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 6 部分：安全规范

China financial mobile payment--Interoperability
Part6:Security

（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6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，不同系统间敏感数据信息的安全传递和保护，成为商业银行、非金融支付机构、商户之间的互联互通及信息共享必不可少的一环。

考虑到移动支付涉及面广、业务种类繁杂以及各商业银行和非金融支付机构的业务系统现状，为便于标准的推广，本部分对具有共性的安全要求进行规范，供各入网机构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6部分：安全规范

1　范围

本部分规定了移动支付联网通用网络中传输数据信息应达到的安全标准，包括密钥的管理及控制、报文加密和关键信息保护方法。

本部分适用于所有加入移动支付转接清算系统信息交换网络的入网机构。

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。

GM/T 0002 SM4分组密码算法

JR/T 0071 金融行业信息系统信息安全等级保护指南

JR/T 0055.1 银行卡联网联合技术规范 第一部分：交易处理

ISO 9564-1 Banking—Personal Identification Number Management and Security

ISO 8731-1992 Approved Algorithms for Authentication

3　术语和定义

3.1

个人识别码 personal identification number (PIN)

即个人密码，是在联机交易中识别持卡人身份合法性的数据信息。

3.2

报文鉴别码 message authentication code (MAC)

用于验证发送方和接收方之间的信息源和信息内容完整性的数据。

3.3

主密钥 master key (MK)

用于加密成员主密钥。

3.4

成员主密钥 member master key (MMK)

用于加密工作密钥（WK）。成员主密钥（MMK）受主密钥(MK)加密保护。

3.5

工作密钥 work key (WK)

用于加密PIN和MAC，包括MAC密钥（MAK）和PIN密钥（PIK）。工作密钥（WK）受成员主密钥（MMK）加密保护。

3.6

MAC 密钥 MAC key (MAK)

用于加解密MAC的密钥。

3.7

PIN 密钥 PIN key (PIK)

用于加解密PIN的密钥。

4 移动支付联网通用安全概述

4.1 移动支付联网通用安全标准架构图

移动支付联网通用安全标准架构如图1 所示。

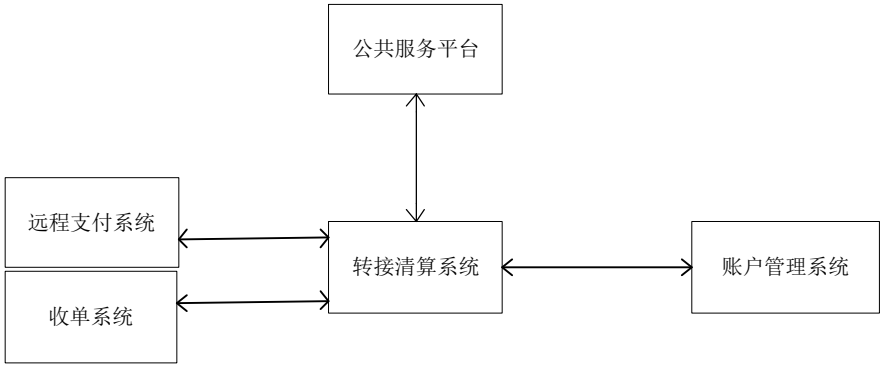

图1 移动支付联网通用安全标准架构图

在联网通用网络中，转接清算系统与公共服务平台之间应采用安全的文件传输方式，其余各系统间数据加密均采用双倍长密钥的对称加密算法。

4.2 入网机构网络接入要求

入网机构与转接清算系统均需以专线方式连接，在通讯接入线路上的选择视各地区具体情况确定，但每一个接入机构都应有主备通讯设备和主备通讯线路，并且主备线尽量选择当地不同的运营商，避免通讯设备与线路的单点故障。

4.3 安全管理的基本要求

入网机构必须满足转接清算系统信息交换网络对数据安全传输控制方面的要求。

入网机构在与转接清算系统联网的接口建设中必须提供严格的系统安全保密机制，保障转接清算系统安全、稳定、可靠地运行，包括信息的存取控制、应用系统操作的安全、物理实体（机房、设备、通信网络、记录媒体等）的安全和安全管理制度等方面。

4.4 管理制度的基本要求

整个联网通用网络的数据安全保密，不仅仅需要技术上的支持，更需要在业务上制定和贯彻各机构间严格的密钥管理制度。基本要求是：

——采用安全可靠并且在联网通用中普遍采用的对称加密算法；
——密钥的生成、存储、销毁和交易信息的加密／解密在硬件加密设备中进行；
——遵循金融业数据安全保密的国家标准和国际标准；
——加强对人员的管理要求；
——定期更换密钥。

4.5 数据传输安全控制的基本要求

数据传输安全控制要求包括以下六个方面：
——密钥管理机制：在技术上实施严格和可靠的密钥分配过程；
——个人标识码（PIN）的加密及转换机制：不允许 PIN 的明码在通信线路上和人工可操作的存储媒体上出现；
——对交易报文作来源正确性鉴别的机制（MAC）；
——对系统之间的敏感数据进行加密并计算 MAC；
——所有入网机构应采用硬件加密装置；
——以转接清算系统为中心的分段密钥处理网络机制。

4.6 硬件加密机的基本要求

硬件加密机的主要功能是实现各种密码算法、验证报文来源的正确性以及安全保存密钥。所有这些操作都在硬件加密机中完成，以保证密钥和交易数据的明码只出现在加密机中，防止泄露。硬件加密机应通过国家密码管理局的安全认证并被允许在国内金融机构中使用。此外还必须满足以下要求：
——支持双倍长（B128，在双倍长密钥算法中使用）的密钥；
——支持本文中对敏感数据及关键信息的规定，验证、转换的密文；
——支持本文中对 MAC 的规定，验证和产生 MAC；
——能对密钥作验证；
——受到非法攻击时，加密机内部保护的密钥自动销毁；
——转接清算系统与入网机构主机均要求配置硬件加密机并对传输的数据进行加密；
——转接清算系统与入网机构之间的数据加密和解密以双倍长密钥算法为基础。

4.7 数据加密传输环境的基本要求

交易数据由收单系统或远程支付系统进入转接清算系统前应已经过加密处理，如PIN加密和MAC计算。账户管理系统从转接清算系统中得到的交易数据也应进行加密处理，如交易数据的加密和MAC计算。

网络中转接清算系统的加密机与各入网机构加密机组成了一个点对点的数据加解密网络。转接清算系统与各相连系统分别约定工作密钥。

5 密钥管理及控制

5.1 总体说明

联网通用密钥体系采用对称密钥体系，通信双方在加密和解密过程中使用相同的密钥，实现对联网通用传输过程中敏感数据的加密和校验。

通信双方应采用技术手段保证密钥在整体生命周期中的安全性，对于密钥发生泄漏等异常情况，应参照《金融行业信息系统信息安全等级保护指南》的要求建立相应的措施进行处理。

5.2 对称加密算法

采用的对称加密算法分为国产SM4对称算法和国际3DES对称算法。

5.3 各层次密钥简介

5.3.1 概述

联网通用系统中各系统间数据传输所采用的对称密钥都分为主密钥、成员主密钥和工作密钥。

在联网通用的密钥体系中，联网通用网络的密钥根据实际使用情况划分成三层，三层密钥体系根据密钥的使用对象而形成，上层对下层提供保护和一定的维护功能，不同层的密钥不许相同，不能相互共享。

同一密钥只能用于其生成时所定义的目的，不能用于其他用途。

各层密钥的结构、生成方法、加密解密对象、存储地点、长度、被保护方式等如表1 所示：

表1 各层密钥表

序号	密钥名	缩写	层	原始生成方法	加密解密对象	存储地点	长度	保护方式
1	主密钥	MK	1	人工输入	成员主密钥	硬件加密机机外分段分人保管	192bit	硬件设备保护
2	成员主密钥	MMK	2	人工输入	工作密钥	硬件加密机和主机	128/192bit	从硬件加密机输出时用主密钥加密
3	工作密钥(PIK和MAK)	WK	3	硬件加密机产生	PIN、MAC	主机	128bit	用成员主密钥加密
注：为保证双倍长密钥算法的有效性，双倍长密钥的前64bit和后64bit应取不同值。								

5.3.2 第一层密钥（MK）

加密机主密钥，即本地主密钥，是最重要的密钥，用于加、解密本地存放的其他密钥数据。MK长度规定为128bit，在硬件加密机以外的地方保管时必须采取严格的安全保管措施。MK一般不更换。

5.3.3 第二层密钥（MMK）

加密机主密钥的下一层为成员主密钥（MMK），作用是加、解密需传递的工作密钥，实现工作密钥的联机实时传输或其他形式的异地传输。成员主密钥在硬件加密机以外的系统中存放和使用时，处于本地MK的保护之下。两组不同的联网通用网络参与方之间不得使用相同的成员主密钥。一般情况下，MMK2－3年更换一次。

5.3.4 第三层密钥(WK)

第三层密钥一般称为工作密钥，包括转接清算系统网络参与方之间使用的成员信息完整性密钥（MAK）和成员PIN保护密钥（PIK），用于加密各种数据，保证数据的保密性、完整性、真实性。

联网通用系统中，工作密钥为最底层的密钥，也是使用最频繁的密钥，在本地存放时，受相应的主密钥、成员主密钥的保护。工作密钥采用定期（原则上每天更换一次），或人工触发方式，或按每隔一定交易笔数申请更换。

5.4 密钥的产生

5.4.1 主密钥（MK）的产生

主密钥用人工方式输入。主密钥由三部分构成，分别由三个人掌管。为了保证输入的正确性，每一部分的密钥必须输入两次，且两次输入必须一致，否则输入失败。在三个人分别输入三部分密钥后，加密机作奇偶校验检查。奇偶校验正确时，加密机产生主密钥。主密钥必须储存在硬件加密机中，受硬件设备的保护。一旦硬件加密机受到非授权的操作，主密钥会自动销毁。

5.4.2 成员主密钥(MMK)的产生

MMK由转接清算系统和入网机构各自产生一部分，分别输入到双方的加密机中合成MMK。

也可由双方商定MMK的产生办法。

5.4.3 工作密钥的产生

PIK与MAK统称为工作密钥，由硬件加密机中的随机发生器产生。密钥产生后，硬件加密机将检查密钥的有效性。弱密钥和半弱密钥将被剔除。

转接清算系统的加密机产生工作密钥，入网机构接收和储存转接清算系统发来的工作密钥。当转接清算系统认为需要时，可以主动向入网机构发起重置密钥报文。

当入网机构需要新密钥的时侯，必须向转接清算系统发出申请重置密钥报文。

5.5 密钥的分发

5.5.1 概述

密钥分发如表2 所示。

表2 密钥的分发

序号	密钥名	密钥的分发
1	主密钥	自主生成，不需分发
2	成员主密钥	用 IC 卡传递或人工输入
3	PIN 和 MAC 密钥	由转接清算系统产生，通过联机报文发送

5.5.2 成员主密钥（MMK）的分发

MMK的分发有三个途径：

——如果转接清算系统和入网机构均使用 IC 卡保存 MMK，则可通过相互邮寄 IC 卡得到；

——如果一方没有 IC 卡或 IC 卡不能通用，则需双方相关人员到场共同输入 MMK；

——也可由双方相关人员协商确定分发途径。

5.5.3 工作密钥的分发

工作密钥由转接清算系统产生，通过联机报文的方式分发。

5.6 密钥的存储

5.6.1 主密钥的存储

主密钥应保存在硬件加密机中，受加密机的保护。

5.6.2 工作密钥和成员主密钥的存储

工作密钥和成员主密钥应保存在硬件加密机内。如果在其他设备中出现，则必须以密文方式出现。

5.6.3 密钥档案的保存

密钥注入、密钥管理功能调试和密钥档案的保管应由专人负责。密钥资料须保存在保险柜内。保险柜钥匙由专人负责。使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录。

5.7 密钥的更新

5.7.1 密钥更新的界定

如发生硬件加密机无法正常工作、更换新的硬件加密设备、密钥发生泄漏或密钥管理人员离职等情况时，均需进行密钥的更新工作。

5.7.2 密钥更新应采取的措施

5.7.2.1 主密钥的更新

重新生成新密钥并马上启用，需生成的密钥包括加密机主密钥、成员主密钥，以及各类工作密钥。

5.7.2.2 成员主密钥的更新

重新生成相应成员主密钥并立即启用，并对该成员主密钥所涉及的所有工作密钥予以更新。

5.7.2.3 工作密钥的更新

工作密钥应立即联机更新。

5.8 密钥的销毁

当新密钥产生后，生命期结束的旧密钥必须从数据库和内存中清除，防止被替换使用；同时所有可能重新构造此密钥的信息也必须清除。新密钥成功启用和旧密钥自动销毁的记录将被更新。

6 报文加密

6.1 PIN 的传输

6.1.1 概述

当报文经发送方进入联网通用网络时，持卡人的个人标识码(PIN)已经用发送方的PIK加密。转接清算系统将PIN用发送方的PIK解密后，立即用接收方的PIK加密，再发往接收方。

PIN是以128位二进制数参与加密和解密运算的，PIN的明码在这个数中的分布，称为PIN数据块。在转接清算系统和入网机构之间，PIN数据块符合ISO 9564-1的规定。

典型的PIN传输过程如图2 所示。这一过程保证了PIN的明码只在人工不可访问的终端和硬件加密机内出现。

当然同时也要求受理方能够掌握终端一侧的密钥管理和PIN数据格式。

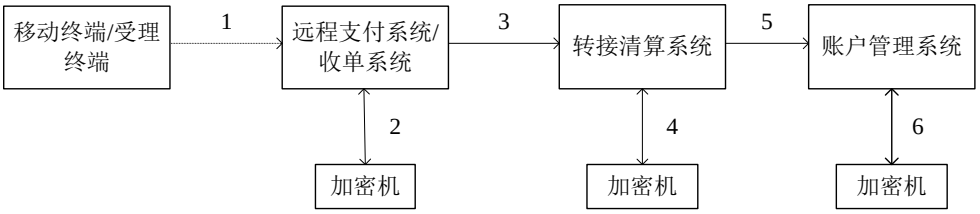

图2 PIN 的传输过程

终端、远程支付系统或收单系统、转接清算系统以及账户管理系统之间的PIN的传输过程为:

步骤1:移动终端或受理终端用K加密Y原文后得到报文的密文MSG=ENC(K)[Y]传送至远程支付系统或收单系统;

步骤2:远程支付系统或收单系统用K解密Y密文后得到报文的原文MSG=DEC(K)[Y],并立即用L加密Y原文后得到的密文MSG=ENC(L)[Y];

步骤3:远程支付系统或收单系统输出密文MSG=ENC(L)[Y]至转接清算系统;

步骤4:转接清算系统用L解密Y密报文后得到原文MSG=DEC(K)[Y], 并立即用M加密Y原文后得到密文MSG=ENC(M)[Y];

步骤5:转接清算系统输出密文MSG=ENC(M)[Y]至账户管理系统;

步骤6:账户管理系统用M解密Y密文后得到报文的原文MSG=DEC(M)[Y]。

6.1.2 PIN 的数据类型

PIN的长度为4-12位数字。

6.1.3 PIN 的字符集

PIN用数字字符表示，表3 给出了它的二进制对照表:

表3 PIN 用数字字符的二进制对照表

PIN 字符	二进制表示
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001

6.1.4 PIN 数据块

6.1.4.1 不异或主账号信息

不异或主账号信息的PIN数据块如表4 所示。

表4 不异或主账号信息的PIN数据块

位置	长度	说明
1	1 BYTE	PIN的长度
2	7 BYTE	4-12位数字的PIN（每个数字占4个BIT），不足部分右补F

示例1：

PIN明文：123456，

PIN BLOCK：0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF

6.1.4.2 异或主账号信息

PIN BLOCK为PIN按位异或主账号（PAN）。

其中，PIN格式如表5 所示：

表5 PIN格式

位置	长度	说明
1	1 BYTE	PIN长度
2	7 BYTE	4-12位数字的PIN(每个字符占4个BIT)，不足部分右补F

PAN格式如表6 所示：

表6 PAN格式

位置	长度	说明
1	2 BYTE	%H0000
3	6 BYTE	取主账号的右12位（不包括最右边的校验位），主账号不足12位左补0

示例2：

PIN明文：123456

获得的PAN：1234 5678 9012 3456 78

经过截取的PAN：6789 0123 4567

则用于PIN加密的PAN：0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67

则PIN BLOCK为： 0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF

异或： 0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67

结果： 0x06 0x12 0x53 0xDF 0xFE 0xDC 0xBA 0x98

示例3：

PIN明文：123456

获取的PAN：1234 5678 9012 3456

经过截取的PAN：4567 8901 2345

则用于PIN加密的主账号：0x00 0x00 0x45 0x67 0x89 0x01 0x23 0x45

则PIN BLOCK为：0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF

异或：0x00 0x00 0x45 0x67 0x89 0x01 0x23 0x45

结果：0x06 0x12 0x71 0x31 0x76 0xFE 0xDC 0xBA

PIN的格式应符合ISO公布的ANSI X9.8标准中以上两种PIN的格式之一，且必须在报文的域53（Security Related Control Information）中标明。

6.1.5 PIN的加密方法

将上述步骤生成的PIN数据块输入到硬件加密机中，并与存储在硬件加密机中的PIK用双倍长密钥算法计算，即可得到PIN的密文。

当报文经受理方进入跨行交易网络时，PIN已被受理方的PIK加密，转接清算系统所连接的加密机将PIN的密文用受理方的PIK解密，再用账户管理系统的PIK加密后发往账户管理系统。

6.2 联机报文 MAC 的计算

6.2.1 概述

报文来源正确性鉴别(MAC-Message Authentication Code)是一种判别报文来源是否正确，以及报文在发送途中是否被篡改的计算方法。

MAC算法取自于ISO 8731。

6.2.2 MAC 的使用条件

MAC通常用于报文域中01xx、02xx、04xx、05xx类的请求报文及01xx、02xx、04xx的成功（应答码类别含意为“批准”）的应答报文中；另外，除了重置密钥使用的08xx号报文使用MAC外，其它管理类（06xx）和网络管理类（08xx）报文均不使用MAC。

转接清算系统既支持机构使用MAC也支持机构不使用MAC，是否使用，应与入网机构具体约定。

6.2.3 MAC 报文域的选择

6.2.3.1 概述

MAC域的选择采用系统约定的方式，MAC算法采用密文块链接(CBC)的模式。

参与MAC计算的数据元集，一般包括以下数据域：

——具有唯一性的数据域（如系统跟踪号、交易传输日期时间等）

——表征报文特征的数据域（如报文类型、交易处理码、服务点条件码等）

——交易相关数据域（如主账号、交易金额、应答码、受理方标识码、接收方标识码等）

各类交易中参与MAC计算的报文域由参与交易的各方根据上述原则进行约定。

6.2.3.2 消息类型为 01xx、02xx、04xx 类的交易的报文域选择

域或tag出现或条件成立时，应该包含在MAC计算中。具体报文域如表7 所示。

表7 消息类型为 01xx、02xx、04xx 类的交易的报文域选择

序号	域	域名或 tag 标签名	属性	说明
1	0	Message-type-identifier	n4	报文类型[a]
2	2	Primary-account-number	n...19(LLVAR)	主账号[b]
3	3	Processing-code	n6	交易处理码
4	4	Amount-of-Transactions	n12	交易金额
5	7	Transmission-date-and-time	n10	交易传输时间
6	11	System-trace-audit-number	n6	系统跟踪号
7	18	Merchants-type	n4	商户类型
8	25	Point-of-service-condition-code	n2	服务点条件码
9	28	Amount_transaction_fee	x+n 8	交易费

序号	域	域名或 tag 标签名	属性	说明
10	32	Acquiring-institution-identification-code	n..11(LLVAR)	受理机构标识码[c]
11	33	Forwarding-institution-identification-code	n..11(LLVAR)	发送机构标识码[d]
12	38	Authorization-identification-response	an6	授权标识应答码
13	39	Response-code	an2	应答码
14	41	Acceptance Terminal Identification	ans8	受理终端标识码
15	42	Acceptance Identification Code	ans15	受理方标识码
16	48	tag（MN）	n15	手机号码
17	48	tag（SE）	ans16	PAMID
18	48	tag（ON）	ans40	订单号信息
19	48	tag（OI）	ansb5	机构标识码
20	48	tag（PO）	ans50	主账号
21	52	Personal Identification Number(PIN) Data	b64	个人标识码数据
22	90	Original-data-elements	n42	原始数据元[e]

[a]Message-type-identifier：报文类型（0100/0110、0200/0210、0220/0230、0420/0430）

[b]Primary-account-number：主账号，内容为两位的 PAN 长度+PAN

[c]Acquiring-institution-identification-code：受理机构标识码，内容为两位的长度（n）+最长 11 位机构标识

[d] Forwarding- institution-identification-code：发送机构标识码，内容为两位的长度（n）+最长 11 位机构标识

[e]Original-data-elements：只取前 20 位数值，内容为：

org-message-type n4 原始报文类型

org-system-trace-number n6 原始报文跟踪号

org-transmission-date-time n10 原始报文的交易传输时间

6.2.3.3 转账类交易的报文域选择

对于转账类交易，只要以下域或tag出现，就应该包含在MAC计算中，如表8 所示：

表8 转账类交易的报文域选择

序号	域	或 tag 标签名	属性	说明
1	0	Message-type	n4	报文类型[a]
2	2	Primary-account-number	n..19(LLVAR)	主账号
3	3	Processing-code	n6	交易处理码
4	4	Amount-of-Transaction	n12	交易金额
5	7	Transmission-date-and-time	n10	交易传输日期时间
6	11	System-trace-audit-number	n6	系统跟踪号
7	18	Merchants-type	n4	商户类型
8	25	Point-of-service-condition-code	n2	服务点条件码
9	28	Amount Transaction Fee	x+n8	交易费
10	32	Acquiring-institution-identification-code	n..11(LLVAR)	受理方机构代码

序号	域	或 tag 标签名	属性	说明
11	33	Forwarding-institution-identification-code	n..11(LLVAR)	转发机构代码
12	38	Authorization-identification-response	n6	授权标识应答码
13	39	Response-code	n2	应答码
14	41	Acceptance Terminal Identification	ans8	受理终端标识码
15	42	Acceptance Identification Code	ans15	受理方标识码
16	48	tag（MN）	n15	手机号码
17	48	tag（SE）	ans16	PAMID
18	48	tag（ON）	ans40	订单号信息
19	48	tag（OI）	ansb5	机构标识码
20	48	tag（PO）	ans50	主账号
21	48	tag(FA)	ans..50	账户标识 1
22	48	tag(SA)	ans..50	账户标识 2
23	52	Personal Identification Number(PIN) Data	b64	个人标识码数据
24	57	issr_addtnl_data	ans...999(LLLVAR)	附加交易信息
25	90	Original-data-elements	n42	原始数据元[b]
26	102	Account Identification 1	ans..28（LLVAR）	转出账户的账（卡）号标识[c]
27	103	Account Identification 2	ans..28（LLVAR）	转入账户的账（卡）号标识[d]

[a]Message-type-identifier：报文类型（0200/0210、0420/0430）

[b]Original-data-elements：只取前 20 位数值，内容为：

org-message-type n4 原始报文类型

org-system-trace-number n6 原始报文跟踪号

org-transmission-date-time n10 原始报文的交易传输时间

[c] Account Identification 1：资金转出账户的账（卡）号标识

[d] Account Identification 2：资金转入账户的账（卡）号标识

6.2.3.4 密钥管理类交易的报文域选择

密钥管理报文指重置密钥请求及其应答报文。其MAC由以下域组成，如表9 所示：

表9 密钥管理类交易的报文域选择

序号	域	或 tag 标签名	属性	说明
1	0	Message-type	n4	报文类型[a]
2	7	Transmission-date-and-time	n10	交易传输时间
3	11	System-trace-audit-number	n6	系统跟踪号
4	39	Response-code	an2	应答码
5	53	Security-related-control-information	n16	安全控制信息码[b]
6	70	Network-management-information-code	n3	网络管理信息码[c]
7	100	Receiving-institution-identification-code	n..11(LLVAR)	接收机构标识码[d]

[a] Message-type-identifier：报文类型（0800/0810）

[b] Security-related-control-information：安全控制信息码参见“域 53”说明，内容为：

1000000000000000 ——重置 PIN 密钥 PIK

2000000000000000 ——重置 MAC 密钥 MAK

[c] Network-management-information-code：网络管理信息码，内容为“101”

[d] Receiving-institution-identification-code：接收机构标识码，内容为两位的长度（n）+最长 11 位机构标识

6.2.4 MAC 域的构成规则

6.2.4.1 MAC 字符的选择

对所选择的MAC报文域，应进一步作字符处理。除去一些冗余信息，以提高MAC的质量。处理方法如下：

——带长度值的域在计算 MAC 时应包含其长度值信息；

——在域和域之间插入一个空格；

——所有的小写字母转换成大写字母；

——除了字母(A-Z)，数字(0-9)，空格，逗号(，)和点号(.)以外的字符都删去；

——删去所有域的起始空格和结尾空格；

——多于一个的连续空格，由一个空格代替。

6.2.4.2 MAC 块(MAB)的构成

数据从报文中选择出来后，经MAC字符选择处理，然后构成MAB(Message Authentication Block)。构成MAB的方法是：

将MAC字符选择处理后的数据按128bit划分成128bit的块，一直划分到数据的最后一块，它的位数小于或等于128bit，不满128bit时补二进制0。

6.2.5 MAC 的计算

6.2.5.1 概述

当下列情况发生时，不需计算MAC，并返回相应的报文错误信息：

——报文上没有时间域；

——时间失效；

——报文标识越界；

——密钥无效。

在发出报文前，首先从报文中截取MAC所需的报文域，然后进行MAC字符选择处理，再构成MAB并计算出MAB的长度。入网机构应将MAB、长度、MAK的值输入到硬件加密机中，产生MAC并将MAC随报文一起发送。

当收到报文后，应首先作MAC鉴别。如果产生的新MAC与传送的MAC一致，则接受报文，否则MAC鉴别失败，报文被拒绝。

6.2.5.2 硬件加密机通过 MAB 计算 MAC 的方法

本节只定义双倍长密钥算法计算 MAC 的方法。

参照ISO9.9中的做法，将MAB中的每8个字节分为一组（最后一组如不足8个字节，则右补0X00），用PIK（注意这里的密钥不是MAK，而是PIK）作为双倍长密钥依次进行如下操作：

——进行双倍长密钥运算；

——将运算结果与后一组 8 个字节的 MAB 异或，结果取代后一组，继续进行操作。对最后一组进行双倍长密钥运算，得出 8 个字节的加密值。

6.2.5.3 联机报文 MAC 域的取值

——普通交易

MAC 域（128 域）为按照双倍长密钥算法计算 MAC 得到的 8 字节二进制数据的前半部分（4 字节的二进制数），表示成 16 进制字符串形式（8 个 16 进制字符）。

入网机构或转接清算系统在发出一个报文前，应产生一个MAC值随报文一起发送。

入网机构或转接清算系统在收到一个报文后，应按照各方约定产生一个MAC值，并将该MAC值与报文中的MAC值进行对比，如果一致则认为报文正确可以接受，否则认为报文不可信任，应予以拒绝。

——转接清算系统发起的重置密钥交易

对于重置密钥交易请求和应答报文,转接清算系统和入网机构应用新下发的密钥计算MAC；重置PIN密钥时计算MAC也应用新下发的PIN密钥。

- 请求报文中的 MAC 计算方法

请求报文中的MAC域（128域）为按照双倍长密钥算法计算MAC得到的8字节二进制数据的前半部分（4字节二进制数），和按照双倍长密钥算法计算CheckValue得到的8字节二进制数据的前半部分（4字节二进制数）的组合（8字节二进制数）。

- 应答报文中的 MAC 计算方法

应答报文的MAC计算方法采用双倍长密钥算法，不需计算CheckValue，但其使用的密钥为新下发的密钥。

- CheckValue 的计算方法

CheckValue的计算方法为用新密钥对8个字节的二进制0双倍长密钥运算。

- 重置 PIK 交易的 MAC 计算方法

由于在重置PIN密钥时，新产生的PIN密钥是128字节的双倍长密钥，此时计算请求和应答报文中的MAC值和请求报文中包含的CheckValue值均采用双倍长密钥算法计算。计算MAC和CheckValue的流程为先进行双倍长密钥运算，然后将运算结果与后一组8个字节的MAB异或，异或结果用双倍长密钥运算以后取代后一组，依此类推，直到对最后一组进行双倍长密钥运算。

6.3 新旧密钥的切换

新旧密钥的切换，即在入网机构和转接清算系统通过重置密钥交易完成工作密钥（即PIK和MAK）的切换，启用新密钥的处理过程。

入网机构用新密钥加解密是在收到转接清算系统发往入网机构的重置密钥请求报文,并成功解开密钥之后。入网机构成功解开新密钥之后，会用新密钥构造入网机构返回转接清算系统的重置密钥应答报文中的MAC值。

转接清算系统用新密钥加解密是在收到并成功验证入网机构返回转接清算系统的重置密钥应答报文的MAC值之后。

因此入网机构成功接收新密钥后再发出的所有报文应启用新密钥加密,此时新旧密钥共存,即为“新旧密钥切换时间窗口”。在这个时间差中，有用旧密钥加密的交易，也有用新密钥加密的交易，必须设置一段新旧密钥共存的时期。考虑到网络的延迟和抖动，本部分将这个窗口时间定为3分钟。

3分钟之内，各交易的加解密处理流程是：先用新密钥计算和验证，如果不正确，再采用旧密钥计算和验证。一般而言，用新密钥不成功，用旧密钥就会成功。但如果用旧密钥也不成功，则说明密钥重置很可能出现了问题，导致双方密钥不同步，此时建议及早进行人工干预。

3分钟结束以后，时间窗口就应关闭，这时所有交易的加解密操作都应用新密钥。如果发现在启用新密钥后，仍然存在大量交易加解密错误的话，则说明密钥重置很可能出现了问题，导致双方密钥不同步，此时建议及早进行人工干预。

7 关键信息保护

移动支付各相关系统和转接清算系统都必须对发往对方的报文的关键数据域进行加密。

在加密处理的前后，报文的整体形式不变，但包含这些关键数据元素的报文均要进行PIN加密或MAC验证。

表10 定义了需要进行加密处理的数据元素，一旦这些数据元素在报文中出现，则该报文域或tag就要进行保护处理：

表10 需要保护的关键数据域

元素名称	保护方式	所属报文域	数据类型
手机号码	MAC校验	48	n11
订单号信息	MAC校验	48	ans..40
PAMID	MAC校验	48	n16
收款方账户	MAC校验	48	ans..50
机构标识码	MAC校验	48	ans11
主账号（P0）	MAC校验	48	ans..50
账户标识1（FA）	MAC校验	48	ans..50
账户标识2（SA）	MAC校验	48	ans..50

以上关键信息为移动支付特有报文关键域，其他关键报文域如主账号(PAN)、个人标识码数据等需遵照JR/T 0055.1相关规定执行。