ICS 35.020
CCS L70

团　　体　　标　　准

T/ISC 0105—2026

可信智能体空间建设指南
第1部分：总体架构与安全要求

Guidelines for the Construction of Trusted Agent Space
Part 1: Overall Architecture and Security Requirements

（发布稿）

2026－05－11 发布　　2026－06－11 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。

本文件由中国互联网协会提出并归口。

本文件起草单位：清雁科技（北京）有限公司、中国信息通信研究院、北京航空航天大学、山东省征信有限公司、山东港口阳光慧采服务有限公司、中国交通信息科技集团有限公司、上海明品医学数据科技有限公司、河北清华发展研究院、中国民航科学技术研究院、北京数据集团有限公司、山东云天安全技术有限公司、国家管网集团北方管道有限责任公司、润泽河北算力产业技术研究院、南方电网数据平台与安全（广东）有限公司。

本文件主要起草人：汤珂、王远、赵富春、王理、赵志通、姚娟娟、高柳村、王少伟、韩鹏、潘彤、李伟、周煜坤、张超群、王楹、高凯、李怡慧、冯森、吕荣男、蔡华利、于丁垚、李峰、程志忠、李荣光、冯永强、张秀芳，胡华、卢有飞，杨光。

引　言

本标准立足我国智能体技术与数据空间融合发展的现实需求，围绕“可信智能体空间”的核心理念，提出了涵盖平台功能、数据管理、算网协同、智能体协同、可信机制及治理监管等方面的总体架构与安全要求。通过引入确定性网络、可信执行环境、区块链存证、隐私计算、零信任安全等关键技术，构建覆盖“数据—智能体—算力—网络”全要素的可信协同环境，为智能体在跨域、异构、高并发场景下的安全运行与高效协同提供系统性技术指导。

1. 范围

本文件规定了可信智能体空间的总体架构、功能组件、安全机制、业务流程及评估方法等技术要求。

本文件适用于基于确定性网络的智能体可信数据空间的设计、开发、部署及验收，为政府机构、行业用户和第三方评估机构提供技术依据。

本文件不规定数据传输范围，若涉及数据跨境存储和传输，必须严格遵守中华人民共和国相关法律法规，如《数据出境安全评估办法》（国家互联网信息办公室令第11号）等。

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 1.1—2020 标准化工作导则 第1部分

GB/T 22239—2019 网络安全等级保护基本要求

GB/T 35273—2020 个人信息安全规范

GB/T 37737—2019 云计算分布式块存储系统总体技术要求

GB/T 44109—2024 数据治理实施指南

GB/T 45574—2025 敏感个人信息处理安全要求

IEEE 802.1 TSN 系列标准

ITU-T Y.1564 确定性网络性能测试方法

GB/T 37737-2019 信息技术 云计算 分布式块存储系统总体技术要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 44109-2024 信息技术 大数据 数据治理实施指南

GB/T 45574-2025 数据安全技术 敏感个人信息处理安全要求

GB/T 38627—2020 多方安全计算技术规范

ISO/IEC 27001:2013 信息安全管理体系

TC609—6—2025—01 可信数据空间 技术架构

NDI—TR—2025—01 数据基础设施 参考架构

IEEE 2755-2017 Agent Communication Language (ACL) Framework

W3C DID 1.0 Decentralized Identifiers

3. 术语和定义

下列术语和定义适用于本文件。

3.1 智能体 Agent

能够在可信数据空间内自主感知环境、基于内置算法或外部策略进行决策、调用算力资源并完成与其他智能体或人类用户协同任务的软件实体。

3.2 可信数据空间 Trusted Data Space；TDS

面向智能体全生命周期，通过确定性网络、可信计算、隐私计算与区块链等技术，为数据存储、流通、处理与算力调度提供“安全、可控、协同、可追溯”服务的一体化环境。

3.3 确定性网络 Deterministic Network；DetNet

通过资源预留、时间同步、流量整形、冗余路径等手段，为特定业务流提供可预期、可验证的端到端时延、抖动和带宽保障的网络技术体系。

3.4 算网协同 Compute-Network Synergy

依据任务实时需求、算力分布及网络状态，在云、边、端之间动态调度计算与网络资源，并实现 SLA 级服务质量保障的机制。

3.5 数字身份证书 Digital Identity Certificate

由可信认证机构签发、包含智能体唯一标识、属性声明及权限策略，并通过密码学手段保证不可伪造、不可抵赖的加密凭证。

3.6 数据确权 Data Provenance

对数据产生、流转、加工、使用、销毁全生命周期进行权属标识、时间戳记录与可追溯验证的过程。

3.7 智能体确权 Agent Provenance

对智能体的开发、部署、运行、更新、退役全过程进行权属标识、版本管理、行为记录与责任追溯的机制。

3.8 网络切片 Network Slicing

在共享物理网络上通过虚拟化技术划分出多个逻辑隔离的网络实例，为不同业务提供差异化 SLA 的能力。

3.9 可信执行环境 Trusted Execution Environment；TEE

在主处理器内部或旁路提供的硬件级隔离区域，用于安全地执行敏感代码与处理机密数据。

3.10 差分隐私 Differential Privacy

通过向数据或查询结果添加受控噪声，使得单个记录的变化不会显著影响输出结果，从而在统计可用性与个体隐私之间提供可量化保障的隐私保护技术。

3.11 同态加密 Homomorphic Encryption

允许在密文域直接进行特定运算，运算结果解密后等价于在明文域执行相应运算的加密体系。

3.12 QoS SLA 绑定 QoS SLA Binding

将确定性网络的时延、抖动、带宽 SLA 与数据空间的服务等级协议进行映射、监测、计费和违约处置的全过程。

4. 缩略语

下列缩略语适用于本文件。

DetNet：确定性网络（Deterministic Network）

DID：去中心化标识符（Decentralized Identifier）

HL7：健康信息交换标准（Health Level Seven）

MQTT：消息队列遥测传输（Message Queuing Telemetry Transport）

NFT：非同质化通证（Non-Fungible Token）

SLA：服务等级协议（Service Level Agreement）

SRv6：IPv6段路由（Segment Routing over IPv6）

TEE：可信执行环境（Trusted Execution Environment）

TSN：时间敏感网络（Time-Sensitive Networking）

5. 概述

可信数据空间以智能体为核心，以确定性网络为传输底座，通过分布式存储、区块链存证、可信计算、隐私计算、算网协同调度等关键技术，构建覆盖“数据-智能体-算力-网络”全要素的安全可控环境。其目标是在跨域、异构、高并发场景下，实现数据的可信流通、智能体的可信协同、算力的高效利用以及服务的确定性保障，支撑政府治理、工业互联网、智慧城市、车联网、元宇宙等关键领域的数字化转型。可信数据空间打破传统数据孤岛，采用数字身份与确权机制确保每一次数据调用与算力调度都可验证、可追溯、可追责；同时通过 DetNet 技术保障毫秒级甚至亚毫秒级的实时业务需求，实现“东数西算”等国家战略工程的技术落地。

6. 技术要求**功能要求**

1.1.1 平台功能

可信数据空间需要具有平台功能。

a）支持智能体注册、注销、身份认证与权限管理；

b）支持检查分类：常规智能体、实时控制智能体、批处理智能体；

c）支持会诊关系配置：跨域智能体协同策略、分组管理；

d）支持费用管理：算力、网络、存储计费模型；

e）支持模板管理：策略模板、诊断术语库、隐私策略库；

f）支持危急值设置：异常行为、延迟超限、资源耗尽等预警；

g）支持质控方案：数据完整性、一致性、时效性评分；

h）支持统计报表：算力利用率、网络时延、数据调用量；

i）支持预约登记：任务优先级、资源预留、时隙管理；

j）支持单点登录：与国家/行业身份认证平台对接。

1.1.2 数据层功能

a）分布式存储：多副本、纠删码；

b）区块链存证：交易、权属、日志不可篡改；

c）数据分级：冷、温、热多级存储策略；

d）数据版本：时间戳、哈希校验、差异对比。

6.1.3 控制层功能

a）策略引擎：基于属性的动态授权；

b）智能合约：自动触发数据交换、费用结算；

c）审计日志：全生命周期可追溯；

d）合规检查：敏感数据识别、跨境合规判断。

1.1.3 算力层功能

a）云-边-端三级调度：任务粒度、亲和性、优先级；

b）异构算力抽象：CPU/GPU/FPGA/NPU 统一描述；

c）弹性伸缩：水平扩展、垂直扩展、突发资源池。

1.1.4 网络层功能

a）DetNet 管道：时延、抖动、带宽 SLA 绑定；

b）网络切片：点到点、点到多点、点到平台；

c）协议栈：TSN/SRv6/DetNet 统一封装；

d）实时监控：链路状态、队列深度、路径可视化。

1.1.5 智能体协同功能

a）请求-响应：同步调用、超时重试；

b）发布-订阅：主题管理、消息持久化；

c）任务编排：DAG 工作流、失败回滚；

d）资源协商：算力竞价、网络预留。

1.1.6 可信引擎功能

a）可信根：TEE 启动度量、远程证明；

b）密钥管理：生成、分发、轮换、撤销；

c）隐私计算：差分隐私、同态加密、安全多方计算；

d）证据链：日志链式存储、跨链互认。

1.1.7 治理监管功能

a）合规策略：数据分级分类、跨境审批；

b）风险评分：异常访问、资源异常；

c）报表输出：PDF/JSON/XML，定时推送；

d）API 接口：第三方监管系统对接。

1.2 性能要求

1.2.1 网络性能

——端到端时延分级：Level-1<1 ms、Level-2<5 ms、Level-3<20 ms、Level-4<100 ms、Level-5<500 ms；

——抖动：≤10 μs（工业控制场景）；

——带宽保障：≥1 Gbps（可切片升级至 100 Gbps）。

1.2.2 软件性能

——并发智能体：≥100 000；

——P99 响应：≤200 ms；

——云端热升级：零中断，灰度窗口≤30 s。

1.2.3 存储性能

——亿级数据秒级检索；

——异地多活 RPO=0，RTO<30 s；

——加密存储：AES-256，SM4 可选。

6.3 安全要求

1.2.4 系统安全

——等级保护≥三级；

——年度渗透测试≥1 次；

——漏洞响应≤24 h。

1.2.5 数据安全

——传输：TLS1.3、国密 SM9；

——存储：加密、匿名化、脱敏；

——密钥：HSM、D-H 轮换周期≤90 天。

1.2.6 网络安全

——零信任架构；

——微隔离、DDoS 防护≥500 Gbps；

——7×24 SOC、AI 异常检测。

1.2.7 用户信息安全

——注册/注销、权限最小化；

——敏感信息静态脱敏；

——访问审计≥180 天。

1.3 平台服务能力要求

1.3.1 完备性

——覆盖 6.1 全部条款；

——故障记录、演练、报告自动生成。

1.3.2 可靠性

——MTBF ≥ 100 000 h；

——故障自恢复 ≤ 30 s。

1.3.3 稳定性

——在线率 ≥ 99.99%；

——灰度发布、回滚策略。

1.3.4 可维护性

——统一运维门户；

——一键升级、在线诊断。

1.3.5 可扩展性

——水平扩展≥10 倍；

——兼容主流 OS、数据库、云平台。

1.3.6 易用性

——图形化驾驶舱；

——低代码流程编排；

——在线帮助与培训体系。