ICS 35.020
I651

T/ SIA

中 国 软 件 行 业 协 会 团 体 标 准

T/ SIA 004—2017

智能终端应用软件检测一般要求

Intelligent Terminal Application Software Testing General Requirements

2017–12–08 发布　　2017–12–08 实施

中国软件行业协会　发 布

目次

前言

本标准按照GB/T 1.1-2009 《标准化工作导则第1部分：标准的结构与编写》起草。

本标准主体部分包括功能性要求、安全性要求、可靠性要求、兼容性要求、易用性要求、服务能力要求。根据每类质量属性的特点，本标准进一步给出了一级、二级和三级要求。在附录部分，列出了软件达到每一级别所需完成的对应要求。

本标准由中国软件行业协会提出并归口。

本标准起草单位：工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、山西省信息化和信息安全评测中心、河北省软件评测中心、国家体育总局体育彩票管理中心、国家体育总局信息中心、北京银行股份有限公司、北京洋浦伟业科技发展有限公司、中国电力科学研究院、东软集团股份有限公司、中云天下科技有限公司、山东远邦科技集团有限公司、深圳市怡化时代科技有限公司、新开普电子股份有限公司、安徽奇智科技有限公司、广东盘古信息科技股份有限公司、江苏蓝创智能科技股份有限公司、厦门安胜网络科技有限公司、北京航天智造科技发展有限公司、武汉中地数码科技有限公司、北京东软望海科技有限公司、山东创泽信息技术股份有限公司、吉林省爱信网络信息科技有限公司、广西电网有限责任公司电力科学研究院、国网信通产业集团、北京简易科技有限公司、同方鼎欣科技股份有限公司、世纪龙信息网络有限责任公司。

本标准主要起草人：杨珬、刘法旺、石竹君、曾晋、付晓宇、张然、董红芳、邵剑、唐义梅、周兵、刘明君、李凌、张明胜、赵成林、刘德启、纪莎、毛立爽、胥蕊、杨捷、李江、干静、胡阳、魏晓静、杨心恩、杨春伟、罗娟、王江嫚、陈维帅、王岩、李刚、保拉、黄秀丽、肖海莲、徐勣、陈志坚。

本标准为首次制定。

智能终端应用软件检测一般要求

1 范围

本标准对运行于智能终端设备上的应用软件提出了检测一般要求，用于指导第三方测评机构、认证机构进行测评认证等工作，也为智能终端应用软件有关的用户单位、研发单位及相关机构提供了技术参考，致力于提升智能终端应用软件的技术水平。

本标准可作为第三方测评机构、认证机构的测评和认证依据。

本标准适用于软件和信息技术服务企业，政府机关、事业单位、社会团体等组织和机构也可参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件；凡是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 25000.51-2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE）第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则
- GB/T 18336.1-2015 信息技术 安全技术 信息技术安全评估准则 第1部分：简介和一般模型
- GB/T 18336.2-2015 信息技术 安全技术 信息技术安全评估准则 第2部分：安全功能组件
- GB/T 18336.3-2015 信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件
- GB/Z 28828-2012 信息安全技术 公共及商用服务信息系统个人信息保护指南
- T/ SIA 001-2017 企业个人信息安全管理规范

3 术语和定义

3.1 智能终端设备 intelligent terminal device

具有开放式操作系统，使用宽带、无线移动通信技术实现互联网接入，通过下载、安装应用软件并为用户提供数字内容服务的终端产品，简称智能终端。

注：智能终端通常具有高速网络接入能力，开放的、可扩展的操作系统平台，较强的处理能力和丰富的人机交互方式，如智能手机、平板电脑等。

3.2 智能终端操作系统 intelligent terminal operating system

运行在智能终端上的系统软件，控制、管理智能终端上的硬件和软件，提供用户操作界面和应用软件编程接口，简称操作系统，如Android、iOS等。

3.3 智能终端应用软件 intelligent terminal application software

运行在智能终端操作系统上的应用软件，简称应用软件（app）。

3.4 **恶意代码** malicious code

违反相关法律法规或具有其它不正当目的的可执行文件、代码模块或代码片段。

3.5 **关键业务** key business

应用软件实现的核心功能及支撑这些功能的相关服务，如金融应用中登录、查询、转账等业务，当发生异常或中断，可能造成损失。

3.6 **敏感信息** sensitive information

一旦遭到泄露或修改，会对应用软件关键业务或使用关键业务的用户造成不良影响的信息，如个人敏感信息和关键业务信息等。

3.7 **权限** permissions

允许应用软件以特定方式使用特定的系统功能或访问特定的数据。

3.8 **一级要求** the first level requirements

应用软件的一级要求为能够根据使用说明正常运行，不包含恶意代码，不主动泄露敏感信息，在产生自身故障、网络故障或被外部攻击时，可能造成关键业务异常、敏感信息泄露和经济损失。

3.9 **二级要求** the second level requirements

应用软件在满足一级要求的基础上，应具备一定的功能、安全、可靠、兼容、易用和服务能力要求，在产生自身故障、网络故障或被外部攻击时，要求保证关键业务正常运行（或故障恢复后正常运行），可能造成敏感信息泄露和经济损失。

3.10 **三级要求** the third level requirements

应用软件在满足二级要求的基础上，应具备较强的功能、安全、可靠、兼容、易用和服务能力要求，在产生自身故障、网络故障或被外部攻击，要求保证关键业务正常运行（或故障恢复后正常运行），不应造成敏感信息泄露和经济损失。

4 功能性要求

4.1 功能要求

4.1.1 一级要求

1） 应用软件的功能应和其使用说明书保持一致；
2） 应能在其声明支持的智能终端操作系统上正常安装、启动、卸载；在安装时能够向操作系统提供开发方、版本、权限等信息；在卸载时能够通过操作系统的通用卸载功能卸载应用软件的所有组件；
3） 应能显示当前版本信息，必要时能够进行新版本检查和提示，并引导用户进行更新。

4.1.2 二级要求

对于操作系统无法自动清除的由应用软件创建的数据，如缓存、配置等，应提供手动清除功能，并在清除时提示用户。

4.1.3 三级要求

与二级要求相同。

4.2 内容要求

4.2.1 一级要求

不应包含或引入色情、暴力、反动等不良信息，不应违反国家相关法律和政策要求。

4.2.2 二级要求

应提供对非法内容的投诉举报功能。

4.2.3 三级要求

与二级要求相同。

5 安全性要求

5.1 程序安全

5.1.1 一级要求

1） 不应包含或引入恶意代码；
2） 不应包含与应用软件自身无关的文件，如测试数据、其他工具生成的相关文件等；
3） 不应过度申请、使用权限，即申请的权限不应与应用软件的自身描述功能无关，使用的权限不得侵害用户的知情权与合法利益。

5.1.2 二级要求

1） 应能校验自身的完整性；
2） 不应使用包含已知安全风险的第三方插件、SDK，不应调用包含已知安全风险的API。

5.1.3 三级要求

1） 应能防止被动态调试，或在被动态调试时立即结束正常业务流程，并提示用户；
2） 不能被准确反编译为源代码。

5.2 数据安全

5.2.1 一级要求

1） 应对存储的敏感信息设置相应的访问权限；
2） 不应通过日志等方式输出敏感信息。

3） 执行缓存清理、数据删除等不可恢复性操作时，应提示用户，并要求用户确认。

5.2.2 二级要求

1） 应对应用软件存储在本地的敏感信息进行适当的加密处理；
2） 应采用设置访问权限等手段保护自身组件不受非法访问和调用；
3） 不应以明文方式直接显示敏感信息；
4） 在传输敏感信息时，应对其进行适当的加密，并提前告知用户去向和用途。

5.2.3 三级要求

1） 运行在内存中的敏感信息不应被第三方程序截获；
2） 存储在智能终端中的敏感信息不应被第三方程序利用；
3） 处理关键业务时，如需切换用户，应保证前一用户的身份、配置、历史记录等敏感信息已从内存中完全清除。

5.3 通信安全

5.3.1 一级要求

不应以明文方式传输敏感信息。

5.3.2 二级要求

1） 应能保护关键业务的通信完整性，具备超时处理机制；
2） 应采用有效的密码技术保证通信过程中敏感信息或整个报文的保密性。

5.3.3 三级要求

1） 应能抵御SQL注入、重放攻击、中间人攻击等典型攻击；
2） 与服务器端进行敏感信息通信前，应验证服务器身份。

5.4 业务安全

5.4.1 一级要求

在处理关键业务时，应鉴别用户身份。

5.4.2 二级要求

1） 用户输入密码等敏感信息时，应用软件应采用软键盘或密码控件等安全措施；
2） 在处理关键业务时，应具备会话超时处理机制，用户登录后无操作超过一定时间或从系统锁定重新唤醒时，应强制退出登录或重新进行身份认证；
3） 在处理关键业务时，应限制登录的错误尝试次数；
4） 涉及交易、支付等关键业务的用户密码等不应在本地存储。

5.4.3 三级要求

1） 在处理关键业务时，应对用户身份采取两种或两种以上的鉴别机制；
2） 与关键业务相关的密码应允许包含数字和字母以外的特殊字符，并具有相应的复杂度，密码长度最低要求6位；
3） 在处理关键业务时，应要求用户重新输入密码。

5.5 系统安全

5.5.1 一级要求

对系统安全无特别要求。

5.5.2 二级要求

1） 应能防止包含敏感信息的用户界面被第三方程序劫持，或在被劫持时提示用户；
2） 应能防止通过截屏方式获取敏感信息。

5.5.3 三级要求

在处理关键业务前，应用软件应检测当前操作系统的环境安全，如存在安全风险应提示用户，必要时可拒绝执行该关键业务。

6 可靠性要求

6.1 运行稳定性

6.1.1 一级要求

1） 在其声明的所需运行环境下，应用软件能够无故障运行且不影响其它应用软件和操作系统的稳定性；
2） 需要网络环境支撑的应用软件，在网络中断的情况下，应提示用户；
3） 应按照使用说明书连续正常使用；
4） 在连续3次以上启动退出或反复操作的情况下，应用软件仍能正常使用。

6.1.2 二级要求

应具有失效检测机制，在发生如联网失败、存储空间不足等异常时，不应产生崩溃或停止响应；在需要用户进行额外操作时，应提示用户。

6.1.3 三级要求

与二级要求相同。

6.2 容错性

6.2.1 一级要求

应在用户操作错误时，提示用户。

6.2.2 二级要求

应对输入的数据进行有效性校验，避免用户输入错误或不符合要求的数据，并提示用户。

6.2.3 三级要求

发生崩溃等异常情况后，应记录异常原因，并且能够通过自动或手工操作等方式重新启动软件，保持软件正常运行。

7 兼容性要求

7.1 硬件设备兼容性

7.1.1 一级要求

应用软件应能在其声明支持的智能终端设备上正常运行，不应导致智能终端设备出现崩溃、死机等异常现象。

7.1.2 二级要求

用户界面应适配其声明支持的智能终端，用户能够正常操作，界面无异常黑边、无变形等。

7.1.3 三级要求

与二级要求相同。

7.2 软件兼容性

7.2.1 一级要求

应用软件应能在其声明支持的操作系统及版本上正常运行，不应影响操作系统上的其他应用软件的正常功能。

7.2.2 二级要求

与一级要求相同。

7.2.3 三级要求

与一级要求相同。

8 易用性要求

8.1 易理解性

8.1.1 一级要求

1） 应能通过界面或菜单来定位功能；
2） 向用户反馈的信息应易于理解；
3） 应能正确标识数据输入、输出格式。

8.1.2 二级要求

与一级要求相同。

8.1.3 三级要求

与一级要求相同。

8.2 易学性

8.2.1 一级要求

提供用户帮助或使用说明文档。

8.2.2 二级要求

与一级要求相同。

8.2.3 三级要求

具有向导、教学等功能，能够指导用户学习应用软件的基本功能和业务流程。

8.3 易操作性

8.3.1 一级要求

1） 整个应用软件应采取惯用的操作方式；
2） 整个应用软件的界面布局应一致；

8.3.2 二级要求

与一级要求相同。

8.3.3 三级要求

与一级要求相同。

9 服务能力要求

9.1 服务响应

9.1.1 一级要求

对服务响应无特别要求。

9.1.2 二级要求

应具有在线帮助或服务能力反馈功能。

9.1.3 三级要求

与二级要求相同。

10　附录：等级划分概览

技术等级 技术要求类别	一级要求	二级要求	三级要求
功能性	4.1.1、4.2.1	4.1.2、4.2.2	4.1.3、4.2.3
安全性	5.1.1、5.2.1、5.3.1、5.4.1、5.5.1	5.1.2、5.2.2、5.3.2、5.4.2、5.5.2	5.1.3、5.2.3、5.3.3、5.4.3、5.5.3
可靠性	6.1.1、6.2.1	6.1.2、6.2.2	6.1.3、6.2.3
兼容性	7.1.1、7.2.1	7.1.2、7.2.2	7.1.3、7.2.3
易用性	8.1.1、8.2.1、8.3.1	8.1.2、8.2.2、8.3.2	8.1.3、8.2.3、8.3.3
服务能力	9.1.1	9.1.2	9.1.3