Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 006.4—2007

代替Q/CUP 006.4-2006

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

Technical Specifications on Bankcard Interoperability V2.0

Part 4 Specification on Data Secure Transmission Control

2007-08-10 发布 2007-08-10 实施

中 国 银 联 股 份 有 限 公 司 发布

目　　次

前　言

本标准对中国银联跨行交易网络中安全传输数据信息应达到的要求做了规定。包括数据传输安全要求、密钥管理方法和加密方法。

1. 增加支持Cupsecure网上安全支付交易
2. 增加支持品牌服务费
3. 增加支持PBOC电子钱包/电子存折交易
4. 增加支持农民工银行卡特色服务
5. 其它修订

——改为由CUPS产生原始币种汇率信息文件；

——删除与不良信息有关的风险信息共享文件；

——为 05 应答码增加一个适用条件是“CVN 验证失败”；

——更新入网机构标识码，并根据业管委发【2006】11 号，修改入网机构标识码中地区代码的规定；

——根据业管委发【2006】12 号，修改 43 域用法；

——增加了对 ATM 双向代理业务的支持；

——修改商户类别码的引用标准，规定商户类别代码要符合《金融零售业务 商户类别代码》（GB/T 20548-2006）。

本标准由中国银联股份有限公司提出。

本标准由中国银联股份有限公司制定。

本标准起草单位：中国银联股份有限公司、国内入网机构。

本标准主要起草人：戚跃民、郭锐、郑澎、徐静雯、李洁、吴金坛、王力斌、苗恒轩、万高峰、陆尔东。

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

1 范围

本标准对中国银联跨行交易网络中安全传输数据信息应达到的要求做了规定，包括数据传输安全要求、密钥管理方法和加密方法。

本标准适用于所有加入中国银联银行卡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。

GB/T 2260　　中华人民共和国行政区划代码

GB/T 2659-94　　世界各国和地区名称代码

GB/T 4754-94　　国民经济行业分类与代码

GB/T 12406-94　　表示货币和资金的代码

GB 13497-92　　全国清算中心代码

GB/T 15150-94　　产生报文的银行卡-交换报文规范-金融交易内容（ISO8583-1987）

JR/T 0025-2005　　中国金融集成电路(IC)卡规范

全国银行卡办公室：《银行卡联网联合技术规范》V1.0　2001.1

全国银行卡办公室：《银行卡联网联合业务规范》　2001.1

《银联卡业务运作规章》第二卷《业务规则》

EMV2000 Integrated Circuit Card Specification for Payment Systems：Book1～Book4

3 术语和定义

3.1

PIN; personal identification number

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，在计算机和网络系统中任何环节都不允许PIN以明文的方式出现。

3.2

PIN block

PIN 格式块。

3.3

MAC; message authentication code

报文鉴别码，是消息来源正确性鉴别的数据。

3.4

MMK; member master key

成员主密钥。指在银行卡安全体系中，分配给成员机构的密钥加密密钥，用于加密下一层密钥，受主密钥(MK)加密保护。

3.5

MAK; MAC key

用于生成交易报文合法性验证数据(MAC)的密钥。。

3.6

PIK; PIN key

用于加密PIN的密钥。

3.7

数据密钥 data key

指加密PIN和计算MAC的密钥，包括MAC密钥（MAK）和PIN密钥（PIK），也称为工作密钥。

3.8

HSM; hardware and security module

硬件加密机，对传输的数据进行加密的外围硬件设备，用于PIN的加密和解密、验证报文和文件来源的正确性以及存储密钥。

4 密钥管理与控制

4.1 安全管理基本要求

入网机构必须满足银联信息交换网络对数据安全传输控制方面的要求。

入网机构在与银联联网的接口建设中必须提供严格的系统安全保密机制，保障银联银行卡信息处理系统安全、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。

4.1.1 管理制度的基本要求

整个银行卡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：

a) 采用安全可靠并且在银行卡交换系统中普遍采用的加密算法。
b) 密钥的存贮和交易信息的加密／解密在硬件加密设备中进行。
c) 遵循金融业数据安全保密的国家标准和国际标准。
d) 加强对人员的管理要求。
e) 定期更换密钥。

4.1.2 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五个方面：

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) 对交易报文作来源正确性鉴别的机制（MAC）。
d) 所有入网机构采用硬件加密装置。
e) 点对点的数据加解密网络机制。

4.1.3 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，防止泄露。硬件加密机应通过国家商用密码委员会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：

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）的密钥。
b) 支持本文中对 PIN 的规定，验证、转换 PIN 的密文。
c) 支持本文中对 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。

CUPS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。

CUPS与入网机构之间的数据加密和解密以单倍长密钥算法为基础。

4.1.4 数据加密传输环境的基本要求

报文数据由入网机构进入CUPS前应已被加密。入网机构从CUPS中得到的报文数据也是加密数据。

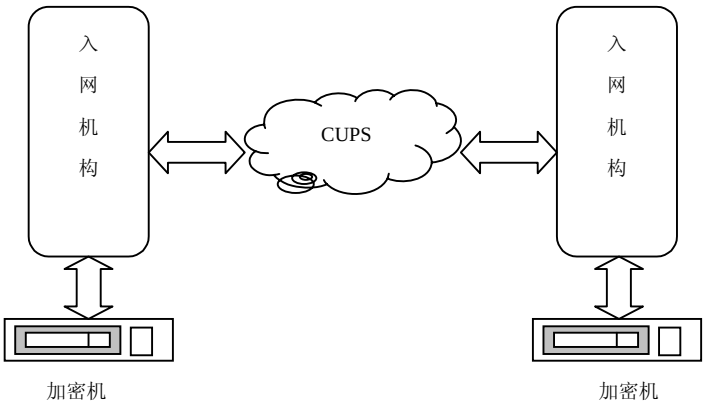


图1 数据加密传输环境

网络中CUPS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。CUPS与各联网入网机构分别约定数据密钥。

4.2 各层次密钥简介

在数据安全保密、传输机制中，密钥是关键数据。CUPS系统与每个入网机构之间约定的各层密钥都要求具有唯一性。

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

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	数据密钥	硬件加密机和主机	128bit/192bit	从硬件加密机输出时用主密钥加密
3	PIN 密钥	PIK	3	硬件加密机产生	PIN	主机	64bit/128bit	用成员主密钥加密
4	MAC 密钥	MAK	3	硬件加密机产生	MAC 计算	主机	64bit/128bit	用成员主密钥加密

主密钥和成员主密钥的生成方法及输入过程应由相关的安全管理制度规定。

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	CUPS 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。

CUPS的加密机产生数据密钥，入网机构接收和储存CUPS发来的数据密钥。

当入网机构需要新密钥的时侯，必须向CUPS发出密钥重置申请报文。

4.3.2 成员主密钥(MMK)的产生

MMK由CUPS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 CUPS 产生，通过联机报文发送
4	MAC 密钥	由 CUPS 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CUPS产生，通过联机报文的方式分发。具体分发方式请参见本规范第6章的详细描述。

4.4.2 成员主密钥（MMK）的分发

MMK的分发有三个途径：

a) 如果 CUPS 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 数据的加密处理

为保证数据的安全传输,网络中的报文采用了PIN加密和报文来源正确性鉴别(MAC)两种加密技术。

5.1 PIN 的加密和解密

当报文经受理方进入银行卡网络时，持卡人的个人标识码(PIN)已经用受理方的PIK加密。CUPS将PIN用受理方的PIK解密后，立即用发卡方的PIK加密，再发往发卡方。

PIN 是以 64 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CUPS和入网机构之间，PIN数据块符合《ISO 9564-1 Banking—Personal Identification Number Management and Security》，其格式如下图所示。

C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

注 1：C－控制码 %B0000

注 2：N－PIN 的长度（4-bit）

注 3：P－4-bit 二进制 PIN 的数码

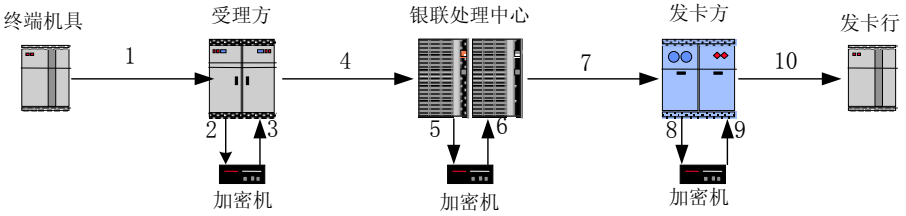
注 4：P/F－4-bit 二进制 PIN 的数码 / FILLER

注 5：4-bit %B1111（FILLER）

图2 PIN 数据块格式

典型的 PIN 加密解密过程如图3表示。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。



上图中终端机具、受理方、CUPS 以及发卡方之间的加密解密信息为:

——1: 终端机具输出 PIN 的密文

——2: 受理方用与终端机具约定的密钥解密

——3: 受理方用与 CUPS 约定的密钥加密

——4: 受理方输出 PIN 的密文

——5: CUPS 用与受理方约定的密钥解密

——6: CUPS 用与发卡方约定的密钥加密

——7: CUPS 输出 PIN 的密文

——8: 发卡方用 CUPS 约定的密钥解密

——9: 发卡方用与发卡行约定的密钥加密

——10:发卡方输出 PIN 的密文

图3 PIN 的加密解密过程

5.1.1 PIN 的长度

PIN的长度为4-12位数字。

5.1.2 PIN 的字符集

PIN用数字字符表示，下表给出了它的二进制对照表：

表4 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

5.1.3 PIN BLOCK

PIN的格式应符合ISO公布的ANSI X9.8标准中PIN的两种格式之一：

——ANSI X9.8 格式（不带主账号信息）

表5 ANSI X9.8 格式（不带主账号信息）表

位置	长度	说明
1	1 BYTE	PIN 的长度
2	7BYTE	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：

明文 PIN 123456，

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

——ANSIX9.8 格式（带主账号信息）

PIN BLOCK为PIN按位异或主账号（PAN）。

其中，PIN格式如下表所示：

表6 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格式如下表所示：

表7 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

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 BLOCK 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

示例 3：

PIN 明文：123456

磁卡上PAN：1234 5678 9012 3456

截取下的PAN：4567 8901 2345

则用于PIN加密的主账号为：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

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

PIN的格式（格式1或格式2）必须在报文的域53（Security Related Control Information）中标明。

5.1.4 PIN 的加密方法

将根据上述步骤生成的PIN BLOCK输入到硬件加密机中，并与存储在硬件加密机中的PIK用单倍长密钥算法或双倍长密钥算法计算，即可得到PIN的密文。

5.1.5 PIN 异常的处理

参见《交易处理说明》中第11章交易的异常处理流程。

5.2 联机报文 MAC 的计算方法

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《ISO8731-1992 Approved Algorithms for Authentication》。

5.2.1 MAC 的使用条件

MAC通常用于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”，参见本规范《附录》部分A.4应答码分类汇总）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。

CUPS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。

5.2.2 MAC 报文域的选择

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（流水号、日期、时间等）

——表征报文特征的数据域（报文类型、交易种类等）

——交易相关数据域（卡号、金额、应答码等）

5.2.2.1 消息类型为 01xx、02xx、04xx、05xx 类交易的报文域选择

以下域出现或条件成立时，就应该包含在MAC计算中。

表8 消息类型为 01xx、02xx、04xx、05xx 类交易的报文域选择

序号	域	域名	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	交易手续费
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]

序号	域	域名	属性	说明
12	38	Authorization-identification-response	an6	授权标识应答码
13	39	Response-code	an2	应答码
14	41	Card-acceptor-terminal-identification	ans8	受卡方终端标识码
15	42	Card-acceptor-identification-code	ans15	受卡方标识码
16	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、0422/0432）

[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

5.2.2.2 转账类交易的报文域选择

转账类交易包括转账、转出转账、转入转账、转出冲正、转入确认等。对于转账类交易，只要以下域出现，就应该包含在MAC计算中：

表9 转账类交易的报文域选择

序号	域	域名	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
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	Card-acceptor-terminal-identification	an8	受卡机终端标识码
15	42	Card-acceptor-identification-code	an15	受卡方标识码
16	90	Original-data-elements	n42	原始数据元 [b]
17	102	Account Identification 1	ans..28（LLVAR）	转出账户的账（卡）号标识 [c]
18	103	Account Identification 2	ans..28（LLVAR）	转入账户的账（卡）号标识 [d]

序号	域	域名	属性	说明
[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				

5.2.2.3 对账类交易的报文域选择

对于对账类交易，只要以下域出现，就应该包含在MAC计算中：

表10 对账类交易的报文域选择

序号	域	域名	属性	说明
1	0	Message-type-identifier	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	66	Settlement-code	n1	清算代码
5	82	Processing-fee-amount-of-credits	n12	贷记服务费金额
6	84	Processing-fee-amount-of-debits	n12	借记服务费金额
7	86	Amount-of-credits	n16	贷记交易金额
8	87	Reversal-amount-of-credits	n16	冲正贷记金额
9	88	Amount-of-debits	n16	借记交易金额
10	89	Reversal-amount-of-debits	n16	冲正借记金额
11	97	Amount-of-net-settlement	X+n16	净清算额 [b]
[a] Message-type-identifier：报文类型（0520/0530、0522/0532） [b] Amount-of-net-settlement：净清算额，内容为 1 位符号位（C—贷记/D—借记）+16 位数字的净清算额				

5.2.2.4 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：

表11 密钥管理类交易的报文域选择

序号	域	域名	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				

5.2.3 MAC 域的构成规则

5.2.3.1 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：

a) 带长度值的域在计算 MAC 时应包含其长度值信息；
b) 在域和域之间插入一个空格；
c) 所有的小写字母转换成大写字母；
d) 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；
e) 删去所有域的起始空格和结尾空格；
f) 多于一个的连续空格，由一个空格代替。

5.2.3.2 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64bit划分成64bit的块，一直划分到数据的最后一块，它的位数小于或等于64bit，不满64bit时补二进制0。

5.2.4 MAC 的计算

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：

a) 报文上没有时间域；
b) 时间失效；
c) 报文标识越界；
d) 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。

5.2.4.1 硬件加密机通过 MAB 计算 MAC 的方法（单倍长密钥算法）

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MAK作为单倍长密钥依次进行如下操作：

a) 进行单倍长密钥运算；
b) 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。对最后一组进行单倍长密钥运算，得出 8 个字节的加密值。

5.2.4.2 联机报文 MAC 域的取值

5.2.4.2.1 普通交易

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字节的二进制数），表示成16进制字符串形式（8个16进制字符）。

5.2.4.2.2 CUPS 发起的重置密钥交易

CUPS发起的重置密钥请求和应答报文的MAC计算所用的密钥为新下发的密钥，切换PIN密钥时也用新下发的PIN密钥作为密钥计算MAC。

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）。

应答报文的MAC计算方法同1中描述的普通交易，不需计算CheckValue，但其使用的密钥仍为新下发的密钥。

CheckValue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，由于有可能在重置PIN密钥时，新产生的PIN密钥是128字节的双倍长密钥，因此此时计算请求和应答报文中的MAC值都应采用双倍长密钥算法。同理，对于请求报文中包含的CheckValue值也采用双倍长密钥算法计算。这里计算MAC和CheckValue的流程与5.2.4.1节中的描述完全一致，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，依此类推，直到对最后一组进行双倍长密钥运算。

5.2.5 MAC 错误异常处理

参见《银行卡联网联合技术规范V2.0》第一部分《交易处理说明》中第11章交易的异常处理流程。

5.3 顺序文件 MAC 的计算方法

顺序文件是指文件中带有文件头（000）和文件尾（001）的文件，如双信息文件、风险信息共享文件等，具体可参见《文件接口规范》中的相关描述。所有的顺序文件都必须进行MAC校验，本节规定顺序文件的MAC校验规则。

5.3.1 MAC KEY 和 MAC 的字符组成

文件尾中有 MAC KEY 和 MAC 两个字段，每个字段都是由16个字符组成的字符串，字段之间没有分隔符，其后没有结束符，这两个字符串中每个字符都必须是16进制字符（即“0”—“9”、“A”—“F”且“A”—“F”必须大写），用于表示8个字节的 MAC 密钥和8个字节的MAC，采用这种表示方式是为了方便显示，使文件不含有不可打印的字符。

5.3.2 MAC KEY 的产生方式

MAC KEY 为生成文件时随机产生的密钥，这里是用机构主密钥加密的密文。同时MAC KEY必须满足奇校验。

5.3.3 MAC 块（MAB）的构成

将整个文件（不含MAC KEY和MAC）以256字节为一组分组，结尾不满256字节补二进制0；把各组按位异或，最后得到一个256字节的数据块，即为顺序文件MAC块。

5.3.4 MAC 的计算

MAC 分成左右两部分，生成方法如下：

前128字节按照单倍长密钥算法计算MAC，取结果的前半部分（4字节二进制数据），将其表示成16进制字符串形式（8个16进制字符），即为文件MAC字段的前半部分；同样，将256字节的数据块的后128字节按照单倍长密钥算法计算MAC，取结果的前半部分（4字节二进制数据），将其表示成16进制字符串形式（8个16进制字符），即为文件MAC字段的后半部分。

5.3.5 MAC 错误异常处理

当文件中的MAC校验未通过时，系统会生成一个拒绝文件，其中的拒绝原因指明是MAC校验失败，具体格式请参见《银行卡联网联合技术规范V2.0》第三部分《文件接口规范》中的5.4常用记录格式约定。

5.4 VIP 文件主账号的加密和解密

当VIP文件在网络上传输时，为保护VIP用户的利益，需要对记录中的账号（简记为VIPPAN）进行加解密操作。发送方执行加密操作，接收方执行解密操作。

VIPPAN是以128位二进制数参与加密和解密运算，VIPPAN的明码在这个数中的分布，称VIPPAN数据块。在CUPS和入网机构之间，其格式如下图所示。

N	N	P	P	P	P	P	P	P	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F	F	F	F	F	F	F	F	F

注1：N为VIPPAN的长度（4－bit）

注2：P为4-bit二进制VIPPAN的数码

注3：P/F为4-bit二进制VIPPAN的数码/FILLER

注4：F为4-bit %B1111（FILLER）

图4　VIPPAN 数据块格式

5.4.1　VIPPAN 的长度

对于内卡，VIPPAN的长度为13～19位；对于外卡，VIPPAN的长度为11～19位。

5.4.2　VIPPAN 的字符集

VIPPAN用数字字符表示，下表给出了它的二进制对照表：

表12　VIPPAN 字符的二进制对照表

VIPPAN 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

5.4.3　VIPPAN BLOCK

VIPPAN的格式应符合如下规则：

表13　VIPPAN 的格式

位置	长度	说明
1	1 BYTE	VIPPAN 的长度
2	15BYTE	11-19 位 VIPPAN（每个字符占 4 个 BIT，不足部分右补 F）

示例 4：

明文 VIPPAN：1234567890123456789

则 VIPPAN BLOCK 为：

0x19 0x12 0x34 0x56 0x78 0x90 0x12 0x34 0x56 0x78 0x9F 0xFF 0xFF 0xFF 0xFF 0xFF

5.4.4　VIPPAN 的加密方法

加密VIPPAN的算法：采用双倍长密钥算法，所用到的VIPPAN KEY的生成方式类似于MAC KEY的生成方式，为生成文件时随机产生的密钥，也是用机构主密钥加密的密文，也必须满足奇校验，存放于VIP文件TC500的段0位置，具体位置请参见《银行卡联网联合技术规范V2.0 第三部分 文件接口规范》VIP文件格式描述。

5.5　互联网支付密码的加密和解密

网上交易的互联网支付密码需要通过联机报文转发到发卡方，为保证该密码的安全性，要求其在网络上务必要密文传输。发送方执行加密操作，接收方执行解密操作。

互联网支付密码是以192位二进制数参与加密和解密运算，其明码在这个数中的分布，称互联网支付密码数据块。在CUPS和入网机构之间，其格式如下图所示。

N	N	P	P	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

注1：P表示Password，F表示Filler

注2：N为互联网支付密码的长度（8－bit）

注3：P为8-bit二进制互联网支付密码的字符

注4：P/F为8-bit二进制互联网支付密码的字符/填充字符

注5：F为8-bit二进制互联网支付密码的填充字符

图5　互联网支付密码数据块

5.5.1　互联网支付密码的长度

互联网支付密码的长度必须在6到20个字符以内。

5.5.2　互联网支付密码的字符集

互联网支付密码均为ASCII码字符，既可为字符，也可以为数字，或其它符号。

5.5.3　互联网支付密码 BLOCK

互联网支付密码的格式应符合如下规则：

表14　互联网支付密码的格式

位置	长度	说明
1	2 BYTE	互联网支付密码的长度
2	22BYTE	6～20 位互联网支付密码的字符（每个字符占 1 个 Byte，不足部分右补空白字符，即 0xFF）

示例 5：

明文互联网支付密码：Hello!123

由于互联网支付密码都是字符明文显示，所以这里需将其首先转换为 ASCII：

互联网支付密码明文	H	e	l	l	o	!	1	2	3
每个字符对应的ASCII	72	101	108	108	111	33	49	50	51
每个字符对应的十六进制	0x48	0x65	0x6C	0x6C	0x6F	0x21	0x31	0x32	0x33

根据图5显示的补充原则，前面补两个字符的长度位，该密码共9个字符，因此补09两个字符，转换为ASCII是48和57，转换为十六进制是0x30和0x39。后面需要补充13位的空白字符，转换为十六进制为0xFF，因此最终得到的互联网支付密码BLOCK如下：

0x30 0x39 0x48 0x65 0x6C 0x6C 0x6F 0x21 0x31 0x32 0x33 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF

5.5.4　互联网支付密码的加密方法

将根据上述步骤生成的互联网支付密码 BLOCK输入到硬件加密机中，并与存储在硬件加密机中的单倍长PIK或双倍长PIK用单倍长密钥算法或双倍长密钥算法计算，即可得到24个字节的互联网支付密码的密文。

这里需要注意两点：1）计算互联网支付密码的密钥也是PIK；2）若银行采用的是单倍长PIK，则采用单倍长密钥算法；若入网机构采用的是双倍长PIK，则采用双倍长密钥算法。

5.5.5　互联网支付密码异常的处理

异常处理流程和错误应答码都同PIN的处理方式。

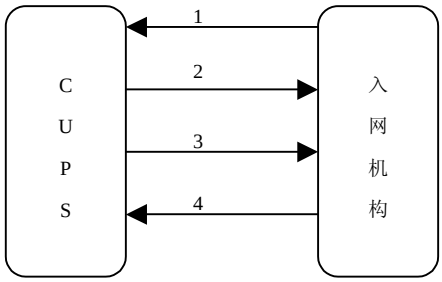
6　重置密钥

6.1　入网机构发起的申请重置密钥

6.1.1　交易流程

入网机构将申请重置密钥请求发送给CUPS，CUPS接收到该请求后，将立即返回应答。同时CUPS启动密钥更新模块，为请求方生成新密钥，并将新密钥用重置密钥请求报文发送给入网机构。

当CUPS无法将申请重置密钥应答或重置密钥请求发送给入网机构时，将丢弃该报文。



1—入网机构发往 CUPS 的申请重置密钥（0820）

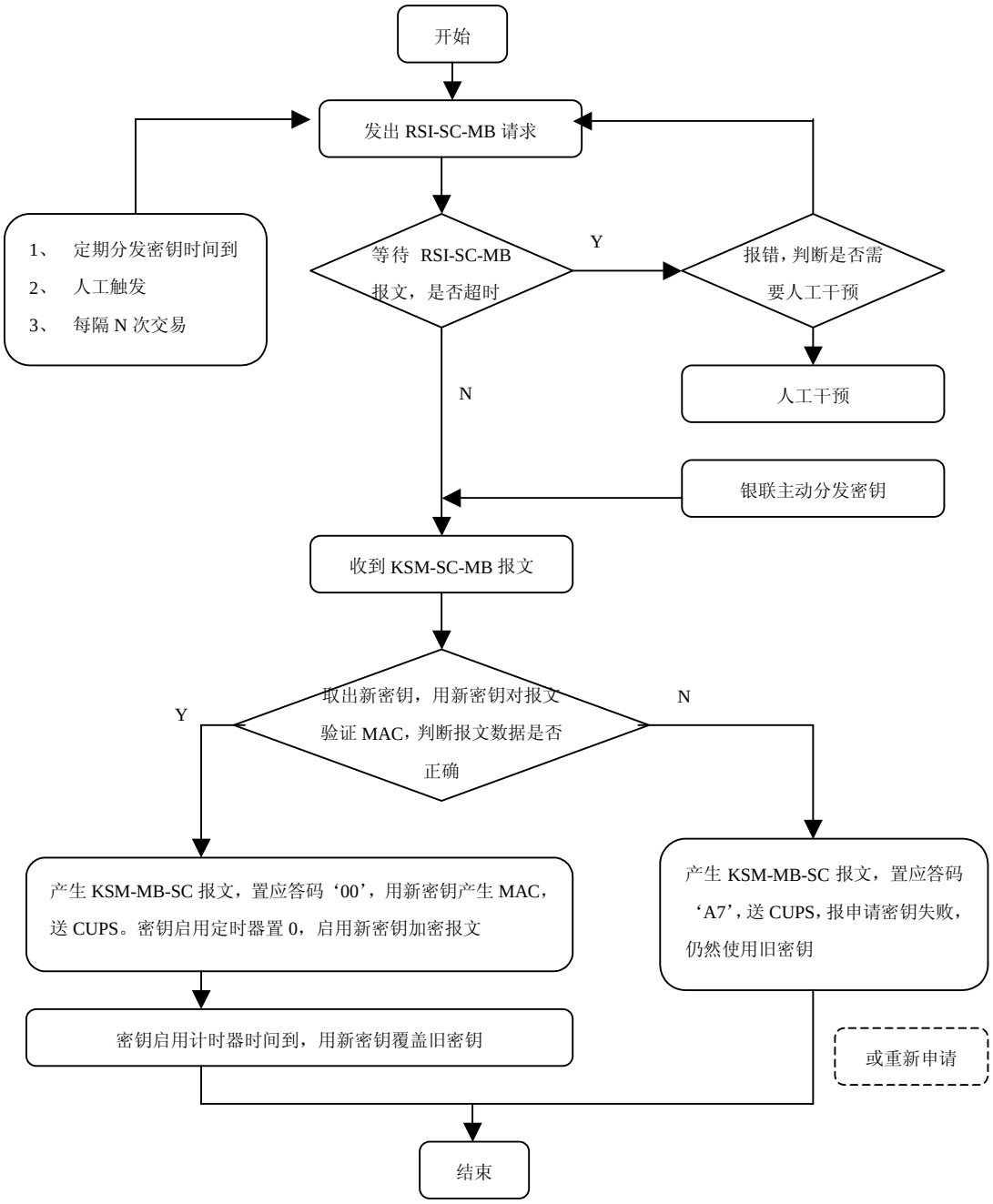
2—CUPS 发往入网机构的应答（0830）

3—CUPS 发往入网机构的重置密钥请求（0800）

4—入网机构发往 CUPS 的重置密钥请求的应答（0810）

图6　入网机构申请重置密钥流程

6.1.2　流程图



注 1：RSI-MB-SC：入网机构发往 CUPS 的重置密钥请求报文（0820）

注 2：RSI-SC-MB：CUPS 返回入网机构的重置密钥应答报文（0830）

注 3：KSM-SC-MB：CUPS 发往入网机构的重置密钥报文（0800）

注 4：KSM-MB-SC：入网机构返回 CUPS 的重置密钥应答报文（0810）

图7　入网机构发起的申请重置密钥流程图

6.1.3　入网机构申请重置密钥说明

第一阶段：向CUPS发送申请重置密钥的请求

入网机构在认为必要的时侯，可以向CUPS发送申请重置密钥的请求(RSI-MB-SC)（0820），将请求的密钥类型发往CUPS，然后等待CUPS返回的入网机构申请重置密钥的应答报文(RSI-SC-MB)（0830）。如果在规定的时间里未得到应答，可重试若干次，若仍然未得到应答，请求人工干预。

第二阶段：接收新密钥

CUPS在发送CUPS重置密钥报文(KSM-SC-MB)（0800）时已采用新密钥计算MAC，当入网机构收到CUPS发来的KSM-SC-MB后，取出新密钥，并用新密钥对报文验证MAC。然后向CUPS发送对CUPS重置密钥的应答报文(KSM-MB-SC)（0810），应答报文用新密钥产生MAC。

成功接收新密钥后，加设新密钥启用标记，由入网机构发出的所有报文应启用新密钥加密。新旧密钥切换窗口定义为3分钟，此时新旧密钥共存。这时，入网机构对接收到的CUPS发送来的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，则必须再用旧密钥进行解密、转换或验证，如再出错，则为实际出错，加、解密操作失败。在限定时间结束后，入网机构执行下述工作：

a) 新密钥替换旧密钥；

b) 消除新密钥启用标记；

c) 重置密钥结束。

6.1.4 报文格式

入网机构申请重置密钥报文 (RSI-MB-SC) 报文格式如下：

表15 入网机构申请重置密钥报文格式

位	域 名	动 作
	MESSAGE-TYPE－IDENTIFIER	值 "0820“
	BIT-MAP	b128
7	TRANSMISSION-DATE-AND-TIME	系统时间
11	SYSTEM-TRACE-AUDIT-NUMBER	系统跟踪号
33	FORWARDING-INSTITUTION-IDENTIFICATION-CODE	发送机构标识代码
53	SECURITY-RELATED-CONTROL-INFORMATION	第 1 位：密钥类型(最左) 1 PIK 2 MAK 第 2 位：加密算法类型 0 单倍长密钥算法 6 双倍长密钥算法 第 3 位－第 16 位：保留，暂填零。
70	NETWORK-MANAGEMENT-INFORMATION-CODE	值“101”

入网机构申请重置密钥的应答报文 (RSI-SC-MB) 格式如下：

表16 入网机构申请重置密钥的应答报文格式

位	域 名	动 作
	MESSAGE-TYPE－IDENTIFIER	值 "0830“
	BIT-MAP	b128
7	TRANSMISSION-DATE-AND-TIME	系统时间
11	SYSTEM-TRACE-AUDIT-NUMBER	系统跟踪号
33	FORWARDING-INSTITUTION-IDENTIFICATION-CODE	发送机构标识代码
39	RESPONSE-CODE	应答码

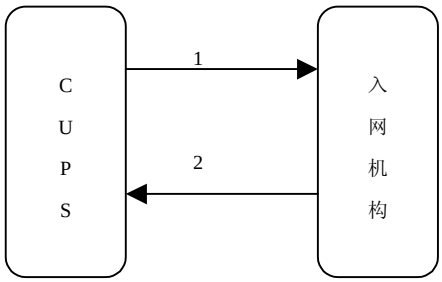
位	域 名	动 作
53	SECURITY-RELATED-CONTROL-INFORMATION	第 1 位：密钥类型(最左) 1 PIK 2 MAK 第 2 位：加密算法类型 0 单倍长密钥算法 6 双倍长密钥算法 第 3 位－第 16 位：保留，暂填零。
70	NETWORK-MANAGEMENT-INFORMATION-CODE	值“101”

当入网机构的主密钥和成员主密钥安装成功后，应首先向CUPS发出重置密钥的请求。 每一请求仅能申请一个数据密钥，所以入网机构将根据需要向CUPS发出数个请求。

6.2 CUPS 发起的重置密钥

6.2.1 交易流程

CUPS将重置密钥请求发送给入网机构，入网机构接收到该请求后将应答返回CUPS。当入网机构故障，CUPS收不到应答时，直接进行人工处理。

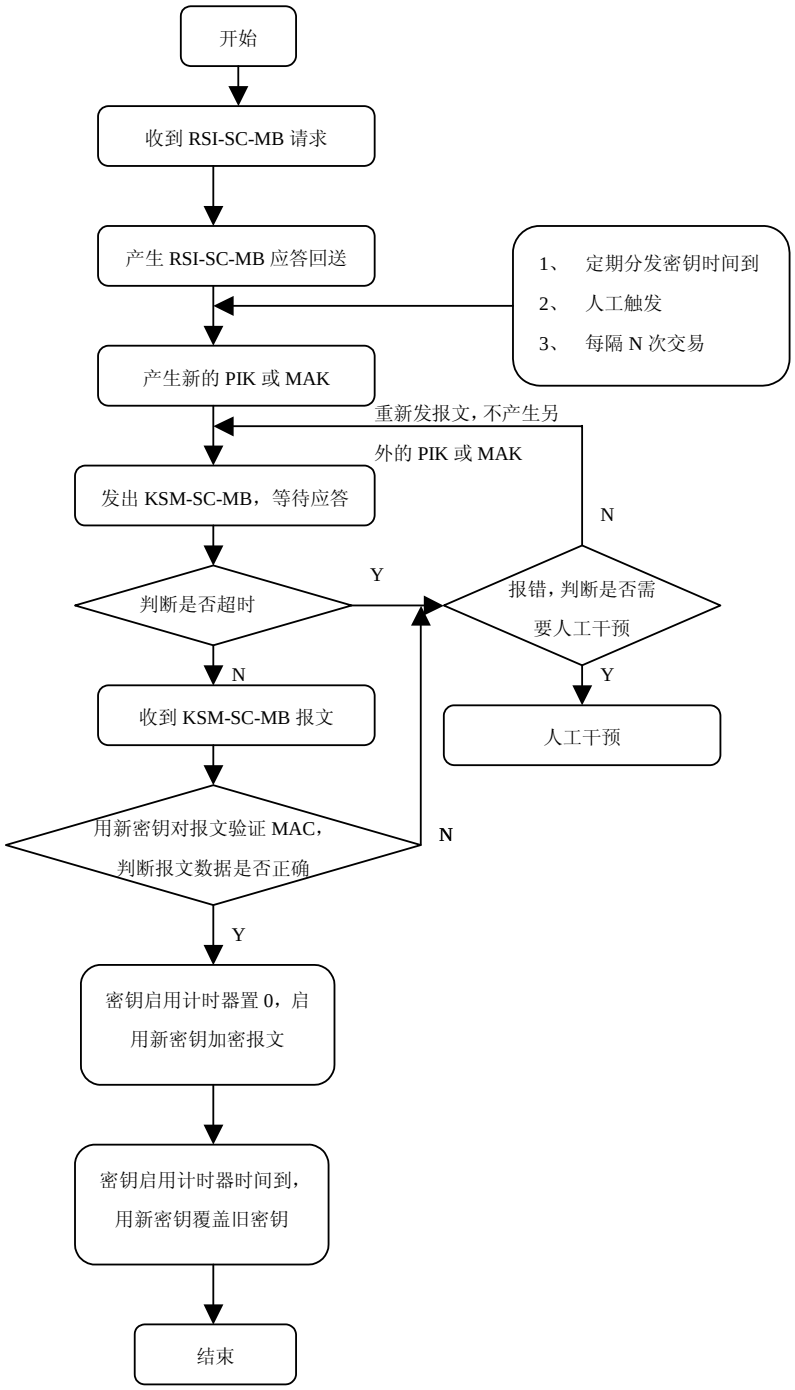


1—CUPS 发往入网机构的重置密钥请求（0800）（简记为 KSM－SC－MB）

2—入网机构发往 CUPS 的重置密钥应答（0810）（简记为 KSM－MB－SC）

图8 CUPS 重置密钥流程

6.2.2 流程图



注 1：RSI-MB-SC：入网机构发往 CUPS 的重置密钥请求报文（0820）

注 2：RSI-SC-MB：CUPS 返回入网机构的重置密钥应答报文（0830）

注 3：KSM-SC-MB：CUPS 发往入网机构的重置密钥报文（0800）

注 4：KSM-MB-SC：入网机构返回 CUPS 的重置密钥应答报文（0810）

图9 CUPS 发起的重置密钥流程图

6.2.3 CUPS 发起的重置密钥说明

CUPS向入网机构发送重置密钥请求(KSM-SC-MB)（0800）报文后，等待入网机构返回的重置密钥的应答(KSM-MB-SC)（0810）报文。

如CUPS在一定时间内没有得到应答报文,则CUPS向入网机构重发重置密钥请求(KSM-SC-MB)(0800)报文，超过一定的次数，如仍没有响应，必须请求人工干预处理。

CUPS收到入网机构成功的重置密钥应答报文(KSM-MB-SC)后，加设新密钥启用标记，由CUPS发出的所有报文启用新密钥加密。新旧密钥的切换窗口为3分钟，此时新旧密钥共存。这时，CUPS对接收到的入网机构发送来的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，则必须再用旧密钥进行解密、转换或验证，如再出错，则为实际出错，加、解密操作失败。在限定时间结束后，CUPS执行下述工作：

a）新密钥替换旧密钥

b）消除新密钥启用标记

c）重置密钥结束。

6.2.4 报文格式

CUPS重置密钥报文(KSM-SC-MB) 格式如下：

表17 CUPS 重置密钥报文格式

位	域 名	动 作
	MESSAGE-TYPE－IDENTIFIER	值 "0800“
	BIT-MAP	b128
7	TRANSMISSION-DATE-AND-TIME	系统时间
11	SYSTEM-TRACE-AUDIT-NUMBER	系统流水号
48	ADDITIONAL-DATA-PRIVATE	新密钥的密文
53	SECURITY-RELATED-CONTROL-INFORMATION	第 1 位：密钥类型(最左) 1 PIK 2 MAK 第 2 位：加密算法类型 0 单倍长密钥算法 6 双倍长密钥算法 第 3 位－第 16 位：保留，暂填零。
70	NETWORK－MANAGEMENT－INFORMATION－CODE	值“101”
96	MESSAGE－SECURITY－CODE	新密钥的密文，最大长度为 8 字节
100	RECEIVING-INSTITUTION-IDENTIFICATION-CODE	接收机构标识代码
128	MAC	Message Authentication Code

CUPS重置密钥的应答报文 (KSM-MB-SC) 格式如下：

表18 CUPS 重置密钥的应答报文格式

位	域 名	动 作
	MESSAGE-TYPE－IDENTIFIER	值 "0810“
	BIT-MAP	b128
7	TRANSMISSION-DATE-AND-TIME	系统时间
11	SYSTEM-TRACE-AUDIT-NUMBER	系统流水号
39	RESPONSE-CODE	应答码

位	域 名	动 作
53	SECURITY-RELATED-CONTROL-INFORMATION	第 1 位：密钥类型(最左) 1 PIK 2 MAK 第 2 位：加密算法类型 0 单倍长密钥算法 6 双倍长密钥算法 第 3 位－第 16 位：保留，暂填零。
70	NETWORK－MANAGEMENT－INFORMATION－CODE	值“101”
100	RECEIVING-INSTITUTION-IDENTIFICATION-CODE	接收机构标识代码
128	MAC	Message Authentication Code

6.3 新旧密钥的切换处理（同步）

新旧密钥的切换处理（同步），即在重置密钥过程中何时启用新密钥。

入网机构用新密钥加密是在收到 KSM-SC-MB，并成功解开密钥之后。CUPS用新密钥加密是在收到并成功验证入网机构的 KSM-MB-SC 之后。

重置密钥事件的时间和事件图示：

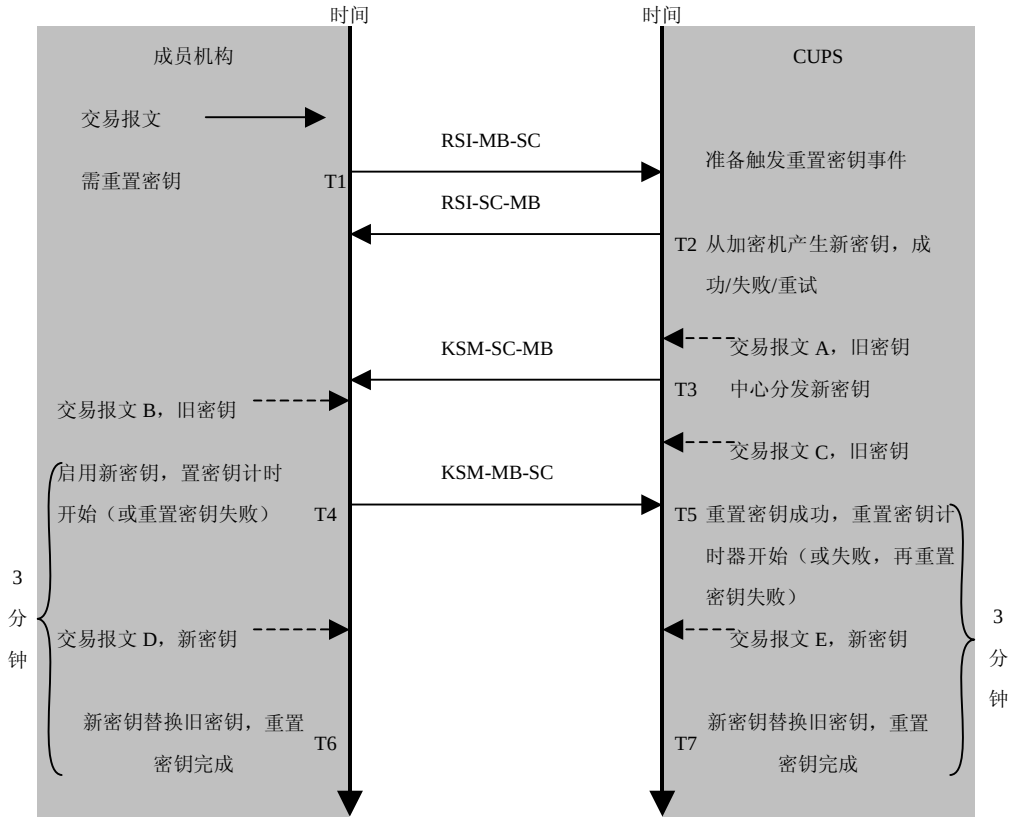


图10 重置密钥事件的时间和事件图

7 PBOC 借/贷记标准 IC 卡安全说明

7.1 PBOC 借/贷记标准 IC 卡的安全认证功能

安全认证功能是IC卡中的一项关键功能。在IC卡的联机认证过程中涉及到2个层次的认证。

——联机交易时，发卡行对卡片的认证（Online Card Authentication）

联机交易时，卡片产生ARQC（Authorization Request Cryptogram）。发卡行对ARQC进行验证，判断卡片真伪。

——联机交易时，卡片对发卡行的认证（Online Issuer Authentication）

联机交易时，发卡行产生ARPC（Authorization Response Cryptogram）。卡片对ARPC进行验证，判断发卡行的真伪。

7.2 ARQC 的生成算法

7.2.1 ARQC 的生成过程

ARQC的生成首先需要计算UDK（Unique Derivation Key，唯一分散密钥），然后通过计算得到的UDK再计算一个过程密钥（Session Key），最终通过计算得到的过程密钥再计算出ARQC。

7.2.2 密钥分散算法（MDK 生成 UDK）

IC卡的密钥是由发卡方发卡密钥发散而来，每张IC卡的密钥都不相同，只要记录根密钥和发散算法，即可推算出每张IC卡的密钥。

a) 约定参与分散算法的数据。由于 UDK 针对每一卡片唯一，所以需要通过每张卡片独有的数据分散得到，例如卡号、卡片序列号、地区代码等。该数据源将由发卡方自行决定，但在需要处理中心代为校验 ARQC 时，需将数据源通知处理中心。计算 UDK 的数据源共计 8 字节，并规定发卡行参与分散算法的数据不超过 5 个。

b) 将与发卡方约定参与分散算法的数据取出，按发卡行约定顺序逐一排列，构成数据块 D1（8 字节，包含 16 个 16 进制数字）。如果该数据块不包含 16 个 16 进制数字，那么：

- 如果长度小于 16，右对齐，前面补 0x00
- 如果长度大于 16，取最右边 16 个 16 进制数字

上述数据块 D1 取反得到 D2。

c) 将 D1 使用 MDK 密钥采用双倍长密钥算法计算得到 8 字节 UDK A；同样，将 D2 使用 MDK 密钥采用双倍长密钥算法可得到 8 字节 UDK B；

UDK B 紧邻 UDK A 排列，即可得到 UDK。如图所示：

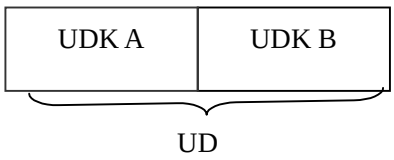


图11 密钥分散算法（MDK 生成 UDK）

7.2.3 双倍长密钥（Session Key）分散算法

a) 获得根据 MDK 计算的 UDK 密钥；

b) 将报文中的 ATC（tag 为 9F36）左边用十六进制数字'0'填充到 8 个字节，用 UDK 对该数据进行双倍长密钥运算产生过程密钥的前 8 个字节 Session Key A；

c) 将 ATC（16bit）异或十六进制值 FFFF（16bit）后在其左边用十六进制数字'0'填充到 8 个字节，再次用 UDK 对该数据进行双倍长密钥运算产生过程密钥的后 8 个字节 Session Key B；

d) 组合前 8 个字节和后 8 个字节即得到过程密钥（共 16 字节）。如图所示：

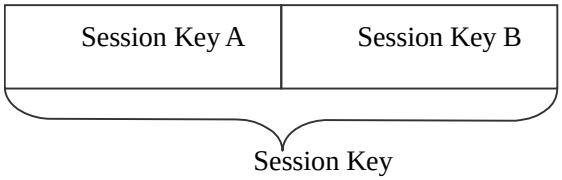


图12　双倍长密钥（Session Key）分散算法

计算得到的过程密钥必须满足奇校验要求。

7.2.4　计算 ARQC

7.2.4.1　数据源

发卡方可以自行决定计算ARQC的数据源和排列顺序，若发卡方没有自行决定，则可以采用通用的数据源和排列顺序，如下：

表19　ARQC 的数据源

顺序	数据元	来自终端的数据	参与计算终端域哈什结果的终端数据	卡片内数据	对应的报文tag
1	授权金额	√	√		9F02
2	其他金额	√	√		9F03
3	终端国家代码	√	√		9F1A
4	终端验证结果	√	√		95
5	交易货币代码	√	√		5F2A
6	交易日期	√	√		9A
7	交易类型	√	√		9C
8	不可预知数	√	√		9F37
9	应用交互特征（AIP）			√	182
10	应用交易计数器（ATC）			√	9F36
11	发卡行应用数据中的卡片验证结果（CVR）部分			√	9F10

按照通用方法，这三类数据源（终端域，终端域的哈什结果，卡片内数据）都将参加计算ARQC。

终端域的哈什结果将采用SHA-1哈什算法计算获得，共20个字节。该哈什结果后紧跟终端数据，终端数据不经过任何处理，直接按照上表顺序，逐一排列。终端数据后紧跟卡片数据，卡片数据也不经过任何处理，直接按照上表顺序，逐一排列。因此，计算ARQC的数据源排列方式如下图所示：

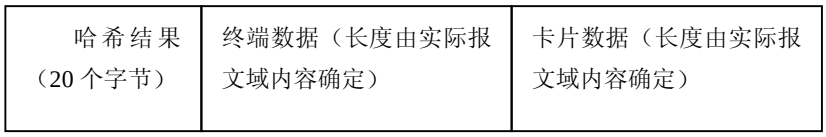


图13　ARQC 的数据源排列方式图

7.2.4.2　计算 ARQC 的步骤

a)　将上述数据块分成 8 字节一组：D1，D2，D3...；

b)　如果最后一块数据块的长度为 8 字节，则后面再补一个 8 字节数据块，该数据块由如下数据构成：0x80 0x00 0x00 0x00 0x00 0x00 0x00 0x00。 如果最后一块数据块的长度小于 8 字节，则需要将该数据块补满到 8 字节。若该数据块为 7 字节，则后面补一个字节 0x80；如果

该数据块为 6 字节，则后补两个字节的 0x80 0x00，以此类推，即，如果在补了一字节 0x80 后，整个数据块长度仍然不够 8 字节，补 0x00 直到 8 字节；

c) 过程密钥作为双倍长密钥依次对每一组进行如下操作：

1) 进行双倍长密钥运算

2) 将运算结果与后一组的 8 个字节异或，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。

7.2.4.3 计算终端域哈什结果的数据域组成

计算终端域哈什结果的数据域由卡片中的TDOL数据指定。从TDOL中读取数据名称，再从报文中取得相应的数据。根据下面的规则连接这些数据信息：

a) 如果 TDOL 中指出的数据对象的标签无法被识别；或这个标签代表的数据不是 IC 卡上的可选的静态数据；或是这个标签不代表在当前交易中适用的数据，则需要把代表该数据对象的命令域部分用 16 进制的 0 来填充；

b) 如果在 TDOL 条目中指出的长度小于实际数据对象的长度，则需要将实际的数据对象削减至 TDOL 指出的长度：

1) 如果数据对象是数字格式(n)的，则从数据单元的最左端开始削减字节；

2) 如果数据对象是其它格式的，则从数据单元的最右端开始削减字节；

如果指出的长度比实际的数据长度大，需要把实际的数据填充至指定长度：

1) 如果数据对象是数字格式(n)的，则从数据单元的最左端开始填充 16 进制的 0；

2) 如果数据对象是其它格式，则在数据单元的最右端开始填充 16 进制的 FF；

报文中数据信息的连接顺序应该与相应的数据对象在TDOL 中出现的顺序一一对应。

7.2.5 计算 ARPC

ARPC由ARQC生成，具体实现方法如下：

a) 将应用密文与授权响应密文的响应代码（tag 为 91 子域的后面部分）进行异或。应用密文包括在上传的请求报文 tag 为 9F26 的子域域中，通常是 ARQC，在一些特殊情况下是 AAC。授权响应密文的响应代码在执行异或前左对齐后面补 6 个字节 0x00。

b) 上述异或的结果是一个 8 字节的数据块 D1，对 D1 用过程密钥采用双倍长密钥计算得到 8 个字节的 ARPC。

8 相关报文域说明

8.1 域 48

附加数据——私有

8.1.1 变量属性

ans...512(LLLVAR)，3个字节的长度值＋最大512个字节(字母、数字和特殊字符)的私有附加数据

8.1.2 域描述

其中，该域的用法十一用于表示与密钥相关的信息。

8.1.3 用法十：新密钥

用于重置密钥报文中，存放CUPS向入网机构约定的新密钥，主要为了满足入网机构需要采用双倍长或三倍长甚至更长的密钥需求。

a) 用法标志—2 字节，取值“NK”。

b) 4080bit 的二进制数。

用在CUPS主动重置密钥交易和CUPS应入网机构要求重置密钥交易中。当CUPS重置数据密钥后，将产生的新数据密钥用入网机构主密钥（即MMK）加密后存放于本域发送给入网机构。

新密钥由CUPS的硬件加密机产生，入网机构收到CUPS分发的新密钥后，应由硬件加密机解密后安装使用。

8.2 域 52

个人标识码数据

8.2.1 变量属性

64bit的二进制数

8.2.2 域描述

个人标识码PIN的密文。

8.2.3 用法

如果域22指明有PIN输入，则本域必须出现。客户的个人标识码(PIN)必须加密后存放在此域中。PIN的格式在域53中标明。

本系统允许的PIN长度最大为12位数字。

8.2.4 错误代码

10525＝非法代码

8.3 域 53

安全控制信息

8.3.1 变量属性

n16，16位定长数字字符

8.3.2 域描述

与安全相关的控制信息

8.3.3 用法一：密钥管理类报文中的使用

在密钥管理类报文中（0800/0810、0820/0830），该域数据结构定义如下：

表20 域 53 数据结构 1

名称	数据类型	含义	取值
KEY-TYPE	n1	重置密钥的类型	1：PIK 2：MAK
ENCRYPTION-METHOD-USED	n1	加密算法标志	0：单倍长密钥算法 6：双倍长密钥算法 1-9：其它加密算法(未用)
RESERVED	n14	保留使用	置成全“0”

8.3.4 用法二：交易报文类中的使用

在交易类报文中，该域用于标识PIN的格式。数据结构定义如下：

表21 域 53 数据结构 2

名称	数据类型	含义	取值
PIN-FORMAT-USED	n1	PIN 格式	1：ANSI X9.8 Format(不带主账号信息) 2：ANSI X9.8 Format（带主账号信息）
ENCRYPTION-METHOD-USED	n1	加密算法标志	0：单倍长密钥算法 6：双倍长密钥算法 1-9：其它加密算法(未用)
RESERVED	n14	保留使用	置成全“0”

8.3.5 拒绝码

10535＝非法字符

8.4 域 55

IC 卡数据域

该域采用TLV（tag－length－value）的表示方式，根据不同的交易种类包含不同的子域，因此该域包含很多的子域，但只有tag为“9F10”、“9F26”和“91”的子域才含有与IC卡交易加解密相关的内容，具体描述请参见《中国金融集成电路（IC）卡借记贷记规范V2.0－卡片部分》和《中国金融集成电路（IC）卡借记贷记规范V2.0－终端部分》。

8.5 域 70

网络管理信息码

8.5.1 变量属性

n3，3位定长数字字符

8.5.2 域描述

网络管理功能码，用于区别报文类型码和报文格式均相同而实际功能不同的几种报文。有四种用法，但只有用法一涉及密钥管理，如下：

8.5.3 用法一：网络管理及密钥更新类报文标识

与报文类型码0800/0810、0820/0830一起组合表示网络管理及密钥更新类报文。其中：

表22 网络管理信息码用法 1

报文类型	网络管理信息码	交易类型
0820/0830	001	入网机构签到/CUPS 打开入网机构
0820/0830	002	入网机构签退/CUPS 关闭入网机构
0800/0810	101	CUPS 重置密钥
0820/0830	101	入网机构申请重置密钥
0820/0830	201	CUPS 开始日期切换
0820/0830	202	CUPS 终止日期切换
0820/0830	301	线路测试

8.5.4 拒绝码

10705＝非法代码

8.6 域 96

报文安全码

8.6.1 变量属性

64bit二进制数

8.6.2 域描述

CUPS与入网机构约定的单倍长新密钥

8.6.3 用法

当CUPS重置数据密钥后，将产生的新数据密钥用入网机构主密钥（即MMK）加密后发送给入网机构。当新密钥是双倍或三倍长甚至更长（16字节或24字节或更长）时，新密钥存放在48域（参见48域用法十一），本域以二进制零填充。

新密钥由CUPS的硬件加密机产生，入网机构收到CUPS分发的新密钥后，应由硬件加密机解密后安装使用。

CUPS分发的新密钥长度为8个字节。

8.7 域 128、192

报文鉴别码

8.7.1 变量属性

64bit二进制数

8.7.2 域描述

报文来源正确性鉴别码。

8.7.3 用法

报文来源正确性鉴别码是对报文中的某些敏感域的数据用53域指定的算法计算出MAC值。

产生和验证MAC应由加密机完成。加密机计算出的8个字节的二进制MAC，还需取前4个字节扩展转换成16进制表示的字符串存放在本域中。

扩展方法如下：HEX(2345ABCD) → “2345ABCD”

一般交易报文中MAC表示成ASCⅡ码是可见的字符（即“0”—“9”、“A”—“F”且“A”—“F”是大写），当交易报文被发送者发出之前，应由发送者产生MAC；接收者收到报文后，将重新计算MAC值，以鉴别报文在传送途中是否被篡改。

密钥分发时(重置密钥请求报文中)，128域的前32bit填入MAC的前32bit，128域的后32bit放入新密钥的checkvalue，是否需要验证checkvalue由入网机构自己选择。

注意事项：

a) CUPS 重置密钥的请求报文（0800）和应答报文（0810）中产生 MAC 所使用的密钥是要重置的新密钥 PIK 或 MAK 的明文。

b) CUPS 重置密钥的请求报文（0800）的 128 域 MAC 的填写方法与其它报文的 MAC 域填写方法不同。其值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 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）。对 CUPS 重置密钥的应答报文（0810）的 128 域 MAC 的填写方法与正常报文的相同，但计算 MAC 使用的密钥为新密钥的明文。所以重置密钥请求报文中 MAC 用 ASCⅡ码表示时，可能有无法显示的字符。但有一点需要注意，由于有可能在重置 PIN 密钥时，新产生的 PIN 密钥是 128 字节的双倍长密钥，因此此时计算请求和应答报文中的 MAC 值都应采用双倍长密钥算法。同理，对于请求报文中包含的 CheckValue 值也采用双倍长密钥算法计算。

c) 差错处理通知和收付费通知的 MAC 报文域的选择方式与 POS 交易类报文的 MAC 报文域的选择方式相同。

参考文献

[1] VISA 国际信用卡公司：《V.I.P. System Documentation INT'L》

[2] VISA国际信用卡公司：《Visa Smart Debit/Visa Smart Credit System Technical Manual》，2001.4

[3] MASTERCARD国际信用卡公司：《Member Publication》，2002.6

[4] ISO 8583 Financial transaction card originated messages-Interchange message specifications(5First edition 2003-06-15)

[5] 中国银联股份有限公司：《中国银联信息交换处理中心系统业务需求》2004.1

[6] 银行卡信息交换总中心：《技术业务文档汇编》，1999.8

[7] 全国银行卡办公室：《银行卡文件汇编》1993-1999， 2000.1

[8] 中国标准出版社：《信息系统安全技术国家标准汇编》，2000.9