编号：NFCC-IR-A05-01

IPv6 金融应用服务认证规则

V2.0/0

发布日期：2025 年 6 月 12 日　　实施日期：2025 年 6 月 12 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 认证等级划分 1
4 认证模式 2
5 认证基本环节 2
6 认证实施 3
6.1 认证基本程序 3
6.2 认证申请及评审 3
6.2.1 认证申请 3
6.2.1 认证申请评审 3
6.3 认证受理 4
6.4 认证评价 5
6.4.1 服务管理审核 5
6.4.2 服务特性测评 5
6.4.3 认证评价报告 5
6.5 认证复核及决定 6
6.5.1 认证复核 6
6.5.2 认证决定 7
6.6 证后监督 7
6.6.1 证后监督频次和方式 7
6.6.2 证后监督审查的内容 8
6.6.3 证后监督结果评价与判定 9
6.7 认证时限 9
6.8 再认证 10
7 认证变更 10
8 认证证书 11
8.1 认证证书有效期 11
8.2 认证证书和认证标识的使用 11
8.2.1 认证证书的使用 11
8.2.2 认证标识的使用 12
8.3 认证证书的管理 13
8.3.1 暂停认证证书 13
8.3.2 撤销认证证书 14
8.3.3 注销认证证书 15
9 信息沟通机制 15
10 申诉、投诉 16
11 收费 ..... **错误！未定义书签。**
12 认证责任 16

1 适用范围

IPv6 金融应用服务适用于金融业相关机构面向公众服务的互联网应用及信息基础设施（以下简称互联网应用系统）的 IPv6 接入访问服务能力，包括 IPv6 接入访问服务的标准符合性、安全性和可维护性等方面。

2 认证依据

1. JR/T 0336-2025《IPv6 技术金融应用规范》;
2. 适用的法律法规及其他要求。

3 认证等级划分

IPv6 金融应用服务认证分为三级:

一级认证：面向公众服务的互联网应用系统完成 IPv6 改造，符合第 2 章所列标准或认证规范的基本要求，并且量化指标评分大于等于 60 分，小于 75 分。

二级认证：面向公众服务的互联网应用系统完成 IPv6 改造，符合第 2 章所列标准或认证规范的基本要求，并且量化指标评分大于等于 75 分，小于 85 分。

三级认证：面向公众服务的互联网应用系统完成 IPv6 改造，符合第 2 章所列标准或认证规范的基本要求，并且量化指标评分大于等于 85 分。

4 认证模式

服务管理审核+服务特性测评。

认证模式选择和组合如下:

初次认证: 模式 A+模式 G+模式 I;

再认证: 模式 A+模式 G+模式 I;

监督评价（保持认证）: 模式 A+模式 G+模式 I。

其中:

“A”: 公开的服务特性检验;

“G”: 服务能力确认或验证;

“I”: 服务管理审核。

5 认证基本环节

认证基本环节:

1）认证申请及评审;

2）认证受理;

3）认证评价

--服务管理审核

--服务特性测评

4）现场审查或远程审查;

5）认证结果评价与决定;

6）获证后监督。

6 认证实施

6.1 认证基本程序

认证申请方向认证机构申请认证，认证机构对申请材料进行评审，并对其认证范围进行识别和判定，确认合格后向认证申请方发放《受理通知书》。认证申请方获得《受理通知书》后按要求接受认证机构审查。认证机构依据第 2 章所列标准和规范的要求开展审查，实施认证评价、复核和决定，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。

6.2 认证申请及评审

6.2.1 认证申请

认证申请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。认证申请方应提交给认证机构的材料包括但不限于:

1. 认证申请书（须加盖公章、法人章）;

2. 认证委托方的营业执照复印件（须加盖公章）;

3. 申请认证的网站或信息系统备案信息;

4. 相关技术文档。

6.2.1 认证申请评审

认证中心收到认证申请方的申请材料后，应安排认证评审人员对所获得的认证申请材料中的齐备性、完整性等进行评审，确认认证申

请方具备认证的基本条件，并将评审结果形成文件。认证评审人员在评审时应至少关注以下几个方面:

- 申请方与受评价方不一致时，应清楚两者的行政关系和法律地位关系，应有据可查;
- 针对认证申请方提供的资质、行政许可材料等，应核查提交的相关证明材料，包括发证的部门、有效期限等;
- 应核查认证申请方申请认证覆盖的范围、活动表述的规范和完整性，范围的界定应合理，符合本文件中有关认证范围界定的要求。不一致时，应及时与认证申请方沟通、确认;
- 对于被执法监管部门责令停业整顿或在全国企业信用信息公示系统中被列入“严重违法企业名单”的申请组织，不应受理其认证申请;
- 其他（如是否扩大或缩小认证范围、双方理解的分歧是否已经解决等）。

6.3 认证受理

认证机构在接收到认证申请方的申请材料后，在 5 个工作日内确定是否受理（因申请材料不齐备而补充材料的时间不计算在内），确认予以受理，认证中心应向认证申请方发送受理通知。确认不予以受理，认证中心应向认证申请方说明不受理原因。

适用本规则 8.3.2 的认证申请，认证机构不予受理。

6.4 认证评价

认证中心制定审查方案，安排审查人员按照第 2 章所列标准、认证中心认证程序和本文件等要求，对认证申请方进行认证审查，审查分为服务管理审核和服务特性测评。

6.4.1 服务管理审核

服务管理审核认证模式为审核模式 G+模式 I，是对认证申请方 IPv6 技术应用管理体系建立及其执行有效性的审查，包括但不限于 IPv6 技术应用服务管理相关制度建立和执行情况。

6.4.2 服务特性测评

服务特性测评认证模式为模式 A+模式 G，是对 IPv6 技术应用服务提供标准的符合性审查。

审查组根据审查计划安排进行审查，就审查发现问题与申请方相关负责人进行确认。

服务特性测评如发现存在不能满足评估准则通过要求，认证申请方应在问题提出的 6 个月内按照评估准则要求，采取有效的纠正措施并完成整改，向认证机构申请整改后的验证审查。认证机构可采用模式 A+模式 G+模式 I 方式进行验证。未按期完成整改的，审查结论为“不推荐认证注册”。

6.4.3 认证评价报告

审查结论分为推荐通过和推荐不通过两种。

1. 推荐通过

若审查结果证明认证申请方的互联网应用系统等信息基础设施支持 IPv6 连接访问，且申请方未被列入严重违法失信名单，则审查结论判定为“推荐通过”。

2. 推荐不通过

推荐不通过的判定依据包括程序上的不通过和评估准则的不通过。

（1）若审查过程中发现认证申请方提供材料虚假或者证据不足以及提供的材料不能充分证明其符合性，认证申请方在双方约定时间内不能提供补充材料或材料不充分，则审查报告审查结果为“推荐不通过”。

（2）若服务管理审核、服务特性测评结果证明认证申请方的互联网应用系统等信息基础设施不支持 IPv6 连接访问，或发现申请方被列入严重违法失信名单，则审查结论判定为“推荐不通过”。

若审查结论为“推荐不通过”，认证机构应对认证申请方提出整改要求，认证申请方可在 6 个月的整改期内申请整改验证审查。过期未整改完成的视为自动放弃本次认证。

6.5 认证复核及决定

6.5.1 认证复核

认证复核人员依据第 2 章所列标准或认证规范、认证程序和本实施规则等要求，结合认证评价过程中收集的信息，对评价结果进行复核。

6.5.2 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，做出是否授予认证资格的决定。必要时，认证机构应对认证申请方满足认证依据的情况进行风险评估，做出是否授予认证资格的决定。

对授予认证资格的认证申请方，认证机构应对其颁发认证证书并提供查询渠道，根据认证申请方的意愿在其申请认证的互联网应用系统首页中放置通过 IPv6 金融应用认证的认证标识。

对于不授予认证资格的认证申请方，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。

6.6 证后监督

6.6.1 证后监督频次和方式

为确保获证机构对 IPv6 部署标准的持续符合性，认证机构应对获证机构开展定期证后监督和特殊监督，并综合评估获证机构的符合性情况，依据评估结果采用不同的证后监督方式。

(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。

定期监督采用模式 A+模式 G+模式 I。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认证申请材料，获证机构提交的材料包括但不限于:

（1）本监督审查期间互联网应用系统变更情况。

（2）本监督审查期间 IPv6 部署措施变更情况。

（3）第 2 章所列标准或认证规范中相关指标变更情况。

(2)特殊审查。认证机构根据 IPv6 部署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特殊审查。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特殊审查频次:

（1）出现重大网络安全事故。

（2）互联网应用系统不支持 IPv6 连接访问。

（3）本监督审查期间 IPv6 部署措施变更。

（4）核心网络或网络安全基础设施发生变更。

（5）疑似存在受审互联网应用系统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。

（6）认证机构有足够理由对获证互联网应用系统与本规则中规定的标准要求的符合性提出质疑时。

（7）相关主管机构或采信方的要求。

（8）认证机构认为有必要增加特殊审查的其他情况。

（9）获证机构提出与认证相关变更。

必要情况下，认证机构可采取事先不通知的方式对认证申请方的互联网应用系统的相关设备或指标进行飞行审查。

6.6.2 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. 在本监督审查期间支持 IPv6 连接访问情况审查。
2. 在本监督审查期间的 IPv6 部署措施变更情况审查。
3. 在本监督审查期间的互联网应用系统变更情况审查。
4. 在本监督审查期间的核心网络或网络安全基础设施发生变更情况审查。
5. 认证机构认为存在重大安全隐患或疑似与本规则中规定的标准要求不符的关键点。

6.6.3 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，授权认证标识持续使用。对监督审查不合格的获证机构，认证机构应依据第 2 章所列标准、认证规范和本实施规范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。

6.7 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，认证申请方提交申请材料后 20 个工作日内，认证机构应完成对材料的审核，确定是否受理申请，并将受理结果反馈认证申请方；正式受理后，认证机构在与认证申请方沟通确认时间安排，在 10 个工作日内安排现场审查。认证审查完成后，认证机构于 20 个工作日内完成发证流程。认证时限一般在 80 个工作日内，最长不应超过 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。

6.8 再认证

认证证书为有效状态的获证机构可申请再认证，再认证申请应至少于认证证书有效期满前三个月提出，再认证的申请和受理程序与初次认证相同。

再认证须在原证书有效期内完成，原证书到期时如不能完成再认证，原证书按照本规则 8.1 节要求执行，新证书按照初次认证颁发。

7 认证变更

获证机构认证证书状态变更，发生互联网应用系统 IPv6 技术应用措施变更，ICP/IP 备案变更，网络变更，核心网络或网络安全基础设施发生变更等情况时，应向认证机构提出变更申请，并按照认证机构公示要求提交相关材料，更新认证相关信息。

认证机构识别变更的类型和范围，评估变更的影响策划并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备案网站名称、网站负责人的变更，认证申请方提交相关申请材料，经核实通过后，认证机构换发认证证书，证书到期日与原证书保持一致;

（2）如果获证机构申请扩大认证范围（互联网应用系统）时，根据初次认证程序对新增的互联网应用系统进行审查，审查通过后换发认证证书，有效期与初次获证证书一致，扩大的认证范围监督审查日期与原证书监督审查日期保持一致;

（3）如果获证机构申请缩小认证范围（互联网应用系统）时，认证申请方提交相关申请材料，经核实通过后，认证机构换发认证证书，证书到期日与原证书保持一致;

（4）如果发生 IPv6 技术应用措施变更、核心网络或网络安全基础设施发生变更等重大变更，认证申请方需按照初次认证程序执行，审查通过后换发证书;

（5）如果获证机构在认证证书有效期以内申请互联网应用系统认证升级，升级认证申请应至少于认证证书有效期满前三个月提出，升级认证的申请和受理程序与初次认证相同。升级认证须在原证书有效期内完成，原证书到期时如不能完成升级认证，原证书按照本规则 8.1 节要求执行，新证书按照初次认证颁发。

认证要求发生变更时，认证机构应通知相关获证机构。

8 认证证书

8.1 认证证书有效期

IPv6 金融应用认证证书有效期为 3 年，证书到期后自动失效。

8.2 认证证书和认证标识的使用

8.2.1 认证证书的使用

认证证书是认证机构颁发给认证申请方证明其 IPv6 技术应用服务符合认证要求的一种证明性文件。

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互联网应用系统获得认证，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。

8.2.2 认证标识的使用

认证标识是认证机构颁发给获证机构证明其系统的 IPv6 部署符合认证要求的一种证明性标识。认证标识按照获证系统的三个级别对应三个不同的标识。如下表所示。

系统获证级别	认证标识
一级	
二级	

三级	

获证机构可按照系统获证级别（一/二/三级）使用对应级别的认证标识。认证标识放置于获证系统首页以证明该系统获得了 IPv6 部署认证，标识图案在使用时，应根据认证机构提供的图样按比例放大或缩小。

认证标识由认证机构授权后获证机构方可在获准认证范围内使用，不得以任何方式转让、转送、出售、借用、冒用。未经授权不得使用。

8.3 认证证书的管理

认证证书的变更依照第 8 章所列场景处理，认证证书的暂停、恢复、撤销和注销要求:

8.3.1 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识。

(3) 监督结果证明获证机构的 IPv6 部署不符合认证要求或不支持 IPv6 连接访问，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) 获证机构被发现列入严重违法失信名单，或其他在特定时期国家或行业管理部门有要求予以暂停。

暂停期限为三个月。在三个月内，获证机构应完成认证证书恢复，获证机构至少在撤销期前 1 个月提出恢复认证申请。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。如超期仍未完成，原证书按照本规则 8.3.2 节要求执行。

8.3.2 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. 获证机构出现不支持 IPv6 连接访问问题且长期（15 日以上）无法恢复，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或证书到期未申请再认证的。

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，并在相关媒体上予以公告。

原则上，因1、3、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。

8.3.3 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和认证标识，并在相关媒体上予以公告。

9 信息沟通机制

获证机构应建立信息通报制度，在发生第7章描述的变更和6.6.1节触发特殊审查的情况时应及时向认证机构通报相关信息。

认证机构应建立信息沟通渠道，及时了解获证机构意见，加强对认证要求的宣贯培训。

认证机构应宣传普及认证业务知识，积极拓展认证结果采信和信息传播渠道，如：认证机构应按照要求及时将认证结果信息通报相关政府监管部门。

10 申诉、投诉

认证中心按照《处理客户申诉、投诉与争议程序》的相关规定对IPv6金融应用服务认证业务产生的申诉、投诉和争议进行处理。（具体详见公司官网-客户服务-投诉建议）

11 收费

收费由认证机构按国家有关规定统一收取，详见收费标准。

12 认证责任

认证申请方对其系统及文档、认证申请资料及声明等信息的真实性负责。

认证机构对其检测结果及检测报告、认证结果的公正性、客观性负责。