ICS 35.020
I65

T/SIA

中 国 软 件 行 业 协 会 团 体 标 准

T/SIA 050—2025

移动互联网服务可访问性安全要求

Security Requirements for Accessibility of Mobile Internet Services

2025-4-3 发布　　2025-4-3 实施

中 国 软 件 行 业 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。

本文件由中国软件行业协会提出并归口。

本文件起草单位：北京邮电大学、中国联合网络通信集团有限公司、联通云数据有限公司、天翼安全科技有限公司、北京航空航天大学、北京交通大学、中国科学院自动化研究所、北京中软国际信息技术有限公司、北京软件和信息服务业协会。

本文件主要起草人：徐国胜、王晨宇、李朝霞、刘金春、康和、卢光明、谭火彬、陈乃月、陈波、王晓华、张磊。

移动互联网服务可访问性安全要求

1 范围

本文件描述了移动互联网服务可访问性安全框架和安全风险，提出了无障碍技术安全要求、智能体技术安全要求、操作系统安全要求以及用户权益保护要求等内容。

本文件适用于所有访问移动互联网服务的技术和产品，以及提供相关技术、产品和服务的各类主体。

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 37668-2019 信息技术 互联网内容无障碍可访问性技术要求与测试方法

GB/T 42884-2023 信息安全技术 移动互联网应用程序（App）生命周期安全管理指南

ISO/IEC 22989:2022 信息技术 人工智能 人工智能概念和术语（Information technology-ArtificiAI intelligence-ArtificiAI intelligence concepts and terminology）

3 术语和定义

GB/T 37668-2019、GB/T 42884-2023 中界定的以及下列术语和定义适用于本文件。

3.1

可访问性 accessibility

通过无障碍、智能体等技术手段使得互联网内容对于用户（包括残疾人、老年人和其他用户）具备内容本身可感知、内容中的界面组件可操作，内容和控件定义可理解。

[来源：GB/T 37668-2019，2.2，有修改]

3.2

智能体 artificial intelligent agent

能够感知和响应环境并能执行操作以完成其目标的自动化实体。

[来源：ISO/IEC 22989:2022，3.1.1，有修改]

注：本文件中指通过获取系统无障碍服务等系统权限访问 APP 执行特定任务的智能体，可以是软件、硬件或其他实体。

3.3

移动互联网应用程序 mobile internet application

运行在移动智能终端上向用户提供信息服务的应用软件。

注：简称 App。

[来源：GB/T 42884-2023，3.2，有修改]

4 移动互联网服务可访问性安全框架

移动互联网服务可访问性是指通过无障碍、智能体等技术手段的运用，优化用户交互过程，使得更多人群（包括老年人、残障人士等群体）能够享受移动互联网提供的便利和服务。随着 AI 大模型技术的发展，智能体能够执行各种各样的任务，进一步优化了交互过程，提升了移动互联网服务可访问性，同时也引入了新的安全风险。

移动互联网服务可访问性安全包括无障碍技术安全、智能体技术安全、操作系统安全、用户权益保护等内容，整体框架如图 1 所示。

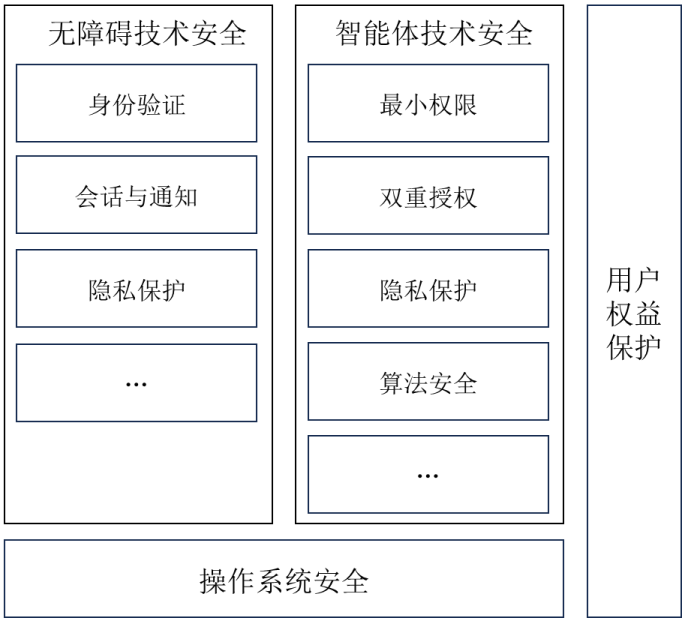

图1 移动互联网服务可访问性安全框架

5 移动互联网服务可访问性安全风险

5.1 无障碍技术安全风险

无障碍技术安全风险，包括如下内容：

a)人机交互流程简化，导致缺少必要的身份验证环节。这使得 App 更容易被他人访问或操作，从而增加身份冒用风险；

b)会话与通知机制不利于残障人士使用，如登录界面不支持无障碍方式输入、会话超时不友好、安全事件通知不易被用户感知和理解等；

c)用户隐私泄露风险，如屏幕阅读器读出敏感信息等。

5.2 智能体技术安全风险

利用智能体进行用户意图感知和自动化操作时，需要申请大量系统权限，包括用户数据访问权限、硬件访问权限、系统执行权限等，可能存在权限滥用、执行未授权操作、过度收集用户数据、算法歧视等风险。

5.3 操作系统安全风险

操作系统安全风险，包括如下内容：

a) 无障碍服务滥用:操作系统无障碍服务具有高权限特性,包括读取窗口内容、执行模拟点击等，可能被滥用于读取 APP 活动窗口信息，执行模拟点击等操作；

b) 系统权限滥用：系统权限保护不当可能被滥用于超范围获取用户数据、干扰第三方 APP 正常运行等。

6 无障碍技术安全要求

无障碍技术安全要求，包括但不限于：

a)无障碍功能设计在简化人机交互流程时，应采取安全措施避免身份冒用，如设置必要的身份验证环节；

b)应确保身份验证机制对所有用户都是可访问的，如确保登录界面可以通过屏幕阅读器读取，并支持无障碍方式输入；

c)应考虑用户隐私保护，如避免屏幕阅读器读出敏感信息，从而被未授权用户获取；

d)应确保会话超时机制对用户是友好的，如采取延长会话或安全地重新登录等方式；

e)无障碍功能中的提示和引导信息应清晰准确，避免被恶意利用进行社会工程学攻击；

f)应确保安全相关的通知和警报对所有用户都是可访问的，如通过音频通知、振动等方式。

7 智能体技术安全要求

智能体技术安全要求，包括但不限于：

a)应遵循“最小权限”原则，仅申请实现可访问性所需的最小权限，以防范未经授权的访问和潜在的恶意行为；

b)智能体在进行用户意图识别、通过第三方 App 执行各类任务时，应遵循”双重授权“原则，即先通过第三方 App 授权，并在获得用户授权后执行；

c)智能体应在隐私政策中向用户明确告知个人信息收集、存储、使用、共享、删除/撤销同意等情况，并获得用户同意，法律法规要求获得用户单独同意的情形，还应获得用户的单独同意；

d)智能体使用操作系统无障碍服务的，应在隐私政策中声明无障碍服务的使用目的、使用场景和数据处理方式，仅在声明的目的范围内使用无障碍服务，不得将无障碍服务用于其他目的；

e)应确保 AI 算法决策过程透明，针对同一类型第三方 App 的调用和访问，应允许用户自主选择。

8 操作系统安全要求

操作系统安全要求，包括但不限于：

a)操作系统应谨慎为智能体开通无障碍服务权限，开通无障碍权限必须经过用户明确授权，不得在预装、首次安装智能体时默认开通，或者强制、诱导用户开通；

b)操作系统应提供清晰、友好的无障碍权限设置页面，设置页面应准确展示所有申请无障碍服务权限的 App，并提供便捷的权限撤销选项，允许用户随时查看、开通和关闭无障碍服务权限；

c)操作系统无障碍服务权限应仅用于服务残障或其他需要特殊辅助的用户，不得滥用无障碍服务权限执行读屏、模拟点击等操作；

d)操作系统不得利用系统权限优势，在第三方 App 授权前获取第三方 App 数据、调用第三方 App 功能,干扰第三方 APP 正常运行。

9 用户权益保护要求

用户权益保护要求，包括但不限于：

a)智能体进行用户意图识别、通过第三方 App 执行各类任务时，不得侵害用户及其他主体的数据权益。第三方 App 有权拒绝不合理操作以保护用户权益；

b)应向用户明确告知收集的数据将如何处理，不得未经授权收集和处理数据，涉及向第三方共享数据、将用户个人信息上传云端处理的需额外说明；

c)应加强用户教育，引导用户在开通无障碍服务权限前，仔细阅读权限说明和隐私政策，确保用户在完全理解的前提下自主授权开通无障碍服务权限；

d)应建立有效的用户投诉和反馈机制，及时解决用户移动互联网服务安全和隐私问题。

参 考 文 献

[1] 《工业和信息化部 中国残联关于推进信息无障碍的指导意见》，工信部联信管〔2020〕146号
[2] Accessibility requirements for ICT products and services, EN 301 549
[3] Web Content Accessibility Guidelines, WCAG