

中华人民共和国金融行业标准

XX/T XXXXX—XXXX

证券期货业移动互联网应用程序
安全检测要求

Security testing requirements for mobile internet applications of
securities and futures industry

(征求意见稿)

(本稿完成日期：2020.11.14)

XXXX - XX - XX 发布

XXXX - XX - XX 实施

中国证券监督管理委员会 发布

目 次

前言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	1
4 检测总体要求.....	2
4.1 移动互联网应用程序类型.....	2
4.2 检测框架.....	2
4.3 检测范围.....	3
4.4 检测过程.....	3
4.5 检测方法.....	3
4.6 增强项和一票否决项要求.....	3
4.7 检测结论.....	3
5 检测要求及检测方式.....	4
5.1 身份鉴别.....	4
5.2 网络通信安全.....	7
5.3 数据安全.....	9
5.4 终端安全.....	11
5.5 开发安全.....	16
5.6 安全审计.....	17
5.7 个人信息保护.....	19
附录 A （资料性） 检测案例.....	20
附录 B （规范性） 检测项权重表.....	27
附录 C （规范性） 一票否决项和增强项统计.....	29
附录 D （规范性） App 违法违规收集使用个人信息行为认定方法.....	31

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范》的规定起草。

本文件由全国金融标准化技术委员会证券分技术委员会提出。

本文件由全国金融标准化技术委员会归口管理。

本文件起草单位：中国证券监督管理委员会科技监管局、中证信息技术服务有限责任公司、上海市信息安全测评认证中心、上海证券交易所、国泰君安证券股份有限公司、光大证券股份有限公司、华福证券股份有限公司、国泰君安期货有限公司。

本文件主要起草人：姚前、刘铁斌、周云晖、周桢、李宏达、倪惠康、沙明、俞枫、陈凯晖、刘嵩、甘张生、万晓鹰。

本标准为首次发布。

证券期货业移动互联网应用程序安全检测要求

1 范围

本文件规定了证券期货业移动互联网应用程序安全检测的总体要求、检测要求及检测方法。

本文件适用于信息安全检测服务机构、运营使用单位对证券期货业发布的移动互联网应用程序进行的安全测试评估，自动化安全检测工具开发商进行设计与开发工作。国家信息安全监管职能部门及证券期货监管部门依法进行的信息安全监督检查可以参考使用。

注1：本标准中涉及到的密码应用，依据国家密码管理局规定实施。

注2：本标准仅给出了证券期货业移动互联网应用程序安全技术要求及测试评价方法，对具体技术实现方式、方法等不作规定。

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 25069	信息安全技术	术语
GB/T 18336—2015（所有部分）	信息技术	安全技术 信息技术安全评估准则
GB/T 22239—2019	信息安全技术	网络安全等级保护基本要求
GB/T 28448—2019	信息安全技术	网络安全等级保护测评要求
GB/T 30284—2020	信息安全技术	移动通信智能终端操作系统安全技术要求
GB/T 32927—2016	信息安全技术	移动智能终端安全架构
GB/T 35273—2017	信息安全技术	个人信息安全规范
JR/T 0060—2010	证券期货业信息系统安全等级保护基础要求（试行）	
JR/T 0067—2011	证券期货业信息系统安全等级保护检测要求（试行）	
JR/T 0192—2020	证券期货业移动互联网应用程序安全规范	

3 术语和定义

GB/T 35273—2020、JR/T 0192—2020界定的以及下列术语和定义使用于本文件。

3.1

移动终端 mobile terminal

以手机、平板电脑等智能设备为代表，能够安装并使用证券期货移动互联网应用程序，可以在移动中使用的计算机设备。

[来源：JR/T 0192—2020，3.1]

3.2

移动互联网应用程序 mobile internet application

由证券期货行业机构（核心机构或经营机构）或其它参与机构（行情商）发布的，安装在移动终端上，用于证券期货查询、交易等业务相关的原生应用程序。

3.3

移动终端环境 mobile terminal environment

支撑移动互联网应用程序运行的硬件（包括智能手机、平板电脑等终端）及该硬件上的操作系统和其它程序等软件所组成的整体运行环境。

3.4

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

[来源：GB/T 35273—2020, 3.1,有修改]

3.5

个人敏感信息 personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注：通常情况下，14岁以下（含）儿童的个人信息和涉及自然人隐私的信息属于个人敏感信息。

[来源：GB/T 35273—2020, 3.2,有修改]

4 检测总体要求

4.1 移动互联网应用程序类型

移动互联网应用程序分为3种类型：

- 办公类移动互联网应用程序；
- 信息披露类移动互联网应用程序；
- 证券期货交易类移动互联网应用程序。

4.2 检测框架

检测框架见图1。

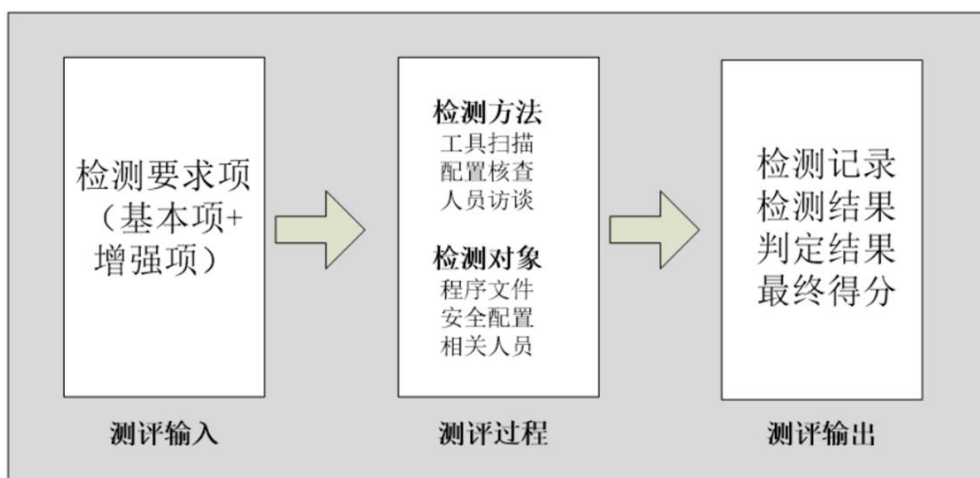


图1 检查框架

4.3 检测范围

系统检测范围一般为证券期货业移动互联网应用程序的客户端部分,包括各类移动操作系统的客户端程序。但移动端的网页浏览程序(如H5、浏览器插件等)不包含在内。此外还包括部分移动互联网应用程序服务端的核心安全内容。

4.4 检测过程

检测过程如下:

- a) 被测单位提供移动互联网应用程序的相关开发设计文档、未进行安全加固的应用程序和已安全加固后的应用程序。
- b) 检测人员查看相关开发设计文档,并进行人员访谈,获取相关核查信息。
- c) 检测人员使用工具对未进行安全加固的应用程序和已安全加固后的应用程序分别进行扫描,获得不同的检测结果。
- d) 检测人员通过人工方式验证工具扫描的结果,并测试其他工具未覆盖的检测项。
- e) 检测人员依据本标准的计算方式,经过综合计算,给出最终检测结论。

4.5 检测方法

检测方法分为工具扫描和人工验证两种。

工具扫描即利用预定的方法/工具,查看输出与预期的差异,判断系统保护措施的有效性。

人工验证即人工参考工具扫描的结果,通过对系统、文档等的观察、分析等活动,验证工具得出的检测结果,判断系统安全保护措施的有效性。

4.6 增强项和一票否决项要求

4.6.1 本文件根据移动互联网应用程序的类别提出了不同等级的要求,证券期货交易类的移动互联网应用程序应遵照基本项要求和增强项要求执行。办公类、信息披露类的移动互联网应用程序应遵照加其综合得分。

4.6.2 本文件中的基本项和增强项要求均有部分项包含一票否决属性。若移动互联网应用程序中存在部分一票否决项未完全符合,则检测结论的综合得分将低于60分。具有一票否决属性的检测项见附录C。

4.7 检测结论

根据4.1~4.6要求得到检测结果,计算移动互联网应用程序的综合得分。

综合得分计算方式见表1。

表1 综合得分计算方式

是否存在一票否决项	综合得分计算公式
信息系统中所有一票否决项均为符合。	$\frac{\sum_{k=1}^p \text{测评项得分} \times \text{测评项权重}}{\sum_{k=1}^p \text{测评项最高得分} \times \text{测评项权重}} \times 100$ <p>p为总检测项数,包含符合的增强项,不含不适用的检测项。</p>

是否存在一票否决项	综合得分计算公式
信息系统中部分一票否决项未完全符合。	$\frac{\sum_{k=1}^P \text{测评项得分} \times \text{测评项权重}}{\sum_{k=1}^P \text{测评项最高得分} \times \text{测评项权重}} \times 60$ <p>p 为总检测项数，包含符合的增强项，不含不适用的检测项。</p>

附录B规定了检测项的权重值。

5 检测要求及检测方式

5.1 身份鉴别

5.1.1 鉴别方式

5.1.1.1 二次认证

5.1.1.1.1 检测目的

检查移动互联网应用程序在资金类交易、个人信息修改等关键业务处，是否增设二次认证的环节，是否使用存放在移动终端的信息进行认证。

5.1.1.1.2 检测流程

检查移动互联网应用程序在资金类交易、个人信息修改等关键业务处，是否增设二次认证的环节，查看其认证方式。尝试替换移动终端的信息绕过认证。

5.1.1.1.3 通过要求

对于资金类交易、个人信息修改等关键业务，不应仅通过第三方移动互联网应用程序进行认证，应增设二次认证的环节，认证方式包括口令、生物特征、短信、令牌、图形手势等中的至少一种。二次认证不应使用存放在移动终端的信息进行认证。

5.1.1.2 实名登记

5.1.1.2.1 检测目的

若采用第三方移动互联网应用程序的认证方式，检查移动互联网应用程序应再次进行实名登记核验。

5.1.1.2.2 检测流程

检查送检文档中关于实名登记的说明，查看在哪些情况下应用程序移动互联网应用程序进行实名登记。

使用第三方移动互联网应用程序进行认证，检查移动互联网应用程序是否会再次进行实名登记核验。

5.1.1.2.3 通过要求

采用第三方移动互联网应用程序的认证方式，移动互联网应用程序应再次进行实名登记核验。

5.1.1.3 登录失败处理

5.1.1.3.1 检测目的

移动互联网应用程序是否提供了登录失败处理机制。

5.1.1.3.2 检测流程

检查开发文档中，移动互联网应用程序是否提供连续鉴别失败处理机制。

检查移动互联网应用程序在认证用户身份时是否有认证失败处理机制。

5.1.1.3.3 通过要求

应采取限定连续登录失败次数的措施，如设置登录失败次数上限、多次登录失败后的账户锁定策略等。

5.1.1.4 会话超时

5.1.1.4.1 检测目的

移动互联网应用程序是否提供了会话超时重鉴别机制。

5.1.1.4.2 检测流程

检查开发文档中，移动互联网应用程序是否提供会话超时重鉴别机制。

检查证券期货业移动互联网应用在会话超时后是否需再次进行身份鉴别。

5.1.1.4.3 通过要求

应具备登录超时锁定或注销功能，在设定的时间段内没有任何操作的情况下，终止登录会话，需要再次进行身份鉴别才能够重新操作。

5.1.2 口令安全

5.1.2.1 存储安全

5.1.2.1.1 检测目的

检查移动互联网应用程序是否将口令保存在移动终端上。

5.1.2.1.2 检测流程

检查移动互联网应用程序在运行过程中是否将口令保存在移动终端上。

5.1.2.1.3 通过要求

口令不应以任何形式保存在移动终端上。

5.1.2.2 传输安全

5.1.2.2.1 检测目的

检查移动互联网应用程序在通信过程中是否传输明文口令信息。

5.1.2.2.2 检测流程

检查移动互联网应用程序在与服务器的通信过程中是否对敏感信息进行加密处理。

5.1.2.2.3 通过要求

口令在传输过程中不应以明文形式传输。

5.1.2.3 残留信息保护

5.1.2.3.1 检测目的

检查移动互联网应用程序是否在缓存和日志中输出口令和密钥信息。

5.1.2.3.2 检测流程

检查移动互联网应用程序在运行过程中是否在缓存和日志中输出口令和密钥信息。

5.1.2.3.3 通过要求

口令和密钥不在缓存和日志中输出。

5.1.2.4 安全输入

5.1.2.4.1 检测目的

检查移动互联网应用程序在输入口令时是否采取技术措施防止口令被盗取。

5.1.2.4.2 检测流程

检查开发文档中，移动互联网应用程序是否提供技术措施防止口令被盗取。

检查移动互联网应用程序在输入口令信息时是否可防截屏操作。

检查移动互联网应用程序在输入口令信息时是否可防信息截获。

5.1.2.4.3 通过要求

输入口令信息时应采取技术措施防止口令被盗取。

5.1.2.5 敏感信息显示

5.1.2.5.1 检测目的

检查移动互联网应用程序是否以非明文的形式显示口令。

5.1.2.5.2 检测流程

检查移动互联网应用程序在口令输入处，是否以非明文的方式显示口令。

5.1.2.5.3 通过要求

口令输入框应禁止明文显示口令。

5.1.2.6 口令复杂度

5.1.2.6.1 检测目的

检查移动互联网应用程序是否提供口令复杂度校验功能。

5.1.2.6.2 检测流程

检查开发文档中，移动互联网应用程序是否提供口令复杂度校验功能。

检查移动互联网应用程序在口令设置处是否提供口令复杂度校验功能。

5.1.2.6.3 通过要求

应提供口令复杂度校验功能，保证用户设置的口令达到一定的强度。

5.2 网络通信安全

5.2.1 通讯协议

5.2.1.1 安全通讯协议

5.2.1.1.1 检测目的

检查移动互联网应用程序与服务器之间的通信是否使用安全的通信协议。

5.2.1.1.2 检测流程

检查移动互联网应用程序与服务器是否正确配置SSL/TLS。

检查通信协议是否支持SSL 2.0等低版本的通信协议。

5.2.1.1.3 通过要求

应使用SSL3.0/TLS1.0以上版本协议保障移动互联网应用程序与服务器之间所有的连接，保证传输敏感数据的机密性和完整性。

应使用通讯协议的安全版本，取消对存在安全隐患版本协议的支持。

5.2.1.2 数据保密性

5.2.1.2.1 检测目的

检查移动互联网应用程序与服务器通信过程中是否使用强壮的加密算法。

5.2.1.2.2 检测流程

检查开发文档中，移动互联网应用程序与服务器通信过程中是否使用强壮的加密算法。

检查移动互联网应用程序与服务器通信过程中使用的加密算法是否安全，密钥长度是否安全。

5.2.1.2.3 通过要求

应采用强壮的加密算法、安全的密钥长度保证传输敏感数据的机密性和完整性。

5.2.2 会话管理

5.2.2.1 缓存信息保护

5.2.2.1.1 检测目的

检查移动互联网应用程序在认证结束后是否立即清除缓存，防止信息泄露。

5.2.2.1.2 检测流程

检查开发文档中，移动互联网应用程序在认证结束后是否有清除缓存的措施。

检查移动互联网应用程序在认证结束后是否立即清除缓存。

5.2.2.1.3 通过要求

移动互联网应用程序在认证结束后立即清除缓存。

5.2.2.2 安全提示

5.2.2.2.1 检测目的

检查移动互联网应用程序在不同移动终端上登录时是否向用户进行信息提示。

5.2.2.2.2 检测流程

检查开发文档中，移动互联网应用程序是否具备不同移动终端上登录的用户提示措施。

使用不同终端登录移动互联网应用程序，检查程序是否向用户进行信息提示。

5.2.2.2.3 通过要求

在不同移动终端上登录时应向用户进行信息提示。

5.2.2.3 会话鉴别

5.2.2.3.1 检测目的

检查服务端是否对移动互联网应用程序登录后所有的请求进行合法身份鉴别。

5.2.2.3.2 检测流程

检查服务端是否对登录完成后的会话管理阶段的所有请求进行合法身份鉴别，尝试删除身份鉴别信息进行请求。

5.2.2.3.3 通过要求

登录完成后的会话管理阶段的所有请求都需要对用户的合法身份进行鉴别（如token方式），鉴别通过后才能进行操作。

5.2.2.4 操作提醒

5.2.2.4.1 检测目的

检查移动互联网应用程序在用户进行关键业务操作后是否进行提醒。

5.2.2.4.2 检测流程

检查开发文档中，移动互联网应用程序是否具备关键业务操作的用户提示措施。

检查移动互联网应用程序在进行关键业务操作后是否通过短信、微信等手段对用户进行提醒。

5.2.2.4.3 通过要求

在用户进行关键业务操作后应当通过短信、微信等手段对用户进行提醒。

5.2.3 第三方网络传输

5.2.3.1 安全通道

5.2.3.1.1 检测目的

移动互联网应用程序和服务器之间的通信如经过第三方服务器，检查是否遵守国家、行业的有关规定和要求。

检查移动互联网应用程序和第三方服务器之间是否使用加密安全通道。

5.2.3.1.2 检测流程

检查开发文档中，移动互联网应用程序和服务器中间的通信是否经过第三方服务器。

检查移动互联网应用程序与服务器是否正确配置SSL/TLS。

5.2.3.1.3 通过要求

移动互联网应用程序和服务器之间的通信如经过第三方服务器，应遵守国家、行业的有关规定和要求，并且建立服务器与移动互联网应用程序之间的加密安全通道，避免信息被第三方获取或修改。

5.3 数据安全

5.3.1 数据录入

5.3.1.1 数据录入加密

5.3.1.1.1 检测目的

检查移动互联网应用程序在用户输入口令等个人敏感信息时，是否提供加密功能

5.3.1.1.2 检测流程

检查移动互联网应用程序在用户输入口令等个人敏感信息时，是否以非明文形式显示。

5.3.1.1.3 通过要求

用户输入的口令等个人敏感信息应予以加密。

5.3.1.2 页面返回保护

5.3.1.2.1 检测目的

检查移动互联网应用程序是否支持页面返回后自动清除个人信息的机制。

5.3.1.2.2 检测流程

检查开发文档中关于页面返回后自动清除个人信息的说明。

检查移动互联网应用程序哪些页面涉及敏感数据的显示和处理。

操作移动互联网应用程序进入涉及敏感数据显示和处理的页面，输入敏感数据后通过各种方式（切到其它页面、切到后台等）重新进入该页面，检查敏感数据是否自动清除。

调出后台列表界面，查看移动互联网应用程序客户端在后来列表中的预览界面是否采取模糊或其他防护措施。

5.3.1.2.3 通过要求

移动互联网应用程序在页面返回后自动清除个人信息。移动互联网应用程序客户端宜对后台任务列表中的预览界面采取模糊或其他防护措施。

5.3.2 数据存储

5.3.2.1 敏感信息存储

5.3.2.1.1 检测目的

检查移动互联网应用程序是否在移动终端存储个人敏感信息，是否在身份认证结束后存储个人敏感信息。

5.3.2.1.2 检测流程

检查开发文档中对于移动互联网应用程序在个人敏感信息存储的规定。

个人敏感信息的范围包括但不限于账户口令、身份证号码等。

使用文件系统管理工具检查移动互联网应用程序是否在移动终端保存个人敏感信息，与开发文档中的规定是否一致。

5.3.2.1.3 通过要求

移动互联网应用程序不在移动终端存储个人敏感信息。

5.3.2.2 剩余信息保护

5.3.2.2.1 检测目的

检查移动互联网应用程序删除后，移动终端中是否仍有个人信息残留，可否保证个人信息所在的存储空间被释放或重新分配给其他应用程序前得到完全清除。

5.3.2.2.2 检测流程

检查开发文档中，移动互联网应用程序删除后移动终端中是否仍有个人信息残留。

使用文件系统管理工具检查移动互联网应用程序删除后，移动终端中是否仍有个人信息残留。尝试通过技术手段恢复已清除的个人信息及敏感数据，查看是否可以成功恢复。

5.3.2.2.3 通过要求

移动互联网应用程序删除后，移动终端中应无个人信息残留。无法恢复已清除的个人信息及敏感数据。

5.3.2.3 业务数据安全

5.3.2.3.1 检测目的

检查移动互联网应用程序退出时，是否清除文件系统中非业务功能运行所必须留存的业务数据，保证个人信息的安全性。

5.3.2.3.2 检测流程

检查开发文档中,关于移动互联网应用程序退出时是否清除文件系统中非业务功能运行所必须留存的业务数据的相关说明。

使用文件管理工具或内存搜索工具检查移动互联网应用程序退出时是否清除文件系统中非业务功能运行所必须留存的业务数据。

5.3.2.3.3 通过要求

移动互联网应用程序退出时,应清除文件系统中非业务功能运行所必须留存的业务数据。

5.4 终端安全

5.4.1 应用程序保护

5.4.1.1 防逆向

5.4.1.1.1 检测目的

移动互联网应用程序客户端是否采取防动态调试、代码混淆等防逆向措施,防止被反编译或逆向分析,确保程序逻辑的机密性。

5.4.1.1.2 检测流程

对移动互联网应用程序客户端及其安装包进行动态调试及反编译测试,检查移动互联网应用程序客户端是否采取防动态调试、代码混淆等确保程序逻辑机密性的有效措施。

5.4.1.1.3 通过要求

采取防动态调试、代码混淆等防逆向措施,防止被反编译或逆向分析,确保移动互联网应用程序逻辑的机密性。

5.4.1.2 输入保护

5.4.1.2.1 检测目的

移动互联网应用程序是否能够保障输入信息的机密性。

5.4.1.2.2 检测流程

检查开发文档中有关敏感信息防截获的安全机制,评估其安全机制是否可行。对移动互联网应用程序客户端进行测试,尝试截获用户输入的敏感数据。

5.4.1.2.3 通过要求

移动互联网应用程序能够保障输入信息的机密性,如采取自定义键盘、随机键盘位、防范键盘窃听技术等措施。

5.4.1.3 输入校验

5.4.1.3.1 检测目的

检查移动互联网应用程序客户端是否提供数据有效性校验功能,保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。

5.4.1.3.2 检测流程

检查开发文档中关于移动互联网应用程序客户端数据有效性校验的要求。尝试输入异常字符，验证数据有效性校验功能是否生效。

5.4.1.3.3 通过要求

对输入信息的合法性进行识别。

5.4.1.4 外部资源授权

5.4.1.4.1 检测目的

检查移动互联网应用程序客户端程序在访问、修改、删除移动终端上与业务无关的数据前，是否得到用户许可。

5.4.1.4.2 检测流程

检查移动互联网应用程序客户端在对移动终端上与业务无关的数据进行操作前，是否具有用户许可模块，并在许可描述中明确对所操作的相关资源、数据进行描述。

5.4.1.4.3 通过要求

移动互联网应用程序在未得到用户许可前，不应访问、修改、删除移动终端上与业务无关的数据。

5.4.1.5 完整性校验

5.4.1.5.1 检测目的

移动互联网应用程序客户端是否具备完整性校验机制。

5.4.1.5.2 检测流程

尝试对移动互联网应用程序客户端的配置文件、运行库、可执行文件等内容进行篡改，检查移动互联网应用程序客户端是否具备完整性校验机制。

5.4.1.5.3 通过要求

移动互联网应用程序客户端具备完整性校验机制。

5.4.1.6 异常处理

5.4.1.6.1 检测目的

移动互联网应用程序客户端或服务端出现异常时，客户端是否提示明确、易理解的业务操作信息，避免将程序代码错误直接返回给用户。

5.4.1.6.2 检测流程

检查移动互联网应用程序客户端或服务端在发生异常时，是否对客户端提示明确、易理解的业务操作信息，避免将程序代码错误直接返回给用户。

5.4.1.6.3 通过要求

移动互联网应用程序客户端或服务端出现异常时，客户端提示明确、易理解的业务操作信息，避免将程序代码错误直接返回给用户。

5.4.2 移动终端环境

5.4.2.1 运行环境安全

5.4.2.1.1 检测目的

移动互联网应用程序是否在每次运行前对运行环境安全性进行检测，并提示发现的风险。

5.4.2.1.2 检测流程

检查移动互联网应用程序客户端是否具备运行环境安全行检测功能，对诸如终端操作系统是否已获取最高管理员权限、是否运行于虚拟环境等内容进行检测，并提示发现的风险。

5.4.2.1.3 通过要求

移动互联网应用程序应在每次运行前对运行环境安全性进行检测，提示发现的风险。

5.4.2.2 进程保护

5.4.2.2.1 检测目的

移动互联网应用程序是否采取进程保护措施，防止非法程序获取该进程的访问权限。

5.4.2.2.2 检测流程

尝试使用进程注入等技术，试图获取移动互联网应用程序进程的访问权限，检验进程保护措施是否有效。

5.4.2.2.3 通过要求

移动互联网应用程序启动及运行过程，应采取相应的进程保护措施，防止非法程序获取该进程的访问权限。

5.4.2.3 异常监测

5.4.2.3.1 检测目的

移动互联网应用程序是否采取有效措施监测并向后台服务端反馈移动终端环境安全状况。

5.4.2.3.2 检测流程

检查移动互联网应用程序采取了何种有效的移动终端环境安全状况监测措施。

5.4.2.3.3 通过要求

应采取有效措施监测并向后台系统反馈移动终端环境安全状况。

5.4.3 安装、卸载与更新

5.4.3.1 终端授权提示

5.4.3.1.1 检测目的

移动互联网应用程序客户端获取移动终端上相关权限时，是否以明显方式提示用户。

5.4.3.1.2 检测流程

检查移动互联网应用程序客户端在获取移动终端上其他权限过程中，是否以明显方式提示用户，包括但不限于图标、文字，声音提示等。

5.4.3.1.3 通过要求

移动互联网应用程序客户端获取移动终端上相关权限，应以明显方式提示用户，包括但不限于图标、文字，声音提示等。

5.4.3.2 剩余信息保护

5.4.3.2.1 检测目的

移动互联网应用程序客户端使用过程中的缓存数据是否能完全删除，删除用户使用过程中生成的数据时是否有提示。

5.4.3.2.2 检测流程

检查移动互联网应用程序客户端卸载完成后，用户使用过程中在移动终端设备产生的缓存数据是否已完全删除。

5.4.3.2.3 通过要求

移动互联网应用程序客户端使用过程中的缓存数据应能完全删除，且删除用户使用过程中生成的数据时应有提示。

5.4.3.3 系统配置复原

5.4.3.3.1 检测目的

移动互联网应用程序客户端安装时修改的移动终端操作系统配置信息是否在卸载后能复原。

5.4.3.3.2 检测流程

记录移动互联网应用程序客户端安装前的终端操作系统配置信息，检测客户端卸载后，移动终端操作系统的配置信息是否与客户端安装前一致。

5.4.3.3.3 通过要求

移动互联网应用程序客户端安装时修改的移动终端操作系统配置信息应在卸载后能复原。

5.4.3.4 系统安全

5.4.3.4.1 检测目的

检测移动互联网应用程序客户端是否影响移动终端操作系统和其他应用软件的功能。

5.4.3.4.2 检测流程

检测移动互联网应用程序客户端是否植入了会影响移动终端操作系统和其它应用软件功能的恶意代码，包括但不限于：木马类、病毒类、后门类、僵尸类、间谍类等。

5.4.3.4.3 通过要求

移动互联网应用程序客户端应不影响移动终端操作系统和其他应用软件的功能。

5.4.3.5 完整性校验

5.4.3.5.1 检测目的

移动互联网应用程序客户端在安装及更新时是否进行真实性和完整性校验，防范移动互联网应用程序被篡改或替换。

5.4.3.5.2 检测流程

检查移动互联网应用程序客户端对更新源是否具有真实性校验措施，对安装包及更新内容（热更新方式）是否具有完整性校验措施。

5.4.3.5.3 通过要求

移动互联网应用程序客户端在安装及更新时应进行真实性和完整性校验，防范移动互联网应用程序被篡改或替换。

5.4.3.6 更新推送

5.4.3.6.1 检测目的

检查是否采取有效措施，保证移动互联网应用程序客户端升级的时效性。

5.4.3.6.2 检测流程

检查移动互联网应用程序客户端是否采取自动升级、更新通知等手段，保证客户端升级的时效性。

5.4.3.6.3 通过要求

至少采取一种安全机制，保证升级的时效性，例如自动升级、更新通知等手段。

5.4.3.7 强制更新

5.4.3.7.1 检测目的

检查移动互联网应用程序客户端在发生重大安全问题需要升级时，是否能够采取强制更新的方式修复客户端问题。

5.4.3.7.2 检测流程

移动互联网应用程序服务端发起强制更新，并尝试使用旧版本移动互联网应用程序客户端访问应用系统，检查系统强制升级策略是否有效。

5.4.3.7.3 通过要求

当应用移动互联网应用程序因重大安全问题需要升级时，能够强制用户升级后方可使用。

5.5 开发安全

5.5.1 安全架构

5.5.1.1 安全需求

5.5.1.1.1 检测目的

检查移动互联网应用程序开发时是否制定安全需求。

5.5.1.1.2 检测流程

查看移动互联网应用程序的安全需求，查看需求中对移动互联网应用程序安全功能的描述。

5.5.1.1.3 通过要求

移动互联网应用程序开发时应制定安全需求，描述移动互联网应用程序应具备的安全功能。

5.5.1.2 安全设计

5.5.1.2.1 检测目的

检查是否制定安全设计文档。

5.5.1.2.2 检测流程

查看移动互联网应用程序的安全设计文档，查看移动互联网应用程序中是否有违反和绕过安全措施的任何类型的接口和设计文档中未说明的任何模式的接口。

5.5.1.2.3 通过要求

对移动互联网应用程序的开发应制定安全设计文档，并依据安全设计文档进行软件开发。

5.5.1.3 安全编码

5.5.1.3.1 检测目的

检查是否制定移动互联网应用程序开发编码安全手册。

5.5.1.3.2 检测流程

查看移动互联网应用程序开发编码安全手册，查看程序代码是否遵守编码安全手册编写。

5.5.1.3.3 通过要求

移动互联网应用程序开发过程中应遵守编码安全，减少应用程序安全漏洞。

5.5.1.4 安全测试

5.5.1.4.1 检测目的

检查移动互联网应用程序正式上线前是否进行安全测试。

5.5.1.4.2 检测流程

查看移动互联网应用程序上线前的安全测试报告。

5.5.1.4.3 通过要求

移动互联网应用程序在开发完成，正式上线前，应进行安全测试。

5.5.1.5 安全插件

5.5.1.5.1 检测目的

检查是否使用安全的第三方插件。

5.5.1.5.2 检测流程

查看移动互联网应用程序中的第三方插件安全测试报告或证书。

5.5.1.5.3 通过要求

应使用安全的第三方插件。

5.5.1.5.4 检测目的

检查移动互联网应用程序是否采用发布机构的证书进行签名。

5.5.1.5.5 检测流程

查看移动互联网应用程序的签名证书，查看证书的标识是否与来源保持一致。

5.5.1.5.6 通过要求

移动互联网应用程序应采用发布机构的证书进行签名，标识应用程序的来源的发布者。

5.6 安全审计

5.6.1 日志生成

5.6.1.1 登录日志

5.6.1.1.1 检测目的

查看移动互联网应用程序服务端是否对用户登录成功和失败进行记录。

5.6.1.1.2 检测流程

登录后台服务器日志系统，查看系统的登录成功和失败日志，查看日志信息是否包括日期、时间、用户标识、设备标识、网络信息、事件描述和结果等信息。

5.6.1.1.3 通过要求

移动互联网应用程序服务端应对用户登录成功和失败进行记录。

5.6.1.2 操作日志

5.6.1.2.1 检测目的

查看移动互联网应用程序服务端是否对用户重要操作进行记录。

5.6.1.2.2 检测流程

登录后台服务器日志系统，查看系统的用户操作日志，查看日志信息是否包括日期、时间、用户标识、设备标识、网络信息、事件描述和结果等信息。

5.6.1.2.3 通过要求

移动互联网应用程序服务端应对用户重要操作进行记录。

5.6.1.3 调试日志

5.6.1.3.1 检测目的

查看移动互联网应用程序是否在移动终端产生开发过程的调试日志。

5.6.1.3.2 检测流程

查看移动互联网应用程序客户端操作系统的日志记录文件，查找移动互联网应用程序是否向操作系统提供开发过程的调试日志。

5.6.1.3.3 通过要求

移动互联网应用程序不能在移动终端产生开发过程的调试日志。

5.6.2 日志管理

5.6.2.1 保存时间

5.6.2.1.1 检测目的

查看日志是否存放于移动互联网应用程序服务端，保存时间是否符合要求。

5.6.2.1.2 检测流程

查看移动互联网应用程序服务端的日志记录，查看最早记录的日志时间。

5.6.2.1.3 通过要求

日志应存放于移动互联网应用程序服务端且保存的时间不少于六个月。

5.6.2.2 集中存储

5.6.2.2.1 检测目的

检查日志是否集中存储，是否仅允许授权用户访问日志。

5.6.2.2.2 检测流程

询问管理员是否将审计日志集中存储，是否仅相关管理员才可能访问该日志资源。

5.6.2.2.3 通过要求

日志应集中存储，且仅允许授权用户访问日志。

5.6.2.3 敏感日志信息

5.6.2.3.1 检测目的

查看服务端日志是否记录个人敏感信息。

5.6.2.3.2 检测流程

查看服务端的日志记录，查看个人信息，根据信息的敏感性进行筛选和甄别。

5.6.2.3.3 通过要求

日志不应记录个人敏感信息。

5.7 个人信息保护

5.7.1 检测目的

行业机构应符合法律法规要求，采取有效措施加强移动互联网应用程序的个人信息保护。

5.7.2 检测流程

依据当前法律法规要求，通过管理和技术手段，检测移动互联网应用程序是否完全满足个人信息保护要求，App违法违规收集使用个人信息行为认定方法见附录D。

5.7.3 通过要求

移动互联网应用程序的个人信息保护能力完全符合相关法律法规要求。

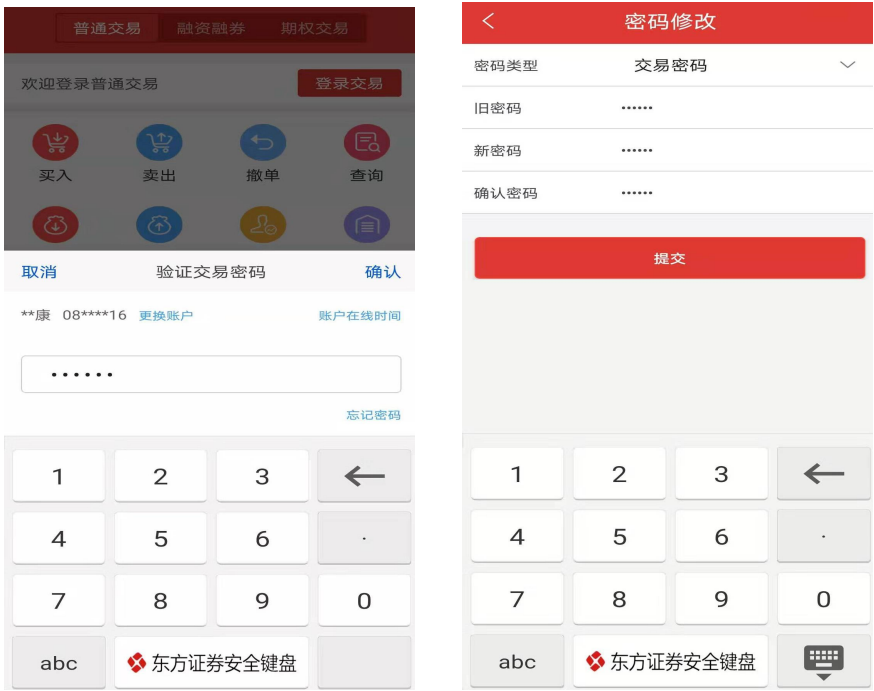
附录 A (资料性) 检测案例

A.1 案例一：身份鉴别测试

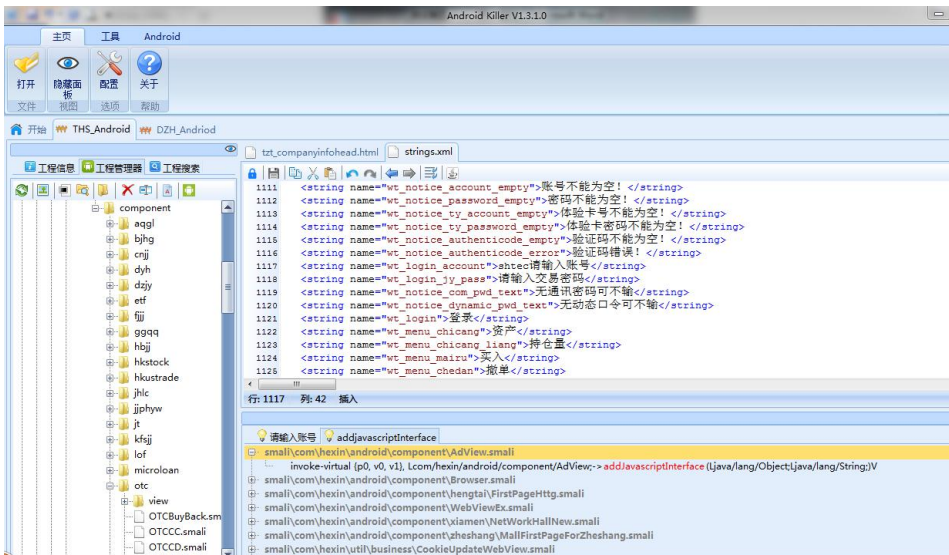
测试环境	Android客户端
测试项	5.1.1.1 二次认证
测试内容及过程	<p>检查客户端是否使用本地信息进行二次认证：</p> <ol style="list-style-type: none"> 1. 截包观察二次认证时客户端是否向服务端发送可能的认证报文；app未发送报文，很可能采用了本地认证。 2. 在root测试机中查看app本地目录，查看是否有文件存储了口令信息：  <p>经测试，apk在本地目录/databases/***.db文件的userRecord字段明文存储手势口令。</p>
测试结论	Apk使用本地存储手势口令进行二次认证，该项不符合。

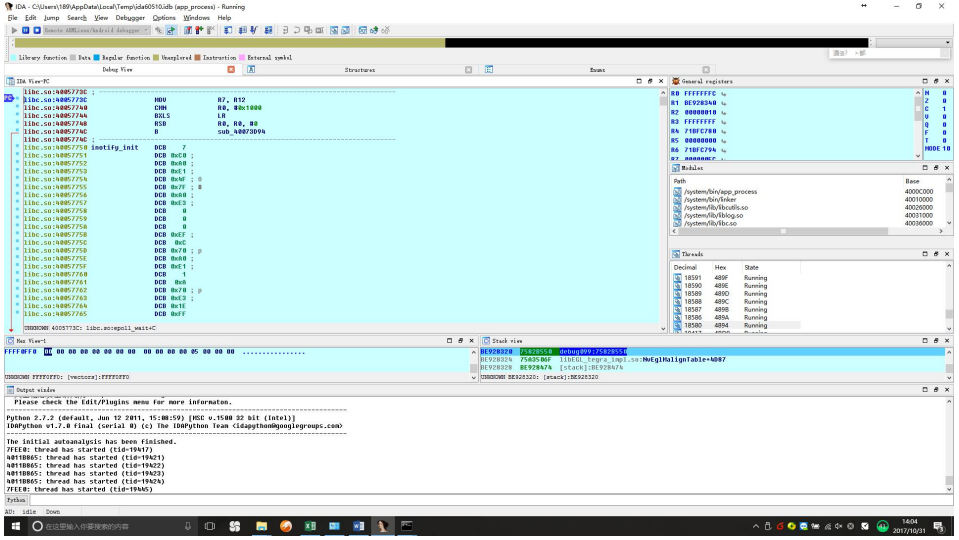
A.2 案例二：数据安全测试

测试环境	Android客户端
测试项	5.3.1.1 数据录入加密
测试内容及过程	检查移动互联网应用程序在用户输入口令等客户敏感信息时，是否以非明文形式显示。

	 <p>经测试，发现客户端程序在用户输入口令等敏感信息时经过加密键盘转换，以*号方式显示。</p>
测试结论	用户输入的口令等敏感信息以加密方式显示。

A.3 案例三：终端安全测试

测试环境	Android客户端
测试项	5.4.1.1 防逆向
测试内容及过程	<p>防逆向测试：对apk进行反编译，并且检查反编译得到的代码是否有经过混淆处理。</p> 

	<p>经测试，发现apk未采取防反编译、代码混淆等防逆向分析措施</p> <p>动态调试测试：对安装后的客户端程序进行动态调试。</p>  <p>经测试，发现客户端程序未采取防动态调试措施。</p>
测试结论	Apk未采取防反编译及代码混淆措施，且未对动态调试进行防护，通过静态分析级动态分析，程序逻辑机密性无法得到有效保护。该项不符合。

A.4 案例四：终端安全测试

测试环境	Android客户端
测试项	5.4.1.2 输入保护
测试内容及过程	检查输入模块是否具有输入保护，如：使用自定义键盘、随机键盘位、防范键盘窃听技术等措施。

	 <p>在关键信息（如交易口令）的输入模块未提供自定义键盘，存在被键盘记录软件获取敏感信息的风险。</p>
测试结论	在关键信息输入模块未采用自定义键盘、随机键盘位、防范键盘窃听技术等措施，该项不符合。

A.5 案例五：终端安全测试

测试环境	Android客户端
测试项	5.4.1.3 输入校验
测试内容及过程	<p>检查客户端是否对人机接口和通信接口输入的内容进行合法性校验：</p> <ol style="list-style-type: none"> 1. 在PC上开启热点并启用截包工具，测试手机连接该热点，并在手机上信任配置证书让截包工具可以解密HTTPS流量。 2. 通过功能查找需要校验的输入字段，如查询字段、交易字段。

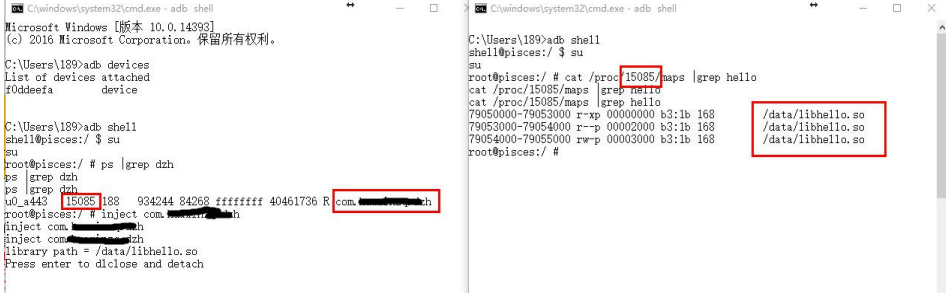
	 <p>经测试，app中可以修改交易金额为负数，并增加余额；字段未对不合法的负值进行校验。</p>
测试结论	Apk未对字段进行充分的合法性校验，存在导致非法交易的漏洞，该项不符合。

A.6 案例六：终端安全测试

测试环境	Android客户端																				
测试项	5.4.1.5 完整性校验																				
测试内容及过程	<p>对客户端安装包进行篡改，修改相关模块代码或资源内容后进行二次编译并安装运行。查看篡改后的安装包是否能够正常安装，并成功运行。</p>  <p>1. shotec_TEST!!! 请输入您的手机号码，点击“免费获取短信验证码”按钮。 2. 输入您收到的验证码点击“验证”按钮即可。</p> <p>根据证监会相关要求，手机进行证券交易必</p> <table border="1" data-bbox="491 1747 976 2004"> <tr> <td>600</td> <td>1</td> <td>2</td> <td>3</td> <td>DEL ← X</td> </tr> <tr> <td>300</td> <td>4</td> <td>5</td> <td>6</td> <td>03</td> </tr> <tr> <td>000</td> <td>7</td> <td>8</td> <td>9</td> <td>04</td> </tr> <tr> <td>字母</td> <td>系统键</td> <td>0</td> <td>.</td> <td>关闭</td> </tr> </table>	600	1	2	3	DEL ← X	300	4	5	6	03	000	7	8	9	04	字母	系统键	0	.	关闭
600	1	2	3	DEL ← X																	
300	4	5	6	03																	
000	7	8	9	04																	
字母	系统键	0	.	关闭																	

	经测试，发现篡改后的apk可以成功安装并运行。
测试结论	篡改后的apk可以成功安装，并能够成功运行，该项不符合。

A.7 案例七：终端安全测试

测试环境	Android客户端
测试项	5.4.2.2 进程保护
测试内容及过程	<p>通过使用进程注入等技术，试图获取应用进程的访问权限，检验进程保护措施是否有效。此处使用ptrace注入方式进行测试。</p>  <p>成功注入进程，并在进程中注入了libhello.so。</p>
测试结论	成功通过ptrace对目标进程注入了libhello.so，进程保护不完善，该项不符合。

A.8 案例八：终端安全测试

测试环境	Android客户端
测试项	5.4.3.2 剩余信息保护
测试内容及过程	1. 卸载程序后，使用工具对“卸载残留”进行检测，查看是否能检测到卸载残留。

	 <p>上午11:28</p> <p>清理加速</p> <p>GB</p> <p>5.21 已发现</p> <p>正在扫描:/storage/emulated/0/SogouMiniMap</p> <ul style="list-style-type: none"> 内存垃圾 0B/0B ✓ 系统垃圾 ○ 缓存垃圾 7.25GB/10.4GB ○ 广告垃圾 3.73KB/3.73KB ✓ 大文件 0B/317MB ○ 卸载残留 ✓ 安装包 ○ <p>停止扫描</p> <p>工具扫描结果显示，未发现卸载残留。</p> <p>2. 查看客户端软件是否会在系统公共目录（如：照片、视频等）保存敏感信息。</p>
测试结论	检测结果显示，未发现卸载残留，且未在公共目录进行数据保存，该项符合。

附 录 B
(规范性)
检测项权重表

检测的项的权重值见表B.1。

表 B.1 检测项权重表

序号	检测类别	检测大项	检测小项	综合权重值
1	身份鉴别	鉴别方式	二次认证	0.5
2			实名登记	0.5
3			登录失败处理	1
4			会话超时	0.5
5		口令安全	存储安全	1
6			传输安全	1
7			残留信息保护	1
8			安全输入	1
9			敏感信息显示	1
10			口令复杂度	0.5
11	网络通信安全	通讯协议	安全通讯协议	1
12			数据保密性	1
13		会话管理	缓存信息保护	0.5
14			安全提示	0.5
15			会话鉴别	0.5
16			操作提醒	0.25
17		第三方网络传输	安全通道	1
18	数据安全	数据录入	数据录入加密	1
19			页面返回保护	0.5
20		数据存储	敏感信息存储	1
21			剩余信息保护	1
22			业务数据安全	0.5
23	终端安全	应用程序保护	防逆向	1
24			输入保护	1
25			输入校验	1
26			外部资源授权	0.5
27			完整性校验	1
28			异常处理	0.5
29			移动终端环境	运行环境安全
30		进程保护		0.5
31		异常监测		0.25

序号	检测类别	检测大项	检测小项	综合权重值
32		安装、卸载与更新	终端授权提示	0.25
33			剩余信息保护	0.5
34			系统配置复原	0.25
35			系统安全	1
36			完整性校验	0.5
37			更新推送	0.25
38			强制更新	0.5
39			开发安全	安全架构
40	安全设计	0.5		
41	安全编码	0.5		
42	安全测试	1		
43	安全插件	0.5		
44	安全发布	证书签名		0.5
45	安全审计	日志生成	登录日志	1
46			操作日志	1
47			调试日志	0.5
48		日志管理	保存时间	0.5
49			集中存储	0.5
50			敏感日志信息	1
51	个人信息保护	个人信息保护	个人信息保护	1

附 录 C
(规范性)
一票否决项和增强项统计

一票否决项和增强项见表C.1。

表 C.1 一票否决项和增强项

检测项编号	检测类别	检测大项	检测小项	增强项	一票否决属性
5.1.1.1	身份鉴别	鉴别方式	二次认证	✓	
5.1.1.2			实名登记		
5.1.1.3			登录失败处理		✓
5.1.1.4			会话超时		
5.1.2.1		口令安全	存储安全		✓
5.1.2.2			传输安全	✓	
5.1.2.3			残余信息保护	✓	
5.1.2.4			安全输入	✓	
5.1.2.5			敏感信息显示		
5.1.2.6			口令复杂度		
5.2.1.1	网络通信安全	通讯协议	安全通讯协议		✓
5.2.1.2			数据保密性	✓	
5.2.2.1		会话管理	缓存信息保护		
5.2.2.2			安全提示		
5.2.2.3			会话鉴别		
5.2.2.4			操作提醒		
5.2.3.1		第三方网络传输	安全通道		✓
5.3.1.1	数据安全	数据录入	数据录入加密	✓	
5.3.1.2			页面返回保护	✓	
5.3.2.1		数据存储	敏感信息存储	✓	
5.3.2.2			剩余信息保护		
5.3.2.3			业务数据安全		
5.4.1.1	终端安全	应用程序保护	防逆向		✓
5.4.1.2			输入保护		✓
5.4.1.3			输入校验	✓	
5.4.1.4			外部资源授权		
5.4.1.5			完整性校验		
5.4.1.6			异常处理		
5.4.2.1		移动终端环境	运行环境安全		
5.4.2.2			进程保护		
5.4.2.3			异常监测	✓	
5.4.3.1		安装、卸载与更	终端授权提示		

检测项编号	检测类别	检测大项	检测小项	增强项	一票否决属性
5.4.3.2		新	剩余信息保护		
5.4.3.3			系统配置复原		
5.4.3.4			系统安全		✓
5.4.3.5			完整性校验		
5.4.3.6			更新推送		
5.4.3.7			强制更新	✓	
5.5.1.1			开发安全	安全架构	安全需求
5.5.1.2	安全设计				
5.5.1.3	安全编码				
5.5.1.4	安全测试				
5.5.1.5	安全插件				
5.5.2.1	安全发布	证书签名			
5.6.1.1	安全审计	日志生成	登录日志		
5.6.1.2			操作日志	✓	
5.6.1.3			调试日志		
5.6.2.1		日志管理	保存时间		
5.6.2.2			集中存储		
5.6.2.3			敏感日志信息		
5.7.1.1	个人信息保护	个人信息保护	个人信息保护		✓

附录 D

(规范性)

App 违法违规收集使用个人信息行为认定方法

D.1 未公开收集使用规则

以下行为可被认定为“未公开收集使用规则”：

- a) 在 App 中没有隐私政策，或者隐私政策中没有收集使用个人信息规则；
- b) 在 App 首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；
- c) 隐私政策等收集使用规则难以访问，如进入 App 主界面后，需多于 4 次点击等操作才能访问到；
- d) 隐私政策等收集使用规则难以阅读，如文字过小过密、颜色过淡、模糊不清，或未提供简体中文版等。

D.2 未明示收集使用个人信息的目的、方式和范围

以下行为可被认定为“未明示收集使用个人信息的目的、方式和范围”：

- a) 未逐一列出 App(包括委托的第三方或嵌入的第三方代码、插件)收集使用个人信息的目的、方式、范围等；
- b) 收集使用个人信息的目的、方式、范围发生变化时，未以适当方式通知用户，适当方式包括更新隐私政策等收集使用规则并提醒用户阅读等；
- c) 在申请打开可收集个人信息的权限，或申请收集用户身份证号、银行账号、行踪轨迹等个人敏感信息时，未同步告知用户其目的，或者目的不明确、难以理解；
- d) 有关收集使用规则的内容晦涩难懂、冗长繁琐，用户难以理解，如使用大量专业术语等。

D.3 未经用户同意收集使用个人信息

以下行为可被认定为“未经用户同意收集使用个人信息”：

- a) 征得用户同意前就开始收集个人信息或打开可收集个人信息的权限；
- b) 用户明确表示不同意后，仍收集个人信息或打开可收集个人信息的权限，或频繁征求用户同意、干扰用户正常使用；
- c) 实际收集的个人信息或打开的可收集个人信息权限超出用户授权范围；
- d) 以默认选择同意隐私政策等非明示方式征求用户同意；
- e) 未经用户同意更改其设置的可收集个人信息权限状态，如 App 更新时自动将用户设置的权限恢复到默认状态；
- f) 利用用户个人信息和算法定向推送信息，未提供非定向推送信息的选项；
- g) 以欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限，如故意欺瞒、掩饰收集使用个人信息的真实目的；
- h) 未向用户提供撤回同意收集个人信息的途径、方式；
- i) 违反其所声明的收集使用规则，收集使用个人信息。

D.4 违反必要原则，收集与其提供的服务无关的个人信息

以下行为可被认定为“违反必要原则，收集与其提供的服务无关的个人信息”：

- a) 收集的个人信息类型或打开的可收集个人信息权限与现有业务功能无关；
- b) 因用户不同意收集非必要个人信息或打开非必要权限，拒绝提供业务功能；
- c) App 新增业务功能申请收集的个人信息超出用户原有同意范围，若用户不同意，则拒绝提供原有业务功能，新增业务功能取代原有业务功能的除外；
- d) 收集个人信息的频度等超出业务功能实际需要；
- e) 仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，强制要求用户同意收集个人信息；
- f) 要求用户一次性同意打开多个可收集个人信息的权限，用户不同意则无法使用。

D.5 未经同意向他人提供个人信息

以下行为可被认定为“未经同意向他人提供个人信息”：

- a) 既未经用户同意，也未做匿名化处理，App 客户端直接向第三方提供个人信息，包括通过客户端嵌入的第三方代码、插件等方式向第三方提供个人信息；
- b) 既未经用户同意，也未做匿名化处理，数据传输至 App 后台服务器后，向第三方提供其收集的个人信息；
- c) App 接入第三方应用，未经用户同意，向第三方应用提供个人信息。

D.6 未按法律规定提供删除或更正个人信息功能或未公布投诉、举报方式等信息

以下行为可被认定为“未按法律规定提供删除或更正个人信息功能”或“未公布投诉、举报方式等信息”：

- a) 未提供有效的更正、删除个人信息及注销用户账号功能；
- b) 为更正、删除个人信息或注销用户账号设置不必要或不合理条件；
- c) 虽提供了更正、删除个人信息及注销用户账号功能，但未及时响应用户相应操作，需人工处理的，未在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理；
- d) 更正、删除个人信息或注销用户账号等用户操作已执行完毕，但 App 后台并未完成的；
- e) 未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）受理并处理的。