**证券期货业移动互联网应用程序安全认证自评价表**

中证信息技术服务有限责任公司：

本机构*（认证申请方名称）*及申请认证的APP*（填写名称/版本号/操作系统平台）*对JR/T 0192-2020《证券期货业移动互联网应用程序安全规范》及JR/T 0240-2021《证券期货业移动互联网应用程序安全检测规范》中相关标准内容自评价结果如下：

填表说明：

1.“自评价结果”一栏应根据“评价要点”进行自查，Y表示“符合”，N表示“不符合”， N/A表示“不适用”。

2.认证申请方在自评价过程中，如对检测项符合情况有待确定、因自身的技术限制无法完成自评价或无法判断等情况，请在“自评价结果”栏中进行说明。

3.如认证申请方根据APP具体情况“自评价结果”为N/A时，需在“备注”栏中进行不适用说明。

| **评价类别** | **评价子类** | **评价项** | **评价要点** | **自评价结果** | **备注** |
| --- | --- | --- | --- | --- | --- |
| **移动终端****安全** | 应用程序保护 | **防逆向。**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 | 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。 |  |  |
| **安全接口。**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 | 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 |  |  |
| **输入保护。**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 | 开发文档是否具有敏感信息防截获的安全机制，其安全机制是否可行。 |  |  |
| 使用技术手段尝试是否可以截获用户输入的敏感数据。 |  |
| **输入校验。**对输入信息的合法性进行识别 | 开发文档中是否具有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。 |  |
| **外部资源授权。**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 | 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。 |  |  |
| **授权提示。**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 | 移动互联网应用程序客户端在获取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。 |  |  |
| **完整性校验。**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 | 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。 |  |  |
| **异常处理。**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 | 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。 |  |  |
| 移动终端环境 | **运行环境安全。**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 | 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。 |  |  |
| **进程保护。**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 | 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。 |  |  |
| **异常监测。**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 | 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。 |  |  |
| 安装与卸载 | **安装确认。**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 | 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，让用户对其使用的终端资源（包含通信资源和外设接口）、终端系统权限和终端数据进行确认。 |  |  |
| **剩余信息保护。**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 | 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。 |  |  |
| **系统安全。**不应影响终端操作系统和其他应用软件的功能 | 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 |  |  |
| 升级与更新 | **完整性校验。**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 | 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。 |  |  |
| **更新推送。**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 | 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。 |  |  |
| **强制更新。**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 | 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 |  |  |
| **身份鉴别** | 鉴别方式 | **二次认证。**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 | 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 |  |  |
| **用户登记。**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 | 若首次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是否再次进行用户名密码登记并核验 |  |  |
| **登录失败处理。**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 | 开发文档中是否提供移动互联网应用程序连续鉴别失败处理机制。 |  |  |
| 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。 |  |
| **登录超时。**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 | 开发文档中是否提供移动互联网应用程序登录会话超时重鉴别机制。 |  |  |
| 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。 |  |
| 鉴别数据保护 | **授权保护。**不应未授权查阅或修改 | 移动互联网应用程序是否存在未授权查阅或修改鉴别数据的功能， |  |  |
| 移动互联网应用程序是否在查阅或修改鉴别数据时需要进行二次身份鉴别。 |  |
| **用户提醒。**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 | 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。 |  |  |
| **身份绑定。**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 | 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。 |  |  |
| 同一用户身份信息是否可注册多个用户。 |  |
| 密码安全 | **存储安全。**密码不应以任何形式明文保存在移动终端的本地存储上 | 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。 |  |  |
| **传输安全。**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 | 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。 |  |  |
| 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。 |  |
| **残留信息保护。**密码禁止在缓存和日志中输出 | 移动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。 |  |  |
| **安全输入。**输入密码信息时应采取技术措施防止密码被盗取 | 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。 |  |  |
| 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。 |  |
| 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。 |  |
| **密码显示。**密码输入框默认禁止明文显示密码 | 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。 |  |  |
| **密码复杂度。**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 | 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 |  |  |
| 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。 |  |
| **密码修改。**应在对密码进行修改前验证用户身份 | 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。 |  |  |
| **网络通信安全** | 通讯协议 | **安全协议。**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 | 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。 |  |  |
| **安全版本。**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 | 移动互联网应用程序与服务器是否采用安全的通信协议，检查是否存在安全隐患的通信协议。 |  |  |
| **密码安全。**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 | 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。 |  |  |
| 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和证券期货业主管部门要求。 |  |
| 会话管理 | **缓存信息保护。**会话结束后应立即清除敏感数据缓存，防止信息泄露 | 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。 |  |  |
| 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。 |  |
| **安全提示。**在不同移动终端上登录时应向用户进行信息提示 | 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。 |  |
| **会话鉴别。**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 | 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）。 |  |  |
| 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。 |  |
| **会话保护。**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 | 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。 |  |  |
| 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。 |  |
| 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。 |  |
| **会话终止。**应确保用户在执行注销/登出后，会话被安全终止 | 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。 |  |
| **会话超时。**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 | 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。 |  |  |
| **并发限制。**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 | 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。 |  |  |
| 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。 |  |
| 第三方网络传输 | **安全通道。**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 | 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。 |  |  |
| 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认可。 |  |
| **数据安全** | 数据录入 | **数据录入安全。**用户输入密码等客户敏感信息时，不应明文显示 | 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。 |  |  |
| **页面返回保护。**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 | 开发文档中是否有关于页面返回后自动清除个人信息的说明。 |  |  |
| 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）重新进入该页面时，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。 |  |
| 数据存储 | **敏感信息存储。**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 | 开发文档中是否有对于移动互联网应用程序在个人敏感信息（包括但不限于账户口令、身份证号码、财产信息等）存储的规定。 |  |  |
| 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。 |  |
| 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。 |  |
| **客户信息保护。**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 | 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。 |  |  |
| 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。 |  |
| **敏感信息保护。**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 | 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。 |  |  |
| 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。 |  |
| **开发安全** | 安全需求 | **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。 | 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。 |  |  |
| 安全开发 | **安全编码。**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 | 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。 |  |  |
| **安全插件。**所使用的第三方开发工具和第三方插件应是安全的 | 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。 |  |  |
| 所使用的第三方开发工具是否经过安全认定和检查。 |  |
| **安全逻辑。**认证逻辑、校验功能应在服务器端完成 | 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。 |  |  |
| 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。 |  |
| 安全测试 | **上线测试。**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 | 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。 |  |  |
| **功能测试。**应提供安全性功能操作文档，应提供安全性功能测试文档 | 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。 |  |  |
| 安全发布 | **测试数据。**正式版本发布时，应删除测试数据和所有用于调试的代码 | 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。 |  |  |
| **证书签名。**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 | 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。 |  |  |
| 签名证书是否由专门岗位管理。 |  |
| **上线发布。**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 | 移动互联网应用程序上线发布流程的规范文档。 |  |  |
| 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。 |  |
| **安全审计** | 日志生成 | **日志内容。**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 | 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。 |  |  |
| **操作日志。**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 | 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。 |  |  |
| **调试日志。**正式发布的移动终端程序不能包含调试过程中的日志 | 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。 |  |  |
| 日志管理 | **日志存储。**日志应存储于掉电非易失性存储介质中 | 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。 |  |  |
| **日志访问。**仅允许授权用户以只读形式访问日志，且支持日志审计 | 是否将审计日志提供审计管理员进行日志审计。 |  |  |
| 日志的权限管理管理功能，是否仅允许授权用户以只读形式访问日志。 |  |
| **日志查询。**日志应具备查询功能 | 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。 |  |  |
| **敏感日志保护。**日志不应记录客户敏感信息 | 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。 |  |  |
| **存储位置。**日志应存放于服务器端 | 移动互联网应用程序服务端的日志记录。 |  |  |
| **保存时间。**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 | 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。 |  |  |
| **个人信息保护** | 个人信息保护 | **个人信息保护** | 认证申请方应逐一对照《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）中的规定要求，参照《网络安全标准实践指南—移动互联网应用程序（App）收集使用个人信息自评估指南》等规章、技术文件进行自查，如对检测项符合情况有待确定，应在“备注”栏填报。 |  |  |