ICS 03.060
A 11

JR

中华人民共和国金融行业标准

JR/T 0192—2020

证券期货业移动互联网应用程序安全规范

Security specification for mobile internet application of securities and futures industry

2020－07－10 发布　　2020－07－10 实施

中国证券监督管理委员会　发布

目　　次

前　言

本标准按照GB/T　1.1—2009给出的规则起草。

本标准由全国金融标准化技术委员会证券分技术委员会（SAC/TC　180/SC4）提出。

本标准由全国金融标准化技术委员会（SAC/TC　180）归口。

本标准起草单位：中国证券监督管理委员会信息中心、上海证券交易所、深圳证券交易所、中证信息技术服务有限责任公司、上海期货交易所、大连商品交易所、中国金融期货交易所、中国证券登记结算有限责任公司、中国期货市场监控中心有限责任公司、中国期货业协会、兴业证券股份有限公司、国泰君安证券股份有限公司、东吴证券股份有限公司、光大证券股份有限公司、华泰证券股份有限公司、海通期货股份有限公司、兴业基金管理有限公司、公安部第三研究所、上海市信息安全测评认证中心。

本标准主要起草人：姚前、刘铁斌、周云晖、叶婧、朱立、马卿平、甘张生、陈磊、居红伟、卫飞、丁新杰、冯小根、焦东亮、周桉、崔慧阳、艾青、王玥、陈凯晖、梅克波、华仁杰、刘嵩、张嵩、王勇斌、徐正伟、张艳、李宏达。

引　言

随着移动互联网新兴技术的蓬勃兴起，层出不穷的创新业务，在商业模式应用、技术风险控制等方面对金融业构成了新的挑战。在当前的互联网金融浪潮中，信息系统建设与安全运行的压力越来越大，所面临的信息安全形势日趋复杂。金融行业的移动互联网应用程序（APP）安全问题尤其严峻。

国家为加强对移动互联网应用程序信息服务的规范管理，鼓励有关行业协会等依法制定自律性管理制度，加强用户权益保护。

行业移动终端应用安全规范，对市场主流移动终端应用开展安全检测与风险评估，完善监测渠道与预警机制，建立移动终端应用安全风险提示系统，及时发现并通报移动终端应用的设计缺陷与安全漏洞，以及假冒、篡改的移动终端应用。督促经营机构加强对移动终端应用的安全管理，切实提高投资者风险防范意识。

证券期货业移动互联网应用程序安全规范

1 范围

本标准规定了证券期货业移动互联网应用程序的移动终端安全、身份鉴别、网络通信安全、数据安全、开发安全和安全审计。

本标准适用于证券期货业机构开发和发布移动互联网应用程序。

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，仅所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 22239—2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 25069—2010 信息安全技术 术语

JR/T 0060—2010 证券期货业信息系统安全等级保护基础要求

3 术语和定义

GB/T 25069—2010、GB/T 22239—2008和JR/T 0060—2010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。

3.2

移动互联网应用程序 mobile internet application; app

安装在移动终端上，用于证券期货查询、交易、业务办理等业务相关的原生应用程序。

注：移动互联网应用程序包含并不限于涉及业务办理类、证券期货交易类的移动互联网应用程序，办公类、信息披露类的移动互联网应用程序，证券期货业其他参与机构（服务机构）发布的移动互联网应用程序。

3.3

客户信息 customer information

移动互联网应用程序所处理，与特定自然人、法人相关，能够单独或通过与其他信息结合识别该特定自然人的计算机数据。

注：计算机数据是与自然人身份属性、财产属性相关的一组数据。

3.4

敏感信息 sensitive information

一旦泄漏、非法提供或者滥用可能危害人身和财产安全，极易导致个人或企业名誉财产受到损害等的个人及企业信息。

4 移动终端安全

4.1 移动互联网应用程序

移动互联网应用程序以独立的程序形式存在移动终端上，其自身应满足安全性要求：

a) 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；
b) 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；
c) 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；
d) 对输入信息的合法性进行识别；
e) 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；
f) 获取移动终端上其他权限，应以明显方式提示用户，包括但不限于图标、文字和声音提示等；
g) 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；
h) 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。

4.2 移动终端环境

移动终端环境应支持以下安全检查：

a) 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；
b) 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；
c) 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。

4.3 安装与卸载

移动互联网应用程序的安装需得到明确授权，且安装过程中不应破坏移动终端环境。卸载时，应能删除由其生成的数据和信息。安装与卸载应满足以下要求：

a) 安装时应提示用户对其使用的终端资源（包含通信资源和外设接口）、终端权限和终端数据进行确认；
b) 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有提示；
c) 不应影响终端操作系统和其他应用软件的功能。

4.4 升级与更新

移动互联网应用程序应支持软件的安全更新，及时提升安全性。升级与更新应满足以下要求：

a) 在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；
b) 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；
c) 当因重大安全问题需要升级时，在应用市场允许的情况下能够强制用户升级后方可使用。

5 身份鉴别

5.1 鉴别方式

移动互联网应用程序应满足以下鉴别认证方式，安全技术要求：

a) 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。认证方式包括密码、生物特征、短信、令牌、图形手势等中的至少一种；
b) 若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；

c） 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；

d） 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。

5.2 鉴别数据保护

应提供以下鉴别数据保护功能：

a） 不应未授权查阅或修改；

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

c） 身份认证绑定对象为用户身份信息，不局限移动终端的设备单一信息。

5.3 密码安全

应保障密码的安全性，满足以下安全性要求：

a） 密码不应以任何形式明文保存在移动终端的本地存储上；

b） 密码在传输过程中不应以明文的形式传输，宜采用国密算法或国际数据加密算法；

c） 密码禁止在缓存和日志中输出；

d） 输入密码信息时应采取技术措施防止密码被盗取；

e） 密码输入框默认禁止明文显示密码；

f） 应提供密码复杂度检查功能，防止用户设置易于猜测的密码；

g） 应在对密码进行修改前验证用户身份。

6 网络通信安全

6.1 通讯协议

移动互联网应用程序在与服务器通信时，应满足以下要求：

a） 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；

b） 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；

c） 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。

6.2 会话管理

移动互联网应用程序在与服务器通信时，应满足以下要求：

a） 会话结束后应立即清除敏感数据缓存，防止信息泄露；

b） 在不同移动终端上登录时应向用户进行信息提示；

c） 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，鉴别通过后才能进行操作。

d） 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；

e） 应确保用户在执行注销/登出后，会话被安全终止；

f） 应设计合理的账户登录超时控制策略，当用户闲置在线状态超出时限时，自动退出登录状态；

g） 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。

6.3 第三方网络通信

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。

7 数据安全

7.1 数据录入

移动互联网应用程序在数据录入时，应满足以下要求：

a) 用户输入密码等客户敏感信息时，不应明文显示；
b) 移动互联网应用程序应支持界面返回后自动清除该界面客户敏感信息的机制。

7.2 数据存储

移动互联网应用程序在数据存储时，应满足以下要求：

a) 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客户敏感信息，且不应以任何形式存储密码信息；
b) 移动互联网应用程序删除后，应清除移动终端中的所有客户信息；
c) 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。

8 开发安全

8.1 安全需求

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。

8.2 安全开发

移动互联网应用程序在开发时，应满足以下要求：

a) 移动互联网应用程序开发过程中应考虑编码安全性，减少应用程序安全漏洞；
b) 所使用的第三方开发工具和第三方插件应是安全的；
c) 认证逻辑、校验功能应在服务器端完成。

8.3 安全测试

移动互联网应用程序应满足以下安全性功能要求：

a) 移动互联网应用程序在开发完成，正式上线前，应进行安全测试和渗透测试；
b) 应提供安全性功能操作文档，应提供安全性功能测试文档。

8.4 安全发布

移动互联网应用程序在发布时，应满足以下要求：

a) 正式版本发布时，应删除测试数据和所有用于调试的代码；
b) 移动互联网应用程序应采用发布机构的证书进行签名，标识应用程序的发布者，签名证书应由专门岗位管理；
c) 移动互联网应用程序应有规范的上线发布流程，并应提供安全可靠的移动应用软件下载、发布、升级渠道。

9 安全审计

9.1 日志生成

日志生产基本要求包括：

a) 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；
b) 日志应该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阀值导致会话连接终止等；
c) 正式发布的移动终端程序不能包含调试过程中的日志。

9.2 日志管理

日志管理应满足以下要求：

a) 日志应存储于掉电非易失性存储介质中；
b) 仅允许授权用户以只读形式访问日志，且支持日志审计；
c) 日志应具备查询功能；
d) 日志不应记录客户敏感信息；
e) 日志应存放于服务器端；
f) 日志保存的时间不少于十二个月，满足业务管理、审计、监督检查等需要。

参 考 文 献

[1] GB/T 18336.1—2008 信息技术 安全技术 信息技术安全性评估准则第1部分：简介和一般模型
[2] GB/T 18336.2—2008 信息技术 安全技术 信息技术安全性评估准则第2部分：安全功能要求
[3] GB/T 18336.3 信息技术 安全技术 信息技术安全性评估准则第3部分：安全保证要求
[4] GB/T 20984—2007 信息安全技术 信息系统风险评估规范
[5] 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
[6] JR/T 0068—2015 网上银行系统信息安全通用规范
[7] 证券公司网上证券信息系统技术指引 中国证券业协会 2015年3月13日