

编号：CCRC-CFP-011:2019

金融科技产品认证实施细则

云计算平台

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	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
5.3	型式试验	4
5.4	文件审查	4
5.5	现场检查	4
5.6	认证决定	5
5.7	认证时限	5
5.8	获证后监督	6
5.8.1	证后监督频次和方式	6
5.8.2	证后监督审查的内容	7
5.8.3	证后监督结果评价与判定	8
6	认证证书	8
6.1	认证证书有效期	8
6.2	认证证书的使用	9
6.3	认证证书的管理	9
6.3.1	认证变更	9
6.3.1.1	云服务设施变更	9
6.3.1.2	认证要求变更	10
6.3.2	暂停认证证书	11
6.3.3	撤销认证证书	11
6.3.4	注销认证证书	12
7	认证标志的使用	13
7.1	标志的样式和标志制作	13
7.2	标志的使用	13
8	收费	14

1 适用范围

云计算平台认证是指对提供给金融行业使用的云服务设施的技术架构、安全能力、容灾能力的标准符合性认证工作。本细则适用于为金融行业提供私有云和团体云服务的云服务设施。

2 认证依据

- JR/T 0166 《云计算技术金融应用规范 技术架构》
- JR/T 0167《云计算技术金融应用规范 安全技术要求》
- JR/T 0168 《云计算技术金融应用规范 容灾》

3 认证模式

型式试验+文件审查+现场检查+获证后监督

4 认证的基本环节

认证基本环节：

- (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，并对申请业务的认证范围进行识别和判定，确认在认证范围内后受理认证申请。认证委托方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型式试验。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

认证委托方向认证机构申请认证，提交认证的材料参见认证机构网站公示的认证申请要求。初次进行认证申请的认证委托方应提交给认证机构的材料包括但不限于：

(1) 认证申请书、技术风险自评估表（适用时）；

(2) 认证委托方的营业执照、组织机构代码证、资质证

书的复印件，组织架构图；

(3) 申请业务类型的业务模式说明（包括但不限于云计算部署模式、服务类别、申报的容灾等级等）；

(4) 符合 JR/T 0071（三级及以上）及 GB/T 22239（私有云如有、团体云必需）及符合《云计算服务安全评估办法》和 GB 50174 的相关证明材料；

(5) 规划实施类：包括但不限于提供网络拓扑图、云服务设施的资产清单、系统或各组成部分需求说明书、需求分析文档、总体设计方案、数据库设计方案、概要设计方案、详细设计方案、工程实施方案、开发环境说明等内容或文档；

(6) 运维类：包括但不限于提供涉及风险管理、变更管理、监控管理、业务连续性管理、应急响应、审计管理以及各类用户手册等内容或文档；

(7) 容灾类：包括但不限于提供风险与业务影响分析、近一年安全事件（含中断事故）的自证材料、RTO、RPO、可用性等关键指标、预案与演练、机房管理制度、组织管理、监控管理等内容或文档；

(8) 系统外包情况说明。若无外包，需提交无外包纸质说明；如将系统基础设施运维服务、应用系统运维服务和安全管理服务等外包给第三方机构的认证委托方，需提交外包服务合同、外包风险评估、服务提供商尽职调查、外包服务安全管理、外包服务监控与评价、外包服务中断与终止等相

关措施的文档。

认证机构在接收到认证委托方的申请材料后，在 5 个工作日内确定是否受理（因申请材料不齐全而补充材料的时间不计算在内）。

适用本细则 6.3.2 的认证申请，认证机构不予受理。

5.3 型式试验

认证委托方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型式试验。

检测机构应于型式试验完成后 15 个工作日内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报告。

文件审查应以第 2 章所列标准或认证规范为依据，对认证申请范围内的云服务设施的技术符合性进行审查。认证委托方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。文件审查工作量一般为 12-40 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，对认

证委托方的云服务设施进行现场检查。现场检查的内容主要包括但不限于：

- (1) 文件审查或型式试验中发现的问题；
- (2) 认证依据所要求相关管理制度的执行情况；
- (3) 云服务技术架构、安全性、容灾能力与报告描述的一致性抽查；
- (4) 云服务运行场所现场抽查。

现场检查工作量为 12-40 人日。

5.6 认证决定

认证决定人员依据第 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，结合审查过程中收集的信息，对审查结果进行综合评价。必要时，认证机构应对认证委托方满足认证依据的情况进行风险评估，做出是否通过认证的决定，并向认证委托方发送认证结果通知。

对于授予认证资格的认证委托方，认证机构应对其颁发认证证书并在相关媒体上予以公告。

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

认证时限是指自认证申请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。

检测机构应在认证委托方获得受理通知书后 1 个半月内进场实施型式试验，型式试验时间一般不超过 40 个工作日，并于 6 个月内提交报告。补充材料和整改时间不计算在内。认证机构一般在收到报告后安排审查工作，文件审查、现场检查时间一般不超过 40 个工作日，认证评价、认证决定、证书制作时间共计不超过 20 个工作日。补充材料和整改时间不计算在内。

5.8 获证后监督

5.8.1 证后监督频次和方式

为确保获证机构的云服务设施的标准持续符合性，认证机构应综合评估获证机构的技术风险，依据评估结果采用不同的证后监督方式：定期和不定期的证后监督。

(1) 定期监督。从获证之日起每 12 个月为一个监督审查期，进行一次证后监督。

定期监督一般采用文件审查+现场检查的方式，认证机构根据获证机构提供的材料，评估云服务设施的变更情况确定是否需要重新型式试验或部分型式试验，如需要进行型式试验则审查方式为型式试验+文件审查+现场检查。每次定期监督由认证机构依据认证程序提前通知获证机构，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) 本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）。

(2) 不定期监督。认证机构根据应用在金融领域的云计算技术的特点以及所承担的认证风险，可在定期监督的基础上增加不定期监督。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不定期监督频次：

- 1) 出现重大安全事故；
- 2) 疑似存在受审云服务设施不一致或者重大安全隐患等可能导致证书不具备持续效力的风险因素；
- 3) 认证机构有足够理由对获证云服务设施与本细则中规定的标准要求的符合性提出质疑时；
- 4) 相关主管机构或采信方的要求；
- 5) 认证机构认为有必要增加不定期监督的其他情况。

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云服务设施进行飞行审查。

5.8.2 证后监督审查的内容

证后监督的审查内容包括但不限于：

- (1) 云服务风险控制能力及安全管理能力审查；
- (2) 在本监督审查期间的变更情况审查，必要时可委托检测机构对变更内容进行型式试验；
- (3) 本监督审查期间投诉记录对认证要求符合性影响的审查；
- (4) 认证机构认为存在重大安全隐患或者疑似与本细则中规定的标准要求不符的关键点。

5.8.3 证后监督结果评价与判定

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。对监督审查不合格的获证机构，认证机构应依据第 2 章所列标准、认证规范和本实施规则的认证程序暂停甚至撤销其认证资格。

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

认证证书是认证机构颁发给认证委托方证明其服务符合认证要求的一种证明文件。

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、广告和宣传资料中或广告宣传等商业活动，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服务获得认证，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、评价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

认证证书的变更、暂停、恢复、撤销和注销要求如下：

6.3.1 认证变更

6.3.1.1 云服务设施变更

获证机构在认证周期内，当发生如下场景时认证委托方须及时向认证机构提交变更说明：

- (1) 扩大或缩小认证范围；
- (2) 出现的重大安全事故及变更措施；
- (3) 云服务架构或者支撑环境变更（包括但不限于支撑操作系统变更、支撑数据库产品变更、开发语言变更等）、重要版本变更等；
- (4) 生产中心机房场地迁移或数量变化；
- (5) 获证机构注册名称、注册地址的变更；
- (6) 相关主管部门或者采信方要求。

认证机构识别变更的类型和范围，评估变更影响，策划及实施适宜的审查活动，并按照要求做出认证决定。

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

(2) 如发生以上(2) - (6)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阶段，包括重新认证、在获证后监督期间进行部分检测认证等。审查通过后换发证书。

6.3.1.2 认证要求变更

发生认证依据变更时，认证机构应组织评估变更影响范围，制定变更实施方案，并通知获证机构。

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或申请再认证；
- (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的云服务设施不符合认证要求，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) 未按 9.1 规定及时报告云服务设施变更情况或未按
要求接受检测认证工作。

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，或获证机构在认证范围内无法满足适用的法律法规、认证标准规范要求，并在短期

内无法整改达成要求的；

(2) 获证机构不接受认证机构对其实施的证后监督审查的；

(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，获证机构未完成证书恢复；

(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 收费

收费由认证机构、检测机构按国家有关规定统一收取。