ICS 35.240
CCS L80

团　　体　　标　　准

T/ISC XXX—XXXX

系统智能体权限管理技术要求

Technical Requirements for System Agent Permission Management

在提交反馈意见时，请将您知道的相关专利与支持性文件一并附上。

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 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：××××、××××。

本文件主要起草人：×××、×××。

系统智能体权限管理技术要求

1 范围

本标准规定了系统智能体在权限管理、数据访问控制、外部工具扩展能力等方面的技术要求和规范。

本标准适用于系统智能体（包括手机智能体和PC智能体）的设计、开发和测试。本标准涵盖系统智能体在运行过程中对系统资源、用户数据、第三方应用及外部服务的访问控制要求。

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 35273-2020 信息安全技术 个人信息安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

系统智能体 System Agent

与终端硬件和操作系统深度融合，主要基于终端自身感知、算力、存储、安全能力，通过纯端侧 AI 模型或以端云结合 AI 模型理解用户意图和决策，并自主执行任务的智能体。

3.2

外部工具 External Tool

系统智能体通过标准化接口调用外部服务或执行特定功能的扩展机制。外部工具可由操作系统、第三方应用或独立开发者提供，用于扩展系统智能体的功能边界。

3.3

外部服务 External Service

部署于本地设备之外的远程服务能力，包括云端大模型推理、第三方Web API、跨设备数据同步等服务。

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

5 权限分层模型

5.1 系统控制权限

系统控制权限指访问操作系统核心功能、影响系统安全运行的能力，包括屏幕录制与截图、按键模拟与注入、系统通知读取与拦截、系统设置修改、后台进程管理、系统级无障碍服务等。

系统控制权限应实施最严格的管控。涉及系统控制权限的操作应进行授权，并在执行前向用户明确告知风险。

5.2 跨应用权限

跨应用权限指系统智能体跨应用进行数据交互和功能调用的能力，影响范围为设备上的其他应用，包括跨应用启动与界面解析、应用间数据传递、通过标准化接口与其他应用交互、跨应用任务编排与协作等。

系统智能体通过标准化接口与其他应用进行交互时，应遵循目标应用的安全策略。

5.3 数据访问权限

数据访问权限指访问用户隐私数据的能力，影响范围为用户个人隐私，包括通讯录与联系人、短信与通话记录、相册与媒体文件、位置信息、日历与日程、健康医疗数据、生物特征信息、金融账户信息等。

数据访问权限的管控应建立体系化的安全机制，从以下四个维度实施：数据分类分级体系、访问控制原则、脱敏与保护措施、用户权利保障。

5.3.1 数据分级分类

系统智能体访问的数据应按照敏感程度进行分类分级管理：

a) 公开数据：指系统已公开的非敏感信息，如当前时间、设备电量、网络状态等。此类数据对系统安全和用户隐私无影响，可允许系统智能体在无需授权的情况下访问。
b) 业务数据：指应用运行过程中产生的业务相关数据，如订单信息、物流状态、聊天记录等。此类数据虽不涉及核心隐私，但具有业务敏感性，应实施受限访问管控。
c) 敏感数据：指涉及用户隐私的核心个人数据，包括身份证号、生物特征信息、金融账户信息、精确位置信息、健康医疗数据等。对此类数据的访问应实施严格管控，采用授权机制。
d) 核心数据：指影响系统安全运行的关键数据，如系统密钥、根证书、加密算法参数、安全策略配置等。此类数据的访问应仅限于系统核心组件，禁止系统智能体直接访问。

5.3.2 数据访问控制原则

系统智能体的数据访问应遵循以下原则：

a) 最小必要原则：系统智能体仅能访问完成特定任务所必需的数据，禁止超范围收集和使用数据。
b) 目的限定原则：数据使用目的应在授权时明确告知用户，且不得超出授权目的范围使用数据。
c) 时效限制原则：数据访问权限应设置有效期限，过期后自动失效。
d) 范围限制原则：应明确数据访问的应用范围（单个应用或多个应用）和设备范围（本地设备或跨设备）。跨设备数据传输应获得用户单独授权。

5.3.3 数据脱敏与保护

系统智能体应对数据采取脱敏与安全保护措施，具体要求如下：

a) 展示脱敏：敏感数据在用户界面展示时应进行脱敏处理。
b) 传输保护：敏感数据在传输过程中应使用加密通道，并实施端到端加密。
c) 存储安全：敏感数据本地存储时应进行加密，加密密钥应存储在安全区域。禁止以明文形式存储密码、令牌、密钥等敏感信息。临时缓存数据应及时清理。

5.3.4 用户数据权利保障

系统应保障用户对其个人数据的以下权利：

a) 知情权：系统智能体访问数据前，应以清晰、明确、易懂的方式告知用户访问目的、数据类型、使用范围、存储期限等信息。告知内容应避免使用晦涩的技术术语。
b) 选择权：用户应能自主选择是否授权、授权范围、授权期限。系统应支持用户对不同数据类型分别授权，禁止采用捆绑授权方式强制用户接受所有权限请求。
c) 撤回权：用户应能随时撤回已授予的权限，撤回操作应简便易行。权限撤回后，系统智能体应立即停止相关数据的访问，已获取的数据应在合理期限内删除或匿名化
d) 删除权：用户可要求删除系统智能体已获取的个人数据，系统应在验证用户身份后及时执行删除操作，并确认删除完成。删除操作应包括本地存储数据和云端同步数据。

5.4 外部服务权限

外部服务权限指系统智能体访问本地设备之外的远程服务能力，影响范围为数据外泄风险，包括云端大模型服务调用、第三方Web服务/API接入、跨设备数据同步、远程数据存储与备份、实时信息查询服务等。此类权限应重点防范数据泄露和恶意网络行为，敏感数据向外部传输应获得用户单独授权，并采用端到端加密保护。

外部工具是智能体调用外部服务的主要载体，其权限管控应覆盖接入、运行、安全三个关键环节。

5.4.1 外部工具接入管理

外部工具接入系统智能体生态时，应满足以下管理要求：

a) 注册与审核：外部工具在接入系统智能体生态前，应完成注册并通过安全审核，包括开发者身份验证、工具功能审查、代码安全扫描、隐私政策合规性检查等。。
b) 能力声明：外部工具应明确声明其功能范围、所需权限、数据访问需求等。
c) 版本管理：外部工具应实施版本控制，新版本发布前应重新进行安全审核。
d) 签名验证：外部工具应使用数字签名进行完整性保护，禁止加载未签名或签名验证失败的外部工具。

5.4.2 外部工具运行管控

外部工具运行过程中，操作系统应实施以下运行管控措施：

a) 沙箱隔离：外部工具应运行在独立的沙箱环境中，与系统核心区域和其他工具隔离。
b) 资源限制：系统应对外部工具的 CPU 占用、内存使用、存储空间、网络流量等资源实施限制。
c) 超时控制：外部工具调用应设置超时时间，超时后自动终止调用并返回错误。
d) 日志审计：系统应记录外部工具运行的完整日志，包括调用时间、调用参数、执行结果、资源消耗等。

5.4.3 外部工具权限安全要求

外部工具权限应满足以下安全要求：

a) 权限收敛：外部工具应仅能获取其功能所必需的最小权限。
b) 动态管控：系统应支持运行时动态调整外部工具权限。

6 权限生命周期管理

系统智能体的权限应实施全生命周期管理，包括权限申请、权限授予、权限使用和权限回收四个阶段。

6.1 权限申请

系统智能体在首次使用某项能力前，应向操作系统和用户发起权限申请。申请内容应包括权限类型、使用目的、使用范围、有效期限等要素。高风险权限应提供详细的风险说明。

6.2 权限授予

权限授予可采用系统默认授权、用户主动授权、动态按需授权等方式。涉及敏感数据或高风险操作的权限，必须获得用户的明确同意。用户应能自主选择授权范围，支持部分授权或带条件授权。

权限授予还应符合以下要求：

a) 授权提示：权限申请时应向用户展示清晰、明确的提示界面，包含权限名称、使用场景、使用目的、风险等级等信息。
b) 风险告知：对于高风险权限，应在授权前进行专项风险告知，说明可能的风险后果和防护措施。
c) 精细化授权：系统应提供精细化授权选项，允许用户对权限进行单独设置。可支持用户一键授权常用权限组合，但不应强制捆绑授权。
d) 场景化授权：授权提示应与使用场景关联，在用户触发相关功能时动态申请权限。

6.3 权限使用

系统智能体在使用权限过程中，应实施实时监控和日志记录。操作系统应限制权限的使用频率、使用时段和使用场景，防止权限被滥用。当系统智能体进入后台或休眠状态时，应自动暂停敏感权限的使用。

a） 权限面板：系统应提供统一的系统智能体权限管理入口，集中展示各系统智能体的权限状态、使用记录、授权历史等信息。
b） 实时提示：当系统智能体正在使用敏感权限时，系统应在状态栏或通知区域进行实时提示。
c） 使用记录：系统应记录系统智能体的权限使用历史，包括使用时间、使用权限、使用目的、操作结果等，供用户查询和审计。

6.4 权限回收

权限回收机制包括：用户手动回收、系统智能体自动释放、异常触发回收（如检测到异常行为）。权限回收应及时生效，并通知相关方。

参　　考　　文　　献

[1] ISO/IEC 27001:2022 信息安全管理体系要求
[2] ISO/IEC 27701:2019 隐私信息管理体系要求