ICS

备案号：

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0055.4—2009

银行卡联网联合技术规范
第 4 部分：数据安全传输控制

Technical specifications on bankcard interoperability

—Part 4: Data secure transmission control

2009-06-01 发布　　2009-07-01 实施

中国人民银行 发布

目　　次

前言 II
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 密钥的管理和控制 2
4.1 管理制度的基本要求 2
4.2 密钥的层次 2
4.3 密钥的产生 2
4.4 密钥的分发 3
4.5 密钥的存储 3
4.6 密钥的销毁 3
5 联机报文PIN的加密和解密 4
5.1 PIN的数据类型 4
5.2 PIN的字符集 4
5.3 PIN数据块 4
5.4 PIN的加解密 5
6 联机报文MAC的计算 5
6.1 MAC的使用条件 5
6.2 MAC构成规则 5
6.3 MAC的计算 5
7 基于PBOC借贷记标准的IC卡安全要求 6
8 新旧密钥的切换 6
参考文献 7

前　言

JR/T 0055《银行卡联网联合技术规范》由以下五个部分组成：

——第1部分：交易处理；

——第2部分：报文交换；

——第3部分：文件数据格式；

——第4部分：数据安全传输；

——第5部分：通信接口。

本部分为JR/T 0055的第4部分。

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归口。

本部分负责起草单位：中国人民银行科技司、中国银联股份有限公司。

本部分参与起草单位：中国工商银行、中国农业银行、中国银行、中国建设银行、华夏银行、中国金融电子化公司、银行卡检测中心。

本部分主要起草人：姜云兵、杜宁、黄发国、李洁、万高峰、陆尔东、史大鹏、林松、曾诤、邓立峰、曹瀛、马小琼、刘志刚。

银行卡联网联合技术规范
第 4 部分 数据安全传输控制

1 范围

本标准的本部分规定了银行卡跨行交易传输过程中密钥管理机制和交易数据安全传输的基本要求，以保证交易信息的安全性和完整性。

本标准的本部分适用于所有进行银行卡跨行交易的交换中心、受理方、发卡方等机构。

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部分，然而，鼓励根据本部分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部分。

ANSI X9.8 银行业-个人标识号的管理和安全

JR/T 0025（所有部分） 中国金融集成电路（IC）卡规范

3 术语和定义

下列术语和定义适用于本部分。

3.1

个人标识码（PIN） 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（MAC） 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有效性的数据。

3.3

主密钥（MK） master key (MK)

用于加解密成员主密钥。

3.4

成员主密钥（MMK） member master key (MMK)

用于加解密数据密钥（DK）。成员主密钥（MMK）受主密钥(MK)加密保护。

3.5

数据密钥（DK） data key (DK)

用于加解密PIN和MAC，包括MAC密钥（MAK）和PIN密钥（PIK）。数据密钥（DK）受成员主密钥（MMK）加密保护。

3.6

MAC 加密密钥（MAK） MAC key (MAK)

用于加解密MAC的密钥。

3.7

PIN 加密密钥（PIK） PIN key (PIK)

用于加解密PIN的密钥。

3.8

银行卡交易交换网络

由交换中心、机构以及网络设备（如路由器等）构成的，用于承载银行卡跨行业务的专用网络，以下简称为“银行卡网络”。

4 密钥的管理和控制

机构和交换中心必须满足银行卡网络对数据安全传输控制方面的要求。

机构和交换中心必须提供严格的系统安全保密机制，包括信息存取控制的安全、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。

4.1 管理制度的基本要求

整个银行卡网络的数据安全保密，需要制定和贯彻各机构间严格的密钥管理制度。基本要求是：

a) 应采用安全、可靠、成熟的加密算法；

b) 密钥的生成、存贮、销毁和交易信息的加密／解密应在硬件加密设备中进行；

c) 应遵循金融业有关数据安全保密的国家标准和国际标准；

d) 应加强对操作人员的管理要求；

e) 应定期更换密钥。

4.1.1 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并不限于以下四个方面：

a) 密钥管理机制：在技术上实施严格和可靠的密钥分配过程；

b) 个人标识码（PIN）的加解密及转换机制：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；

c) 所有机构应采用硬件加密装置；

d) 点对点的数据加解密网络机制。

4.1.2 硬件加密机的基本要求

硬件加密机的主要功能是对PIN加密和解密，验证报文来源的正确性以及存储密钥。所有这些操作都应在硬件加密机中完成，以保证密钥和PIN的明码只出现在加密机中，防止密钥和PIN的泄露。硬件加密机应通过国家商用密码主管部门的安全认证，此外还应满足以下要求：

a) 支持单倍长（B64，在单倍长密钥算法中使用）和双倍长（B128，在双倍长密钥算法中使用）密钥；

b) 支持本部分对 PIN 的规定，验证、转换 PIN 的密文；

c) 支持本部分中对 MAC 的规定，验证和产生 MAC；

d) 能对密钥作验证；

e) 受到非法攻击时，加密机内部保护的密钥自动销毁。

4.2 密钥的层次

银行卡交易安全体系中包括三级密钥。表1中说明了这三级密钥之间的关系。

表1 三级密钥体系

密钥	级别	生成方法	加密解密对象	长度(bit)	保护方式
MK	1	人工输入	MMK	192	硬件设备保护
MMK	2	人工输入	DK(即 PIK 和 MAK)	128/192	用 MK 加密
PIK	3	硬件加密机产生	PIN	128	用 MMK 加密
MAK	3	硬件加密机产生	MAC	64/128	用 MMK 加密
注：为保证双倍长密钥算法的有效性，PIK 的前 64bit 和后 64bit 应取不同值。					

4.3 密钥的产生

表2 密钥的产生

序号	密钥名	产生
1	主密钥	人工产生
2	成员主密钥	交换中心与入网机构各产生一半，在硬件设备中合成
3	PIN 密钥	由硬件设备随机数发生器产生，并须经密钥有效性检查
4	MAC 密钥	由硬件设备随机数发生器产生，并须经密钥有效性检查

4.3.1 数据密钥的产生

PIK与MAK统称为数据密钥，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。

交换中心的加密机产生数据密钥，入网机构接收和储存交换中心发来的数据密钥。

当入网机构需要新密钥的时侯，必须向交换中心发出密钥重置申请报文。

4.3.2 成员主密钥(MMK)的产生

MMK由交换中心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。

4.3.3 主密钥的产生

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。

4.4 密钥的分发

表3 密钥的分发

序号	密钥名	密钥的分发
1	主密钥	自主生成，不须分发
2	成员主密钥	用 IC 卡传递或人工输入
3	PIN 密钥	由交换中心产生，通过联机报文发送
4	MAC 密钥	由交换中心产生，通过联机报文发送

4.4.1 数据密钥的分发

数据密钥由交换中心产生，通过联机报文的方式分发。具体分发方式请见本标准第1部分和第2部分的详细描述。

4.4.2 成员主密钥（MMK）的分发

MMK的分发有三个途径：

a) 如果交换中心和入网机构均使用 IC 卡保存 MMK，则可通过相互邮寄 IC 卡得到。

b) 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。

c) 也可由双方相关人员协商确定分发途径。

4.5 密钥的存储

4.5.1 数据密钥和成员主密钥的存储

数据密钥和成员主密钥应保存在硬件加密机内。如果出现在主机的数据库中，则必须以密文方式出现。

4.5.2 主密钥的存储

主密钥必须保存在硬件加密机中，受加密机的保护。

4.5.3 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。

4.6 密钥的销毁

当新密钥产生后，生命期结束的老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。新密钥成功启用和老密钥自动销毁的记录将被更新。

5 联机报文 PIN 的加密和解密

5.1 PIN 的数据类型

PIN是4-12位数字。

5.2 PIN 的字符集

PIN用数字字符表示，表4给出了它的二进制对照表：

表4 PIN 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

5.3 PIN 数据块

PIN的格式应符合ANSI X9.8标准中PIN的两种格式之一：不异或主账号信息的PIN数据块、异或主账号信息的数据块。

5.3.1 不异或主账号信息

表5说明了不异或主账号信息的PIN数据块的构成：

表5 不异或主账号信息的 PIN 数据块

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

示例 1：

PIN 明文是 123456，则 PIN 数据块为 0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF

5.3.2 异或主账号信息

PIN数据块为PIN按位异或主账号（PAN）。

表6 PIN 格式

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

表7 PAN 格式

位置	长度(BYTE)	说明
1	2	X00X00
3	6	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

磁卡上的 PAN：1234 5678 9012 3456 78

截取下的PAN：6789 0123 4567

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

则PIN数据块为： 0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF

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

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

5.4 PIN的加解密

将5.3中生成的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，交换中心将PIN的密文用受理方的PIK解密，再用发卡方的PIK加密后发往发卡方。

6 联机报文MAC的计算

6.1 MAC的使用条件

MAC通常用于01XX、02XX、04XX类的请求报文及01XX、02XX、04XX的成功（应答码类别含意为“批准”）应答报文中。参与交易的各方可约定联机交易过程中是否使用MAC。

6.2 MAC构成规则

6.2.1 报文域的选择

参与构成MAC数据块的信息一般包括以下报文域：

——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（报文类型、交易处理码、服务点条件码等）；

——交易相关数据域（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。

6.2.2 MAC字符的选择

对所选择的用于构成MAC数据块的报文域，应做如下处理：

——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。

6.2.3 MAC块的构成

按如下方法对上述数据（即6.2.2产生的结果数据）进行处理，得到MAC数据块，即MAB(Message Authentication Block)。

将MAC字符选择处理后的数据划分成大小为64bit的块，一直划分到数据的最后一块。最后一块位数不足64bit时，右补二进制0。

6.3 MAC的计算

6.3.1 非重置密钥联机交易

将根据上述步骤生成的MAC数据块输入到硬件加密机中，并与存储在硬件加密机中的MAK用单倍长或双倍长密钥算法计算，即可得到MAC的密文。以单倍长密钥算法计算为例，具体计算步骤如下：

a)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）；

b)对第一组MAB数据进行单倍长密钥运算；

c)将运算结果与后一组MAB数据异或，结果取代后一组MAB数据，依次进行操作。对最后一组异或结果进行单倍长密钥运算，得出8个字节的加密值，即为MAC值。

机构或交换中心在发出一个报文前，应产生一个MAC值随报文一起发送。

机构或交换中心在收到一个报文后，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。

6.3.2 重置密钥交易

对于重置密钥交易请求和应答报文,交换中心和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域（128域）为按照单倍长密钥算法计算MAC得到的8字节二进制数据的前半部分（4字节二进制数）和按照单倍长密钥算法计算校验值得到的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）。

应答报文的MAC计算方法同6.3.1中描述的普通交易，不需计算校验值，但其使用的密钥仍为新下发的密钥。

校验值的计算方法为用新密钥对8个字节的二进制“0”作单倍长密钥运算。

但有一点需要注意，交换中心发出的重置密钥报文MAC值是用该报文中新的密钥值来加密的，所以当重置的是双倍长PIK时，此报文的MAC应采用双倍长密钥算法进行加密，这是MAC加密的一个特例。同理，对于请求报文中包含的校验值也采用双倍长密钥算法计算。这里计算MAC和校验值的流程与6.3.1节中描述的流程完全一致，即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，结果取代后一组MAB，依此类推，直到对最后一组进行完双倍长密钥运算。

7 基于 PBOC 借贷记标准的 IC 卡安全要求

按照JR/T 0025－2005 中国集成电路（IC）卡规范的相关要求执行。

8 新旧密钥的切换

机构和交换中心通过重置密钥交易完成数据密钥（即PIK和MAK）的切换（见本标准第1部分）。切换处理流程中存在一个切换窗口，本节描述切换窗口中机构和交换中心的处理。

交换中心在发送重置密钥报文时已采用新密钥计算MAC，当机构收到交换中心发来的重置密钥报文后，取出新密钥，并用新密钥对报文验证MAC，然后向交换中心发送对交换中心重置密钥的应答报文，应答报文用新密钥产生MAC。

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“切换窗口”，在切换窗口时间（窗口时长可由参与交易的各方自行约定）内，机构对接收到的PIN和MAC的信息，首先用新密钥进行解密、转换或验证，如果出现PIN格式错误或MAC验证错误，则再用旧密钥进行解密、转换或验证，如再出错，则认为交易失败。

参考文献

[1] GB/T 15150—1994 产生报文的银行卡 交换报文规范 金融交易内容（ISO 8583:1987，IDT）

[2] 中国银联股份有限公司.Q/CUP 006.4-2007 银行卡联网联合技术规范V2.0 第4部分 数据安全传输控制规范

[3] 银行卡联网联合安全规范 JR/T 0003-2001