编号：**ISCCC-SR-001:2014**

非金融机构支付业务设施技术认证实施规则

2014-07-15 发布　　**2014-08-01** 实施

中国信息安全认证中心 发布

目录

1　适用范围

本规则适用于认证机构开展的非金融机构支付业务设施技术认证工作。非金融机构支付业务设施技术认证，是指对申请《支付业务许可证》的非金融机构或《非金融机构支付服务管理办法》所指的支付机构，其支付业务处理系统、网络通信系统以及容纳上述系统的专用机房进行的技术标准符合性和安全性认证工作。非金融机构支付业务设施技术认证业务包括互联网支付、移动电话支付、固定电话支付、数字电视支付、预付卡发行与受理、银行卡收单以及中国人民银行确定的其他支付服务。

2　认证依据

《非金融机构支付业务设施技术认证规范》

3　认证等级划分

非金融机构支付业务设施技术认证分为两级：一级和二级。

一级认证：《非金融机构支付业务设施技术认证规范》基本要求

二级认证：《非金融机构支付业务设施技术认证规范》基本要求和增强要求

4　认证模式

检测+文件审查+现场审查+获证后监督

5　认证的基本环节

认证基本环节包括：

（1）认证申请及受理

（2）检测

（3）文件审查

（4）现场审查

（5）认证决定

（6）获证后监督

（7）再认证

6 认证实施

6.1 认证申请及受理

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的认证申请书要求。初次进行认证申请的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（纸质和电子各 1 份）

（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）认证申请方至申请提交日一年内的与申请认证业务范围相关的投诉记录；若无投诉，请提交纸质说明。皆须盖公章。（纸质 1 份）

（4）系统网络结构拓扑图及生产环境软硬件配置说明（电子 1 份）

（5）技术管理文档（电子或纸质 1 份）：系统运维管理文档应包括运维管理制度、系统应急手册、业务中断影响分析、变更管理制度、运维人员管理制度、数据备份与恢复制度；系统安全管理文档应包括安全管理制度、安全审计报告、风险管

理制度、漏洞扫描制度

（6）外包管理材料（适用于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申请方，提交电子或纸质 1 份），至少包括以下材料：

1) 外包商的营业执照、组织机构代码证

2) 外包合同

3) 外包安全保密协议

4) 业务外包评估材料

5) 外包商评估材料

6) 外包商资质材料

7) 外包商的监督管理制度

8) 外包服务应急计划

9) 外包服务的控制和监督措施

10) 项目交付材料清单和业务培训证明材料

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）。

6.2 检测

认证机构应选择具有本项认证相关检测能力的检测机构，与检测机构签署《检测合作协议书》，并将检测机构名单公布在其网站上。

认证申请方在获得受理通知书后选择检测机构实施检测。

检测机构应在不迟于检测实施之前 2 个工作日，向认证机构提交《非金融机构支付服务业务系统检测项目实施计划安排告知单》。

检测机构应在出具检测报告或合同异常终止后，将检测项目合同履行情况按照《非金融机构支付服务业务系统检测项目告知与备案登记薄》填写，并于当月 25 日前批量向认证中心备案。出具检测报告的检测机构应于检测完成后 10 个工作日向认证申请方提交正式的检测报告及相关材料（一式五份），认证申请方将其中一份递交认证机构。

6.3 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，安排审查员进行文件审查。文件审查的范围包括所有申请材料及检测报告。

文件审查应以《非金融机构支付业务设施技术认证规范》为标准，对认证申请范围内的业务设施的技术符合性进行审查，获取认证申请方为申请认证业务所提供的非金融机构支付业务设施技术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。

6.4 现场审查

认证机构按照《非金融机构支付业务设施技术认证规范》的要求，对申请认证的申请方进行现场审查。现场审查的内容主要包括但不限于：

（1）文件审查或检测中发现的问题；

（2）认证依据所要求相关管理制度的执行情况；

（3）系统一致性检查（重点核实系统名称及版本号、系统所用的软硬件和网络环境与检测报告所标明的内容是否一致）；

（4）系统运行场所。

6.5 审查结论判定

审查结论分为推荐通过和推荐不通过两种。

（1）推荐不通过

1) 若审查过程中发现材料不足，或提供的材料不能充分证明其符合性，认证机构要求检测机构或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，则审查结果为推荐不通过。

2) 若文件审查或现场审查结果证明认证申请方提供的支付业务设施技术不满足其申请的认证业务范围技术要求，则审查结论判定为推荐不通过。

（2）推荐通过

若审查结果证明认证申请方提供的支付业务设施技术满足其申请的认证业务范围技术要求，则审查结论判定为推荐通过。

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，认证申请方可在其技术能力达到相关要求后重新申请认证。若审查结论为推荐通过，审查结论提交认证决定。

6.6 认证决定

认证决定由至少两名认证决定人员做出。

6.6.1 认证决定

认证决定人员依据《非金融机构支付业务设施技术认证规范》、认证程序与认证实施规则的要求及相关标准，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"通过认证"或"不通过认证"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，并向认证申请方发送认证结果通知。

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并在相关媒体上予以公告。

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。

6.6.2 对认证决定的申诉

认证申请方如对认证决定结果有异议，可在收到认证结果通知后 10 个工作日内通过认证机构公布的各种渠道提出申诉，认证机构自收到申诉之日起，应在一个月内进行处理，并将处理结果书面通知认证申请方。

6.7 证后监督

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。每次证后监督由认证机构提前 1 个月通知获证组织，要求获证组织向认证机构提交认证申请书及相关材料，提交的材料包括

但不限于：

（1） 本监督审查期间系统变更情况的声明；

（2） 本监督审查期间的安全管理制度、安全审计报告；

（3） 系统当前网络结构拓扑图及生产环境软硬件配置说明；

（4） 本监督审查期间在获证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，请提交纸质说明。皆须盖公章。（纸质 1 份）

6.7.1 证后监督频次和方式

认证机构应根据非金融机构支付业务设施技术的特点以及所承担的认证风险，合理确定证后监督审查的时间间隔和方式。

获证组织正式开办支付业务后，如出现以下情况之一，认证机构可视情况增加证后监督审查的频次：

（1）出现重大安全事故；

（2）业务系统应用架构或支撑环境变更（包括系统架构变更（如 B/S 架构变更为 C/S 架构）、操作系统产品变更、数据库系统产品变更、中间件产品变更、开发语言变更等）、重要版本变更；

（3）生产中心机房场地迁移；

（4）其他中国人民银行要求的情况。

6.7.2 证后监督审查的内容

证后监督可采用文件审查或现场审查的方式。证后监督审查根据《非金融机构支付业务设施技术认证规范》的要求对以下内

容进行审查：

（1） 系统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系统变更情况的审查，必要时可委托检测机构对系统变更内容进行检测；

（3） 在本监督审查期间，出现以下变更内容时，应重新对系统进行检测。包括但不限于：

a) 出现重大安全事故；

b) 业务系统应用架构或支撑环境变更（包括B/S架构变更为C/S架构、C/S架构变更为B/S架构，操作系统产品变更、数据库系统产品变更、中间件产品变更、开发语言变更等）、重要版本变更；

c) 生产中心机房场地迁移；

d) 其他中国人民银行要求的情况。

（4） 本监督审查期间投诉记录对认证要求符合性影响的审查。

6.7.3 证后监督结果评价

对于证后监督审查合格的获证组织，认证机构应做出保持其认证资格的决定；否则，应暂停、撤销其认证资格。

6.7.4 信息通报制度

为确保获证组织的支付业务设施技术标准符合性和安全性，认证机构应要求获证组织建立信息通报制度，及时向认证机构通报以下信息：

（1）出现重大安全事故；

（2）业务系统应用架构或支撑环境变更（包括系统架构变更（如B/S 架构变更为 C/S 架构）、操作系统产品变更、数据库系统产品变更、中间件产品变更、开发语言变更等）、重要版本变更；

（3）生产中心机房场地迁移；

（4）客户重大系统投诉；

（5）公司注册名称、注册地址变更；

（6）非金融机构支付业务设施技术认证业务范围的变更；

（7）其他重要信息。

6.7.5 信息分析

认证机构应对上述信息进行分析，视情况采取相应措施，包括增加证后监督审查频次、暂停或撤销认证资格等。

6.8 再认证

在认证证书有效期满的前三个月内，获证组织可申请再认证。再认证程序与初次认证程序相同。

6.9 认证变更

获证组织扩大/缩小认证范围、认证证书状态变更、业务系统应用架构变更、重要版本变更、生产中心机房场地迁移时，应向认证机构提出变更申请，并提交相关材料。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。审查活动可与支付业务设施技术证后监督或再认证同时进行。

如果认证变更只涉及到注册名称、注册地址的变更，获证组

织须递交变更申请，经书面审查批准后，认证机构仅对证书更新并收回原证书。

认证要求发生变更时，认证机构应通知相关获证组织，在规定的时间内提交认证申请。

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，其中包括检测、文件审查、现场审查、认证决定以及证书制作时间。

检测机构应在认证申请方获得受理通知书后 1 个半月内进场检测，检测时间一般不超过 30 个工作日（因检测项不合格，进行整改和复试的时间不计算在内，整改时间一般不超过 3 个月），并于 6 个月内提交检测报告。

一般在收到检测报告后 5 个工作日内安排文件审查，文件审查和现场审查时间一般不超过 20 个工作日，补充材料和整改时间不计算在内。文件审查和现场审查完成后一般在 2 个工作日内完成评价报告，以在完成文件审查和现场审查后收到并确认认证申请方递交的不合格纠正措施报告之日起计算评价报告完成时间。认证决定、证书制作时间共计不超过 3 个工作日。

8 认证证书

8.1 认证证书有效期

非金融机构支付业务设施技术认证证书有效期为 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。获证组织应妥善保管好证书，以免丢失、损坏。如发生证书丢失、损坏的，获证组织可申请补发。

获证组织应建立认证证书、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 认证标志的使用

获证组织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组织以指定的方式使用指定的认证标志。

认证标志只能由获证组织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。

认证标志在使用时，应与获证组织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。

8.3 认证证书的管理

8.3.1 扩大/缩小认证范围

获证组织需要扩大/缩小认证范围时，应向认证机构提交认证变更申请，同时提交扩大/缩小范围的理由、事实的说明，对扩大/缩小认证范围对其他已获证的认证范围影响的说明，以及扩大的系统服务与已获证系统服务之间的差异性说明。

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服务的有效性，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做检测和审查，并根据获证组织的要求单独颁发认证证书或换发认证证书。审查活动可与支付业务设施技术证后监督或再认证同时进行。

8.3.2 暂停认证证书

获证组织有下列情形之一的，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）获证组织未按规定使用认证证书和认证标志；

（3）监督结果证明获证组织的支付业务设施技术不符合认证要求，但不需要立即撤销认证证书；

（4）获证组织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）获证组织主动请求暂停；

（6）按照人民银行《非金融机构支付服务业务系统检测认证管理规定》相关要求应该重新检测而未检测的；

（7）在特定时期国家或行业管理部门有要求予以暂停的。

暂停期限一般为三个月。在三个月内，获证组织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，获证组织不得继续使用证书。

8.3.3 撤销认证证书

获证组织有下列情形之一，认证机构应当撤销其认证证书。

（1）获证组织出现严重问题，在短期内无法恢复符合性的或获证组织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）获证组织不接受认证机构对其实施的证后监督审查或未申请再认证的；

（3）认证证书暂停使用期间，获证组织未采取有效纠正措施；

（4）认证证书暂停使用期满，获证组织未申请恢复证书。

8.3.4 注销认证证书

获证组织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 收费

收费由认证机构、检测机构按国家有关规定统一收取。