ICS 03.060
CCS A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0240—2021

证券期货业移动互联网应用程序安全检测规范

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

2021－12－29 发布　　2021－12－29 实施

中国证券监督管理委员会　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范》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。

本文件由全国金融标准化技术委员会证券分技术委员会（SAC TC 180）提出。

本文件由全国金融标准化技术委员会（SAC TC 180/SC4）归口管理。

本文件起草单位：中国证券监督管理委员会、中证信息技术服务有限责任公司、大商所飞泰测试技术有限公司、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、信息产业信息安全测评中心。

本文件主要起草人：姚前、蒋东兴、周云晖、陆骋、周思宇、王晓、王恺、周嘉杰、周桉、路一、罗璇、贾石、任亚男、孙瑞超、肖昱、孙川、李宏达、倪惠康、俞枫、陈凯晖、沙明、刘嵩、甘张生、万晓鹰、董晶晶、冀乃杰。

证券期货业移动互联网应用程序安全检测规范

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等。

注1：本文件中涉及到的密码应用，依据国家密码管理局规定实施。

注2：本文件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检测法，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 35273—2020 信息安全技术 个人信息安全规范

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 25069、GB/T 35273—2020、JR/T 0192—2020界定的以及下列术语和定义适用于本文件。

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（信息技术服务机构）发布的，安装在移动终端上，通过互联网方式访问，用于证券期货查询、交易、业务办理等相关业务，或办公、信息披露等的应用程序。

注：包括但不限于可执行文件、组件等。

[来源：JR/T 0192—2020，3.2，有修改]

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）及依托该硬件运行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。

注1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注2：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如，用户画像或特征标签，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，属于个人信息。

[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 1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账户、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下（含）儿童的个人信息等。

注 2：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、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，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 程序类型和检测范围

4.1.1 程序类型

移动互联网应用程序分为以下5种类型：

a) 办公类移动互联网应用程序；
b) 信息披露类移动互联网应用程序；
c) 业务办理类移动互联网应用程序；
d) 证券期货交易类移动互联网应用程序；
e) 证券期货业其他参与机构（信息技术服务机构）发布的非交易类、非业务办理类移动互联网应用程序。

4.1.2 检测范围

检测范围如下：

a) 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；
b) 部分证券期货业移动互联网应用程序服务端的核心安全内容，如安全审计日志等。

4.2 检测框架

检测框架见图1。

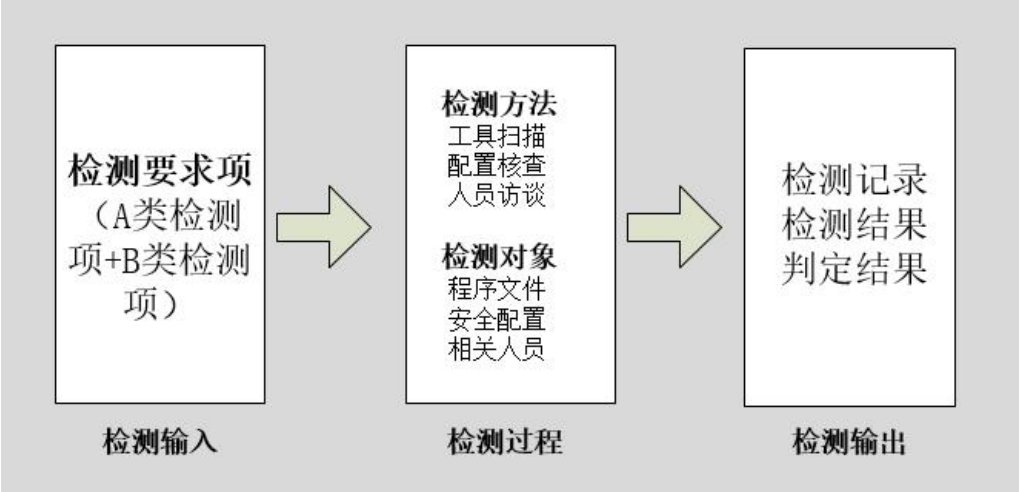

图 1　检测框架

其中，A类检测项和B类检测项的含义见4.5。

4.3　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及相关开发设计文档；

b)　检测人员查看相关开发设计文档，并进行人员访谈，获取相关检测信息，保留检测记录；

c)　检测人员使用工具对移动互联网应用程序进行扫描，获得检测结果；

d)　检测人员通过人工配置核查方式验证工具扫描的结果，并完成工具扫描未覆盖的检测项；

e)　检测人员依据本文件的判定方式，经过综合判定，给出最终判定结果。

4.4　检测方法

检测方法分为人员访谈、工具扫描和配置核查三种，具体如下：

——人员访谈即通过访谈相关负责人了解系统的整体安全状况、技术细节以及安全管理的执行成效等内容，判断系统安全保护措施的有效性；

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

——配置核查即人工参考工具扫描的结果，通过对系统、文档等的观察、分析和技术测试等活动，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。

4.5　A 类检测项和 B 类检测项

本文件根据移动互联网应用程序的类别提出了不同的检测要求，A类检测项要求和B类检测项主要是根据对象类别不同而进行的区分，具体如下：

——属于证券期货交易类、业务办理类的移动互联网应用程序应遵照 A 类检测项要求和 B 类检测项要求执行；

——属于办公类、信息披露类，或证券期货业其他参与机构（信息技术服务机构）发布的非交易类、非业务办理类移动互联网应用程序应遵照 A 类检测项要求执行；

——若同一个移动互联网应用程序属于多种类别，具体检测项应就高执行。

附录A规定了A类检测项和B类检测项。

5 检测要求及检测方式

5.1 移动终端安全

5.1.1 应用程序保护

5.1.1.1 防逆向

5.1.1.1.1 检测目的

检查移动互联网应用程序客户端是否采取防动态调试、代码混淆等防逆向措施，防止被反编译或逆向分析，确保程序的自身安全。

5.1.1.1.2 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的自身安全的有效措施。

5.1.1.1.3 通过要求

应采取防动态调试、代码混淆、防逆向等技术对关键代码、核心逻辑进行保护。

5.1.1.2 安全接口

5.1.1.2.1 检测目的

检查移动互联网应用程序是否制定安全设计文档，移动互联网应用程序自身是否存在接口设计方面的安全问题。

5.1.1.2.2 检测流程

查看移动互联网应用程序的安全设计文档及检测移动互联网应用程序，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。

5.1.1.2.3 通过要求

不应设计有违反和绕过安全措施的任何类型的接口和开发文档中未说明的任何模式的接口。

5.1.1.3 输入保护

5.1.1.3.1 检测目的

检查移动互联网应用程序是否能够保障输入信息的机密性。

5.1.1.3.2 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。

5.1.1.3.3 通过要求

移动互联网应用程序应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。

5.1.1.4 输入校验

5.1.1.4.1 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。

5.1.1.4.2 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，或修改人机接口或通信接口的部分字段，验证数据有效性校验功能是否生效。

5.1.1.4.3 通过要求

应对输入信息的合法性进行识别。

5.1.1.5 外部资源授权

5.1.1.5.1 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、删除移动终端上与个人信息相关的数据前，是否得到用户许可。

5.1.1.5.2 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个人信息相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。

5.1.1.5.3 通过要求

未得到用户许可前，不应访问、修改、删除移动终端上与个人信息相关的数据。

5.1.1.6 授权提示

5.1.1.6.1 检测目的

检查移动互联网应用程序客户端获取移动终端系统上与个人信息相关权限时，是否以明显方式提示用户获取该权限的目的，并得到用户许可。

5.1.1.6.2 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系统上与个人信息相关权限过程中，是否以明显方式提示用户获取该权限的目的，包括但不限于图标、文字，声音提示等，并得到用户许可。

5.1.1.6.3 通过要求

获取移动终端系统上与个人信息相关权限，应以明显方式提示用户获取该权限的目的，包括但不限于图标、文字和声音提示等，并得到用户许可。

5.1.1.7 完整性校验

5.1.1.7.1 检测目的

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。

5.1.1.7.2 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，并进行重签名和二次打包，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。

5.1.1.7.3 通过要求

应具备完整性校验机制，防止被重签名和二次打包。关键的校验代码应得到保护。

5.1.1.8 异常处理

5.1.1.8.1 检测目的

检查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。

5.1.1.8.2 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。

5.1.1.8.3 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，应提示明确、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。

5.1.2 移动终端环境

5.1.2.1 运行环境安全

5.1.2.1.1 检测目的

检查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。

5.1.2.1.2 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性检测功能，对诸如移动终端操作系统是否已被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。

5.1.2.1.3 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，并提示发现的风险。

5.1.2.2 进程保护

5.1.2.2.1 检测目的

检查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。

5.1.2.2.2 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。

5.1.2.2.3 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。

5.1.2.3 异常监测

5.1.2.3.1 检测目的

检查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，是否在必要时停止应用运行。

5.1.2.3.2 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，是否在必要时停止应用运行。

5.1.2.3.3 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并在必要时停止应用运行。

5.1.3 安装与卸载

5.1.3.1 安装确认

5.1.3.1.1 检测目的

检查移动互联网应用程序客户端安装或首次运行时，是否提示用户对其使用的移动终端资源、移动终端系统权限和移动终端数据进行确认。

5.1.3.1.2 检测流程

移动互联网应用程序客户端在安装或首次运行时，检查是否跳出提示窗口，让用户对其使用的移动终端资源（包含通信资源和外设接口）、移动终端系统权限和移动终端数据进行确认。

5.1.3.1.3 通过要求

移动互联网应用程序客户端安装或首次运行时应提示用户对其使用的移动终端资源（包含通信资源和外设接口）、移动终端系统权限和移动终端数据进行确认。

5.1.3.2 剩余信息保护

5.1.3.2.1 检测目的

检查移动互联网应用程序客户端安装和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得到用户许可。

5.1.3.2.2 检测流程

检查移动互联网应用程序客户端卸载完成后，用户安装和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。

5.1.3.2.3 通过要求

安装和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得到用户许可。

5.1.3.3 系统安全

5.1.3.3.1 检测目的

检查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。

5.1.3.3.2 检测流程

通过工具扫描等方式检查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。

5.1.3.3.3 通过要求

移动互联网应用程序客户端不应影响移动终端操作系统和其他应用软件的功能。

5.1.4 升级与更新

5.1.4.1 完整性校验

5.1.4.1.1 检测目的

检查移动互联网应用程序客户端在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。

5.1.4.1.2 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。

5.1.4.1.3 通过要求

移动互联网应用程序客户端在更新时应进行真实性和完整性校验。

5.1.4.2 更新推送

5.1.4.2.1 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。

5.1.4.2.2 检测流程

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

5.1.4.2.3 通过要求

应至少采取一种安全机制，保证升级的时效性，例如用户授权后自动升级、更新通知等手段。

5.1.4.3 强制更新

5.1.4.3.1 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，是否能够采取强制授权升级的方式修复客户端问题。

5.1.4.3.2 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，检查系统强制授权升级策略是否有效。

5.1.4.3.3 通过要求

当因重大安全问题需要升级时，应能够强制用户完成授权升级后才提供服务。

5.2 身份鉴别

5.2.1 鉴别方式

5.2.1.1 二次认证

5.2.1.1.1 检测目的

检查移动互联网应用程序初次认证后，是否在资金类交易、客户信息修改等关键业务处增设二次认证的环节，是否使用存放在移动客户端的信息进行认证。

5.2.1.1.2 检测流程

检查移动互联网应用程序初次认证后，是否在资金类交易、客户信息修改等关键业务处增设二次认证的环节，查看其认证方式。尝试替换移动客户端的信息绕过认证。

5.2.1.1.3 通过要求

对于资金类交易、客户信息修改等关键业务，应增设二次认证的环节，且不应仅使用存放在移动客户端的本地信息进行认证。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。

5.2.1.2 用户登记

5.2.1.2.1 检测目的

若首次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是否再次进行用户名密码登记并核验。

5.2.1.2.2 检测流程

检查送检文档中关于用户登记的说明，查看在哪些情况下移动互联网应用程序进行用户登记。

首次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用户名密码登记并核验。

5.2.1.2.3 通过要求

若首次采用第三方移动互联网应用程序的认证方式，行业机构的移动互联网应用程序应再次进行用户名密码登记并核验。

5.2.1.3 登录失败处理

5.2.1.3.1 检测目的

检查移动互联网应用程序是否提供了登录失败处理机制。

5.2.1.3.2 检测流程

检测流程如下：

a）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；

b）检查移动互联网应用程序在认证用户身份时，是否具备认证失败处理机制。

5.2.1.3.3 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。

5.2.1.4 登录超时

5.2.1.4.1 检测目的

检查移动互联网应用程序是否提供了登录会话超时重鉴别机制。

5.2.1.4.2 检测流程

检测流程如下：

a）检查开发文档中，移动互联网应用程序是否提供登录会话超时重鉴别机制。

b）检查证券期货业移动互联网应用在登录会话超时后是否需再次进行身份鉴别。

5.2.1.4.3 通过要求

应具备登录超时锁定或自动退出功能，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。

5.2.2 鉴别数据保护

5.2.2.1 授权保护

5.2.2.1.1 检测目的

检查移动互联网应用程序是否能够未授权查阅或修改鉴别数据。

5.2.2.1.2 检测流程

检查移动互联网应用程序是否存在查阅或修改鉴别数据的功能，检查是否在查阅或修改鉴别数据时需要进行二次身份鉴别。

5.2.2.1.3 通过要求

不应未授权查阅或修改鉴别数据。

5.2.2.2 用户提醒

5.2.2.2.1 检测目的

检查对于资金类交易、客户信息修改等关键业务是否通过短信等多媒体方式对用户进行提醒。

5.2.2.2.2 检测流程

查看移动互联网应用程序中关于资金类交易（如转账等）、客户信息修改等关键业务的功能模块，并进行相关业务操作，查看是否能够通过短信等多媒体方式对用户进行提醒。

5.2.2.2.3 通过要求

对于资金类交易、客户信息修改等关键业务应通过短信等多媒体方式对用户进行提醒。

5.2.2.3 身份绑定

5.2.2.3.1 检测目的

检查身份认证时绑定对象是否为用户身份信息。

5.2.2.3.2 检测流程

检查移动互联网应用程序身份认证时（如用户注册）绑定对象是否为用户身份信息，检查同一用户身份信息是否可注册多个用户。

5.2.2.3.3 通过要求

身份认证时绑定对象应为用户身份信息，不局限于移动终端的设备单一信息。

5.2.3 密码安全

5.2.3.1 存储安全

5.2.3.1.1 检测目的

检查移动互联网应用程序是否将密码明文保存在移动终端的本地存储上。

5.2.3.1.2 检测流程

通过字段查询等方式检查移动互联网应用程序是否将密码明文保存在移动终端的本地存储上。

5.2.3.1.3 通过要求

密码不应以任何形式明文保存在移动终端的本地存储上。

5.2.3.2 传输安全

5.2.3.2.1 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密码信息。

5.2.3.2.2 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密码进行加密处理，所采用的加密算法是否符合国家密码主管部门认可的密码算法。

5.2.3.2.3 通过要求

密码在传输过程中不应以明文的形式传输，应采用符合国家密码主管部门认可的密码算法。

5.2.3.3 残留信息保护

5.2.3.3.1 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密码和密钥信息。

5.2.3.3.2 检测流程

检查移动互联网应用程序的缓存和日志信息，查看是否存在密码和密钥信息。

5.2.3.3.3 通过要求

密码和密钥不应在缓存和日志中输出。

5.2.3.4 安全输入

5.2.3.4.1 检测目的

检查移动互联网应用程序在输入密码时是否采取技术措施防止密码被盗取。

5.2.3.4.2 检测流程

检测流程如下：

a）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密码被盗取；

b）检查移动互联网应用程序在输入密码信息时是否可防截屏操作；

c）检查移动互联网应用程序在输入密码信息时是否可防信息截获。

5.2.3.4.3 通过要求

输入密码信息时应采取技术措施防止密码被盗取。

5.2.3.5 密码显示

5.2.3.5.1 检测目的

检查移动互联网应用程序是否默认以非明文的形式显示密码。

5.2.3.5.2 检测流程

检查移动互联网应用程序在密码展示处，是否默认以非明文的方式显示密码。

5.2.3.5.3 通过要求

密码展示处不应默认以明文的形式显示密码。

5.2.3.6 密码复杂度

5.2.3.6.1 检测目的

检查移动互联网应用程序是否提供密码复杂度校验功能。

5.2.3.6.2 检测流程

检测流程如下：

a) 检查开发文档中，移动互联网应用程序是否提供密码复杂度校验功能。

b) 检查移动互联网应用程序在密码设置处是否提供密码复杂度校验功能，是否能够设置易于猜测的密码。

5.2.3.6.3 通过要求

应提供密码复杂度校验功能，防止用户设置易于猜测的密码。

5.2.3.7 密码修改

5.2.3.7.1 检测目的

检查移动互联网应用程序是否在对密码进行修改前验证用户身份。

5.2.3.7.2 检测流程

通过移动互联网应用程序的修改密码功能，检查是否程序采取相应的安全措施（如验证旧密码、获取短信验证码等方式）对用户身份进行验证。

5.2.3.7.3 通过要求

应在对密码进行修改前验证用户身份。

5.3 网络通信安全

5.3.1 通讯协议

5.3.1.1 安全协议

5.3.1.1.1 检测目的

检查移动互联网应用程序与服务器之间敏感数据的通信是否使用安全的通信协议和加密算法。

5.3.1.1.2 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安全通信协议，在敏感数据传输时是否对服务端证书的合法性进行校验。

5.3.1.1.3 通过要求

应采用安全的通信协议和加密算法，敏感数据传输时应对服务端证书的合法性进行校验。

5.3.1.2 安全版本

5.3.1.2.1 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。

5.3.1.2.2 检测流程

检查移动互联网应用程序与服务器是否采用安全的通信协议，检查通信协议不应存在安全隐患。

5.3.1.2.3 通过要求

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。

5.3.1.3 密码安全

5.3.1.3.1 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国家密码主管部门认可的安全加密算法和密钥长度。

5.3.1.3.2 检测流程

a) 检查开发文档，了解移动互联网应用程序使用的加密算法和密钥长度；
b) 检查移动互联网应用程序与服务器重要通信过程和重要存储过程中使用的加密算法和密钥长度是否符合国家密码主管部门的要求。

5.3.1.3.3 通过要求

应使用国家密码主管部门认可的安全加密算法和密钥长度。

5.3.2 会话管理

5.3.2.1 缓存信息保护

5.3.2.1.1 检测目的

检查移动互联网应用程序在会话结束后是否立即清除敏感数据缓存，防止信息泄露。

5.3.2.1.2 检测流程

检测流程如下：
a) 检查开发文档中，移动互联网应用程序在会话结束后是否有清除敏感数据缓存的措施；
b) 检查移动互联网应用程序在会话结束后是否立即清除敏感数据缓存。

5.3.2.1.3 通过要求

移动互联网应用程序在会话结束后应立即清除敏感数据缓存，防止信息泄露。

5.3.2.2 安全提示

5.3.2.2.1 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。

5.3.2.2.2 检测流程

检测流程如下：
a) 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；
b) 使用不同移动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。

5.3.2.2.3 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。

5.3.2.3 会话鉴别

5.3.2.3.1 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。

5.3.2.3.2 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（如token方式），尝试删除身份鉴别信息和替换无权限用户的鉴别信息进行请求。

5.3.2.3.3 通过要求

登录完成后的会话管理阶段的所有请求应对用户的合法身份进行鉴别，鉴别通过后才能进行操作。

5.3.2.4 会话保护

5.3.2.4.1 检测目的

检查是否对会话采取保护措施，防止软件与后台服务器之间的会话被窃听、篡改、伪造、重放等。

5.3.2.4.2 检测流程

检测流程如下：

a）通过网络层截包分析等方式获取通信报文，查看程序与后台服务器之间的会话是否采取加密等保护措施；

b）在应用层尝试获取会话信息，获取后进行篡改和伪造，查看服务器后台是否响应该非法报文；

c）在应用层尝试对关键业务操作进行重放攻击，查看服务器后台是否响应该重放报文。

5.3.2.4.3 通过要求

应采取会话保护措施，防止软件与后台服务器之间的会话被窃听、篡改、伪造、重放等。

5.3.2.5 会话终止

5.3.2.5.1 检测目的

检查移动互联网应用程序在用户执行注销/登出后，会话是否被安全终止。

5.3.2.5.2 检测流程

使用正常用户在移动互联网应用程序上进行登录操作获取合法权限，收集正常用户的会话信息然后执行注销/登出操作；尝试使用之前的会话信息与服务器进行数据交互，查看该会话是否仍然存在之前的访问权限。

5.3.2.5.3 通过要求

用户执行注销/登出后，会话应被安全终止。

5.3.2.6 会话超时

5.3.2.6.1 检测目的

检查移动互联网应用程序是否设计合理的会话超时控制策略。

5.3.2.6.2 检测流程

使用正常用户在移动互联网应用程序上进行登录操作建立有效会话，当会话超出预先设定时限时，是否能够自动退出会话状态。

5.3.2.6.3 通过要求

应设计合理的会话超时控制策略，当会话超出预先设定时限时，自动退出会话状态。

5.3.2.7 并发限制

5.3.2.7.1 检测目的

检查移动互联网应用程序与服务器的连接是否限制会话并发连接数，限制同一用户的会话并发连接数。

5.3.2.7.2 检测流程

检测流程如下：

a) 检查服务器配置，是否对同一用户的连接会话数量进行限制；
b) 询问管理员是否限制同一用户的会话并发连接数，然后通过同一用户在不同的移动终端上采用移动互联网应用程序进行登录操作，查看是否触发限制功能。

5.3.2.7.3 通过要求

应限制会话并发连接数，限制同一用户的会话并发连接数，避免恶意用户创建多个并发的会话来消耗系统资源，影响业务的可用性。

5.3.3 第三方网络通信

5.3.3.1 安全通道

5.3.3.1.1 检测目的

检查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是否建立加密安全通道。

5.3.3.1.2 检测流程

检测流程如下：

a) 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；
b) 检查移动互联网应用程序与服务器是否建立安全的加密通道，加密算法和密钥长度是否符合国家密码主管部门的要求。

5.3.3.1.3 通过要求

移动互联网应用程序和服务器之间的通信如使用第三方服务器，应建立服务器与移动互联网应用程序之间的加密安全通道，防止信息被第三方截获或篡改。

5.4 数据安全

5.4.1 数据录入

5.4.1.1 数据录入安全

5.4.1.1.1 检测目的

检查移动互联网应用程序在用户输入密码等个人敏感信息时，是否以非明文显示。

5.4.1.1.2 检测流程

通过检查开发文档等方式，发现移动互联网应用程序需要输入密码的业务功能点，检查在用户输入密码时，是否以非明文形式显示。

5.4.1.1.3 通过要求

用户输入密码时，不应以明文显示。

5.4.1.2 页面返回保护

5.4.1.2.1 检测目的

检查移动互联网应用程序是否支持界面返回后自动清除该界面敏感信息的机制。

5.4.1.2.2 检测流程

检测流程如下：

a) 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；
b) 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；
c) 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；
d) 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。

5.4.1.2.3 通过要求

移动互联网应用程序应支持界面返回后自动清除该界面个人敏感信息的机制。

5.4.2 数据存储

5.4.2.1 敏感信息存储

5.4.2.1.1 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。

5.4.2.1.2 检测流程

检测流程如下：

a) 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；
b) 个人敏感信息的范围包括但不限于账户口令、身份证号码、财产信息等；

c) 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；
d) 检查移动互联网应用程序存储个人敏感信息之前是否获取客户许可或明示同意。

5.4.2.1.3 通过要求

移动互联网应用程序不应在客户未许可或不知情的情况下存储个人敏感信息，且不应以任何形式存储明文密码信息。

5.4.2.2 客户信息保护

5.4.2.2.1 检测目的

检查移动互联网应用程序卸载后，移动终端中是否仍有客户信息残留。

5.4.2.2.2 检测流程

检测流程如下：
a）检查开发文档中，移动互联网应用程序卸载后移动终端中是否仍有客户信息残留相关说明；
b）使用文件系统管理工具检查移动互联网应用程序卸载后，移动终端中是否仍有客户信息残留。

5.4.2.2.3 通过要求

移动互联网应用程序卸载后，应清除移动终端中的所有客户信息。

5.4.2.3 敏感信息保护

5.4.2.3.1 检测目的

检查移动互联网应用程序退出时，是否清除或加密存储客户敏感数据，保证个人敏感信息的安全性。

5.4.2.3.2 检测流程

检测流程如下：
a) 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或加密存储客户敏感数据相关说明。
b) 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客户敏感数据。

5.4.2.3.3 通过要求

移动互联网应用程序退出时，应清除或加密存储客户的敏感数据。

5.5 开发安全

5.5.1 安全需求

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在架构设计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在架构设计时应制定安全需求，描述移动互联网应用程序应具备的安全功能。

5.5.2 安全开发

5.5.2.1 安全编码

5.5.2.1.1 检测目的

检查是否制定移动互联网应用程序的开发编码安全手册，开发过程是否遵循相关编码安全要求。

5.5.2.1.2 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。

5.5.2.1.3 通过要求

移动互联网应用程序开发过程中应遵循编码安全要求，减少应用程序安全漏洞。

5.5.2.2 安全插件

5.5.2.2.1 检测目的

检查是否使用安全的第三方开发工具和第三方插件。

5.5.2.2.2 检测流程

检测流程如下：

a) 检查移动互联网应用程序中的第三方插件是否具有安全测试报告或证书；
b) 检查所使用的第三方开发工具是否经过安全认定和检查。

5.5.2.2.3 通过要求

所使用的第三方开发工具和第三方插件应具有安全检测报告或安全认证。

5.5.2.3 安全逻辑

5.5.2.3.1 检测目的

检查身份认证的逻辑、重要数据的校验功能是否在服务器端完成。

5.5.2.3.2 检测流程

检测流程如下：

a) 检查移动互联网应用程序的身份认证逻辑是否在服务器端完成；
b) 检查重要数据的校验功能是否在服务器端完成，如数据报文的完整性校验、口令的复杂度校验（若口令在客户端采用不可逆算法，则可在客户端进行校验）等。

5.5.2.3.3 通过要求

认证逻辑、校验功能应在服务器端完成。

5.5.3 安全测试

5.5.3.1 上线测试

5.5.3.1.1 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。

5.5.3.1.2 检测流程

询问管理员移动互联网应用程序上线前是否进行安全测试，并查看相关的测试报告。

5.5.3.1.3 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。

5.5.3.2 功能测试

5.5.3.2.1 检测目的

检查是否提供安全功能操作和安全功能测试文档。

5.5.3.2.2 检测流程

检查是否提供安全功能操作和安全功能测试文档，是否与移动互联网应用程序的实际情况保持一致。

5.5.3.2.3 通过要求

应提供安全功能操作文档，应提供安全功能测试文档。

5.5.4 安全发布

5.5.4.1 测试数据

5.5.4.1.1 检测目的

检查正式版本发布时，是否删除测试数据和所有用于调试的代码。

5.5.4.1.2 检测流程

通过工具扫描或人工核查方式查看正式版本发布的移动互联网应用程序是否存在测试文件和测试代码。

5.5.4.1.3 通过要求

正式版本发布时，应删除测试数据和所有用于调试的代码。

5.5.4.2 证书签名

5.5.4.2.1 检测目的

检查移动互联网应用程序是否由发布机构进行签名，签名证书是否标识应用程序的发布者，签名证书是否由专门岗位管理。

5.5.4.2.2 检测流程

检测流程如下：

a) 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；

b) 询问管理员签名证书是否由专门岗位管理。

5.5.4.2.3 通过要求

移动互联网应用程序应由发布机构进行签名，签名证书应标识应用程序的发布者，签名证书应由专门岗位管理。

5.5.4.3 上线发布

5.5.4.3.1 检测目的

检查移动互联网应用程序是否有规范的上线发布流程，是否提供安全可靠的移动应用软件下载、发布、升级渠道。

5.5.4.3.2 检测流程

检测流程如下：

a) 查看移动互联网应用程序上线发布流程的规范文档；

b) 询问管理员移动互联网应用程序的下载、发布、升级渠道，并评估该渠道的安全性。

5.5.4.3.3 通过要求

移动互联网应用程序应有规范的上线发布流程，并提供安全可靠的移动应用软件下载、发布、升级渠道。

5.6 安全审计

5.6.1 日志生成

5.6.1.1 日志内容

5.6.1.1.1 检测目的

检查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。

5.6.1.1.2 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、设备唯一标识、设备型号、设备版本、网络类型、事件描述和结果等信息。

5.6.1.1.3 通过要求

日志应包括事件发生的日期、时间、用户标识、设备唯一标识、设备型号、设备版本、网络类型、事件描述和结果等信息。

5.6.1.2 操作日志

5.6.1.2.1 检测目的

检查移动互联网应用程序服务端是否如实记录用户各项重要操作，如对用户登录成功和失败进行记录。

5.6.1.2.2 检测流程

登录后台服务器日志系统，查看系统是否记录用户的各项重要操作，如登录成功和失败日志等。

5.6.1.2.3 通过要求

日志应如实记录用户各项重要操作，如用户登录成功和失败；校验失败的次数超出阈值导致会话连接终止等。

5.6.1.3 调试日志

5.6.1.3.1 检测目的

检查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

正式发布的移动终端程序应不包含调试过程中的日志

5.6.2 日志管理

5.6.2.1 日志存储

5.6.2.1.1 检测目的

检查日志是否存储于掉电非易失性存储介质中。

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信息，是否采取安全措施（如备份等）进行妥善保护，防止日志丢失。

5.6.2.1.3 通过要求

日志应存储于掉电非易失性存储介质中。

5.6.2.2 日志访问

5.6.2.2.1 检测目的

检查日志是否仅允许授权用户以只读形式访问日志，且支持日志审计。

5.6.2.2.2 检测流程

检测流程如下：

a）询问管理员是否将审计日志提供审计管理员进行日志审计；

b）查看日志的权限管理功能，是否仅允许授权用户以只读形式访问日志。

5.6.2.2.3 通过要求

应仅允许授权用户以只读形式访问日志，且支持日志审计。

5.6.2.3 日志查询

5.6.2.3.1 检测目的

日志是否能够进行查询和分析。

5.6.2.3.2 检测流程

查看移动互联网应用程序服务端的日志信息，是否部署相关工具或开发相关功能能够对日志信息进行整体查询和分析。

5.6.2.3.3 通过要求

日志应具备查询功能。

5.6.2.4 敏感日志保护

5.6.2.4.1 检测目的

检查服务端日志是否记录个人敏感信息。

5.6.2.4.2 检测流程

查看服务端的日志记录，查看客户信息的相关内容，根据信息的敏感性进行筛选和甄别。

5.6.2.4.3 通过要求

日志不应记录个人敏感信息。

5.6.2.5 存储位置

5.6.2.5.1 检测目的

检查日志是否存放于移动互联网应用程序服务端。

5.6.2.5.2 检测流程

查看移动互联网应用程序服务端的日志记录。

5.6.2.5.3 通过要求

日志应存放于服务器端。

5.6.2.6 保存时间

5.6.2.6.1 检测目的

检查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。

5.6.2.6.2 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。

5.6.2.6.3 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十二个月。

5.7 个人信息保护

5.7.1 检测目的

行业机构依据《APP违法违规收集使用个人信息行为认定方法》，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《APP违法违规收集使用个人信息行为认定方法》，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。

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依据《APP违法违规收集使用个人信息行为认定方法》规定。

附 录 A
（规范性）
A 类检测项和 B 类检测项统计

A类检测项和B类检测项见表1。

表 1 A 类检测项和 B 类检测项

序号	检测类别	检测大项	检测小项	A 类检测项	B 类检测项
1	移动终端安全	应用程序保护	防逆向	√	
2			安全接口	√	
3			输入保护	√	
4			输入校验		√
5			外部资源授权	√	
6			授权提示	√	
7			完整性校验	√	
8			异常处理	√	
9		移动终端环境	运行环境安全	√	
10			进程保护	√	
11			异常监测		√
12		安装与卸载	安装确认	√	
13			剩余信息保护	√	
14			系统安全	√	
15		升级与更新	完整性校验	√	
16			更新推送	√	
17			强制更新		√
18	身份鉴别	鉴别方式	二次认证		√
19			用户登记	√	
20			登录失败处理	√	
21			登录超时	√	
22		鉴别数据保护	授权保护	√	
23			用户提醒		√
24			身份绑定		√
25		密码安全	存储安全	√	
26			传输安全		√
27			残留信息保护		√
28			安全输入		√
29			密码显示	√	
30			密码复杂度	√	
31			密码修改	√	

表 1　A 类检测项和 B 类检测项（续）

序号	检测类别	检测大项	检测小项	A 类检测项	B 类检测项
32	网络通信安全	通讯协议	安全协议	√	
33			安全版本	√	
34			密码安全	√	
35		会话管理	缓存信息保护	√	
36			安全提示	√	
37			会话鉴别	√	
38			会话保护	√	
39			会话终止	√	
40			会话超时	√	
41			并发限制		√
42		第三方网络通信	安全通道	√	
43	数据安全	数据录入	数据录入安全		√
44			页面返回保护		√
45		数据存储	敏感信息存储	√	
46			客户信息保护	√	
47			敏感信息保护	√	
48	开发安全	安全需求	安全需求	√	
49		安全开发	安全编码	√	
50			安全插件	√	
51			安全逻辑	√	
52		安全测试	上线测试	√	
53			功能测试	√	
54		安全发布	测试数据	√	
55			证书签名	√	
56			上线发布	√	
57	安全审计	日志生成	日志内容	√	
58			操作日志	√	
59			调试日志	√	
60		日志管理	日志存储	√	
61			日志访问	√	
62			日志查询	√	
63			敏感日志保护	√	
64			存储位置	√	
65			保存时间		√
66	个人信息保护	个人信息保护	个人信息保护	√	

参 考 文 献

[1] JR/T 0060—2021 证券期货业网络安全等级保护基本要求

[2] JR/T 0067—2021 证券期货业网络安全等级保护测评要求

[3] JR/T 0092—2019 移动金融客户端应用软件安全管理规范

[4] 国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、国家市场监督管理总局办公厅.关于印发《App违法违规收集使用个人信息行为认定方法》的通知（国信办秘字〔2019〕191号），2019-11-28