Q/CUP

中国银联股份有限公司企业标准

Q/CUP 006.4-2017

代替Q/CUP 006.4-2016

中国银联银行卡交换系统技术规范
第4部分 数据安全传输控制规范

Technical Specifications on Bankcard Interoperability
Part 4 Specification on Data Secure Transmission Control

版本号： 2017.A

2017-06-30 发布 2017-10-30 实施

中国银联股份有限公司 发布

知识产权声明

中国银联股份有限公司（以下简称“中国银联”）对该规范文档保留全部知识产权权利，包括但不限于版权、专利、商标、商业秘密等。任何人对该规范文档的任何使用都要受限于在中国银联成员机构服务平台（http://member.unionpay.com/）与中国银联签署的协议之规定。中国银联不对该规范文档的错误或疏漏以及由此导致的任何损失负任何责任。中国银联针对该规范文档放弃所有明示或暗示的保证,包括但不限于不侵犯第三方知识产权。

未经中国银联书面同意，您不得将该规范文档用于与中国银联合作事项之外的用途和目的。未经中国银联书面同意，不得下载、转发、公开或以其它任何形式向第三方提供该规范文档。如果您通过非法渠道获得该规范文档，请立即删除，并通过合法渠道向中国银联申请。

中国银联对该规范文档或与其相关的文档是否涉及第三方的知识产权（如加密算法可能在某些国家受专利保护）不做任何声明和担保，中国银联对于该规范文档的使用是否侵犯第三方权利不承担任何责任，包括但不限于对该规范文档的部分或全部使用。

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。

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、鲁志军、宋汉石、李伟、郭锐、郑澎、徐静雯、李洁、吴金坛、王力斌、苗恒轩、万高峰、陆尔东、蒋慧科、杜秉一、赵伟、洪隽、白玫、陈旭、勾传龙。

变更清单

序号	变更章节号	变更内容	变更原因	系统改造影响性分析（仅供机构参考）	变更人员	变更时间
1.						

中国银联银行卡交换系统技术规范
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 密钥管理与控制

2.1 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。

2.1.1 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。

2.1.2 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。

2.1.3 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 DES 中使用）和双倍长（b128，在双倍长密钥算法 3DES 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。

支持SM算法的还应满足以下要求：

f)支持SM4算法（密钥长度 b128）。

g)支持SM3算法（输出长度256位），用于计算ARQC中的哈希结果数据元。

h)支持在加密机内实现PIN密文的SM4算法与3DES算法之间的转换。例如受理机构用3DES 密钥算法对上送CUPS的PIN加密，CUPS收到报文后用与受理机构约定的3DES密钥解密，再用与发卡机构约定的SM4算法密钥对PIN加密，最后将报文发送至发卡行，由发卡行用SM4算法密钥解密后决定是否对交易授权。

2.1.4 数据加密传输环境的基本要求

交易数据由入网机构进入CUPS前应已经过加密处理，如PIN加密和MAC加密。入网机构从CUPS中得到的交易数据也应进行加密处理，如PIN加密和MAC加密。

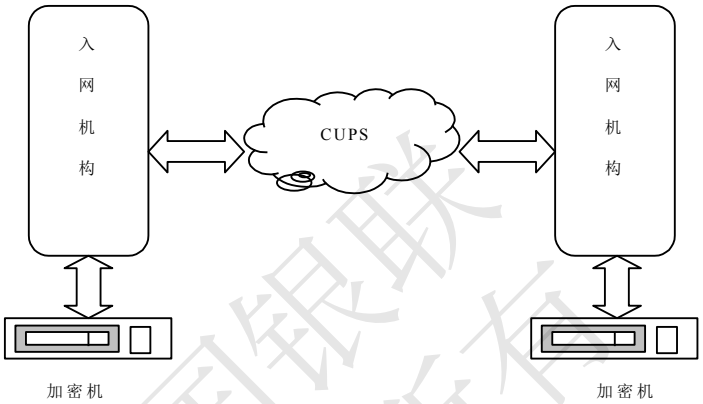


图1 数据加密传输环境

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。

2.2 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（3DES）和 128bit（SM4）	硬件设备保护
2	成员主密钥	MMK	2	人工输入或加密机随机生成	数据密钥	硬件加密机和主机	128bit（3DES）和 128bit（SM4）	从硬件加密机输出时用主密钥加密
3	数据密钥（例如，PIN密钥和MAC密钥）	data key（PIN密钥为PIK，	3	硬件加密机产生	PIN	主机	64bit/128bit（3DES）和128bit(SM4)	用成员主密钥加密

		MAC 密钥为 MAK）						

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。

2.3 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；或由 CUPS 在加密机中随机生成并散列出 2 个分量；或由双方商定该密钥的产生办法
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

2.3.1 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CUPS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CUPS发出申请重置密钥报文。

2.3.2 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。

或由CUPS在加密机中随机生成并散列出2个分量。

也可由双方商定MMK的产生办法。

2.3.3 主密钥的产生

主密钥用人工方式输入。当使用DES/3DES算法时，主密钥由三部分构成，分别由三个人掌管；当使用SM4算法时，主密钥由两部分构成，分别由两个人掌管。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。在每人分别输入密钥后，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。

2.4 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 卡传递或保密信封传递；或需双方相关人员到场共同输入；或由双方相关人员协商确认分发途径
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

2.4.1 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。

2.4.2 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，则通过保密信封传递或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。

2.5 密钥的存储

2.5.1 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。如果出现在硬件加密机外，则必须密文方式出现。

2.5.2 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。

2.5.3 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。

2.6 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。

3 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。基于DES/3DES算法的PIN、MAC长度为8字节；基于SM4算法的PIN为16字节，MAC长度为8字节。

3.1 PIN 的加密和解密

当报文经发送方进入银行卡网络时，持卡人的个人标识码(PIN)已经用发送方的PIK加密。CUPS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。

在使用DES/3DES算法时，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

在使用SM4算法时，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。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	F	F	F	F	F	F	F	F	F	F	F	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

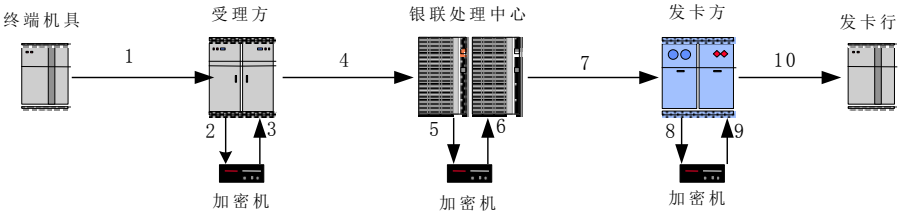
注 4：P/F－4-bit 二进制 PIN 的数码 / FILLER

注 5：4-bit %B1111（FILLER）

图3　SM4 算法的 PIN 数据块格式

典型的 PIN 加密解密过程如图4　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4　PIN 的加密解密过程

3.1.1　PIN 的长度

PIN的长度为4-12位数字。

3.1.2　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

3.1.3　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，PIN的格式必须在报文的域53（Security Related Control Information）中标明。

3.1.3.1　DES/3DES 算法 PINBLOCK 示例

——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	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：

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（报文第2域）。基于Token的支付交易，对于受理机构，Token号为主账号，对于发卡机构，真实卡号为主账号。。

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

3.1.3.2 SM4 算法 PINBLOCK 示例

——ANSI X9.8 格式（不带主账号信息）

表8 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	15BYTE	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 0xFF 0xFF 0xFF 0xFF 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（报文第2域）。基于Token的支付交易，对于受理机构，Token号为主账号，对于发卡机构，真实卡号为主账号。

其中，PIN格式如下表所示：

表9 PIN 格式

位置	长度	说明
1	1 BYTE	PIN 长度
2	15 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10 PAN 格式

位置	长度	说明
1	2 BYTE	%H0000
3	14BYTE	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 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67

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

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

结果为：0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0x98 0x76 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 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x45 0x67 0x89 0x01 0x23 0x45

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

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

结果为：0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xBA 0x98 0x76 0xFE 0xDC 0xBA

3.1.4 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用双倍长密钥3DES算法或SM4算法计算，即可得到PIN的密文。

3.1.5 PIN 异常的处理

参见《交易处理说明》中第8章交易的异常处理流程。

3.2 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》。

3.2.1 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”，参见本规范《附录》部分A.2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。

3.2.2 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）

3.2.2.1 消息类型为 01xx、02xx、04xx 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11 消息类型为 01xx、02xx、04xx 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]
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）

[b] Primary-account-number：主账号，内容为两位的主账号长度+主账号。基于 Token 的支付交易，对于受理机构，Token 号为主账号，对于发卡机构，真实卡号为主账号。

[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

3.2.2.2 转账类交易的报文域选择

转账类交易的范围如下：

1、 传统意义上的转账交易，含转账、转出转账、转入转账、转出冲正、转入确认；

2、 基于UICS借贷记标准的电子现金应用的IC卡非指定账户圈存交易，含转账圈存、转出圈存、转入圈存、转出圈存冲正、非指定账户圈存冲正。

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12 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 [e]
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]

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

[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

[e] Primary-account-number：主账号，内容为两位的主账号长度+主账号。基于 Token 的支付交易，对于受理机构，Token 号为主账号，对于发卡机构，真实卡号为主账号。

3.2.2.3 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13 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：

1600000000000000 —— 重置 PIN 密钥 PIK（3DES 算法）

2000000000000000 —— 重置 MAC 密钥 MAK（DES 算法）

1400000000000000 —— 重置 PIN 密钥 PIK（SM4 算法）

2400000000000000 —— 重置 MAC 密钥 MAK（SM4 算法）

[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

3.2.3 MAC 域的构成规则

3.2.3.1 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。

3.2.3.2 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)。

DES算法构成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。

SM4算法构成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。

3.2.4 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。

3.2.4.1 硬件加密机通过 MAB 计算 MAC 的方法

3.2.4.1.1 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。

示例：

假设 MAB 可分为四组：A1、A2、A3、A4，单倍长密钥算法运算过程如下：

用 MAK 对 A1 进行单倍长密钥运算，得到结果 B1；

B1 与 A2 异或，用 MAK 对异或结果进行单倍长密钥运算，得到结果 B2；

B2 与 A3 异或，用 MAK 对异或结果进行单倍长密钥运算，得到结果 B3；

B3 与 A4 异或，用 MAK 对异或结果进行单倍长密钥运算，得到最终 8 个字节的加密值。

3.2.4.1.2 双倍长密钥算法

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：

a) 进行双倍长密钥运算；

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。对最后一组进行双倍长密钥运算，得出 8 个字节的加密值。

示例：

假设 MAB 可分为四组：A1、A2、A3、A4，双倍长密钥算法运算过程如下：

用 PIK 对 A1 进行双倍长密钥运算，得到结果 B1；

B1 与 A2 异或，用 PIK 对异或结果进行双倍长密钥运算，得到结果 B2；

B2 与 A3 异或，用 PIK 对异或结果进行双倍长密钥运算，得到结果 B3；

B3 与 A4 异或，用 PIK 对异或结果进行双倍长密钥运算，得到最终 8 个字节的加密值。

3.2.4.1.3 SM4 算法

将MAB中的每16个字节分为一组（最后一组如不足16个字节，则右补0X00），用MAK或PIK作为SM4密钥运算依次进行如下操作：

a) 进行 SM4 加密运算；

b) 将运算结果与后一组16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SM4密钥运算，得出16个字节的加密值。

3.2.4.2 联机报文 MAC 域的取值

3.2.4.2.1 普通交易

使用DES算法时，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）。

使用SM4算法时，MAC域（128域）为按照SM4算法用MAK计算MAC得到的16字节二进制数据的前4个字节二进制数，表示成16进制字符串形式（8个16进制字符）。

3.2.4.2.2 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MAC密钥时用新下发的MAC密钥作为密钥计算MAC；切换PIN密钥时用新下发的PIN密钥作为密钥计算MAC。

3.2.4.2.2.1 请求报文中的 MAC 计算方法

DES/3DES算法的请求报文MAC计算方法：

请求报文中的MAC域（128域）为按照单倍长密钥算法（针对重置MAK）或双倍长密钥算法（针对重置PIK）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（针对重

置MAK）或双倍长密钥算法（针对重置PIK）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）。

SM4算法的请求报文MAC计算方法：

请求报文中的MAC域（128域）为按照SM4算法使用MAK（针对重置MAK）或PIK（针对重置PIK）计算MAC得到的16字节二进制数据的前4字节二进制数和按照SM4算法计算CheckValue得到的16字节二进制数据的前4字节二进制数的组合（8字节二进制数）。

3.2.4.2.2.2 应答报文中的 MAC 计算方法

如果重置的是MAK，那么应答报文的MAC计算方法同3.2.4.1.1 节，不需计算CheckValue，但其使用的密钥仍为新下发的密钥。

如果重置的是PIK，那么应答报文的MAC计算方法同0节，也不需计算CheckValue，也需使用新下发的密码。

3.2.4.2.2.3 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作单倍长密钥运算（针对重置MAK）或双倍长密钥运算（针对重置PIK）。

SM4算法计算CheckValue的方法为用新密钥对16个字节的二进制0作SM4运算。

3.2.4.2.2.4 重置 PIK 交易的 MAC 计算方法

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（3DES算法和SM4算法），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或SM4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或SM4算法计算。这里计算MAC和CheckValue的流程与0节中的描述一致，即先进行双倍长密钥运算或SM4算法运算，然后将运算结果与后一组8个字节（SM4算法位16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。

3.2.5 MAC 错误异常处理

参见《中国银联银行卡交换系统技术规范》第一部分《交易处理说明》中第8章交易的异常处理流程。

3.3 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、700）和文件尾（010、710）的文件，如双信息文件、风险信息共享文件、IC卡脱机交易文件、批量交易文件等，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。

3.3.1 MAC KEY 和 MAC 的字符组成

DES/3DES算法的格式要求：

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。

SM4算法的格式要求：

文件尾中有 MAC KEY 和 MAC 两个字段，每个字段都是由32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16个字节的 MAC 密钥和16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。

3.3.2 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。基于SM4算法的MAC KEY无须满足奇校验。

3.3.3 MAC 块（MAB）的构成

将文件中的每条记录（含文件头记录和文件尾记录，但不含MAC KEY和MAC）以256字节为一组分组，每条记录结尾不满256字节补二进制0；把各分组依次按位异或，最后得到一个256字节的数据块，即为顺序文件MAC块。

3.3.4 MAC 的计算

MAC 分成左右两部分，生成方法如下：

DES算法：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。

SM4算法：前128字节按照SM4算法计算MAC，取结果的前半部分（8字节二进制数据），将其表示成16进制字符串形式（16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SM4算法计算MAC，取结果的前半部分（8字节二进制数据），将其表示成16进制字符串形式（16个16进制字符），即为文件MAC字段的后半部分。

3.3.5 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《中国银联银行卡交换系统技术规范》第三部分《文件接口规范》中的5.4常用记录格式约定。

3.4 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	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

3.4.1 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。

3.4.2 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。

3.4.3 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

3.4.4　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双倍长PIK用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）互联网支付密码应采用双倍长密钥算法。

3.4.5　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。

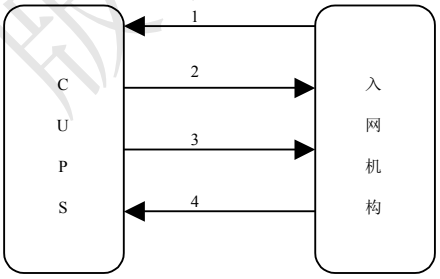
4　新旧密钥切换

4.1　入网机构发起的申请重置密钥

4.1.1　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）

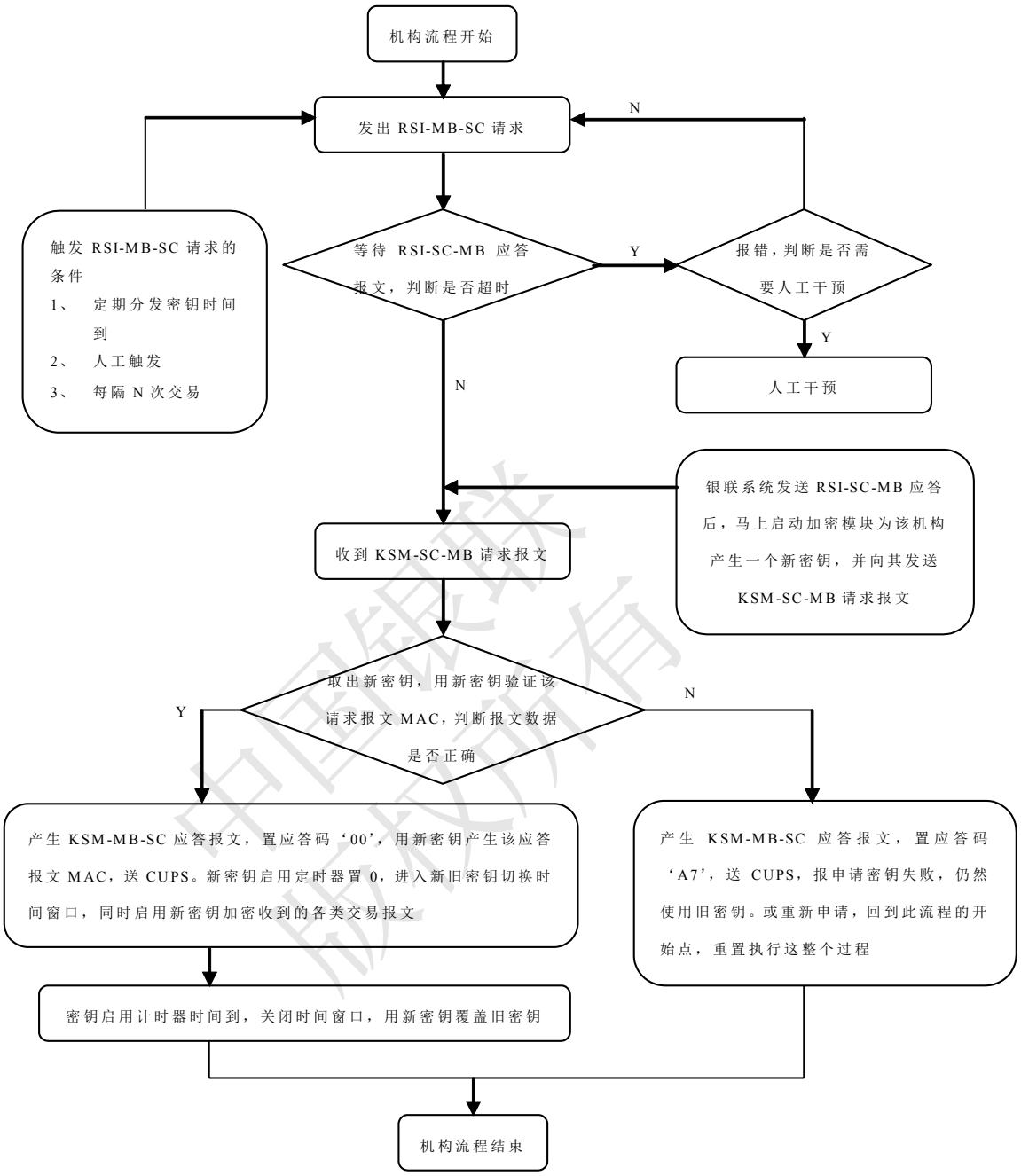
2—CUPS 发往入网机构的应答（0830）

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

4.1.2　流程图



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

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

注 3：KSM-SC-MB：CUPS 发往入网机构的重置密钥请求报文（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

4.1.3　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。请求报文的MAC算法参见3.2.4.2.2.1　节。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。应答报文的MAC算法参见3.2.4.2.2.2　节。

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。在时间窗口之内，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，机构应考虑再次尝试重置密钥，如果仍然失败，则应考虑与银联进行手工密钥重置的应急手段（电话联系银联运维人员）。事后，机构应检查自己的加解密程序是否有问题，并联系银联获取帮助。在时间窗口限定时间结束后，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）申请重置密钥结束。

如果在时间窗口结束以后，机构仍然发现使用新密钥进行的加解密操作出错，应进行人工干预，尽快联系银联工作人员，检查问题所在。

4.1.4　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 4　SM4 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

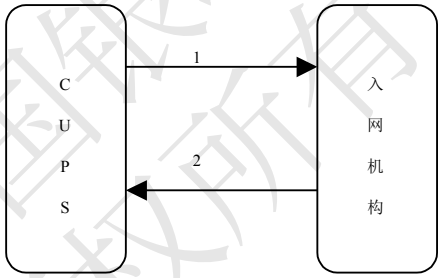
位	域 名	动 作
53	SECURITY-RELATED-CONTROL-INFORMATION	第 1 位：密钥类型(最左) 1 PIK 2 MAK 第 2 位：加密算法类型 0 单倍长密钥算法 6 双倍长密钥算法 4 SM4 密钥算法 第 3 位－第 16 位：保留，暂填零。
70	NETWORK-MANAGEMENT-INFORMATION-CODE	值“101”

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发出申请重置密钥的请求。 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。

4.2 CUPS 发起的重置密钥

4.2.1 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。

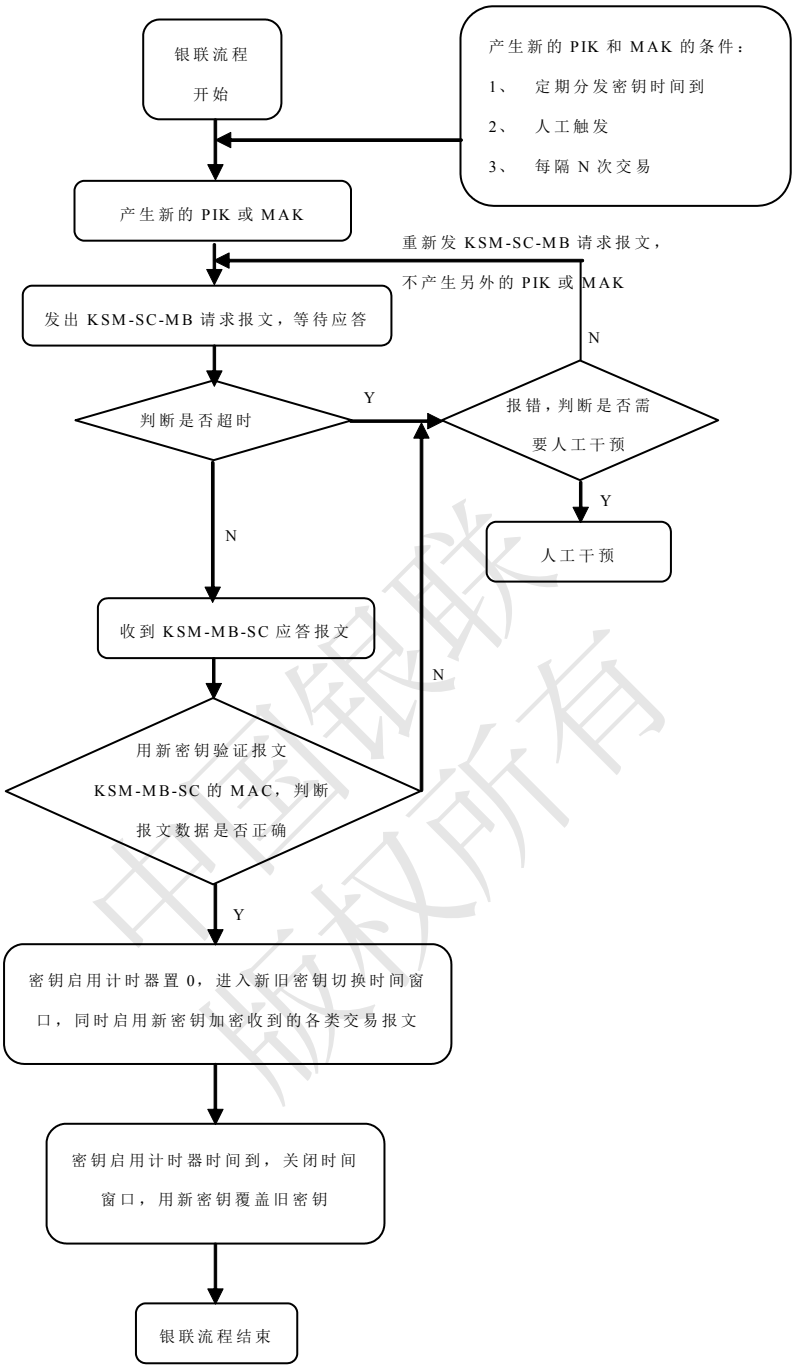


1—CUPS 发往入网机构的重置密钥请求（0800）（简记为 KSM－SC－MB）

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

4.2.2 流程图



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

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

注 3：KSM-SC-MB：CUPS 发往入网机构的重置密钥请求报文（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

4.2.3 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，则直接请求人工干预处理。

CUPS收到入网机构成功的重置密钥应答报文(KSM-MB-SC)后，CUPS必须用新密钥验证MAC，应答报文的MAC算法参见3.2.4.2.2.2　节。在MAC验证成功以后，CUPS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。如果MAC验证不成功，CUPS应采用人工干预，主动联系机构并提供尽可能的帮助和建议。

新旧密钥的切换窗口为3分钟，此时新旧密钥共存。在时间窗口之内，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，CUPS应主动联系机构并提供尽可能的帮助和建议。在时间窗口限定时间结束后，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。

如果在时间窗口结束以后，CUPS仍然发现使用新密钥进行的加解密操作出错，应进行人工干预，尽快联系机构工作人员，检查问题所在。

4.2.4　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 4　　SM4 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 4 SM4 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

特别说明:对于CUPS发起的重置密钥交易本身，在计算报文MAC时采取的算法应与所重置的密钥类型对应的加密算法类型相同。例如，机构PIN加密采用SM4算法，则重置PIK交易报文MAC计算也选择SM4算法；机构MAC算法为DES算法，则重置MAK交易报文MAC计算也采用DES算法。

4.3 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解密是在收到 KSM-SC-MB（重置密钥请求报文，0800），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KSM-MB-SC（重置密钥应答报文，0810）中的MAC值。CUPS用新密钥加解密是在收到并成功验证入网机构KSM-MB-SC（重置密钥应答报文，0810） 的MAC值之后。所以入网机构在CUPS之前启用新密钥，这里面就存在一个时间差。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，这个时间被称为“新旧密钥切换时间窗口”。考虑到网络的延迟和抖动，本规范将这个窗口时间定为3分钟。

3分种之内，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。

重置密钥事件的时间和事件图示：

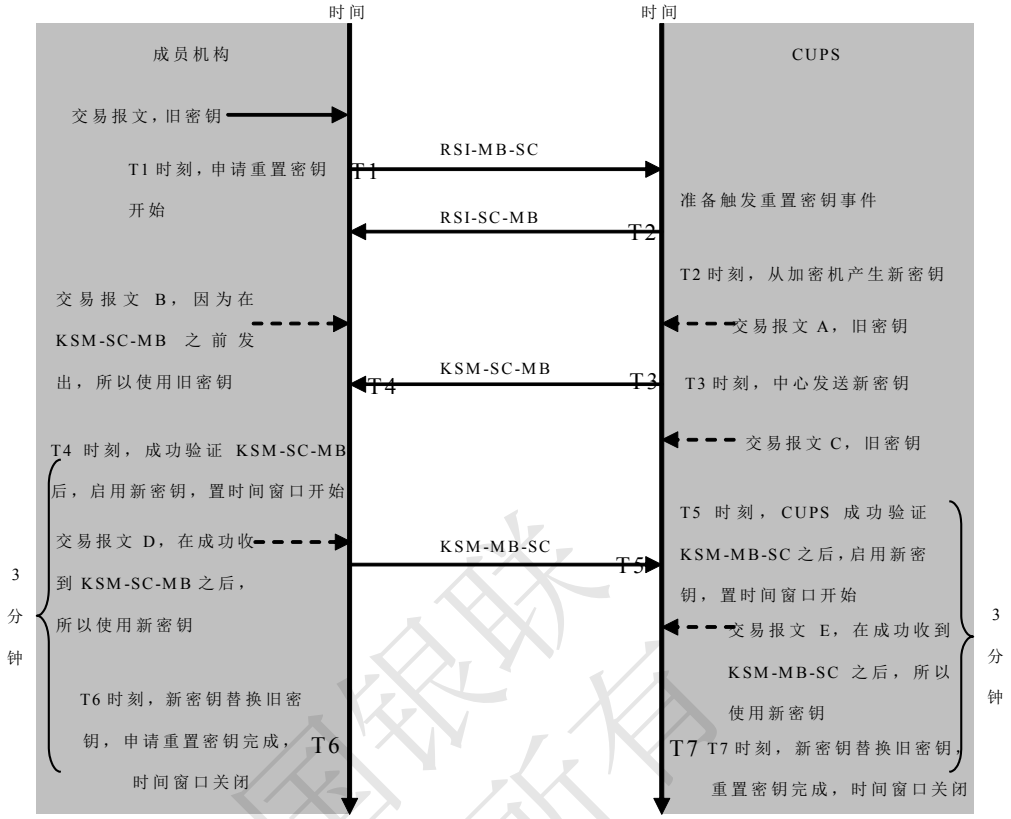


图10　重置密钥事件的时间和事件图

5　UICS 借/贷记标准 IC 卡安全说明

5.1　UICS 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。

5.2　基于 3DES 的 ARQC 的生成算法

5.2.1　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。

5.2.2　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，但在需要银联处理中心代为校验 ARQC 时，需将数据源通知银联处理中心。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：

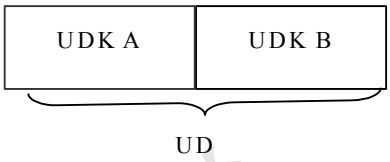


图11 密钥分散算法（MDK 生成 UDK）

5.2.3 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：

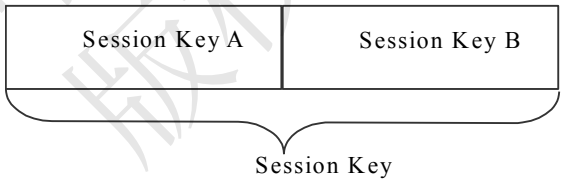


图12 双倍长密钥（Session Key）分散算法

计算得到的过程密钥必须满足奇校验要求。

5.2.4 计算 ARQC

5.2.4.1 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

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
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）			√	82
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：

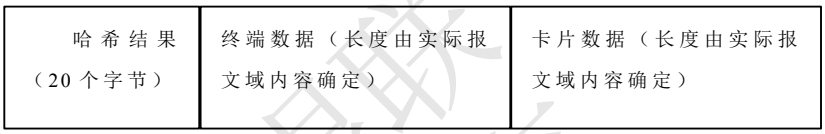


图13 ARQC的数据源排列方式图

5.2.4.2 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) 将过程密钥（128bit）分为左半部分密钥 SKL（64bit）和右半部分密钥 SKR（64bit），依次对数据块进行如下操作：

1) 用 SKL 对补位好的数据块做单 DES CBC 加密（初始向量为 8 字节 0x00），得到结果 MAB（8 字节）；

2) 用 SKR 对 MAB 做单 DES ECB 解密，得到结果 MAB_C；

3）用 SKL 对 MAB_C 做单 DES ECB 加密，得到 8 字节的 ARQC 值。

5.2.4.3 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。

此处描述的“数字格式(n)”的定义与《中国银联IC卡技术规范》中属性n定义保持一致。

5.2.5 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。

5.3 基于 SM4 的 ARQC 生成算法

5.3.1 ARQC 生成算法

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。

5.3.2 密钥分散算法

IC卡的密钥是由发卡方发卡根密钥发散而来，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。

基于SM4密钥算法的密钥分散算法（MDK生成UDK）：

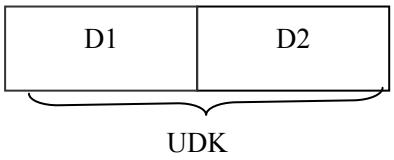
a）约定参与分散算法的数据。由于 UDK 针对每一卡片唯一，所以需要通过每张卡片独有的数据分散得到，例如卡号、卡片序列号、地区代码等。该数据源将由发卡方自行决定，但在需要银联处理中心代为校验 ARQC 时，需将数据源通知银联处理中心。计算 UDK 的数据源共计 8 字节，并规定发卡行参与分散算法的数据不超过 5 个。

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 D2 紧邻 D1 排列，即可得到 UDK，使用 MDK 密钥采用 SM4 密钥算法计算得到 16 字节 UDK ；



5.3.3 生成 Session Key

SM4密钥分散算法生成Session Key:

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个字节记为数据源Data A1；

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个字节记为数据源Data A2；

d)将Data A2紧邻Data A1排列，得到数据源Data A，用UDK对该数据进行SM4密钥运算产生过程密钥的16个字节Session Key；

5.3.4 计算 ARQC

5.3.4.1 数据源

数据源方面SM4算法与3DES算法要求相同。

计算ARQC的数据源排列方式如下图所示：

哈希结果（20个字节）	终端数据（长度由实际报文域内容确定）	卡片数据（长度由实际报文域内容确定）

图14 ARQC的数据源排列方式图

其中对于终端域的哈希结果采用SM3算法计算获得，共32个字节，截取32个字节前面20字节作为杂凑结果。该杂凑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。

5.3.4.2 计算 ARQC 的步骤

SM4算法计算ARQC

a) 将上述数据块分成16字节一组：D1，D2，D3…；

b) 如果最后一块数据块的长度为16字节，则后面再补一个16字节数据块，该数据块由如下数据构成：0x80 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00。 如果最后一块数据块的长度小于16字节，则需要将该数据块补满到16字节。若该数据块为15字节，则后面补一个字节0x80；如果该数据块为14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16字节，补0x00直到16字节；

c) 过程密钥作为SM4密钥依次对每一组进行如下操作：

1) 进行SM4密钥运算

2) 将运算结果与后一组的16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SM4密钥运算，得出16个字节的加密值HK。

d) 取16字节的HK的左边8字节，作为8字节ARQC。

5.3.4.3 计算终端域杂凑结果的数据域组成

计算终端域杂凑或SM3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。

5.3.5 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) SM4 算法模式：上述异或的结果是一个 8 字节的数据块 D1，将数据块 D1 扩充成 16 字节，不足 16 字节的右边补 0x00,对 D1 用过程密钥采用 SM4 密钥计算得到 16 个字节的 H_K。取 16 字节的 H_K 的左边 8 字节 H_{KL}，作为 8 字节 ARPC。

附 录 A
（规范性附录）
PVN、CVN 计算

本节基于《中国银联 PIN 校验码(PVN)算法标准》编制。

基于 3DES 算法的 PVN 算法，PVK 分为 KeyA、KeyB 两部分，各 64 位，数据块为 64 位；基于 SM4 算法的 PVN 算法，PVK 为 128 位，数据块为 128 位。

基于 3DES 算法的 CVN 算法，CVK 分为 KeyA、KeyB 两部分，各 64 位，数据块为 64 位；基于 SM4 算法的 CVN 算法，CVK 为 128 位，数据块为 128 位。

本节不再定义基于 3DES 算法的内容，仅对基于 SM4 算法的内容进行说明。

A.1 基于SM4 算法的PVN算法

A.1.1 PVN计算数据源

计算 PVN 的数据源包括：

——主账号（PAN）右端除校验位以外的 11 位数字

——Key，128 位的 SM4 的 PVK

——PVK 索引号，取值为 1-F（0 为保留）

——持卡人 PIN 最左的 4 位数字

PVK 是一组银联与代授权机构之间约定的 128 位的密钥，最多可 15 个，该组密钥专为代授权交易计算和验证 PVN 使用，该组密钥的索引号为 1—F（0 为保留），可分别用不同的密钥对不同的卡号或卡号段进行 PVN 计算。在机构向银联提交/导入代授权信息文件时，应包含索引信息，以便银联用 PVK 索引号指定的 128 位长的密钥进行 PVN 验证。

A.1.2 PVN算法

计算 PVN 时使用 KeyA 和 KeyB。计算步骤如下：

（1）取 PVK 索引号约定的某个 128 位长的 SM4 密钥 PVK。

（2）取主账号右端除校验位以外的 11 位数字、密钥 PVK 的索引号、PIN 明文左端 4 位数字，依次构成一个 32 位数字串，不足 32 位数右补 0,每位数字用压缩 BCD 码表示，形成 1 个 128 位长的二进制计算块 Block。

（3）将 Block 与 PVK 作为明文和密钥输入，进行 SM4 运算，得出密文 BlockE

（4）对 BlockE 从左到右抽取出所有的数字(0～9)。

（5)对 BlockE 从左到右抽取出所有的十六进制字符(A～F),并对每一个十六进制字符减十进制 10,使之变为数字。

（6)将步骤 4 和 5 得出的数字依次从左至右排列,步骤 5 得出的数字放在步骤 4 得出的数字之后。

（7）取步骤 6 结果的前 4 位数字，即为 PVN 值。

示例：

（注：以下数据实际运算中无需空格）

主账号 PAN= 6228 8888 8888 888 X （X 为校验位）

密钥索引号 I= 3

密钥 PVK= 0123 4567 89AB CDEF FEDC BA98 7654 3210

PIN=123456

步骤 1：

密钥 PVK= 0123 4567 89AB CDEF FEDC BA98 7654 3210

步骤 2：

Block=88888888888 3 1234 0000000000000000

步骤 3：

BlockE=SM4(Encrypt,Block,Key)= 351A2460F1D53087C26F19A03D4191DB

步骤 4：

抽取 BlockE 中的数字=35124601530872619034191

步骤 5：

抽取 BlockE 中的十六进制字符（AFDCFADDB），并作数值化处理=053250331

步骤 6：

组合步骤 5 和步骤 6=351246015308726190341910532503 31

步骤 7：

取步骤 6 前 4 位数字作为 PVN=3512

A.2 基于SM4 的CVN算法

计算 CVN 时使用 128 位 SM4 的密钥 Key。

A.2.1 CVN数据源

计算 CVN 的数据源包括：

主账号（PAN）、卡失效期和服务代码，从左至右顺序编排。

例如 19 位 PAN、4 位卡失效期和 3 位服务代码组成 26 个字符 CVN 数据源。

A.2.2 CVN算法

将 CVN 数据源扩展成 128 位二进制数据块 Block（不足 128 位右补二进制 0）。

使用 Key 对 Block 进行 SM4 加密获得密文 BlockE。

从左至右将加密结果 BlockE 中的数字（0－9）抽出，组成一组数字。

从左至右将加密结果 BlockE 中的字符（A－F）抽出，减 10 后将余数组成一组数字，排列在步骤（3）的数字之后。

步骤（4）的左边第一组三位数即为 CVN 值。

例：

（以下数据实际运算中没有空格）

主 账 号：4123 4567 8901 2345

有 效 期：8701

服务代码：111

Key: 0123 4567 89AB CDEF FEDC BA98 7654 3210

第一步：数据源为 4123456789012345 8701 111

第二步：扩展为 Block:4123 4567 8901 2345 8701 1110 0000 0000

第三步：用 Key 对 Block 进行 SM4 加密得到密文 BlockE: EB14 9BE0 D9E5 3794 40A3 1298 A2C5 E7C2；

第四步：抽出结果 BlockE 中的数字：149095379440312982572

第五步：抽出结果 BlockE 中的字符: EBBEDEAACEC，减 10 后获得数字结果：41143400242。

第六步：将第五步结果连接到第四步的结果之后：14909537944031298257241143400242

第七步：取第六步最左边三位数就是 CVN：149。

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