ICS 35. xxx
CCS Lxx

团　　体　　标　　准

T/ISC XXX—XXXX

安全可信 AI 云电脑能力要求

Requirements for Secure and Trustworthy AI Cloud Computer Capabilities

（征求意见稿）

2025-04-14

2025－04－30 发布　　2025－05－06 实施

中 国 互 联 网 协 会　　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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国互联网协会提出并归口。

本文件起草单位：中国信息通信研究院、阿里云计算有限公司、中移（苏州）软件技术有限公司、联通数字科技有限公司、天翼云科技有限公司、中移(杭州)信息技术有限公司、四川虹微技术有限公司。

本文件主要起草人：。

——

引　言

随着人工智能（AI）与云计算技术的深度融合，AI 云电脑作为创新型信息技术产品，已广泛应用于办公、教育、娱乐等多个领域，显著提升了计算资源利用效率与用户体验。

基于自主基础软硬件构建的安全可信 AI 云电脑，具备数据安全防护能力强、系统自主可控程度高、应用适配兼容性佳等特点，能够有效抵御外部恶意攻击，为党政、医疗等对数据安全和系统可靠性要求严苛的行业提供了智能可信的解决方案，对推动重点行业数字化转型、保障关键领域信息安全具有重要意义。

本文件针对产品厂商研发及行业用户应用安全可信 AI 云电脑过程中面临的主要风险挑战，依据法律法规和行业需求特性，明确技术要求与可信验证机制，厘定产品功能边界，构建基础环境适配、软硬件设施、平台功能的全链条统一标准，规范产品研发、部署应用、服务保障等全生命周期活动。通过安全可信体系建设指引及产品能力量化评估标准，为产业发展提供技术规范，促进市场可持续健康发展。

对本文件中的具体事项，法律法规另有规定的，需遵照其规定执行。

安全可信 AI 云电脑能力要求

1 范围

本文件规定了安全可信 AI 云电脑的整体框架、关键能力指标，从安全可信、产品质量双维度规范产品能力，并给出能力评价的成熟度模型。

本文件适用于从事安全可信 AI 云电脑研发、应用及评价的各类机构。

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 37950—2019 信息安全技术 桌面云安全技术要求

YD/T 3066—2016 电信级虚拟桌面系统 总体技术要求

YD/T 3068—2016 电信级虚拟桌面系统 平台技术要求

YD/T 3067—2016 电信级虚拟桌面系统 终端技术要求

Q/KXY EDCC—XC/C—005—2024 安全可信云电脑技术要求

3 术语和定义

GB/T 37950—2019界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 37950—2019中的某些术语和定义。

3.1

瘦终端 thin client

一种使用处理器、裁剪后的操作系统，可实现对传输协议解码、显示和信息输入，为用户提供云电脑交付的终端设备（3.4）。

[来源：GB/T 37950—2019，3.4，有修改：将原表述中“虚拟桌面”更新为“云电脑”]

注：瘦终端设备形式上不限于云终端盒子、云终端一体机、云终端笔记本、便携屏终端等。

3.2

胖终端 thick client

一种具备通用处理器、本地硬盘、通用操作系统，并可安装云电脑客户端软件的终端设备（3.6）。

[来源：GB/T 37950—2019，3.6，有修改：将原表述中“虚拟桌面”更新为“云电脑”]

注：胖终端设备形式上不限于台式电脑、笔记本、一体机等通用设备。

3.3

安全可信 secure and trustworthy

是对基于自主可控技术构建的信息技术产品或解决方案的描述，指其符合安全可靠要求。

注：本文中意义同“安全可靠”。

3.4

能力成熟度模型 capability maturity model

一种模型，该模型包含一个或多个学科的有效过程的基本要素，并描述了从临时的、不成熟的过程到具有改进的质量和有效性的、受到训练的、成熟的过程的进化改进路径。

[来源：ISO/IEC/IEEE 24765:2017，3.472]

3.5

AI 云电脑 AI cloud computer

一种基于云端虚拟化技术构建的智能终端形态。

注：云端虚拟化指通过虚拟化技术将通用算力、智能算力及智能服务抽象为可动态分配的虚拟资源池，实现跨平台弹性调度与多租户安全隔离。

4 符号和缩略语

下列符号和缩略语适用于本文件。

AI： 人工智能（Artificial Intelligence）
CPU： 中央处理器（Central Processing Unit）
GPU： 图形处理器（Graphics Processing Unit）
SBOM： 软件物料清单（Software Bill of Materials）
IDE： 集成开发环境（Integrated Development Environment）
USB： 通用串行总线（Universal Serial Bus）
HDMI： 高清多媒体接口（High Definition Multimedia Interface）
Type-C：USB Type-C接口（Universal Serial Bus Type-C）
SSL： 安全套接层（Secure Sockets Layer）
TLS： 传输层安全协议（Transport Layer Security）
IPSec： 互联网安全协议（Internet Protocol Security）
RAG： 检索增强生成（Retrieval-Augmented Generation）

5 概述

本文件从安全可信、产品技术要求两个维度对安全可信AI云电脑产品或解决方案能力进行规范，并提供用于评价安全可信AI云电脑能力的成熟度模型。

5.1 安全可信维度

该维度从企业及产品基本信息、设计研发、安全合规、运营保障、生态合作、可持续性等方面规范安全可信AI云电脑产品或解决方案提供方能力。详细条款见第6章 安全可信要求。

5.2 产品技术维度

该维度从环境兼容、终端、网络传输、平台侧、应用生态、安全等方面规范安全可信AI云电脑产品或解决方案技术能力。详细条款见第7章 产品技术要求

5.3 能力成熟度模型

成熟度模型结合安全可信和产品技术两个维度的条款要求，评定安全可信AI云电脑能力成熟度,成熟度评价结果分别为1级（基础级）、2级（增强级）、3级（优秀级），级别越高代表安全可信AI云电脑能力在本标准的条款要求下越优越。详细评价方案见第8章 能力成熟度模型。

6 安全可信要求

6.1 基础信息

6.1.1 企业资质

企业指安全可信AI云电脑产品或解决方案提供方。

a) 注册地、法人、股权结构（最终受益人）等企业基本信息应满足安全可信要求。
b) 应提供近3年无重大违纪违规的声明文件。
c) 资产负债率应不高于XX%，制造业企业应不高于XX%。

6.1.2 产品信息

a) 应具备产品相关软件著作权或专利证书（已在国家知识产权局备案）等知识产权证明材料。
b) 应具备产品使用手册或技术方案等说明文档（软件部分应明确SBOM）。
c) 应具备安全可信环境下的适配测试报告（内容涵盖产品主要功能和基础性能）。

6.2 设计研发

6.2.1 研发团队

a) 应具备不少于XX人规模的自有研发团队，核心成员应具备3年以上安全可信相关经验。
b) 核心技术研发人员应安全可信，且整体团队内外部人员占比不可超过10%，如涉及外部人员，应具备工作报备、记录等保障措施（外部人员指非本机构正式员工，但因业务合作、服务提供或其他工作需要，需临时或长期进入机构场所或访问信息系统资源的个人或团队）。
c) 应具备安全可信技术培训机制，人均年度培训时长不少于40小时。

6.2.2 研发流程

a) 应具备覆盖需求分析、设计、开发、测试、发布的全生命周期研发管理体系。
b) 核心技术代码（如加密算法、底层框架）应100%在安全可信环境下完成研发，禁止依赖外部闭源技术，且核心技术（代码、算法模型）应存储于安全可信环境中。
c) 宜使用安全可信研发工具开展产品研发和管理工作。

6.2.3 环境配套

a) 应至少具备2套基于不同芯片基础架构的安全可信技术栈环境，用于产品的兼容性测试。
b) 测试环境应年度更新至主流安全可信生态最新版本。

6.3 安全合规

6.3.1 安全管理

a) 云平台应具备漏洞分级管理和响应机制，对高危漏洞的修复时间应不超过24小时，中危漏洞不应超过7天。
b) 云平台应通过等保三级或以上认证，并提供年度安全风险评估报告。
c) 云平台应使用安全可信密码算法（如SM2/SM3/SM4）实现核心数据加密。

6.3.2 技术合规

a) 产品源代码自主率应不低于XX%，禁止包含未授权开源代码或境外闭源组件。

注：产品源代码自主率以中国信息通信研究院等国家级检验机构出具的报告为准。

6.4 运营保障

6.4.1 服务保障

a) 应提供7×24小时技术支持服务，一般问题响应时间应不超过4小时，问题解决时间不超过8小时。
b) 产品安全库存应不少于3个月。
c) 应承诺关键行业客户现场服务到达时间不超过8小时（提供声明文件）。
d) 应具备备品备件库。

6.4.2 供应链保障

a) 应具备供应商白名单且具备更新机制，关键元器件供应商应通过安全可信认证。
b) 应具备供应链中断应急方案，确保供应链安全。
c) 供应链中断恢复时间应不超过72小时，因不可抗力导致的延迟需提供第三方证明或权威报道（提供声明文件）。

6.5 生态合作

6.5.1 生态适配

a) 应兼容至少2家主流安全可信技术栈。
b) 宜通过权威机构组织的生态适配认证。

6.5.2 生态共建

a) 应为信创相关生态平台或组织的成员单位，并参与推进信创生态建设。
b) 宜加入至少1个国家级开源社区，并贡献代码或文档。
c) 宜参与安全可信相关标准制定，年度参与数量不少于2项。

6.6 可持续性

6.6.1 可持续发展

a) 年度研发费用占比应不少于15%。
b) 应具备产品版本迭代计划，年度至少发布2版次主版本更新。
c) 应具有核心技术演进路线图，确保3年内关键技术全部实现安全可信。
d) 应承诺产品支持周期不低于6年。

7 产品技术要求

7.1 基础环境兼容性要求

7.1.1 云终端

a) 应基于安全可信CPU、操作系统构建云终端。
b) 应支持国密安全芯片TCM2.0标准。

7.1.2 云平台

a) 应基于安全可信CPU、GPU、操作系统、云操作系统构建平台侧能力。
b) 应兼容至少2种安全可信操作系统镜像及虚拟桌面，操作系统版本需涵盖最新2个主版本。

7.2 云终端能力要求

7.2.1 云终端多样性

a) 应支持多种类型的安全可信终端设备，包括胖终端、瘦终端。

7.2.2 外设丰富度

a) 应支持鼠标、键盘、显示器、打印机、扫描仪、摄像头、麦克风、外部存储设备等。

7.2.3 接口丰富度

a) 应支持USB、RJ45、电源接口；音频接口类型支持3.5mm孔径3段式或4段式接口；视频接口类型应至少支持VGA、HDMI、DVI、DP、Type-C中1种显示接口，若提供HDMI、DP、Type-C作为显示接口，应支持音频和视频同步输出。

7.2.4 终端核心软件

a) 应支持可进行界面操作的BIOS并支持更新、回滚、密码设置等核心功能。
b) 固件应支持升级、信息查看、设置口令、设置网络引导等功能。
c) 所有预装软件应满足安全可信要求。

7.2.5 终端核心硬件

a) 应支持网络连接、网络开启/关闭功能，宜支持无线网络连接；
b) 宜支持L2HC高清音频编解码标准，可根据采购人实际使用需求支持蓝牙模块物理拆卸功能。

7.3 网络传输要求

7.3.1 传输协议

a) 宜支持数据完整性传输，支持SM3/HMAC等国密算法，密钥长度不少于128位。
b) 应支持基于UDP的高效传输协议，以减少网络延迟并提高数据传输效率。

7.3.2 低时延

a) 延迟应小于200ms（100Mbps 网络）；延迟应小于100ms（500Mbps 网络）；延迟应小于50ms（万兆网络）。

7.4 平台能力要求

安全可信AI云电脑平台能力从云电脑基础能力和AI能力两个维度进行规范，AI能力进一步划分为AI支撑能力、AI服务能力、AI定制化能力三个层次。

7.4.1 云电脑基础能力

a) 应支持云电脑、网络、存储管理功能，实现对云电脑的全生命周期管控。
b) 应支持用户管理（包含多租户管理）、权限管控等功能，支持云电脑运营管理。
c) 应支持镜像、模板等云电脑部署和运维相关能力。
d) 应具备日志、资源监控告警等审计监控能力。

7.4.2 AI 支撑能力

a) 应具备AI云电脑基础模型，且具备对模型的开发、优化等能力。
b) 应具备可本地化部署大模型能力，包括第三方大模型。
c) 应具备拓展可接入多种大模型能力。
d) 应支持智能体调用不同模态的大模型，支持平滑切换。
e) 应支持智能体的长短期记忆存储，可在复杂任务中存储信息、调用会话记录等。
f) 应支持对智能体开发模板进行自定义及相应操作。
g) 应具备多种智能体开发方式，如无代码方式、低代码方式、全代码方式。
h) 应支持智能体的开发调试，提供智能体功能预览能力，使开发者在正式发布前可体验智能体的效果，支持预览调试和中间步骤结果展示。
i) 应支持对智能体的效果进行评估，支持自定义或上传效果评测数据集，对评测结果进行分析。

7.4.3 AI 服务能力

a) 应至少具备1个垂直行业领域AI应用市场解决方案。
b) 应具备基于大模型，可支持语音、图像、文档等信息输入的智能解析、智能问答等AI基础能力。
c) 应支持对智能体的版本进行迭代和优化。
d) 应支持依据已创建智能体的名称、类型、描述、创建时间、更新时间、创建者、状态信息等信息进行查询检索。
e) 应支持对智能体在公有市场、私有市场的上下架进行管理。
f) 应支持对智能体服务进行选择性服务启用及停用。
g) 应支持将智能体能力以API等形式对外发布，对接到其他系统。
h) 应支持多种 AI 服务的组合和编排，满足用户复杂的业务需求。

7.4.4 AI 定制化能力

a) 应支持RAG增强框架，具备基于私域知识定制化AI的能力。
b) 应支持面向企业用户构建专属AI应用，如：企业AI助手。
c) 应支持提供不同的开发组件和工具，支持文档处理、数据处理、数据分析、报告生成、图表生成等组件模块.
d) 应具备知识导入功能，支持txt、doc、docx、xlsx等主流文档格式导入，支持文档批量上传，支持外部链接、在线文档知识导入。
e) 应支持基于文档知识库进行检索问答、知识溯源等能力。

7.5 应用生态要求

7.5.1 应用管理能力

a) 应支持应用管理能力，支持对应用全声明周期管理。
b) 应具备应用的性能监控和分析功能，以及时发现和解决应用运行中的问题。

7.5.2 AI 应用丰富度

a) 应原生具有涵盖办公、教育、政务、生活、娱乐等多领域AI应用。
b) 生态AI应用应涵盖办公、教育等多领域。

7.5.3 开发者工具丰富度

a) 应支持AI开发全流程工具链。
b) 应具备完善的开发者社区和技术支持。

7.6 安全能力要求

7.6.1 数据安全

a) 应确保数据加密存储与传输。
b) 应具备数据备份与恢复机制，保障数据完整性。
c) 应支持用户数据隔离的能力。
d) 应支持对数据的分类分级管理，根据不同级别数据采取相应的加密和访问控制措施。

7.6.2 隐私安全

a) 应提供用户数据自主管理，包括查询、更新、删除、撤回授权等。
b) 应支持隐私政策透明化与用户同意机制。
c) 应支持第三方数据共享管控。

7.6.3 合规性

a) 生成式人工智能相关功能或应用应符合《生成式人工智能服务管理暂行办法》要求（提供声明文件）。

7.6.4 安全管控与防护

a) 应支持多级访问控制、多因素访问控制与权限管理能力。
b) 应支持病毒查杀、漏洞扫描、补丁修复等安全加固能力。
c) 应支持网络流量、用户操作日志、系统异常等安全监控与审计能力。
d) 宜具备网络中断、数据泄露、系统崩溃的应急响应预案，且每年开展1次应急演练，确保业务连续性。

8 能力成熟度模型

能力成熟度模型依据安全可信要求（6）和产品技术要求（7）中规定的能力指标，将安全可信AI云电脑能力成熟度划分为3个等级，分别是：1级（基础级）、2级（增强级）、3级（优秀级），级别越高代表安全可信AI云电脑能力在本标准的条款衡量下越优越。

8.1 成熟度定义

表 1 安全可信 AI 云电脑能力成熟度定义

级别	名称	定义
1 级	基础级	该级别满足安全可信要求的基础上具备基础的 AI 支撑和服务能力，能够为用户提供基础的 AI 应用并能够保障基本安全。
2 级	增强级	该级别满足安全可信要求的基础上能够提供更完善的 AI 支撑和服务能力，初步具备 AI 定制化能力，能够为用户提供较为丰富的 AI 应用，安全保障达到较高水平。
3 级	优秀级	该级别满足安全可信要求的基础上具备完备的 AI 支撑、服务以及定制化能力，能够为普通用户和开发者用户提供丰富的 AI 应用满足其日常办公、开发等各方面需求，同时，数据、隐私等方面的安全保障表现优秀。

8.2 成熟度评价方法

依据本标准内容，通过材料审查与产品能力测试相结合的方式验证安全可信AI云电脑的能力水平，各等级（见表1）具体评价方法如下：

表 2 安全可信 AI 云电脑能力成熟度评价方法

级别	评价方法
1 级	1、安全可信要求 — 安全可信要求（6）满足率：100%。 2、产品技术要求 — 基础环境兼容性要求（7.1）满足率：100%； — 云终端能力要求（7.2）满足率：100%； — 网络传输要求（7.3）满足率：100%； — 平台能力要求（7.4）满足率：电脑基础能力（7.4.1）满足率：100%；其他（7.4.2-7.4.4）满足率：50%； — 应用生态要求（7.5）满足率：50%； — 安全能力要求（7.6）满足率：60%；
2 级	1、安全可信要求 — 安全可信要求（6）满足率：100%。 2、产品技术要求 — 基础环境兼容性要求（7.1）满足率：100%； — 云终端能力要求（7.2）满足率：100%； — 网络传输要求（7.3）满足率：100%；

	— 平台能力要求（7.4）满足率：电脑基础能力（7.4.1）满足率：100%；其他（7.4.2-7.4.4）满足率：75%； — 应用生态要求（7.5）满足率：75%； 安全能力要求（7.6）满足率：80%；
3级	1、安全可信要求 — 安全可信要求（6）满足率：100%。 2、产品技术要求 — 基础环境兼容性要求（7.1）满足率：100%； — 云终端能力要求（7.2）满足率：100%； — 网络传输要求（7.3）满足率：100%； — 平台能力要求（7.4）满足率：电脑基础能力（7.4.1）满足率：100%；其他（7.4.2-7.4.4）满足率：95%； — 应用生态要求（7.5）满足率：95%； 安全能力要求（7.6）满足率：95%；

参 考 文 献

[1] ISO/IEC 24765:2017 Systems and software engineering — Vocabulary