编号：CSTECH-01-01:2022

证券期货业移动互联网应用程序
安全认证实施规则

2022-03-10 发布　　2022-03-10 实施

中证信息技术服务有限责任公司 发布

目 录

1 适用范围

本规则适用于证券期货业移动互联网应用程序（以下简称 APP）的安全认证，验证其标准符合性。本规则所指的 APP 是由证券期货经营机构发布运营的，安装在移动终端上，用于证券/基金/期货查询、交易、业务办理等业务相关的原生应用程序。

2 认证依据

JR/T 0192 证券期货业移动互联网应用程序安全规范

JR/T 0240 证券期货业移动互联网应用程序安全检测规范

上述标准原则上应执行最新版本，当需要使用标准的其他版本时，按认证机构发布的有关文件要求执行。

3 认证模式

型式试验+文件审查+现场检查+获证后监督

获证后监督是指获证后的跟踪检查、生产现场抽取样品检测、市场抽样检测三种方式之一或组合。

4 认证环节

认证环节包括：

（1）认证申请及受理

（2）型式试验

（3）文件审查

（4）现场检查

（5）认证决定

（6）获证后监督

5 认证实施

5.1 认证流程

认证委托方向认证机构申请认证，认证机构审查申请材料，确认合格后受理该申请。认证委托方获得受理后从认证机构公布的检测机构名录中自主选择检测机构实施检测。检测机构应依据相关标准和技术规范进行检测，完成后向认证机构提交检测报告。认证机构针对检测报告及其他技术材料进行文件审查，对认证委托方进行现场检查。认证机构对检测、文件审查、现场检查的结果进行综合评价，向评价合格方颁发认证证书。在证书有效期内，认证机构组织对获证后的 APP 进行定期的监督。

5.2 认证申请及受理

5.2.1 认证单元划分

原则上按 APP 名称/版本申请认证。

5.2.2 申请资料要求

认证委托方在申请认证时，应提交的申请材料包括但不限于：

（1）申请基本信息（纸质和电子版各 1 份，须加盖公章）

- 认证申请书；
- 认证委托方授权委托书；
- 认证委托方承诺函；
- 认证委托方、制造商、生产企业《营业执照》复印件；
- 认证委托方《经营证券期货业务许可证》复印件。

（2）技术文档（电子版 1 份）

- APP 版本控制说明，特别是与安全功能变更相关的版本控制策略；
- 不同发布渠道的版本差异性说明；

- APP 管理制度文档，包括但不限于：设计开发、质量控制、发布管理、运维管理、信息安全和数据安全等方面；
- 对 APP 符合相关技术标准的证明文件，包括但不限于：
  - 系统设计文档，包含接口设计、安全功能相关的设计内容；
  - 开发编码安全手册；
  - 安全测试相关文档，包括但不限于：第三方插件清单（如有）、第三方插件安全测试报告（如有）、第三方开发工具清单（如有）、第三方开发工具安全检查结果（如有）、安全测试报告、渗透测试报告、安全功能操作文档、安全功能测试文档等；
  - APP 上线发布流程记录；
- 证券期货业 APP 安全认证自评价表。

（3）送检样品及其说明文档

（4）外包管理材料（适用于将 APP 开发、安全加固等外包给第三方机构的认证委托方，电子版 1 份），包括但不限于：

- 有效期内的外包合同；
- 有效期内的外包安全保密协议。

5.2.3 受理

认证机构在接收到认证委托方的申请资料后确定是否受理。

5.3 型式试验

检测机构依据证券期货业 APP 相关标准规范（详见本文第 2 部分：认证依据）、适用的法律法规及其他要求，对认证委托方样品的标准符合性进行检测。

5.3.1 样品要求

（1）送样原则

依照认证委托方认证单元中确定的 APP 名称/版本，送该版本的样品。若样品运行在专用移动终端硬件设备环境下时，需提供可运行该样品的所有不同型号的移动终端硬件设备（每型号 1 部）。

（2）送样要求

可提供载有可安装运行送检 APP 的光盘等数据存储介质，该介质和其外包装上应有 APP 名称、版本号、认证委托方联系信息等标识；或提供送检 APP 的下载渠道。

若采用专用移动终端硬件设备时，应提供专用移动终端硬件设备清单，清单内容包括：硬件设备型号、硬件配置、不同型号的设备数量、操作系统环境和基本软件配置等。

APP 的用户文档电子版一份。文档应设置封面、目录、页码等，封面内容应包含 APP 名称、版本号、认证委托方名称和联系方式等标识。文档至少应包括以下内容：

- 指导性文件（APP 应用范围和使用对象的说明、APP 安装过程指南、APP 操作使用说明、使用 APP 的具体操作和步骤，并用图例加以说明等）；
- APP 安装包，或下载渠道；
- 测试环境文件（测试环境账号：APP 登录账号和交易场景业务账号；测试环境要求说明：APP 运行要求的软件、硬件、网络等最低配置说明等）。

检测的样品由认证委托方负责选送，并对选送样品负责。

（3）样品处置

检测机构应在证书有效期内保存检测过程中的样品，证书失效后，认证委托方可向检测机构申请取回样品。

5.3.2 检测报告的提交

检测机构应于检测工作完成后 10 个工作日内向认证机构提交检测报告（电子、纸质各一份）。

其他相关资料由认证委托方和检测机构妥善处置。

5.4 文件审查

认证机构在收到检测机构出具的检测报告及相关材料后，安排检查员进行文件审查。文件审查的范围包括所有申请材料及检测报告。

文件审查依据证券期货业 APP 相关标准规范、适用的法律法规及其他要求，对认证申请范围内的被认证对象的标准符合性进行审查，获取认证委托方所提供的被认证对象是否符合认证规范的证据。如有与申请认证业务范围相关的投诉记录，应分析对认证要求符合性的影响。

文件审查一般为 3 至 4 个人日。

5.5 现场检查

认证机构依据证券期货业 APP 相关标准规范、适用的法律法规及其他要求，对认证委托方申请范围内的 APP 的设计开发情况、发布管理情况、更新维护情况及管理文档的落实情况进行现场检查，获取认证委托方持续满足认证要求的证据。

现场检查一般为 2 至 4 个人日。

在确保认证有效性的前提下，根据申请认证 APP 的具体情况，经认证委托方与认证机构协商一致，可采用远程检查。对于一年内在其他同类 APP 认证项目中现场检查过的同一场所，当前认证项目可不对该场所进行现场检查，需要时，可

采用远程检查方式进行补充检查。在一个证书有效期内，应至少进行一次现场检查。

5.6 认证决定

认证机构对型式试验、文件审查、现场检查的结果进行综合评价，向评价合格方颁发认证证书，并在认证机构网站上予以公告。如认证决定过程中发现不符合认证要求项，允许限期（通常情况下不超过 3 个月）整改，如期完成整改后，认证机构采取适当方式对整改结果进行确认，重新执行认证决定过程。对于不授予认证资格的认证委托方，认证机构应向其以书面形式明示不能获得认证资格的原因。

5.7 认证时限

认证时限是指自申请被正式受理之日起至颁发认证证书时止所实际发生的工作日。其中，认证机构在收到认证申请人的认证申请后，于 10 个工作日内完成申请资料审核，审核通过后受理认证申请。补充材料时间不计算在内。检测机构收到样品后，于 30 个工作日内完成检测，整改时间及补充材料时间不计算在内。认证机构收到检测报告后，于 5 个工作日内完成认证审查安排。认证审查完成后，认证机构于 15 个工作日内完成发证流程。认证时限一般在 80 个工作日内，各认证环节整改时间及补充材料时间不计算在内。

5.8 获证后监督

5.8.1 证后监督的频次和方式

证后监督采用检测+文件审查+现场检查的方式。其中，检测在证后监督环节至少每三年覆盖所有检测项。

证后监督现场检查时间根据获证产品的单元数量确定，并适当考虑获证机构的生产规模。一般不超过初次认证的人日数。证后监督现场检查的方式和内容参照 5.5。

从获证之日起至证书有效期止，每 12 个月为一个监督审查期，进行一次证后监督。每次证后监督原则上由认证机构提前 2 个月通知获证机构（必要情况下，认证机构可采取事先不通知的方式对获证机构实施监督）。

获证机构如出现以下情况之一，认证机构可视情况增加证后监督审查的频次：

（1）获证 APP 出现严重质量问题时,或者用户提出投诉并经查实为证书持有者责任时；

（2）认证机构有足够理由对获证 APP 与本规则中规定的标准要求的符合性提出质疑时；

（3）有足够信息表明获证机构因组织机构、生产条件、质量管理体系等发生变更，从而可能影响 APP 质量时。

5.8.2 获证后监督结果评价

对于获证后监督审查合格的获证机构，认证机构应做出保持其认证资格的决定；

对于获证后监督审查不合格的获证机构，允许其限期（通常情况下不超过 3 个月）采取措施进行纠正，如逾期仍未纠正，应撤销其认证资格。

6 认证证书

6.1 认证证书有效期

认证证书有效期为 3 年。在有效期内，通过每年对获证 APP 进行监督，确保认证证书的有效性。证书有效期届满前 3 个月内，认证委托方可向认证机构提出证书续期申请，认证机构对获证机构实施监督审查，合格即可续期。

6.2 认证证书的管理

6.2.1 认证证书的变更

认证证书有效期内，若发生下列情况之一，获证机构应向认证机构提出变更申请。认证机构策划并实施适宜的审查活动，并按照要求做出认证决定。审查活动可与证后监督同时进行。

（1）APP 名称/版本变更；

（2）证书持有者变更；

（3）认证委托方名称及地址、制造商名称及地址、生产企业名称及地址变更；

（4）认证所依据标准的改变。

如果APP发生功能/版本变化，获证机构应提交变更后APP与已获证APP之间的差异性说明,由认证机构根据附录 1评估是否进行检测和/或现场检查。

如果获证机构需要扩大/缩小认证范围时，应向认证机构同时提交扩大/缩小范围的理由、事实的说明，以及扩大的APP与已获证APP之间的差异性说明。认证机构应按照核查扩大/缩小认证范围与原认证范围的一致性和差异，确认原认证结果对扩展APP的有效性，需要时应针对扩大/缩小认证范围和其对原认证范围的影响进行检测和现场检查，并根据获证机构的要求单独颁发认证证书或换发认证证书。

如果认证变更只涉及到注册名称、注册地址的变更，获证机构须递交变更申请，经书面审查批准后，认证机构仅对证书更新并收回原证书。

认证所依据标准发生变更时，认证机构应通知相关获证机构，并要求其在规定的时间内重新申请认证。

6.2.2 认证证书的暂停

获证机构有下列情形之一的，认证机构应当暂停认证证书。

（1）未按照规定及时接受证后监督审查；

（2）获证机构未按规定使用认证证书和认证标志；

（3）监督结果证明获证机构不符合认证要求，但不需要立即撤销认证证书；

（4）获证机构未履行已签署的认证合同中规定的责任和义务，如未按时支付认证费用等；

（5）获证机构主动请求暂停；

（6）获证机构被发现列入国家企业信用信息公示系统严重违法失信名单，或在特定时期国家或行业管理部门有要求予以暂停的；

（7）获证机构出现严重问题或获证机构发生重大安全事故。

暂停期限一般为 3 个月。在 3 个月内，获证机构可提出恢复证书的申请，认证机构经审查、批准后，方可使用该证书。在认证证书暂停期间，获证机构不得继续使用证书。

6.2.3 认证证书的撤销

获证机构有下列情形之一，认证机构应当撤销其认证证书。

（1）获证机构出现严重问题，在短期内无法恢复符合性的或获证机构在认证范围内无法满足适用的最新法律法规、认证标准规范的要求，并在短期内无法采取措施或采取措施无效的；

（2）获证机构发生重大安全事故，造成客户资金安全受到威胁或损失，造成社会不良影响，或潜在风险短期内无法消除的；

（3）获证机构不接受认证机构对其实施的证后监督审查；

（4）认证证书暂停使用期间，获证机构未采取有效纠正措施；

（5）认证证书暂停使用期满，获证机构未申请恢复证书。

认证证书撤销后，认证机构应收回认证证书，并在认证机构官方网站予以公告。自证书撤销之日起，获证机构不得继续使用认证证书，或宣称获得该认证。

认证证书撤销后，不能以任何理由恢复，且6个月内不得重新申请认证。

6.2.4 认证证书的注销

获证机构因为自身原因申请注销认证证书，认证机构应当给予注销。

认证证书注销后，认证机构应收回认证证书，并在认证机构官方网站上予以公告。

6.3 认证证书的使用

认证证书可以展示在文件、网站、通过认证的工作场所、销售场所、广告和宣传资料或广告宣传等商业活动中，但不得利用认证证书和相关文字、符号，误导公众认为认证证书覆盖范围外的产品、服务、管理体系获得认证，宣传认证结果时不应损害认证机构的声誉。

认证证书不准伪造、涂改、出借、出租、转让、倒卖、部分出示、部分复印。获证机构应妥善保管好证书，以免丢失、损坏。如发生证书丢失、损坏的，获证机构可申请补发。

获证机构应建立认证证书、审核报告使用和管理制度，对认证证书的使用情况如实记录存档。

7 认证责任

认证委托方对其所提交的认证申请资料及样品的真实性、合法性负责，并对获证 APP 持续符合认证要求负主体责任。

检测机构对其检测结果及检测报告负责。

认证机构对其作出的认证结论负责。

8 收费

由认证机构、检测机构按国家有关规定统一收取费用。

附录 1 变更评估

在证书有效期内，APP 安全相关的变更分为重大变更和一般变更，并做如下定义：

重大变更包括但不限于以下情形：

1.APP 的开发语言发生变化；

2.APP 的开发框架发生变化；

3.可能对用户资金安全或个人信息保护产生重大影响的变更；

4.有关管理部门认定的其他情形。

其他情形为一般变更。

在证书有效期内，每年由认证机构对 APP 进行一次监督审查，监督审查时对 APP 安全相关的变更情况进行评估。

在证书有效期内，当 APP 发生重大变更或一般变更时，获证方应主动告知认证机构，认证机构对 APP 安全相关的变更情况进行评估。

评估后如属于重大变更，需要进行重新检测；如属于一般变更，需要根据 APP 变更情况、年度检测项和上一年度遗留问题等进行检测。