ICS 35.240.40
A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T XXXXX—XXXX

中国金融移动支付 联网联合 第5部分：入网管理规范

China financial mobile payment--Interoperability
Part 5: Networked Management

（报批稿）

（本稿完成日期：2012年10月22日）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国人民银行　　发 布

目　　次

前　言

《中国金融移动支付　联网联合》标准由以下6部分构成：
——第1部分：通信接口规范；
——第2部分：交易与清算流程规范；
——第3部分：报文交换规范；
——第4部分：文件数据格式规范；
——第5部分：入网管理规范；
——第6部分：安全规范。
本部分为该标准的第5部分。
本部分按照GB/T1.1-2009给出的规则起草。
本部分由中国人民银行提出。
本部分由全国金融标准化技术委员会（SAC/TC180）归口。
本部分负责起草单位：。
本部分参加起草单位：。
本部分主要起草人：。

引　言

随着移动支付新业务、新产品、新管理模式的不断涌现，以客户需求为主导的移动支付业务出现了不断交融和细化的趋势，不同机构、不同部门、不同业务之间的信息交换和信息共享变得越来越频繁。实现商业银行、非金融支付机构、商户之间互联互通后，对入网机构和商户进行统一管理，降低交易风险，具有必要性和迫切性。

考虑到以非金融支付机构为代表的新型入网机构以及以移动支付远程支付为主要支付形式的商户仍处于不断的发展和创新中，为便于标准的推广，本部分对具有共性的管理要求进行规范，供各入网机构及移动支付商户加入转接清算网络参照执行。

中国金融移动支付　联网联合　第5部分：入网管理规范

1　范围

本部分规定了入网机构和商户加入移动支付联网通用应满足的技术要求。

本部分适用于加入转接清算网络的入网机构和商户。

2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 22239 信息安全技术　信息系统安全等级保护基本要求

GB 2887 电子计算机场地通用规范

GB 9361 计算机场地安全要求

JR/T 0071 金融行业信息系统信息安全等级保护指南

JR/T XXXXX 中国金融移动支付 应用安全规范

3　入网机构管理

3.1　机构代码分配

凡符合移动支付联网联合相关标准，并经审批合格的入网机构，均会被分配唯一的机构代码。

3.2　入网要求

3.2.1　基本要求

入网机构应先满足JR/T XXXXX 《中国金融移动支付 应用安全规范》相关要求。

3.2.2　制度要求

入网机构应建立并执行以下管理制度:

——需建立信息安全制度，支付风险管理制度，并通过有效而正式的方式进行发布；

——需指定专人负责信息安全制度的建立、分发、复查和培训；

——需每年复查信息安全制度，重新评估安全控制及过程，对不适用或需改进的地方进行修订；

——需定期对员工进行安全培训，培训内容包括各类安全制度、信息系统运维手册和应急预案等；

——需审查录用员工的技术能力和背景资料，并签署保密协议；

——需建立安全事件报告流程及应急处理预案,建立不同类别信息安全事件的报告程序，所有相关员工需知道安全事件的报告程序；

——所有相关员工都需注意及报告系统或服务任何可疑的安全弱点或威胁；

——客户提供的身份信息和银行账户信息经多次验证仍未通过的，应予以重点关注，并暂停相关业

务处理；

——发现支付账户信息被盗取、欺诈、洗钱等风险事件的，应对客户采取暂停交易、限制账户使用等相关措施；对于涉嫌犯罪的，应立即向当地公安机关报案，同时向所在地中国人民银行分支机构报告；

——发生与移动支付交易相关的安全事件应及时通知移动支付联网通用管理机构。

3.2.3 机房管理

放置涉及移动支付交易（直接传输或处理移动支付交易、为移动支付交易提供支持服务）的网络设备和系统设备的机房，必须满足以下相关要求：

——应按国家标准 GB 2887 和 GB 9361 的相关规定，采取防震、消防、空调、防潮、防静电、防雷击、供电安全等措施；

——应建立并实行出入安全管理制度，采用专人值守或电子门禁方式，对人员进出机房情况进行日常监控；

——需划分区域进行管理，区域和区域之间设置物理隔离装置，各区分别实行不同的防护措施；

——需使用人工或闭路电视监控系统监视敏感区域；

——应建立值班制度，配备值班人员，对机房内各类设备运行情况进行日常监控，并处置突发事件；

——非授权工作人员或来访人员因工作需要需进入机房，必须经过申请、审批和登记，并由授权人员授权专人全程陪同；

——电子设备或存储介质进出机房，须经审批并登记；

——机房需合理配置供电系统，提供足够的、持续的电源供给。如配备双回路供电系统（来自于不同的变电站），可持续供电时间不低于 3 小时的 UPS 或发电机；

3.2.4 网络安全要求

移动支付交易的网络安全，包括通讯方式和生产网络安全，应满足以下相关要求：

——通讯方式

入网机构应用系统与移动支付业务联网通用环境下的系统之间的连接，应满足以下相关要求：

- 接入方式应使用：专线、基于专网的 MPLS 等；
- 使用基于 MPLS（Internet）的 IPSEC/SSL、基于 Internet 的 MPLS、应充分考虑、接受相关风险，并遵循相关安全要求；
- 禁止未建立安全通道直接通过 Internet 接入。

入网机构应用系统与受理终端之间的连接，应满足以下相关要求：

- 受理终端与入网机构应用系统之间的通讯，如需先经过商户的网络或系统，入网机构应对敏感信息（主要有磁道信息、卡片验证码、个人识别码（PIN）及卡片有效期）加密或督促商户采取安全措施，确保移动支付账户敏感信息不被泄漏,防止支付指令被篡改；
- 受理终端采用 GPRS/CDMA 方式接入入网机构系统时需对敏感信息加密。

——生产网络安全

入网机构涉及移动支付交易信息的网络（以下简称为生产网络），包括直接传输或处理移动支付交易的系统和为移动支付交易提供支持服务的系统，但不包括受理终端，应满足以下相关要求：

- 接入转接清算系统的入网机构生产网络必须与不涉及移动支付交易信息的网络（如办公网络）逻辑隔离；

- 入网机构应对互联网接入本单位生产网络严格审批，如因业务需要必须接入，须在互联网接入处布放防火墙和入侵检测（防御）设备等安全设备，监视可能的攻击行为，记录入侵事件的发生，并报警正在发生的入侵事件；
- 应建立对所有的路由配置和防火墙策略的批准、测试和变更的正式流程，路由配置和防火墙策略在每次变更后须及时归档；
- 定期对路由配置和防火墙策略进行检查，对路由器和防火墙的事件日志、入侵检测（防御）设备的告警事件进行分析和处理；
- 对登录网络及网络安全设备的用户进行身份鉴别，严格控制可以修改网络及网络安全设备配置的账号；
- 及时进行网络及网络安全设备的补丁安装和版本升级，及时更新入侵检测（防御）系统的防护知识库；
- 如果有拨号访问网络方式，要对拨号用户严格访问控制，每个用户须分别自行设置口令，口令不得少于 8 位，并应定期修改；不允许外部拨号或其他方式的远程维护连接；
- 定期或在网络发生重大变更后，对安全控制措施、网络连接和限制措施进行渗透性测试或漏洞扫描，对网络及网络安全设备系统设置、补丁配置和已知的漏洞进行检查，并确认没有生产网络用户私自连接到外部网络，外部访问不能非授权进入生产网络；
- 应在网络边界处布防入侵检测（防御）设备，监视可能的攻击行为，记录入侵事件的发生，并报警正在发生的入侵事件；
- 为阻止非授权用户对内部网络中敏感数据的访问，需采取物理隔离、划分 VLAN、主机路由等方式分隔不同的用户和信息系统；
- 定期进行对网络和网络安全设备的内部或外部审计，以验证其配置或策略是否适合入网机构的安全要求；
- 需在网络边界及核心业务网段处对恶意代码（主要是病毒和木马）进行检测或清除。

3.2.5 主机系统安全要求

入网机构涉及移动支付交易的主机系统，包括直接传输或处理移动支付交易的主机系统和在入网机构生产网络内，为移动支付交易提供支持服务的主机系统，应满足以下相关要求：

——根据“知所必需”原则，严格进行对软件和系统的访问控制，禁用不必要的缺省用户。定期对用户访问文件、目录、数据库等权限进行检查，加强用户管理，剔除不活动用户，防止用户权限过大；

——参考国际通行的相关安全规范要求，制订用户口令密码使用、管理和更新制度和措施。加强系统身份认证等关键数据传输加密，防止口令泄露；

——遵照行业认可的系统加固标准，对系统进行安全加固。如禁用所有不必要的、不安全的服务、协议和应用程序；设定系统安全参数以防止误用/滥用，删除默认设置；严禁下载或使用免费软件或共享软件；移除系统或应用程序中不必要、不安全的功能等；

——在软件补丁安装以前，须在测试系统中进行严格测试，确保测试通过后再进行安装；

——制定软件补丁管理制度和流程，对所有生产系统安装必须的操作系统和应用系统补丁；

——厂商定期维护活动须进行审批并记录，维护人员进出须专人陪同并记录相关操作；

——Windows 平台的服务器和受理终端设备应安装恶意代码（主要是病毒和木马）防护系统，如防病毒软件、主机防火墙等；

——开启必要审计接口，定期分析并处理系统内重要的安全相关事件，包括重要用户行为、系统资源的异常使用和重要系统命令的使用；

——应进行主机运行监控，监控主机的 CPU、硬盘、内存、网络等资源的使用情况，监控特定进程

（主要的系统进程）的状态，限制对重要账户的添加和更改；

——需定义硬件的非正常状态，并在故障持续预设定时间后，作为安全事件进行报告；

——需定期对设备进行检查，确保运行安全，并确认关键的生产设备都在维保期内；设备维护需建立维护记录制度；

——主机和应用系统采用两种以上组合的鉴别技术实现用户身份鉴别。

3.2.6 应用系统安全要求

入网机构涉及移动支付交易的应用系统，包括直接传输或处理移动支付交易的应用系统和在入网机构生产网络内，为移动支付交易提供支持服务的应用系统，应满足以下相关要求：

——应用系统用户应进行用户身份鉴别，并须根据“知所必需”原则，严格进行访问控制；

——须建立口令管理规则，设定各类口令长度（不得小于 6 位）、复杂度（必须包含数字和字符）、修改周期（不得长于 3 个月）、不可明文传输、应加密存储等要求；

——应根据安全策略控制用户对客体的访问，实现最小授权原则，分别授予不同用户承担任务所需的最小权限，实现应用系统用户的权限分离；

——应用系统设计中应留有审计接口或记录日志，以便进行系统事件审计，如重要用户行为、重要系统功能的执行、不成功的鉴别尝试等；

——审计日志应受到保护，仅接受授权用户的访问，审计日志需至少保存三个月；

——按安全规范编写代码，如在关键应用系统开发中，不能在程序中写入固定的口令。应在关键应用系统上线前，对程序代码进行代码复审，识别可能的恶意代码和可能的安全漏洞，如缓冲区溢出漏洞等；

——应保证所有开发，测试或审计中所用的账户在进入生产环境前都已经删除或禁用；

——应保证软件开发人员与运维人员的职责分离。生产系统操作由操作员按权限控制要求执行，不允许软件开发人员等其他人员对生产系统的任何实质性操作；

——大容量存储介质在实施外包数据恢复时，应确保数据安全；在更换或废弃时，应对其中数据彻底销毁，确保数据不可恢复。在需要废弃、销毁含重要信息的介质时，应严格报批手续，做好登记，由双人负责实施，在保卫人员的监督下，采用物理破坏盘片的形式予以彻底销毁。移动支付联网通用生产相关数据不得直接在入网机构的测试环境中使用；

——软件或系统的配置更改，补丁安装以及升级需受内部变更管理控制，需保留相应的日志；

——需记录并定期查阅生产系统设备中的所有软件名称及版本，并对关键软件的参数配置以及安装文件进行备份以防止意外损坏；

——需建立生产系统变更操作的审批和实施流程。需制定变更计划，按计划实施变更；在变更实施前制定、评审并测试变更方案；在变更实施时，要求双人复核；

——需对各类信息系统基础设施和应用系统制定运维手册，并定期补充更新；

——只有授权的用户才可以获取应用软件源代码。

3.2.7 账户信息安全和密钥管理要求

以下是对入网机构在账户信息安全和密钥管理上的要求：

——入网机构的系统只能存储用于交易清分、差错处理所必需的最基本的账户信息，不得存储卡磁道信息、卡片验证码、个人识别码的明文和密文及卡片有效期；

——交易处理如涉及对个人识别码进行加解密操作的，应配备经权威部门安全认证的硬件加密设备，并采用双倍长密钥算法加解密；

——严格控制存有账户信息的数据库系统的访问权限，对系统管理员和应用系统专用账号外或其他用户应进行必要的系统审计；

——应用系统专用账号仅供应用程序访问数据库使用，不将其作为访问账号向用户提供。正常情况下数据库操作应通过交易或应用程序访问的方式进行，关闭非必须的访问数据库应用工具；
——入网机构如存在交易监控，监控屏应屏蔽持卡人敏感数据，如账号（屏蔽账号校验位前的若干位），磁道信息、卡片验证码、个人识别码及卡片有效期；
——应遵循本标准 《中国金融移动支付 联网联合 第6部分：安全规范》中第5章“密钥管理及控制”的要求。

3.2.8 恶意代码防护

以下是对入网机构在恶意代码防护方面的要求：
——需配备相应的人员负责恶意代码防护工作的日常管理及维护，监控计算机系统恶意代码防护情况，定期察看恶意代码威胁日志，并对日志中的威胁记录进行处理；
——用户在装载外部介质上的数据和程序之前必须对外部介质进行扫描以防止病毒。

3.2.9 运营管理要求

以下是对入网机构生产网络或涉及移动支付处理的主机或应用系统的运营管理要求：

——需制定信息系统运行安全应急预案和应用系统安全应急预案，指定相关员工的责任，并定期进行演练；
——应急预案需包括病毒感染、网络攻击、数据丢失或被篡改、业务连续性被破坏等事件发生后的应急处置步骤；
——应急预案需进行定期查阅并更新，以保证反映业务的变动；
——对每次应急处置需有书面记录，并事后总结并更新应急预案；
——需定期进行应急演练，并进行书面记录；
——涉及移动支付交易的应用系统数据需每日进行增量备份，定期进行全备份。备份的数据需定期进行同城异处存放；
——需定期进行备份数据恢复，以检验备份数据的有效性；
——需将数据备份与恢复的策略和操作说明制定相关文档；
——重要的生产系统服务器需采用双机备份的设计，其所连接的磁盘阵列需为冗余阵列；
——防火墙、路由器、交换机等网络设备均需有热备份，接入移动支付联网通用管理机构网络的通信线路需有备份，并且备份线路与主线路采用不同运营商提供的路由。

4 入网商户管理

4.1 商户分类

商户是指为消费者提供商品及服务的商业企业、个人或机构，与支付机构或收单机构签有支付或收单服务协议。在移动支付联网通用环境下，商户、消费者、收单机构通过移动支付与支付机构建立起支付关系。

根据移动支付方式的不同，商户分为线上商户和线下商户。线上商户是指通过互联网、移动运营商通信网络、专用网络提供商品信息、并通过移动支付进行远程支付账务结算服务的商户，通常指网上商店。线下商户是指通过实体商店、互联网等多种方式提供商品信息，通过移动支付进行近场支付账务结算服务的商户，通常指实体商店。

4.2 商户代码分配

商户代码分配应遵循以下要求：

——线上商户、线下商户在入网前，应向转接清算系统的运营方提交入网申请，明确商户的受理机构；

——受理机构签约商户，应调查了解商户的实际主营业务、业务范围和经营状况，确保商户经营信誉良好、财务状况稳定；

——受理机构按照相关标准与规定为商户设定商户类别码（MCC），设定的商户类别码必须与商户的主营业务保持一致。受理机构为商户选取并设置商户类别码时，建议采用如下步骤：

步骤1：确定特约商户所属的行业类别；

步骤2：确定商户主营业务所提供的商品或服务的性质和类型；

步骤3：确认所选商户类别码最恰当地描述了商户的业务范围和业务性质。

如果某商户在所列的商户类别码中没有合适的匹配代码，受理机构则可为该商户设置相应的通用代码；

——受理机构按照相关标准与编码规则为商户分配商户代码，商户代码的编码长度需符合报文域42的要求。在同一报文中，域42商户代码包含的MCC应与域18填写的MCC保持匹配。

4.3 线下商户管理

对于线下商户，使用近场支付服务时，技术上要求按照受理终端及通讯网络提供方规定执行，并由其确保支付过程的安全性。

4.4 线上商户管理

4.4.1 基本安全要求

线上商户通过支付内容平台向消费者提供商品或服务，本节描述支付内容平台与远程支付系统互联的基本安全要求。

支付内容平台与远程支付系统互联可以划分为网络传输层、业务数据层及交易处理层。网络传输层是指信息系统之间的网络传输协议和数据的集合;业务数据层是指信息系统之间基于网络传输协议封装的业务和应用数据的集合。交易处理层是指在支付交易处理过程中，信息系统的处理过程集合。根据三个层面安全需求的不同，分别对其定义相应的安全要求。

网络传输安全要求:主要基于目前已成熟、得到广泛应用的网络传输协议，规定了信息系统适用的网络协议的集合。

业务数据安全要求:主要规定了业务数据在信息系统之间进行网络传输及存储的安全要求，包括业务数据的存储、传输、处理等。

交易过程安全要求:主要规定了在交易过程中，各参与方在信息传递、交易交互及业务处理过程中的要求。

4.4.2 传输安全

交易数据传输应满足以下安全要求：

——应使用足够强度的加密算法和安全协议保护移动终端与远程支付系统之间的连接，且尽可能进行双向认证，例如可使用SSL/TLS或IPSEC等协议；

——如使用SSL协议，应使用3.0及以上相对高版本的协议，取消对低版本协议的支持；

——移动终端到远程支付系统的SSL加密密钥长度应不低于128位，用于签名的RSA密钥长度应不低于1024位，用于签名的ECC密钥长度应不低于160位；

——定时重新协商会话密钥。

4.4.3 业务数据安全

业务数据处理应满足以下安全要求：

——支付内容平台与远程支付系统应当对发送的报文关键要素计算 MAC 或进行签名加密，以供接收方校验报文的真实性及保证关键要素数据的机密性。关键要素包括但不限于商户代码、订单编号、订单日期时间、交易金额等。报文的接收方，用与发送方相同的方法计算 MAC 或进行验签，并验证报文 MAC 或签名的正确性；

——交易原始数据包括但不限于交易报文，交易数据保存应将敏感信息进行加密处理，包含但不仅限于姓名、联系方式、交易内容等信息，保存时间不少于法律法规及国家或行业相关部门规章规定的年限。

4.4.4 交易过程安全

交易过程应满足但不限于以下安全要求：

——支付内容平台必须支持与远程支付系统之间的相互正常访问，包含但不仅限于负载均衡、限制最大并发连接数等技术手段；

——支付内容平台与远程支付系统应可防止对交易的重放攻击；

——支付内容平台应对常见的 WEB 攻击（如跨站脚本攻击、注入攻击、拒绝服务攻击等）进行有效防范；

——支付内容平台与远程支付系统实现相互身份鉴别，包含但不仅限于证书签名等技术手段；

——保证交易的抗抵赖性，包含但不仅限于证书签名等技术手段；

——支付内容平台与远程支付系统应防止对支付成功的订单重复支付。