《系统智能体权限管理技术要求》标准编制说明

标准起草小组

1.标准范围

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.工作简况

3.标准编制原则和确定标准主要内容

本标准依据《标准化工作导则 第1部分：标准化文件的结构和起草规则》（GB/T 1.1-2020）编制。本标准规定了系统智能体的权限分层模型、权限生命周期管理等技术要求，适用于系统智能体（含手机智能体、PC智能体）的设计、开发与测试，可为终端厂商、操作系统厂商、应用开发者、安全评估机构提供权限管理技术规范与合规依据。

本标准核心内容包括：1.权限分层模型：构建系统控制权限、跨应用权限、数据访问权限、外部服务权限的四层管控体系，明确各层级权限边界与管控强度。2.数据访问安全：建立数据分类分级、访问控制原则、脱敏保护与用户权利保障机制，强化隐私数据全流程安全。3.外部服务与工具安全：规范外部工具接入审核、运行管控、权限安全要求，防范外部调用带来的数据泄露与恶意行为风险。4.权限生命周期管理：覆盖权限申请、授予、使用、回收全流程，明确精细化授权、实时监控、异常熔断与权限自动失效要求。

4.主要试验(或验证)的分析、综述报告

无。

5.标准在起草过程中遇到的问题及解决办法；重大分歧意见的处理经过和依据；有无重要技术问题需要说明

在本文件的修订过程中，无重大分歧意见和技术问题。

6.与国外标准的关系：包括：采用国际标准和国外先进标准的程度，与国外标准主要技术内容的差异

该项目没有对应的国际标准或国外先进标准。

7.修订标准时，说明与标准前一版本的重大技术变化，并列出所涉及的新、旧版本的有关章条(可引用标准前言的内容)；废止/代替现行有关标准的建议

不涉及。

8.说明标准与其他标准或文件的关系(可引用标准前言的内容)，特别是与有关的现行法律、法规和强制性国家标准的关系

符合现行法律、法规要求。

9.标准作为强制性标准或推荐性标准的建议

建议本文件作为推荐性标准。

10.贯彻国家标准的要求和措施建议(包括组织措施、技术措施、过渡办法等内容)；标准发布后，对国内外业界可能产生的影响

建议本文件作为推荐性标准发布实施。

本标准旨在规范系统智能体权限管理全流程技术要求，覆盖权限分层、权限申请、权限授予、权限使用与权限回收等关键环节，明确安全基线、管控规则与用户权益保障机制。

随着系统智能体在手机、PC 等终端广泛应用，其跨应用、跨系统、自主执行的运行特性显著扩大了权限攻击面，面临越权操作、隐私数据泄露、后台静默调用、外部工具恶意接入等特有风险，现有操作系统与应用权限标准无法完全覆盖，制定专用规范势在必行。本标准的必要性在于落实个人信息保护与数据安全合规要求，解决权限滥用、行为不可控、用户权益保障不足等难题，为产品研发、安全测试、合规评估提供技术依据。

通过规范权限分层及权限全流程管控，指导开发者构建可信、可控、可追溯的系统智能体。实施本标准有助于提升行业整体安全治理水平，降低权限滥用与隐私泄露风险，保障用户知情权、选择权与决策权，增强用户对系统智能体服务的信任，促进系统智能体技术生态的安全、可控与健康发展。

11.标准是否涉及知识产权的情况说明；如标准中含有自主知识产权，说明产品研发程度、产业化基础及进程

本文件未涉及。

12.其他应予说明的事项

本文件未涉及。