编号：NFCC-IR-B01-14

金融科技产品认证实施细则

商业银行应用程序接口

V1.0/0

发布日期：2022 年 6 月 14 日　　实施日期：2022 年 6 月 14 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

本规则适用于商业银行应用程序接口的认证工作。商业银行应用程序接口是由商业银行定义的用于与合作方互联的应用程序接口，合作方可以通过该接口获取商业银行的金融服务能力与信息技术能力。

2 认证依据

- JR/T 0185-2020 《商业银行应用程序接口安全管理规范》
- T/PCAC 0008-2020 《商业银行应用程序接口安全管理检测规范》

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）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 认证程序

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。检测机构依据第 2 章所列标准和规范的要求进行型式试验。型式试验完成后，检测机构向认证机构提交报告。认证机构依据第 2 章所列标准和规范的要求，进行文件审查和现场检查。认证机构对型式试验结果、文件审查和现场检查结果进行综合评价，向认证决定为“通过认证”的申请方颁发证书。在证书有效期内，认证机构对获证机构进行证后监督。

5.2 认证申请及受理

5.2.1 认证的单元划分

商业银行应用程序接口服务参与方包括商业银行与应用方，认证委托方角色可分为商业银行与应用方，两者可单独申请认证，认证单元具体划分原则如下：

认证委托方	认证单元	划分原则
商业银行	应用程序接口服务系统	按系统名称/版本

认证委托方	认证单元	划分原则
应用方	集成应用程序接口系统	按系统名称/版本

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）基本材料（纸质和电子各 1 份）

- 认证申请书（须加盖公章）
- 认证委托方的营业执照复印件（须加盖公章）
- 商业银行应用程序接口系统架构图，需明确被认证产品的主要模块/功能，边界范围等
- 被认证产品的接口说明列表，需明确金融服务场景、接口类型、接口分类定级说明等相关内容或文档

（2）商业银行方相关材料（电子 1 份）

- 被认证产品的中文版功能说明书、用户手册、各角色操作手册
- 被认证产品支持的可选部署配置说明文档、网络拓扑架构指南
- 依照商业银行应用程序接口自查表，提交自查说明及相应的制度文档、记录等自查材料
- 测试开发套件说明文档、开发测试报告
- 配置管理文档
- 运维管理相关文档等

（3）应用方相关材料（电子 1 份）

- 依照应用方应用程序接口自查表，提交自查说明及相应的制度文档、记录等自查材料

（4）如有外包，应提供外包管理材料（适用于将产品开发、生产、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提供的申请基本信息相关材料后确定是否受理。

5.3 型式试验

检测机构应依据第 2 章的相关标准规范、适用的法律法规及其他要求，对认证委托方的应用程序接口实施标准符合性检测。

检测机构应于型式试验完成后 15 个工作日向认证机构提交正式的报告及相关材料（电子、纸质各一份）。

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（第 2 章的依据），对认证申请范围内的被认证对象的标准符合性进行审查，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 8 个人日。

5.5 现场检查

认证机构按照第 2 章所列标准或认证规范的要求，对申请认证产品的标准符合性进行检查，检查内容主要为商业银行应用程序接口的服务终止与系统下线、安全管理，并对其安全设计、安全部署、安全集成、安全运维等进行抽查。

现场检查一般为 4 至 8 个人日。

需要说明的是：在不可抗拒等因素情况下（如自然灾害、疫情等），应在确保认证有效的前提下，根据申请认证产品的具体情况， 经认证委托方与

认证机构协商一致，可采用远程方式的检查。

5.6 认证决定

认证决定人员应根据第 2 章所列标准或认证规范、认证程序与认证实施规则等要求，结合型式试验、文件审查、现场检查的结果进行综合评价，做出认证决定。对符合认证要求的，颁发认证证书，并在认证机构网站或相关媒体上予以公告；对暂不符合认证要求的，可要求认证委托方限期（通常情况下不超过 3 个月）整改，整改后仍不符合的则书面通知认证委托方终止认证；若按期完成整改后，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。其中包括型式试验、文件审查、现场检查、认证评价、认证决定以及证书制作时间。

认证机构在收到认证委托方的认证申请后，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。检测机构应在认证委托方获得受理通知书后 30 个工作日内完成型式试验，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 80 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 证后监督

5.8.1 证后监督频次和方式

为确保获证机构的被认证对象的标准持续符合性，认证机构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。每次证后监督由认证机构提前 1 个月通知获证机构。

证后监督一般采用文件审查+现场检查（或远程审查）的方式，认证机构根据获证机构提供的材料，评估被认证对象的变更情况确定是否需要重新型式试验或部分检测，如需要进行则监督方式为型式试验+文件审查+现场检查（或远程审查）。每次证后监督要求获证机构向认证机构提交的认证申请材料包括但不限于：

1)上次审查结束后，至本次监督审查期间变更情况说明。

2)本监督审查期间在业务范围或拟扩大认证业务范围的相关投诉记录；若无投诉，需提交纸质说明，皆须盖公章。

3)问题整改情况说明。

4)技术风险自评估表（适用时）。

若获证机构在证书有效期内出现以下情况之一，认证机构应视情况增加监督频次：

1)获证产品出现严重质量或安全事故时,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)被认证对象的应用程序接口长时间无法正常访问，并造成用户损失或重大社会不良影响。

4)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。

5)相关主管机构或采信方的要求

6)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。

7)疑似存在获证方应用程序接口存在技术或管理安全隐患等可能导致证书不具备持续效力的风险因素。

必要情况下，认证机构可采取事先不通知的方式对认证委托方的产品进行飞行审查。

5.8.2 证后监督审查的内容

获证后监督的内容和方式参照 5.5 节现场检查，必要时可安排检测工作。

证后监督工作量根据获证产品情况确定，并适当考虑获证机构的规模。一般不超过初次认证的人日数。

5.8.3 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，授权认证标识持续使用。对监督审查不合格的获证机构，认证机构依据本实施细则 6.3 节的认证程序暂停甚至撤销其认证资格，暂停或撤销认证标识的使用授权。

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 90 天内，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。

1)认证委托方、制造商、生产企业、注册地址等变更。

2)认证所依据标准的改变。

3)扩大或缩小认证范围。

4)出现的重大安全事故及变更措施。

5)应用程序接口系统功能/版本、部署地发生变更。

6)相关主管部门或者采信方要求。

如果应用程序接口系统发生功能/版本、部署地变化，获证机构应向认证机构进行报备，提交变更后系统与已获证系统之间的差异性说明，由认证机构根据差异情况评估是否安排检测、文件审查、现场检查等全部或部分工作。

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；提供扩大的范围与原认证范围之间的差异性说明。认证机构应核查扩大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，需要时可安排检测、文件审查、现场检查等全部或部分工作。

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

在规定的时间内完成补充或重新检测等相关认证工作，保证获证产品持续符合认证依据。

如发生以上情况时，获证机构应按照 5.2 要求向认证机构提交相关材料。认证机构经评估后确认型式试验方式和审查模式，包括重新认证、部分检测认证等。审查通过后换发证书。

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)获证机构出现严重问题或发生重大安全事故。

7)在特定时期国家或行业管理部门有要求予以暂停的。

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）获证机构不接受认证机构对其实施的证后监督审查。

（3）认证证书暂停使用期间，获证机构未采取有效纠正措施。

（4）认证证书暂停使用期满，获证机构未申请恢复证书。

（5）出现重大安全事故，社会影响恶劣或者性质特别严重的。

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。

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，并在认证机构官方媒体上予以公告。

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。