编号：CCRC-CFP-007:2019

金融科技产品认证实施细则
移动终端可信执行环境(TEE)

2019-12-31 发布　　2020-01-01 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

本实施细则适用于个人移动终端上基于硬件和软件结合的移动终端支付可信环境(TEE),包括与TEE安全功能应用相关的硬件(SoC平台及相关硬件资源)、固件及相关软件（可信执行环境操作系统、可信虚拟化层等)。

2 认证依据

JR/T 0156 移动终端支付可信环境技术规范

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，按认监委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 认证的基本环节

认证基本环节包括：

（1）认证申请及受理

（2）型式试验

（3）文件审查

（4）现场检查

（5）认证结果评价与批准

（6）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申请认证，认证机构对申请材料进行初审，确认合格后向检测机构（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文件审查，组织进行现场检查。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。认证机构组织对获证后的产品进行定期的监督。

5.2 认证申请及受理

5.2.1 认证的单元划分

原则上按产品名称/型号(版本)划分申请单元。以多于一个型号(版本)作为同一申请单元时，认证委托方应提交同一申请单元中型号(版本)间的差异说明。

5.2.2 申请材料要求

认证委托方向认证机构申请认证，应提交的申请材料包括但不限于：

（1）申请基本信息（纸质和电子各 1 份，须加盖公章）

- 认证申请书；
- 认证委托方、生产者（制造商）、生产企业营业执照复印件；
- 质量体系相关文件；
- 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）安全保证能力相关文档（电子 1 份）：

- 配置管理
- 开发安全
- 交付与运行
- 开发文档
- 指导性文件

（3）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基本信息相关材料后确定是否受理。

5.3 型式试验

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，下同），对认证委托方样品的标准符合性进行检测。

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协商并妥善处置。

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。

文件审查依据金融科技产品相关标准规范，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 4 至 6 个人日。

5.5 现场检查

5.5.1 检查内容及场所范围

现场检查的内容为安全保证能力、质量保证能力、产品一致性检查。现场检查的场所范围原则上应覆盖产品的设计研发环境

5.5.2 安全保证能力检查

认证机构组织检查员对认证委托方按照《金融科技产品认证实施细则 安全保证能力及质量保证能力要求》进行检查。

5.5.3 质量保证能力检查

认证机构组织检查员对认证委托方按照《金融科技产品认证实施细则 安全保证能力及质量保证能力要求》进行检查。

5.5.4 产品一致性检查

现场检查时，应对被认证对象进行一致性检查。重点核实以下内容：

（1）产品名称/型号(版本)与检测报告上所标明的内容是否一致；

（2）认证证书与认证标志的使用是否符合要求。

5.5.5 现场检查时间

现场检查时间根据认证委托方的规模和分布情况，通常每个场所为 4 至 6 个人日。

5.6 认证决定

认证机构对文件审查、型式试验、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。对于不授予认证证书的认证委托方，认证机构应向其以书面形式明示不能获得认证证书的原因。

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委托人的认证申请后，于 5 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 70 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。认证时限原则上不超过 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 证后监督频次和方式

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。证后监督可采用现场检查或文件审查的方式。每次证后监督原则上由认证机构提前 1 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）认证机构有足够理由对获证产品与本细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，从而可能影响产品质量时。

5.8.2 证后监督审查的内容

获证后监督的内容与现场检查一致，必要时可委托检测机构对产品进行抽样检测。需要进行抽样检测时，抽样检测的样品应在获证机构的产品中（包括生产线、仓库、市场）随机抽取。抽样检测的数量一般与初次申请认证结束时备案样品的数量一致，如需要可

以根据实际情况增加抽样的数量。初次认证申请时的检测项均可以作为监督时的检测项，认证机构可根据具体情况进行部分或全部的检测。

证后监督检查工作量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。

5.8.3 获证后监督结果评价

对于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；

对于证后监督审查不合格的获证机构，允许限期（通常情况下不超过 3 个月）完成纠正措施，逾期认证机构应根据情况暂停/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，通过每年对获证产品进行监督，确保认证证书的有效性。证书有效期届满前，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）产品名称/功能/型号(版本)变更；

（2）证书持有者变更；

（3）扩大或缩小认证范围；

（4）获证机构所在地变更；

（5）认证所依据标准的改变。

如果产品发生功能/版本变化，获证机构需重新申请认证。

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。

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。

6.3.2 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）未及时接受证后监督审查或证书到期未再申请认证；

（2）获证机构未按规定使用认证证书和认证标志（见 6.2 和 7.2）；

（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。

6.3.3 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。

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。

6.3.4 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《金融科技产品认证标志管理要求》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 样品管理

8.1 送样原则

申请单元中只有一个型号(版本)的，送该型号(版本)的样品。

以多型号(版本)产品作为同一单元申请认证时，应从中选取典型的型号(版本)作为典型样品进行完整检测，其他型号(版本)的产品可进行差异化检测。送样应符合认证机构核查申请单元内产品差异的相关要求。

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移动终端硬件设备。

8.2 送样要求

检测的样品由认证委托方负责选送，并对选送样品负责。

8.3 样品处置

检测机构应在认证有效期内保存检测过程中的样品，认证失效后，认证委托方可取回检测机构保存的送检样品。

9 收费

收费由认证机构、检测机构按国家有关规定统一收取。