挑战/应答机制，抵抗证明报告的重放攻击；
b) 应支持生成机密计算环境的证明报告；
c) 应支持生成机密计算应用程序启动时的证明报告；
d) 应基于硬件信任根对证明报告签名，保证证明报告的完整性和真实性；
e) 宜支持对 CVM、容器内运行的应用程序进行动态度量，保障完整性和真实性验证。

6.3.5 安全存储

安全存储提供数据加密存储服务。安全存储满足以下要求：

a) 应支持机密计算环境中的数据保存到外部存储介质中时加密存储，外部存储的加密数据加载到机密计算环境时可正确解密；
b) 应保证加密的数据解密后只能被授权实体访问；
c) 应保证安全存储所使用密钥的机密性和完整性。

6.3.6 密码运算

密码运算为机密计算环境提供密码运算服务。密码运算满足以下要求：

a) 应支持在机密计算环境运行基础的密码运算，包括加密、解密、签名、验签、杂凑等操作；
b) 密码算法应符合密码相关的国际标准、国家标准、行业标准等要求，算法应安全可靠。

6.3.7 密钥管理

密钥管理为机密计算环境密钥生命周期管理功能。密钥管理满足以下要求：

a) 应使用安全的方式派生密钥，如基于硬件密码模块派生等；
b) 密钥（除公钥外）应以密文形式存储或备份或归档在可信的介质中，且无法被非授权访问、使用、修改和替换；
c) 密钥分发过程中应采取身份认证等方式保障分发者/接收者身份的真实性，且保障密钥的机密性和完整性；
d) 应确保对称密钥与非对称私钥只能在机密计算环境内部（包含 TEE 与硬件密码模块内）使用；
e) 密钥在生命周期结束、发生泄漏或有泄漏风险时应支持密钥销毁；
f) 密钥仅能在机密计算环境中使用，支持密钥迁移，不支持明文导出。

6.3.8 异构设备互联

异构设备互联建立了机密计算环境中CPU与异构设备（CPU以外的设备）之间的安全连接，使机密计算环境内应用程序可访问异构设备。异构设备虚拟化可将异构I/O设备虚拟化多个设备实例，提供机密计算环境使用。异构设备互联满足以下要求：

a) 机密计算环境 CPU 与异构设备的通信应支持访问控制机制或加密机制，确保数据的通信安全，采用加密机制时，密码算法应符合密码相关的国际标准、国家标准、行业标准等要求；
b) 机密计算环境宜支持 CPU 与异构设备直接互联请求，建立异构设备与机密计算环境之间的连接；
c) 机密计算环境支持 CPU 与异构设备访问控制机制时，宜支持根据直接互联请求完成异构设备信息的注册，确保异构设备直接访问机密计算环境内存；
d) 机密计算环境宜支持 CPU 与虚拟化 I/O 设备实例互联；
e) 机密计算环境宜支持对虚拟化 I/O 设备的配置能力，保证虚拟化的设备实例能够正常访问机密计算环境中的安全内存；
f) 机密计算环境宜支持对虚拟化 I/O 设备操作进行访问控制，可根据设备标识进行控制设备的数据交互；
g) 宜保证异构机密计算的通信性能损耗符合业务要求；
h) 异构设备宜支持硬件可信根，支持可信度量或远程证明，确保设备安全可靠。

6.3.9 数据封装

数据封装为机密计算环境提供数据封装、解封服务，可根据硬件密码引擎将根密钥、机密计算应用程序标识和机密计算应用程序完整性度量值等参数作为输入，生成封装密钥并返回给机密计算环境。数据封装满足以下要求：

a) 应保证封装密钥的机密性与完整性；
b) 应基于硬件根密钥派生封装密钥；
c) 封装的数据应只能被授权的硬件或服务访问。

6.3.10 安全信道

安全信道为机密计算环境提供数据传输的安全保护服务。建立安全信道的双方应进行身份认证，保证安全信道中的数据不被非授权访问与篡改。

6.3.11 密码硬件加速

密码硬件加速为机密计算环境提供提高密码运算性能服务。密码硬件加速应满足以下要求：

a) 机密计算环境宜提供密码硬件加速功能，提升密码运算效率；
b) 密码算法应采用符合密码相关的国际标准、国家标准、行业标准等要求的密码算法，算法应安全可靠。

7 测试评价方法

7.1 通则

机密计算平台评价方法应符合附录A规定，其中，异构设备互联性能测评方法应符合附录B规定。

7.2 可信硬件层

7.2.1 硬件隔离模块

硬件隔离测试评价方法如下：

a) 测试方法：
   1) 审查机密计算平台的文档，检查硬件隔离模块设计；
   2) 尝试在普通计算环境中，包含宿主机、VM、容器等，访问机密计算环境中硬件资源中的数据，包括但不限于CPU、内存、I/O设备等，验证是否可以获取机密计算环境数据。
b) 预期结果：
   1) 机密计算平台的硬件隔离机制可以有效保护机密计算环境中的数据；
   2) 普通计算环境与机密计算环境硬件资源隔离使用，普通计算环境无法访问机密计算环境数据。
c) 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.2 硬件根密钥

硬件根密钥的测试评价方法如下：

a) 测试方法：
   1) 审查机密计算平台的文档，检查硬件根密钥设计方案；
   2) 尝试非授权获取读取硬件根密钥，验证是否可以非法获取或篡改。
b) 预期结果：
   1) 机密计算平台具备根密钥保护机制；
   2) 根密钥无法被非法获取或篡改。
c) 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3 硬件密码模块

硬件密码模块的测试评价方法如下：

a) 测试方法：
   1) 审查机密计算平台的文档，检查是否具备硬件密码模块；
   2) 调用硬件密码模块进行密码运算，验证算法是否符合要求；
   3) 使用硬件密码模块的随机数生成器生成随机数，验证是否符合要求；
   4) 尝试篡改或非授权访问硬件密码模块的密钥，验证密钥是否可以被篡改或非法访问。
b) 预期结果：
   1) 机密计算平台具备硬件密码模块；

2) 密码算法应采用符合密码相关的国际标准、国家标准、行业标准等要求的密码算法，算法应安全可靠；
3) 随机数生成器的随机数质量符合GM/T 0005的规定，或密码模块通过第三方权威组织的测评认证；
4) 硬件密码模块密钥具有保护措施，不可被篡改或非法访问。

c) 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.4 内存加密

内存加密的测试评价方法如下：

a) 测试方法：
1) 审查机密计算平台的文档，检查内存加密方案；
2) 尝试获取内存加密数据，检查是否明文存储，验证是否可以还原明文；
3) 尝试获取内存加密密钥，验证是否可以获取加密密钥；
4) 尝试获取不同安全域的密钥，验证是否相同。

b) 预期结果：
1) 机密计算平台内存加密所使用的加密算法与密钥长度符合标准要求；
2) 内存加密后的数据不能在机密计算环境外还原为明文或内存数据不可被被机密计算环境外获取到；
3) 内存加密所使用的密钥不能被非信任实体获取到；
4) 不同信任域使用的内存加密密钥不同。

c) 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.5 硬件信任根

硬件信任根的测试评价方法如下:

a) 测试方法：
1) 审查机密计算平台的文档，检查机密计算环境的硬件信任根设计；
2) 尝试使用未授权的用户访问和篡改硬件信任根的数据和代码，验证访问控制机制是否失效；
3) 尝试替换或篡改硬件信任根数据和代码，验证硬件信任根是否有保护机制。

b) 预期结果：
1) 机密计算平台的硬件信任根具备机密性、完整性、真实性三个基本安全特征；
2) 硬件信任根具有访问控制机制，禁止非授权用户非法访问与篡改；
3) 硬件信任根具有防护机制，禁止被替换或篡改，或者替换与篡改行为执行后，无法绕过硬件信任根安全机制。

c) 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.3 系统软件层

7.3.1 可信虚拟化软件

可信虚拟化软件的测试评价方法如下：

a) 测试方法：
1) 审查机密计算平台的文档，检查可信虚拟化软件设计；
2) 在机密计算环境内动态创建与删除 CVM，并尝试管理 CVM 内部 CPU、内存、外设等硬件资

源；
3) 在机密计算环境内创建多个 CVM，尝试越权访问其他 CVM 的资源；
4) 检查 CVM 是否支持热迁移；
5) 检查机密计算环境系统内部 CVM 的等级权限设置，验证是否赋予最高等级权限。

b) 预期结果：
1) 可信虚拟化软件具备创建、删除等动态管理 CVM 的能力，以及管理 CVM 的 CPU、内存、外设等硬件资源；
2) 机密计算环境内 CVM 仅根据其分配的权限访问相应的资源，不能越权访问；
3) CVM 支持热迁移；
4) 可信虚拟化软件未赋予内部 CVM 最高等级权限，单一 CVB 出现崩溃不会影响到其他 CVM 或机密计算环境。

c) 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.3.2 机密计算操作系统

机密计算操作系统的测试评价方法如下：

a) 测试方法：
1) 审查机密计算平台的文档，检查机密计算操作系统设计；
2) 尝试通过普通计算环境应用程序非授权访问机密计算环境，验证机密计算操作系统是否可拦截；
3) 验证机密计算操作系统是否支持应用程序真实性与完整性验证；
4) 验证机密计算操作系统支持容器化部署，容器内支持权限隔离与资源限制。

b) 预期结果：
1) 机密计算操作系统可拦截普通计算环境应用程序非授权访问；
2) 机密计算操作系统支持对应用程序的真实性与完整性验证；
3) 机密计算操作系统支持容器化部署，且容器内支持权限隔离与资源限制。

c) 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.4 系统服务层

7.4.1 隔离计算

软件隔离的测试评价方法如下：

a) 测试方法：
1) 审查机密计算平台的文档，检查软件隔离设计；
2) 尝试通过非机密计算环境进程访问机密计算环境进程数据，验证是否可以获取机密计算环境数据，包括但不限于 VM 进程间、VM 管理程序与 VM 间等；
3) 尝试使用特权软件访问机密计算内存数据。

b) 预期结果：
1) 机密计算平台的软件隔离机制可以有效保护机密计算环境中的数据；
2) 非机密计算环境与机密计算环境有软件隔离机制，非机密计算环境无法访问机密计算环境数据；
3) 特权软件无法访问机密计算内存数据。

c) 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.4.2 安全启动

安全启动的测试评价方法如下：

a） 测试方法：

1） 审查机密计算平台的文档，检查机密计算环境的安全启动过程；

2） 检查安全启动过程用于完整性和真实性验证的密码算法不存在已公开脆弱性；

3） 尝试替换或篡改硬件信任根，验证安全启动是否正常执行；

4） 尝试替换或篡改安全启动过程参与的组件，验证安全启动是否可正常执行；

5） 尝试非授权替换或篡改相应密钥，验证安全启动是否正常执行；

6） 尝试绕过安全启动信任链的逐级验证过程。

b） 预期结果：

1） 安全启动过程保证机密计算环境系统的完整性和真实性，防止非授权或被恶意篡改的代码执行；

2） 安全启动过程保证用于完整性和真实性验证的密码算法本身的鲁棒性；

3） 硬件信任根被替换或篡改，安全启动失败；

4） 安全启动过程参与的组件被替换或篡改后，可被检测出；

5） 安全启动过程保证用于进行完整性和真实性验证的密钥不可被非授权替换或篡改，并提供安全的密钥更新、撤销功能；

6） 安全启动信任链按序逐级验证，不可被恶意绕过。

c） 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.4.3 可信度量

可信度量的测试评价方法如下：

a） 测试方法：

1） 审查机密计算平台的文档，检查可信度量设计；

2） 验证可信度量的信任链建立起点是否基于硬件信任根，验证是否对关键固件、操作系统或软件进行度量；

3） 验证可信度量是否可以支持动态度量，验证度量的范围是否包含应用程序代码段，动态库，内核代码，内核代码段等。

b） 预期结果：

1） 机密计算平台支持可信度量；

2） 度量的信任链起点为硬件信任根；

3） 支持动态度量。

c） 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.4.4 远程证明

远程证明的测试评价方法如下：

a） 测试方法：

1） 审查机密计算平台的文档，检查远程证明设计；

2） 应验证远程证明通信双方是否有认证机制；

3） 尝试修改远程证明基准值，验证远程证明验证方是否可以检测出；

4） 尝试篡改远程证明报告，验证远程证明验证方是否可检测出；

5） 验证远程证明是否支持挑战应答机制；

6） 验证远程证明是否可以支持对机密容器、容器内运行的程序进行完整性与真实性验证。

b） 预期结果：

1) 机密计算平台远程证明设计可以验证待验证方完整性与真实性；
2) 远程证明通信双方具有认证机制；
3) 修改远程证明基准值，远程证明流程失败或可以被检测出；
4) 篡改远程证明报告，远程证明流程失败或可以被检测出；
5) 厂商提供的远程证明方案支持挑战应答机制；
6) 远程证明可以对运行在 CVM、容器内的程序进行完整性与真实性验证。

c) 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.4.5 安全存储

安全存储的测试评价方法如下：

a) 测试方法：
1) 审查机密计算平台的文档，检查机密计算环境数据安全存储过程及密钥使用是否安全；
2) 被授权的机密计算环境读取存储后的数据，尝试进行解密，验证是否可以获取明文数据；
3) 尝试在非授权环境读取存储后的数据，尝试进行解密，验证是否可以获取明文数据。

b) 预期结果：
1) 厂商提供的方案密钥使用安全，数据存储过程无风险；
2) 被授权的机密计算环境存储的数据可以正常解密；
3) 非授权环境不能被解密还原出明文。

c) 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.4.6 密码运算

密码运算的测试评价方法如下：

a) 测试方法：
1) 审查机密计算平台的文档，检查厂商提供的密码算法实现设计，验证密码算法是否符合标准；
2) 尝试执行多次密码运算，验证算法执行稳定性。

b) 预期结果：
1) 机密计算平台支持加密算法符合密码相关的国际标准、国家标准、行业标准等要求的密码算法，算法应安全可靠；
2) 多次进行密码运算，运算结果一致。

c) 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.4.7 密钥管理

密钥管理的测试评价方法如下：

a) 测试方法：
1) 审查机密计算平台的文档，审核密钥管理过程；
2) 检查密钥的派生方式，是否存在非授权访问、泄露等风险；
3) 检查机密计算环境各个密钥存储过程，是否保证密钥的安全存储，尝试未授权访问、篡改、替换和修改存储的密钥；
4) 密钥分发过程，尝试使用非法身份绕过身份认证机制，获取通信过程中的密钥；
5) 密钥生命周期结束后，尝试获取密钥。

b) 预期结果：
1) 机密计算平台的密钥管理有安全设计，符合安全要求；

2） 密钥派生符合安全要求；
3） 机密计算环境各个密钥安全存储，未授权用户无法访问、篡改、替换和修改等；
4） 密钥分发过程，需要通过身份认证才可以获取密钥；
5） 密钥生命周期结束后，用户无法获取或还原密钥。

c） 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.4.8 异构设备互联

异构设备互联的测试评价方法如下：

a） 测试方法：
1） 审查机密计算平台的文档，检查机密计算环境与I/O设备通信方法是否满足安全性；
2） 尝试从宿主机侧或普通计算环境中获取机密计算环境与I/O设备通信数据，验证是否可以获取数据；
3） 检测机密计算环境与I/O设备（如GPU、NPU、DPU、NIC、磁盘等）交互相比于普通VM与I/O设备交互的损耗，计算损耗是否满足客户要求；
4） 如果设备支持虚拟化，应按照测试方法步骤1)～3)测试其虚拟化功能。

b） 预期结果：
1） 机密计算平台提供的异构互联方案满足机密计算环境与I/O设备通信的安全性；
2） 从宿主机或普通VM中不能访问机密计算环境与I/O设备通信数据；
3） 机密计算环境与I/O设备交互平均损耗应满足业务要求；
4） 支持虚拟化的设备满足预期结果1)～3)。

c） 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.4.9 数据封装

数据封装的测试评价方法如下：

a） 测试方法：
1） 审查机密计算平台的文档，检查数据封装设计方案；
2） 尝试对数据进行封装与解封，验证解封后的数据与原数据一致；
3） 尝试非法获取或篡改封装密钥，验证封装密钥的机密性和完整性保护能力；
4） 尝试通过非授权硬件或服务获取封装数据，验证是否可以获取明文数据或进行数据解封。

b） 预期结果：
1） 机密计算平台具备数据封装功能；
2） 使用封装密钥对数据进行数据封装与解封操作后，解封后的数据与原数据一致；
3） 封装密钥具有机密性与完整性保护能力，无法被非法获取或篡改；
4） 封装数据只能被授权的硬件和服务访问，无法获取明文数据或进行数据解封。

c） 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.4.10 安全信道

安全信道的测试评价方法如下：

a） 测试方法：
1） 审查机密计算平台的文档，机密计算环境安全信道方案；
2） 尝试获取安全信道中的数据，验证数据是否可以被非法第三方还原成明文。

b） 预期结果：
1） 机密计算平台具备机密计算环境建立安全信道功能；

2） 安全信道中的数据无法被非法第三方还原成明文。

c） 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.4.11 密码硬件加速

密码硬件加速的测试评价方法如下：

a） 测试方法：

1） 审查机密计算平台的文档，检查机密计算环境是否提供密码硬件加速功能；

2） 调用密码硬件加速模块运算，验证是否满足要求。

b） 预期结果：

1） 机密计算平台具备密码运算硬件加速功能；

2） 硬件密码算法满足密码算法应采用符合密码相关的国际标准、国家标准、行业标准等要求的密码算法，算法应安全可靠。

c） 结果判定：实际测试结果与预期结果一致则判定为符合，其他情况判定为不符合。

附 录 A
（规范性）
机密计算平台评价方法

表A.1规定了机密计算平台的评价方法，平台模块单项功能指标项符合要求时，得分为满分，不符合要求得分为0分，部分符合的视情况得分。机密计算平台得分为各功能项总分。

表A.1 安全保护能力计分方法

架构	模块	功能	等级	单项计分	单项总分	说明
可信硬件层	硬件隔离模块	支持 CPU 隔离	基础	2	基础：8 增强：8	硬件隔离与内存加密各厂商根据自身路线选择所支持的特性，当支持其中一个特征时，另一特征作为增强级
		支持内存隔离	基础	2		
		支持 IO 隔离	基础	2		
		支持内存映射表隔离	基础	2		
	内存加密模块	支持内存加密	基础	2		
		内存加密算法合规	基础	2		
		密钥无法被外部环境访问	基础	2		
		支持机密计算不同信任域使用不同密钥	基础	2		
	硬件根密钥	支持根密钥不被替换和篡改	基础	3	基础：5	
		支持根密钥无法被非授权访问	基础	2		
	硬件密码模块	随机数生成质量满足要求	基础	2	基础：4	
		硬件派生密钥满足机密性与完整性	基础	2		
	硬件信任根	信任根防非法替换或篡改	基础	3	基础：3 增强：2	
		具备物理防护机制	增强	2		
系统软件层	可信虚拟化软件	支持创建、销毁 CVM 等	基础	2	基础：4 增强：4 基础（补充）：4 增强（补充）：4	厂商根据技术演进，系统软件支持可信虚拟化或机密计算操作系统 注：厂商不同阶段产品对应技术不同
		支持 CPU、内存、外设等管理	基础	2		
		支持热迁移	增强	2		
		支持访问控制	增强	2		
	机密计算操作系统（补充）	支持系统隔离	基础	2		
		支持机密计算环境与普通计算环境通信	基础	2		
		支持容器化部署与资源隔离管理	增强	2		
		业界专业测评机构认证	增强	2		
系统服务层	隔离计算	支持 CVM 进程间隔离	基础	2	基础：2 增强：4	
		支持 CVM 间隔离	增强	2		
		支持容器间隔离	增强	2		

表A.1 安全保护能力计分方法（续）

架构	模块	功能	等级	单项计分	总分	说明
系统服务层	安全启动	具备安全启动功能	基础	3	基础：6	
		启动链防篡改	基础	3		
	可信度量	基于硬件信任根建立度量	基础	3	基础：3 增强：2	
		支持动态度量	增强	2		
	远程证明	支持挑战应答机制	基础	2	基础：8 增强：2	
		支持对机密计算环境生成报告	基础	2		
		支持对应用程序启动阶段生成报告	基础	2		
		报告基于数字签名体系	基础	2		
		支持对 CVM、机密容器内应用程序度量	增强	2		
	安全存储	支持机密计算环境数据存储到外部	基础	2	基础：6	
		存储到外部数据还原明文有访问控制机制	基础	2		
		存储使用的密钥有机密性和完整性保护	基础	2		
	密码运算	加密算法支持国密与国际算法。每支持一项计 1 分（对称：SM4/AES、非对称：RSA/ECC/SM2、哈希：SHA2/SM3）	基础	6	基础：6	
	密钥管理	应支持密钥生命周期管理	基础	2	基础：4	
		密钥支持真实性与完整性验证	基础	2		
	异构设备互联	支持机密计算环境与 I/O 设备互联，每支持一项加 1 分（I/O 设备包含：网卡、磁盘和加速卡）	基础	3	基础：6 增强:19	
		支持机密计算环境与虚拟化 I/O 设备互联，每支持一项加 1 分（I/O 设备包括：网卡和磁盘）	增强	2		
		I/O 设备通信数据保证机密性或隔离性	基础	3		
		虚拟化 I/O 设备通信数据保证机密性或隔离性	增强	2		
		物理 I/O 设备通信损耗应符合附录 B 测评方法计分，包含：网卡、磁盘、加速卡，分数累加（不同等级的得分应符合 A.2）	增强	9		
		虚拟化 I/O 设备通信损耗应符合附录 B 测评方法计分，包含:网卡虚拟化和磁盘虚拟化，分数累加（不同等级的得分应符合 A.2）	增强	6		
	数据封装	支持数据封装与解封	基础	3	基础：7	
		封装密钥应保证机密性与完整性	基础	2		
		封装的数据只能被授权硬件或应用访问	基础	2		
	安全信道	安全信道数据不被非授权访问与篡改	基础	2	基础：2	
	密码硬件加速	加密加速引擎支持国密与国际算法	基础	3	基础：3	
合计				126	126	

表A.2 异构互联设备通信性能损耗等级及计分方法

性能损耗评价等级	分数
A	3
B	2
C	1
D	0.5
注：性能损耗评价等级划分应符合附录B的规定。	

附 录 B
（规范性）
异构设备互联性能损耗测评方法

B.1 概述

基于可信执行环境的安全计算在业务运行时通常会与网卡、磁盘、加速卡（GPU、NPU、DPU等）等I/O设备进行通信，相比于普通计算环境，可信执行环境往往带来I/O通信效率损耗。为衡量性能损耗，本附录给出了异构设备互联性能损耗测试方法，并对网卡、磁盘、加速卡性能损耗给出评价等级建议。

B.2 网卡性能损耗

B.2.1 测试方法

网卡性能损耗测试方法如下：

a) 普通计算环境与机密计算环境采用相同的配置，包含但不限于 CPU 核数、内存大小等；
b) 在普通计算环境中，使用 iperf3 工具分别测试 TCP 与 UDP 模式通信时长；
c) 在机密计算环境中，使用 iperf3 工具分别测试 TCP 与 UDP 模式通信时长；
d) 多次进行测试后，机密计算环境相比于普通计算环境的通信平均损耗。

B.2.2 评价等级

网卡性能损耗Q评价等级应符合表B.1。

表B.1 网卡性能损耗Q评价等级

网卡性能损耗	评价等级
Q≤15%	A
15%＜Q≤35%	B
35%＜Q≤60%	C
Q＞60%	D

B.3 磁盘性能损耗

B.3.1 测试方法

磁盘性能损耗测试方法如下：

a) 普通计算环境与机密计算环境采用相同的配置，包含但不限于 CPU 核数、内存大小等；
b) 在普通计算环境，分别进行 1M 数据大小顺序写、1M 数据大小顺序读、4K 数据大小随机读、4K 数据大小随机写、4K 数据大小随机 7:3 混合读写、4K 数据大小随机读时延、4K 数据大小随机写时延，测量其读写时间；
c) 在机密计算环境中，分别进行 1M 数据大小顺序写、1M 数据大小顺序读、4K 数据大小随机读、4K 数据大小随机写、4K 数据大小随机 7:3 混合读写、4K 数据大小随机读时延、4K 数据大小随机写时延，测量其读写时间；

d) 多次进行测试后，机密计算环境相比于普通计算环境的通信损耗。

B.3.2 评价等级

磁盘性能损耗Q评价等级应符合表B.2。

表B.2 磁盘性能损耗评价等级

磁盘性能损耗	评价等级
Q≤15%	A
15%＜Q≤35%	B
35%＜Q≤60%	C
Q＞60%	D

B.4 加速卡性能损耗

B.4.1 测试方法

加速卡性能损耗测试方法如下：

a) 普通计算环境与机密计算环境采用相同的配置，包含但不限于 CPU 核数、内存大小等；
b) 预备待加载的推理模型；
c) 在普通计算环境，加速卡加载模型进行推理，测试推理速率；
d) 在机密计算环境中，加速卡加载模型推理，测试推理速率；
e) 多次进行测试后，计算机密计算环境相比于普通计算环境的损耗。

B.4.2 评价等级

加速卡性能损耗Q评价建议等级应符合表B.3。

表B.3 加速卡性能损耗评价等级

加速卡性能损耗	评价等级
Q≤15%	A
15%＜Q≤35%	B
35%＜Q≤60%	C
Q＞60%	D

B.5 设备虚拟化性能损耗

B.5.1 网卡虚拟化性能损耗测试方法

网卡虚拟化性能损耗测试方法如下：

a) 普通计算环境与机密计算环境采用相同的配置，包含但不限于 CPU 核数、内存大小等；
b) 使用网卡虚拟化命令将网卡硬件资源进行隔离，分出多个网卡虚拟设备；
c) 在普通环计算境中，使用 iperf3 工具分别测试虚拟设备 TCP 与 UDP 模式通信时长；
d) 在机密计算环境中，使用 iperf3 工具分别测试虚拟设备 TCP 与 UDP 模式通信时长；
e) 多次进行测试后，机密计算环境相比于普通计算环境的通信平均损耗。

B.5.2 磁盘虚拟化性能损耗测试方法

磁盘虚拟化性能损耗测试方法如下：

a) 普通计算环境与机密计算环境采用相同的配置，包含但不限于 CPU 核数、内存大小等；
b) 使用硬盘虚拟化命令将硬盘硬件资源进行隔离，分出多个硬盘虚拟设备；
c) 在普通计算环境，分别进行 1M 数据大小顺序写、1M 数据大小顺序读、4K 数据大小随机读、4K 数据大小随机写、4K 数据大小随机 7:3 混合读写、4K 数据大小随机读时延、4K 数据大小随机写时延，测量虚拟设备读写时间；
d) 在机密计算环境中，分别进行 1M 数据大小顺序写、1M 数据大小顺序读、4K 数据大小随机读、4K 数据大小随机写、4K 数据大小随机 7:3 混合读写、4K 数据大小随机读时延、4K 数据大小随机写时延，测量虚拟设备读写时间；
e) 多次进行测试后，机密计算环境相比于普通计算环境的通信损耗。

B.5.3 评价等级

机密环境设备虚拟化场景性能损耗Q取“网卡虚拟化性能损耗”和“磁盘虚拟化性能损耗”的较小者，评价建议等级应符合表B.4。

表B.4 设备虚拟化性能损耗评价等级

设备虚拟化性能损耗	评价等级
Q≤15%	A
15%＜Q≤35%	B
35%＜Q≤60%	C
Q＞60%	D

参 考 文 献

[1] GB/T 45230-2025 数据安全技术 机密计算通用框架
[2] GB/T 41388-2022 信息安全技术　可信执行环境 基本安全规范