编号：NFCC-IR-A01-02

个人金融信息保护能力服务认证规则 V2.0/0

发布日期：2025 年 06 月 12 日　　实施日期：2025 年 06 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

本规则适用于认证机构开展的个人金融信息保护能力认证工作。个人金融信息保护能力服务认证适用于对金融机构通过金融产品或系统为消费者提供金融服务时的个人金融信息保护服务能力的评价或相关企业为金融机构开展金融服务所需提供的支撑服务时自身的个人金融信息保护服务能力的评价。个人金融信息保护能力服务认证对象为开展或拟开展涉及个人金融信息收集、存储、传输、处理等的专门提供金融服务（包括需要业务系统支撑的服务，例如网上银行业务，以及无需业务系统支撑的服务，例如金融 IT 外包服务、咨询服务等）的法人组织，或其下属及分支机构。

2 认证依据

- JR/T 0171-2020 《个人金融信息保护技术规范》
- JR/T 0197-2020 《金融数据安全 数据安全分级指南》
- GB/T 35273-2020 《信息安全技术 个人信息安全规范》
- 适用的法律规及其他要求。

注：对于开展跨境处理活动的个人信息处理者，应符合《个人信息出境个人信息保护认证办法》的要求。

3 认证模式

服务管理审核+服务特性测评，适用的服务认证模式包括：

“模式 A”：公开的服务特性检验；

“模式 C”：公开的服务特性检测；

“模式 G”：服务能力确认或验证；

“模式 I”：服务管理审核。

其中，初次认证/再认证：模式 A+模式 C+模式 G+模式 I；监督评价（保持认证）：模式 A+模式 G+模式 I。

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) 认证评价

--服务管理审核

--服务特性测评

(3) 认证申请方自查

(4) 认证复核及决定

(5) 获证后监督

(6) 再认证

5 认证等级划分

个人金融信息保护能力认证有 3 个认证等级：

Ⅰ级：具有基础的个人金融信息保护能力；

Ⅱ级：具有增强的个人金融信息保护能力；

Ⅲ级：具有持续优化的个人金融信息保护能力。

6 认证实施

6.1 认证基本程序

认证申请方根据要求填写《个人金融信息保护能力认证申请书》并准备相关材料，向认证机构申请认证。认证机构对申请业务的检测认证范围进行识别和判定，确认符合要求后向申请方发放《受理通知书》，共同确定《个人

金融信息保护能力服务认证审查方案》。认证申请方获得《受理通知书》后按要求开展相关内容的自查，并接受认证中心审查，完成后向认证机构提交相关材料。

认证机构对于需要开展检测的项目安排检测机构开展检测，检测机构在检测工作完成后向认证机构提交检测报告。认证机构收到自查表、检测报告（适用时）后，依据第 2 章所列标准和规范的要求进行服务管理审核和服务特性测评。认证机构对服务管理审核和服务特性测评结果进行综合评价与评定，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，认证中心对获证机构进行证后监督。

6.2 认证申请及受理

6.2.1 认证申请

认证申请方按要求准备申请材料并向认证机构递交认证申请。认证机构对资料进行审核，在确认申请方资料满足要求，受理认证申请。

认证申请方在申请认证时，应提交认证机构的材料包括但不限于：

（1）申请基本信息

- 认证申请书（盖公章，电子纸质各一份）；
- 认证申请方的营业执照（盖公章，电子纸质各一份）、组织机构代码证、资质证书复印件，组织架构图；
- 候选项目列表及概要说明。

（2）安全管理规范方面的文档

- 安全管理架构设置说明；
- 安全策略及安全管理制度、执行记录；

（3）个人金融信息保护相关材料

- 个人金融信息保护策略；
- 最近两期针对个人金融信息安全的内部审计记录；

- 其他个人金融信息保护策略的执行记录。

上述材料除说明外，原则上需提交电子材料 1 份，若材料为外国文字的，应当同时提供中文译本，并以中文译本为准（下同）。

（4）申请方自查

申请方根据要求开展相关内容的自查工作并填写《个人金融信息保护能力服务认证自查表》、整理抽查项目材料，在规定期限针对各抽查项目分别形成报送材料，并内向认证机构提交，各抽查项目应提交的材料包括但不限于：

- 申请方关于抽查项目所对应产品/服务的型号/版本的声明；
- 业务模式说明；
- 针对个人金融信息保护产品/服务的技术材料，包括但不限于以下技术及管理内容：数据分级现状说明、数据安全管理制度与执行记录；已获得的相关金融标准符合性证明（含权威机构出具的评估报告）、及其附属材料；
- 自查表；
- 其他与个人金融信息保护的相关材料：服务业务需求、需求分析、系统设计、数据设计说明、系统运维说明、系统应急预案、安全管理制度、用户操作说明、网络结构拓扑图等。

6.2.2 申请评审及受理

- 申请评审

认证机构在接收到认证申请方的申请材料后进行申请评审，以确定是否受理。评审内容包括材料的完整性和合规性，以及认证机构及认证人员是否有能力实施所申请的认证活动等。其中，合规性包括如下要求：

（一）具备相关法定资质、资格；

（二）委托认证的服务体系等符合相关法律法规的要求；

（三）未列入严重违法失信名单。

适用本规则 7.3.2 中规定的（1）（3）（4）（5）情形的机构，撤销证书后 3 个月内不予受理认证申请。

认证机构根据申请方提交的材料界定相应的认证适用范围，包括：所选取的项目（以下简称为“抽查项目”，选取原则见附件一）、适用的服务特性测评范围。在此期间，申请方应给于相应的配合及协助。在选取抽查项目后，认证机构应根据申请方所获相关金融标准认证情况，对认证结果加以采信，并对适用范围及审查内容进行调整（采信方法见附件二）。

认证机构确定认证适用范围后，形成《审查安排确认通知》发给申请方。

- 认证受理

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

6.3 认证评价

认证机构制定审查方案，安排审查人员按照第 2 章所列标准、认证机构认证程序和本实施规则等要求，对认证申请方进行认证审查，审查包括服务管理审核和服务特性测评。服务管理审核是对认证申请方个人金融信息保护体系建立及其执行有效性的审查，服务特性测评是对提供的产品/服务个人金融信息保护情况提供标准的符合性审查。

6.3.1 服务管理审核

服务管理审核是对认证申请方个人金融信息保护体系建立及其执行有效性的审查，包括但不限于信息系统管理相关制度建立和执行情况。

服务管理审核方式：模式 G+模式 I。

认证机构根据申请方提供的申请材料、自查表、个人金融信息保护制度等对个人金融信息保护体系架构、制度建设的标准符合性审查。

6.3.2 服务特性测评

服务特性测评是对申请方提供的产品/服务个人金融信息保护情况提供标准的符合性审查。

服务特性测评方式：模式 A+模式 C

（1）公开的服务特性检测（适用时）

原则上，对于需要技术设施支撑的抽查项目，认证机构应指定检测机构实施检测。检测机构应根据安排对抽查项目开展检测，并在检测工作完成后按照要求向认证机构提交检测报告（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）。检测活动（适用时）可与申请方自查活动同时开展。

（2）公开的服务特性检验

认证机构按照所选定的抽查项目对已确定的项目中个人金融信息保护能力标准符合性进行审查，主要内容包括：

检测过程中发现的问题。

6.3.3 评价报告

审查组根据审查结果，对认证审查活动出具书面评价报告。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提供的个人金融信息保护能力满足其申请的认证范围要求，且申请方未被列入全国法院失信被执行人名单，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）若审查结果证明认证申请方提供的个人金融信息保护能力不满足其申请的认证范围要求，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，认证申请方可在三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。

6.4 认证复核及决定

6.4.1 认证复核

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

6.4.2 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。

对于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提供查询渠道。

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。

6.5 获证后监督

6.5.1 获证后监督频次和方式

为证明获证机构个人金融信息保护工作持续符合标准要求，认证机构应综合评估获证机构的个人金融信息所面临的风险，对获证机构开展定期和特殊监督。监督采用模式 A+模式 G+模式 I。

6.5.2 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 G+模式 I，认证机构根据获证机构的个人金融信息所面临的风险水平确定审查方式。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，获证机构提交的申请材料包括但不限于：

（1）认证申请书（监督审查）；

（2）认证申请方的营业执照、组织机构代码证、资质证书复印件，组织架构图；

（3）上次审查所选择标准项目在本监督审查期间（指上次审查到本次监督审查之间）的变更情况的说明；

（4）本监督审查期间的个人金融信息保护相关的风险评估报告、安全管理制度及执行记录、安全审计报告；

（5）本监督审查期间个人金融信息保护相关的投诉、重大风险事件记录；若无投诉或重大风险事件，需提交纸质说明。

认证机构根据申请材料以及上次认证审查情况，编制自查表（监督审查），交获证机构开展自查。获证机构自查完毕并填写自查表后，整理个人金融信息保护相关材料提交认证机构，所提交的材料包括但不限于：

（1）安全管理规范方面的文档

- 安全管理架构设置说明；

- 安全策略及安全管理制度、执行记录；

（2）个人金融信息保护相关材料

- 个人金融信息保护策略；
- 最近两期针对个人金融信息安全的内部审计记录；
- 其他个人金融信息保护策略的执行记录。

（3）上次审查所选择的标准项目资料，具体包括：

- 申请方关于标准项目所对应产品/服务的型号/版本的声明；
- 产品/服务的业务模式说明；
- 针对个人金融信息保护产品/服务的技术材料，包括但不限于以下技术及管理内容：数据分级现状说明、数据安全管理制度与执行记录；
- 产品/服务已获得的相关金融标准符合性证明（含权威机构出具的评估报告）、及其附属材料；
- 自查表；
- 其他与个人金融信息保护的相关材料：产品/服务业务需求、需求分析、系统设计、数据设计说明、系统运维说明、系统应急预案、安全管理制度、用户操作说明、网络结构拓扑图等；
- 上次审查发现问题整改情况说明。

认证机构收到获证机构提交的上述材料后，开展文件审查、现场审查并进行综合评价，认证决定结论为“年度监审合格”的，由认证机构对认证证书加盖年审合格专用章。如认证审查过程中发现不符合认证要求的情况：包括申请方个人金融信息保护策略与执行，或各标准项目不符合审查依据要求的，允许在一定限期内（通常情况下不超过 3 个月）进行整改，申请方完成整改后，认证机构采取现场或远程核实的方式对整改结果进行确认，重新执行认证评价过程。

6.5.3 特殊监督

认证机构根据获证机构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：

- 出现重大信息安全事故；
- 出现与个人金融信息保护工作相关违法、违规事件；
- 认证机构有足够理由对获证系统与本规则中规定的标准要求的符合性提出质疑时；
- 相关主管机构或采信方提出要求；
- 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申请方的产品、服务及相关运营场所进行飞行审查。

6.5.4 证后监督审查的内容

证后监督采用模式 A+模式 G+模式 I 的方式，包括但不限于：

（1）个人金融信息保护能力标准服务能力验证；

（2）本监督审查期间投诉记录对认证要求符合性影响的审查；

（3）认证机构认为存在重大安全隐患或者疑似与本规则中规定的标准要求不符的关键点；

（4）本监督审查期间申请方个人金融信息保护策略与执行情况，各标准项目的产品/服务变更情况审查。

6.5.5 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。

6.6 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 3 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，原证书按照本规则第 8.3 章的要求执行，新证书按照初次认证颁发。

7 认证变更

获证机构基本信息、认证证书状态变更等情况时，应向认证机构提出变更申请，并按照认证机构网站公示要求提交相关材料。

认证机构识别变更的类型和范围，评估变更影响并实施相应的审查活动，并按照要求做出认证决定。

（1）如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，经核实后，认证机构对证书更新并收回原证书；

（2）如获证机构拟更换全部或部分抽查项目，应按照重新申请认证流程，认证机构完成申请审查后对证书进行回收换发；

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

个人金融信息保护能力认证证书有效期为 3 年。

8.2 认证证书和认证标志的使用

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业务系统获得认证，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、相关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 认证标志的使用

获证机构若以某种方式使用认证标志时，应事先向认证机构提出书面申请，由认证机构书面授权获证机构以指定的方式使用指定的认证标志。

认证标志在使用时，应与获证机构单位名称和系统名称放在一起。在使用标志图案时，应根据认证机构提供的图样按比例放大或缩小。

认证标志只能由获证机构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。

8.3 认证证书的管理

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志；

（3）监督结果证明获证机构的个人金融信息保护工作不符合相关标准要求，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要求予以暂停。

暂停期限为 3 个月。在 3 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。

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，并在规定期限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）出现重大个人金融信息保护相关风险事件，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。

认证证书注销和撤销后，认证机构应收回认证证书，并在相关媒体上予以公告。

9 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）

10 收费

收费由认证机构、检测机构按国家有关规定统一收取。

附件一 标准项目选取原则

标准项目的选取应遵循以下原则：

（1）至少包括一个与申请方所提供金融服务或产品密切相关的项目；

（2）如申请方提供多种金融服务、金融产品，原则上应覆盖全部种类，即每个种类均需选取至少一个，在项目选取时应优先选取服务覆盖面大、业务规模大、影响较大的项目，不得避重就轻；

（3）金融服务包括通过业务系统支撑的服务（例如手机银行系统、网上银行系统）、以及无需业务系统支撑的服务（例如金融 IT 外包服务），如申请方存在上述两种服务，则每种服务均应至少选取一个。

附件二 采信原则

对于已获个人金融信息保护相关的认证证书、或权威机构出具的评估报告的标准项目，其采信原则如下：

（1）应为国家认证认可监督管理部门批准设立的认证机构所出具的认证证书，或获得行业管理部门（含行业协会）认可的权威机构出具的评估报告；

（2）认证证书、评估报告所依据的标准应为现行有效的，且与个人金融信息保护相关的金融行业标准；

（3）认证证书、评估报告状态应为“有效”，或在标明的有效期内，且有效期原则上不应大于 6 个月；

（4）认证证书、评估报告应包括其相关附属材料。

对于已获符合上述要求的认证证书、评估报告的标准项目，在确认审查适用范围时原则如下：

（1）核实标准项目与认证证书、评估报告注明内容的一致性；

（2）核实认证证书、评估报告相关附属材料所列明存在问题的整改情况；

（3）抽取部分内容进行审查，原则上范围不超过认证证书所标明的与个人金融信息保护相关的部分。