编号：CCRC-CFP-001:2022

# 金融科技产品认证实施细则

# 客户端软件

2022-07-22 发布　　2022-07-22 实施

中国网络安全审查技术与认证中心 发布

# 目 录

## 1 适用范围

本细则所指的客户端软件是在移动终端上为用户提供金融交易服务的应用软件，包括但不限于可执行文件、组件等。

## 2 认证依据标准

JR/T 0092 移动金融客户端应用软件安全管理规范；

JR/T 0098.3 中国金融移动支付 检测规范 第三部分：客户端软件；

T/PCAC 0006 条码支付移动客户端软件检测规范（适用时）；

T/PCAC 0007 移动金融客户端软件安全检测规范；

JR/T 0171 个人金融信息保护技术规范（适用条款6.1.1、 7.1.1）。

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，按认监委发布的有关文件要求执行。

## 3 认证模式

型式试验+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 认证基本环节

认证基本环节包括：

1）认证委托及受理；

2）型式试验委托及实施；

3）现场检查；

4）认证决定；

5）获证后监督。

## 5 认证实施

### 5.1 认证程序

认证委托方向认证机构委托认证，认证机构对认证申请材料进行评审，评审通过后向检测机构（由认证委托方自主从指定检测机构名单中选取）安排检测任务。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。随后，认证机构针对检测报告及其他技术材料进行审核，组织进行现场检查。认证机构对检测、现场检查的结果进行综合评价，评价通过后，向认证委托方颁发认证证书。认证机构组织对获证后的产品进行监督。

## 5.2 认证委托及受理

### 5.2.1 认证的单元划分

原则上按软件名称/版本、适用平台的不同划分认证单元。

### 5.2.2 申请资料要求

认证委托方提交的认证申请材料包括但不限于：

（1）申请基本信息（纸质和电子各 1 份，须加盖公章）

- 认证申请书；
- 相关法律地位证明材料（认证委托方、生产者、生产企业的注册证明如营业执照、组织机构代码等）；
- 认证委托方关于生产产品与被认证产品的一致性声明；
- 被认证产品符合认证依据的适用性声明。

（2）送检样品及其说明文档

其他说明文档包括：样品配置清单、产品安装手册、产品功能说明书等。

（3）技术文档（电子 1 份）

包括但不限于：产品设计文档、开发流程文档、发布管理文档、更新维护文档、产品安装手册、产品功能说明书、安全管理制度等。

（4）外包管理材料（适用于将产品开发、运维和安全管理等外包给第三方机构的认证委托方，提交纸质或电子版 1 份），至少包括以下材料：

- 外包合同；
- 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 检测委托及实施

### 5.3.1 型式试验

检测机构依据金融科技产品相关标准规范（详见本文第 2 部分：认证依据标准）、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。

（1）送样原则

认证委托方依照认证单元中确定的软件名称/版本，将相应样品送至检测机构。当样品运行在专用移动终端硬件设备环境下时，应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 2 部）。

（2）送样要求

提供载有可安装运行送检软件的光盘或其它介质。介质和其外包装上应有软件名称、版本号、软件生产单位和联系方式等标识。

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。

软件产品的用户文档一份，用户文档包括电子文档，文档内容也包括封面、目录、页码等，封面内容包含软件名称、版本号、软件生产单位和联系

方式等标识，纸质文档应装订成册。文档至少应包括以下内容：

1）环境要求：软件运行要求的软件、硬件、网络等最低配置说明等；

2）软件应用范围和对象的说明；

3）软件安装过程指南；

4）软件操作使用说明；

5）使用软件的具体操作和步骤，并用例图加以说明等。

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

检测机构应对样品至少保存三年，认证失效后，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，实施文件审查。审查的范围包括检测报告及申请材料。

文件审查一般为 3-4 人日。

## 5.5 现场检查

认证机构依据金融科技产品相关标准规范、适用的法律法规及其他要求，对认证委托方委托范围内的客户端软件的开发与维护情况、管理文档的落实情况、功能及安全项进行一致性检查，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。

现场检查实施可采用现场方式或远程方式，远程方式应在确保检查结果有效性的前提下实施。

对于一年内在其他同类产品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，可采用远程方式进行检查。

## 5.6 认证决定

认证机构对型式试验、现场检查的结果进行综合评价，评价通过后，向认证委托方颁发认证证书，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，允许认证委托方限期（一般不超过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；对仍然不符合认证要求的，认证机构不予批准认证委托，认证终止，认证机构向认证委托方做出书面说明。

## 5.7 认证时限

认证时限是指自认证委托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委托方的认证委托后，于5个工作日内完成申请评审，补充材料时间不计算在内。检测机构收到样品后，于20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，最长不超过 120 个工作日。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 获证后监督方式和频次

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

证后监督采用检测+现场检查的方式。其中，检测的内容为依据标准的部分条款，至少每 3 年覆盖所有条款。

对村镇银行客户端软件、机构内部使用的客户端软件、资讯查询类客户端软件，在无重大变更的情况下，证后监督可不实施检测。证书有效期届满，申请续期时，进行全项检测。

证后监督的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。现场检查的内容参照 5.4。

获证后的第一次监督审查应当在认证证书签发日起 12 个月内进行。此后，至少每个日历年进行一次，且两次监督审查的时间间隔一般不超过 15 个月。监督审查原则上由认证机构提前 3 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）获证产品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）获证产品被相关机构通报并经查实问题属实时；

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

（4）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，从而可能影响产品质量时。

### 5.8.2 获证后监督结果评价

对于证后监督审查通过的获证机构，认证机构应做出保持其认证资格的决定。

## 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，通过每年对获证产品进行监督，确保认证证书的有效性。

### 6.2 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。

### 6.3 认证证书的管理

#### 6.3.1 变更认证证书

认证证书有效期内，若发生下列情况之一，获证机构应主动告知认证机构并向认证机构提出变更申请。变更情况包括但不限于：

（1）软件名称/版本变更；

（2）认证委托方、生产者、生产企业的名称/地址变更；

（3）认证所依据标准的变更。

认证机构策划并实施适宜的认证评价活动，并按照要求做出认证决定。认证评价活动可与证后监督审查同时进行。

如果产品发生功能/版本变化，获证机构应提交变更后产品与已获证产品之间的差异性说明，认证机构依据附录进行评估。如属于重大变更，应进行全条款检测；如属于一般变更，根据产品变更情况确定检测内容。

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，以及扩大的产品与已获证产品之间的差异性说明。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产品的有效性，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。

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委托认证。

### 6.3.2 暂停认证证书

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）获证机构未履行与认证机构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）在特定时期国家或行业管理部门有要求予以暂停的；

（7）获证产品被相关机构通报并经查实问题属实时；

（8）现场检查时发现存在严重不合规的情况时；

（9）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6个月。在暂停期内，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。认证机构在官方网站上对暂停的证书予以公告。

### 6.3.3 撤销认证证书

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上予以公告。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。

### 6.3.4 注销认证证书

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。

## 7 认证标志的使用

### 7.1 标志的样式和标志制作

认证标志的样式和制作应符合《金融科技产品认证规则》附件《金融科技产品认证标志管理要求》。具体样式如下：

### 7.2 标志的使用

（1）认证标志应加施在铭牌或产品外体的明显位置上；获证产品本体上不能加施认证标志的，其认证标志必须加施在最小的产品外包装上及随附文件中。

（2）获证产品的外包装上可以加施认证标志。

（3）获证企业应建立认证标志使用管理制度，对认证标志的使用情况如实记录和存档。

（4）应符合认证标志有关法规和规定的相关要求。

## 8 收费

收费由认证机构、检测机构按国家有关规定统一收取。

附件

# 变更评估

在证书有效期内，产品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：

（一）产品的开发语言发生变化；

（二）产品的开发框架发生变化；

（三）新增条码支付；

（四）客户端类型变更，例如增加支付功能或个人信息采集功能；

（五）产品变更影响到的依据标准的条款比例大于 30%；

（六）有关管理部门认定的其他情形。

其他情形为一般变更。