

编号：NFCC-IR-000-01

金融科技技术产品通用安全认证 实施规则 V1.0/1

发布日期：2023 年 7 月 17 日 实施日期：2023 年 7 月 17 日

重庆国家金融科技认证中心有限责任公司 发布

目 录

1	适用范围	1
2	认证依据	1
3	认证模式	1
4	认证的基本环节	1
5	认证实施	2
5.1	认证程序	2
5.2	认证申请及受理	2
5.2.1	认证的单元划分	2
5.2.2	申请资料要求	2
5.2.3	受理	4
5.3	跟踪监测	4
5.4	型式试验	4
5.4.1	基本要求	4
5.4.2	型式试验报告的提交	4
5.5	文件审查	5
5.6	现场检查	5
5.7	认证决定	5
5.8	认证时限	5
5.9	获证后监督	6
5.9.1	获证后监督方式和频次	6
5.9.2	获证后监督审查的内容	6
5.9.3	获证后监督结果评价	6
6	认证证书	7
6.1	认证证书有效期	7
6.2	认证证书的使用	7
6.3	认证证书的管理	7
6.3.1	变更认证证书	7
6.3.2	暂停认证证书	8
6.3.3	撤销认证证书	9
6.3.4	注销认证证书	9
7	认证标志的使用	9
8	样品管理	10
8.1.1	送样原则	10
8.1.2	送样要求	10
8.1.3	样品处置	10
9	收费	11

1 适用范围

本规则适用于金融科技技术产品。金融科技技术产品是指在符合现有法律法规、部门规章、规范性文件等要求前提下，在尚不具备管理细则的领域，利用新技术设计出的面向金融用户的产品，包括但不限于硬件设备、软件产品、信息系统、可执行文件等。

2 认证依据

- JR/T 0199 《金融科技创新安全通用规范》
- JR/T 0200 《金融科技创新风险监控规范》

适用的法律法规及其他要求。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）跟踪监测
- （3）型式试验
- （4）文件审查
- （5）现场检查

(6) 认证决定

(7) 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，确认合格后受理申请。

认证受理后，认证机构对被认证产品的运行情况开展跟踪监测，监测期一般不超过 6 个月。

监测期间，被认证产品稳定运行后，认证机构向检测机构安排检测任务。如认证委托方在申请认证时已提供产品的型式试验报告，认证机构需对报告进行差异化分析，必要时向检测机构安排重新检测或补充检测任务。

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型式试验报告。

认证机构针对型式试验报告及其他技术材料进行文件审查，并组织进行现场检查。

现场检查结束且监测期满后，认证机构对跟踪监测、型式试验、文件审查、现场检查的结果进行综合评价，出具评价报告，并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获证后监督。

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（版本号）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。
- 近一年内未涉及投诉说明。

(2) 送检样品及其说明文档

(3) 技术文档（电子 1 份）

- 控管理类文档、运维管理类文档、数据安全类管理文档。

(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。
- 如果不涉及外包，应提供无外包说明。

(4) 标准符合性证明材料

个人金融信息保护方面，应提交符合 JR/T 0171 相关要求的证明材料。

网络安全方面，应提交符合 JR/T 0071 相关要求的证明材料。

当申请认证产品使用云计算技术时，应提交云计算技术符合 JR/T 0166、JR/T 0167、JR/T 0168 相关要求的证明材料。

当申请认证产品使用区块链技术时，应提交区块链技术符合 JR/T 0193 相关要求的证明材料。

如产品在申请认证前已完成型式试验，认证委托方在提交型式试验报告时，还应同时满足以下要求：

1) 出具型式试验报告的检测机构应具备以下资质：实验室认可（CNAS）、检验检测机构资质认定（CMA）、质量管理体系认证（ISO 9001）、信息安全管理体
系认证（ISO 27001）等；

2) 截至申请认证时，型式试验报告的报告日期一般不早于 24 个月；

3) 提交型式试验的委托合同。

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，综合业务运营和系统运行情况，确定是否受理。

如认证委托方在申请认证时提供产品的型式试验报告，认证机构将对型式试验报告进行有效性和差异化分析：

1) 型式试验报告的报告日期早于申请认证日期 24 个月的，不予采信；

2) 型式试验报告的报告日期早于申请认证日期不超过 24 个月的，若产品无变更且型式试验报告可完全覆盖金融科技技术产品相关标准规范要求（详见本文第 2 部分：认证依据），可予以采信。否则需进行差异化评估，确认是否需要委托检测机构进行重新检测或补充检测。

5.3 跟踪监测

认证受理后，认证机构对申请认证产品的运行情况开展跟踪监测。根据本文第 2 部分认证依据，对认证委托方申请认证产品运营过程中的个人金融信息保护、金融交易安全、业务连续性、服务质量、技术使用安全、内控管理、网络安全、意见投诉、公开舆情等进行跟踪监测。如跟踪监测环节发现问题，视发现问题数量及等级情况，在后续认证过程中进行必要的复核。

监测期的时长根据业务运营和系统运行情况确定，一般不超过 6 个月。

5.4 型式试验

5.4.1 基本要求

检测机构依据金融科技技术产品相关标准规范（详见本文第 2 部分：认证依据），对认证委托方样品的标准符合性进行检测。

5.4.2 型式试验报告的提交

检测机构应于型式试验报告完成后 5 个工作日内向认证机构提交型式试验报告（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。

5.5 文件审查

文件审查的范围包括所有申请材料及型式试验报告，必要时对跟踪监测问题进行复核。

文件审查以第 2 部分所列标准规范、适用的法律法规及其他要求为依据，对认证申请范围内的被认证对象的标准符合性进行审查。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。

5.6 现场检查

认证机构按照第 2 部分认证依据的要求，综合跟踪监测、型式试验及文件审查的情况，对申请认证产品的标准符合性进行检查，检查内容主要包括但不限于：

- （1）认证依据所要求相关管理制度的执行情况。
- （2）产品一致性检查。
- （3）跟踪监测发现问题的复核。

5.7 认证决定

认证机构对跟踪监测、型式试验、文件审查、现场检查情况进行综合评价，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的原因。

5.8 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。包含监测期在内，整个认证流程一般在 230 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。

5.9 获证后监督

5.9.1 获证后监督方式和频次

证后监督采用跟踪监测结合现场检查或文件审查的方式。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；同时，认证机构持续对获证产品进行跟踪监测。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（必要时，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现场检查的频次：

（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，从而可能影响产品质量时。

5.9.2 获证后监督审查的内容

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。对于获证后监督审查不合格的获证方，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。

5.9.3 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。

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/型号（版本号）变更；
- (2) 证书持有者变更；
- (3) 制造商、生产企业相关信息变更；
- (4) 认证所依据标准的改变。

如果产品发生功能/版本变化，获证机构应提交变更后产品与已获证产品之间的差异性说明，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

获证机构或证书中所列制造商、生产企业有下列情形之一的，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；
- (2) 获证机构未按规定使用认证证书和认证标志；
- (3) 监督结果证明获证产品不符合认证要求，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) 出现严重问题，在认证范围内无法满足适用的最新法律法规、认证标准规范要求的；
- (8) 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，或存在潜在风险的。

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

获证机构或证书中所列制造商、生产企业有下列情形之一，认证机构应当撤销其认证证书。

- (1) 出现严重问题，在短期内无法采取措施或采取措施无效的；
- (2) 发生重大安全事故，在短期内无法消除负面影响及潜在风险的；
- (3) 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，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，并在认证机构官方媒体上予以公告。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。

原则上，因（1）（2）（4）（5）原因认证证书撤销的获证机构 3 个月内不予受理认证申请。

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

获证企业使用认证标志时，应遵循以下要求：

- (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

8.1.1 送样原则

认证委托方送样样品的产品名称、型号（版本号），应与认证单元中确定的产品名称、型号（版本号）一致，若样品运行在专用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终端硬件设备（每型号 1 部）。

8.1.2 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。应提供送检产品或载有可安装运行送检产品的光盘或其它介质。介质和其外包装上应有产品名称、版本号、软件生产单位和联系方式等标识。

当样品涉及硬件设备时，应提供硬件设备清单，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。

当样品涉及软件产品时，应提供软件产品的用户文档一份。用户文档可包括电子文档，纸质文档应装订成册。文档应包含封面、目录、页码等，封面应有软件名称、版本号、软件生产单位和联系方式等标识。用户文档至少应包括以下内容：

- 环境要求：产品运行要求的软件、硬件、网络等最低配置说明等；
- 产品应用范围和对象的说明；
- 产品安装过程指南；
- 产品操作使用说明；
- 产品使用的具体操作和步骤，并用例图加以说明等。

8.1.3 样品处置

检测机构应在型式试验报告有效期内保存检测过程中的样品，认证失效后，认证委托方可向检测机构申请取回样品。

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。