Technical Specifications on Bankcard Interoperability (Version 2.0)

Part IV Data Secure Transmission Control

April 2010

THIS PAGE INTENTIONALLY LEFT BLANK.

Table of Contents

Using this Document

Purpose

This *Part IV Specification on Data Secure Transmission Control* is one of the six parts comprising the *Technical Specifications on Bankcard Interoperability*. The document specifies the requirements on the secure transmission of data information, including data secure transmission, key management and encryption algorithm.

Audience

The audience of this manual are the staff from China Unionpay (hereinafter referred to as CUP) and CUP Network Participants.

Time Expressed

CUP has operation centers in several locations including Shanghai, Beijing and Hong Kong. For operational purpose, the time frame in this manual, unless particularly indicated, refers to “Beijing time”.

Coordinated Universal Time (UTC) is the basic measuring time throughout the world. Beijing time is 8 hours ahead of UTC. Also, there is no Daylight Saving Time in China.

Unless otherwise specified, the Day in this Volume refers to the calendar day and the Business Day refers to the working day subject to local regulations of the country where the processing Participant is located.

Replacement

The April 2010 version replaces your existing document.

Revisions

CUP will periodically issue revisions to this document as enhancements and changes are implemented, or as corrections are required. Occasionally, revisions or additions to this document will be published in an Operations Bulletin.

Please refer to the Summary of Revisions for changes reflected in this version.

Support

Please address your questions to the service teams as follows:

- For questions related to this manual:

Fax: (86-21) 5036-2339

E-mail: publications_intl@chinaunionpay.com

- For questions related to data secure transmission control:

Fax:	(86-21) 5036-2339
E-mail:	support_intl@chinaunionpay.com

Summary of Revisions

The change listed below is associated with the **April 2010** version.

Description of Change	**Where to look**
Added-File encryption and decryption in flow transmission mode is added.	Section 5.5
Added-That MAC calculation when double-length PIN key is reset is added.	Section 5.2.4.2.3
Revised-MAC calculation through MAB by HSM (DES) is further clarified.	Section 5.2.4.1
Revised-Key reset transaction is further clarified.	Section 5.2.4.2.2
Revised-Figure 6 Flow of Key Exchange Request by a Participant is revised.	Section 6.1.2
Revised-Figure 8 Flow of Key Reset initiated by CUP is revised.	Section 6.2.2
Revised-Switching between new key and old key is further clarified.	Section 6.3
Revised-Figure 9 Key Reset Time and Event is revised.	Section 6.3
Deleted-The content of Data Fields for Transfer Transaction Message (Participants in Mainland of China use only).	
Deleted-The content of Data Fields for Reconciliation Transaction Message (Participants in Mainland of China use only).	
Deleted-The content of Encryption/Decryption of PAN in VIP File (Participants in Mainland of China use only).	

THIS PAGE INTENTIONALLY LEFT BLANK.

1 Application Scope

This Specification applies to all CUP Network Participants.

The document specifies the requirements on the secure transmission of data information, including data secure transmission, key management and encryption algorithm.

THIS PAGE INTENTIONALLY LEFT BLANK.

2 References

The terms and conditions of the following documents quoted by this Specification have become the terms and conditions of the Specification. The modification list (excluding corrected contents) or revised edition attached to the dated documents shall not apply to this Specification. However, Participants may study whether to apply the latest versions of such documents. The latest versions of non-dated documents shall apply to the Specification.

• GB/T 2260	Codes of the Administrative Regions of PRC
• GB/T 2659-94	Codes of the Countries and Regions
• GB/T 4754-94	Category and Codes of National Economic Sectors
• GB/T 12406-94	Codes of Currencies and Funds
• GB 13497-92	Codes of National Clearing Centers
• *GB/T 15150-94*	Bankcard Originating A Message-Specifications on Message Exchange-Content of a Financial Transaction（ISO8583-1987）
• *JR/T 0025-2005*	Regulations on China Finance IC Card
• *National Bankcard Office*	Technical Specifications on Bankcard Interoperability V1.0, January 2001
• *National Bankcard Office*	Business Specifications on Bankcard Interoperability, January 2001
• *CUP*	Volume II Business Rules September 2004
• *EMV2000*	Integrated Circuit Card Specification for Payment Systems: Book 1 ~ Book 4

THIS PAGE INTENTIONALLY LEFT BLANK.

3 Terms and Definitions

The following terms and definitions are applied to this Specification.

PIN (Personal Identification Number)

PIN refers to the personal password, which is the data information identifying the authenticity of the cardholder identity for an online transaction, and shall not be presented in plaintext in any computer and network system.

PIN Block

Formatted PIN block.

MAC (Message Authentication Code)

Message authentication code is the data to authenticate the correctness of message source.

MMK (Member Master Key)

Member master key is a key encryption key which is used to encrypt MAK and PIK, and protected by master key (MK).

MAK (MAC Key)

MAC key is a key used to generate message authentication code (MAC) data.

PIK (PIN key)

PIN key is a key used to encrypt PIN.

Data key

Data key is a key used to encrypt PIN and calculate MAC; including MAC key (MAK) and PIN key (PIK), also to be referred to as working key.

HSM (Hardware Security Module)

Hardware security module is the periphery hardware equipment used for PIN encryption and decryption, MAC calculation and validation, and key storage.

THIS PAGE INTENTIONALLY LEFT BLANK.

4 Key Management and Control

4.1 Security Management

A Participant must comply with the requirements for Data Secure Transmission Control of CUP Network.

When participants establish connectivity with CUP network, a strict system security and secrecy mechanism is required to guarantee a safe, stable and reliable operation of system. The mechanism shall include the following items:

- Data Access Control
- Operation security of application systems
- Security of physical facilities that include computer rooms, equipments, communication networks and storage media etc.
- Security management policies

4.1.1 Management Policies

Data Security for the whole network shall demand not only technical support but also establishment and implementation of strict key management mechanism among CUP Participants in terms of business operation. The basic requirements are as follows:

- To adopt an encryption algorithm that is secure and reliable and generally accepted by bankcard information switch systems
- To preserve key and implement transaction information encryption/decryption in HSM
- To comply with national and international regulations on Data Security and Secrecy in Financial Industry
- To enhance personnel management
- To change key regularly

4.1.2 Data Transmission Security Control

The requirements for Data Transmission Security Control are composed of the following five aspects:

- Key management mechanism: adoption of strict and reliable key distribution procedures with technical methods.
- PIN encryption and conversion mechanism：PIN in plaintext is not allowed to appear in communication lines or manually operated storage media
- Adoption of MAC

- Adoption of HSM for all Participants
- Adoption of point-to-point data encryption/decryption network mechanism

4.1.3 Hardware Security Module (HSM)

HSM mainly performs functions including PIN encryption/decryption, MAC calculation and validation, and key storage. All operations shall be carried out in HSM to guarantee that the plaintext of key and PIN only appears in HSM and to prevent leakage. HSM shall pass the security certification by National Business Cryptogram Committee (In Mainland of China) or local security institution and get the permission to be applied to local financial institutions. In addition, the following requirements also need to be complied:

- Support key of both single length (B64, which is applicable to single DES) and double length (B128, which is applicable to triple DES)
- Validate and encrypt/decrypt PIN in accordance with the PIN requirements in this Specification
- Validate and generate MAC in accordance with the MAC requirements in this Specification
- Be capable of key validation
- Destroy the stored key automatically under illegal attack.

For CUP and Participants, HSM is required to be deployed together with hosts to encrypt the transmitted data.

Data encryption/decryption between CUP system and Participants' systems shall base on single length key algorithm.

4.1.4 Data Encryption and Transmission Environment

Message data shall be encrypted before transmitted to CUP system by Participants. Message data obtained by a Participant from CUP system should also be encrypted.

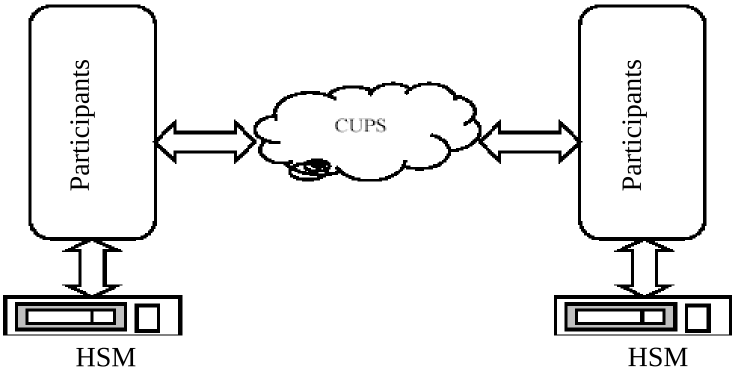


Figure 1 Data Encryption and Transmission Environment

HSMs both at CUP and Participants form a point-to-point data encryption/decryption network. CUP defines data keys with each Participant respectively.

4.2 Keys Introduction

Key is a critical data in the mechanism for data security and transmission. Keys of all levels, which are defined by CUP and Participants, shall be unique.

The structure, generation, encryption/decryption objectives, location, length and protection mode etc. for keys are specified as follows:

Table 1 Table of Keys in Different Levels

No.	Key Name	Abbr.	Level	Original Generation Method	Encryption/ Decryption Objective	Location	Length	Protection Mode
1	Master Key	MK	1	Manually Input	MMK	HSM; if out of HSM, each part of key be kept by different person	192 bit	Hardware
2	Member Master Key	MMK	2	Manually Input	DK	HSM and Host	128 bit/ 192 bit	Encrypted with MK when output from HSM
3	Data Key (e.g. PIN Key, MAC Key)	PIK	3	Generated by HSM	PIN	Host	64 bit/ 128 bit	Encrypted with MMK

The generation and input procedures of MK and MMK shall be regulated by relevant security policies.

4.3 Key Generation

Table 2 Key Generation

No.	Key Name	Generation
1	Master Key	Manually generated
2	Member Master Key	CUP and Participant each generate half of the key, which shall be compounded in HSM
3	PIN Key	Randomly generated in HSM and pass validity test
4	MAC Key	Randomly generated in HSM and pass validity test

4.3.1 Data Key (DK) Generation

Data Key includes PIK and MAK, which are randomly generated in HSM. HSM shall verify the validity of Data Key upon its generation. Weak key and semi-weak key shall be eliminated.

CUP's HSM generates the Data Key, which is received and stored by a Participant. CUP may initiate a key reset message to a Participant actively if necessary.

The Participant shall send key reset message to CUP if a new key is necessary.

4.3.2 Member Master Key (MMK) Generation

CUP and a Participant respectively generate half of MMK, which shall be input to HSM at both parties respectively and compounded in HSM.

CUP and a Participant may also negotiate the generation of MMK.

4.3.3 Master Key (MK) Generation

MK should be input into the HSM manually, which is composed of three parts that are controlled by three persons respectively. In guaranteeing correctness, each part of the key shall be input twice and these two inputs must be the same, otherwise it shall be regarded as input failure.

HSM will implement parity check after the three parts of key are input by the three persons respectively. If no error is found in parity check, then HSM generates a Master Key, which shall be stored and protected in HSM.

MK will be destroyed automatically in case of unauthorized operation to HSM.

4.4 Key Distribution

Table 3 Key Distribution

No.	Key Name	Key Distribution
1	Master Key	Self-generated, no distribution needed
2	Member Master Key	Delivered by IC card (not applicable to Participants outside Mainland of China) or manually input
3	PIN Key	Generated by CUP's HSM, distributed through online message
4	MAC Key	Generated by CUP's HSM, distributed through online message

4.4.1 Data Key (DK) Distribution

Data Key is generated by CUP's HSM and distributed through online message. For detailed information on distribution, please refer to *Section 6* of this Specification.

4.4.2 Member Master Key (MMK) Distribution

MMK can be distributed in three ways:

- Be obtained in IC card by mutual mail delivery if both CUP and Participants store MMK in IC card

- In case a party has no IC card or IC card cannot be used, relevant personnel from both parties shall input MMK jointly on site

- Relevant personnel from both parties negotiate the way of distribution.

4.5 Key Storage

4.5.1 Storage of Data Key (DK)/Member Master Key (MMK)

The Data Key and the Member Master Key shall be stored in HSM. The keys must be in cryptograph unless they are stored in HSM.

4.5.2 Master Key Storage

The Master Key shall be stored and protected in HSM.

4.5.3 Key Documents Keeping

Dedicated persons shall be responsible for key input, testing of key management function and key documents. The key documents shall be kept in a safe whose key shall be kept by dedicated personnel. Usage and destroy of key shall be under supervision with corresponding records.

4.6 Key Destroy

Upon generation of new key, the old ones shall be eliminated from database and memory to prevent replacement and re-usage; meanwhile, all information, which might be possibly used to regenerate the old key, must be eliminated. The records shall be updated which are related with the successful usage of new key and the automatic destroy of old key.

THIS PAGE INTENTIONALLY LEFT BLANK.

5 Data Encryption

To ensure the data secure transmission, two cryptographies, namely PIN encryption and MAC, are adopted in network messages

5.1 PIN Encryption and Decryption

PIN shall be encrypted with Sender's PIK when the message enters CUP system from Sender's system. PIN will be decrypted with Sender's PIK and encrypted with Reciever's PIK immediately by CUP system before the message is sent to Reciever's system.

PIN is formatted in 64-bit binary digit for encryption/decryption. The distributing of PIN plaintext in the 64-bit binary digit is known as PIN data block. For CUP and Participants, PIN data block shall be complied with *ISO 9564-1 Banking--Personal Identification Number Management and Security* with its format as follows.

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

Note 1: C- Control Code ％B0000

Note 2: N- PIN Length (4-bit)

Note 3: P- 4-bit binary PIN digit

Note 4: P/F- 4-bit binary PIN digit/FILLER

Note 5: F- 4-bit ％B1111 (FILLER)

Figure 2 Format of PIN Data Block

A typical process of PIN encryption/decryption is demonstrated in Figure 3. This process guarantees that the PIN plaintext only appears in terminals and HSM which are inaccessible.

Meanwhile, the Acquirer is responsible for the key management and definition of the PIN data format on the terminal side.

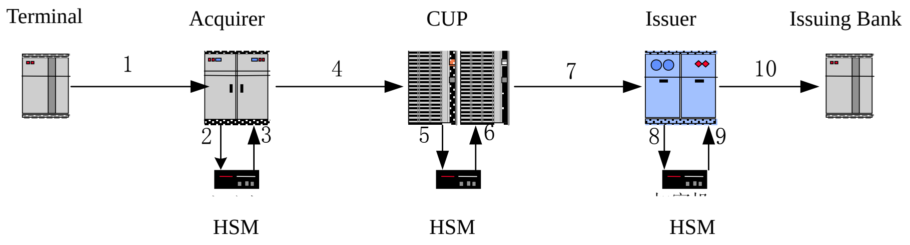


Figure 3 Process of PIN Encryption/Decryption

In Figure 3, the encryption/decryption process between terminal, Acquirer, CUP and Issuer is as follows:

- －1: Terminal sending out PIN cryptograph
- －2: Decryption by Acquirer with key defined by both Acquirer and terminal

- —3: Encryption by Acquirer with key defined by both Acquirer and CUP
- —4: Acquirer sending out PIN cryptograph
- —5: Decryption by CUP with key defined by both CUP and Acquirer
- —6: Encryption by CUP with key defined by both CUP and Issuer
- —7: CUP sending out PIN cryptograph
- —8: Decryption by Issuer with key defined by both Issuer and CUP
- —9: Encryption by Issuer with key defined by both Issuer and Issuing bank
- —10: Issuer sending out PIN cryptograph

5.1.1 PIN Length

PIN length is of 4-12 numeric digits.

5.1.2 PIN Character Set

PIN is denoted with numeric characters. The following table presents the binary code for PIN character set:

Table 4 Binary Code for PIN Character Set

PIN Character	Binary Code
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

The PIN Block format shall be complied with either of the two formats published in *ISO ANSI X9.8*. Acquirers outside Mainland of China may choose to support one of the followings. Issuers outside Mainland of China must support ANSI X9.8 (With PAN information).

Format 1—ANSI X9.8 (without PAN information)

Table 5 Table of ANSI X9.8 (without PAN Information)

Location	Length	Description

Location	Length	Description
1	1 Byte	PIN Length
2	7 Bytes	4-12 digit PIN (each digit expressed in 4 binary bits) and padding with hex F

Example 1:

PIN plaintext: 123456

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

Format 2－ANSIX9.8 (with PAN information)

PIN block is generated with PIN data block XOR PAN data block:

PIN data block is as follows：

Table 6 PIN Data Block

Location	Length	Description
1	1 BYTE	PIN Length
2	7 BYTE	4-12 digit PIN (each digit expressed in 4 binary bits) and padding with hex F

PAN data block is as follows：

Table 7 PAN Data Block

Location	Length	Description
1	2 Bytes	％H0000
3	6 Bytes	The last 12 digits of the PAN(excluding the check digit), 0 shall be padded to the left when PAN is less than 12 digits

Example 2:

PIN plaintext: 123456

PAN of magnetic stripe: 1234 5678 9012 3456 78

PAN intercepted: 6789 0123 4567

PAN data block: 0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67

PIN data block: 0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF

PIN block:

0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF

XOR

0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67

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

Example 3:

PIN plaintext: 123456

PAN of magnetic stripe: 1234 5678 9012 3456

PAN intercepted: 4567 8901 2345

PAN data block: 0x00 0x00 0x45 0x67 0x89 0x01 0x23 0x45

PIN data block: 0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF

PIN block:

0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF

XOR

0x00 0x00 0x45 0x67 0x89 0x01 0x23 0x45

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

PIN block format (Format 1 or Format 2) shall be indicated in Field 53 (Security Related Control Information) of the message.

5.1.4 PIN Encryption Method

PIN cryptograph can be generated by inputting the PIN BLOCK generated according to the above process into HSM, using double length key algorithm with the PIK stored in HSM. For Participants outside Mainland of China, double length key algorithm is mandatory.

5.1.5 PIN Abnormity Processing

Please see Chapter 11: Flow of Transactions Abnormalities Processing in Part I Transaction Processing of Technical Specifications on Bankcard Interoperability.

5.2 MAC Calculation for Online Message

Message Authentication Code (MAC) is a calculation method used to verify the validity of message source as well as the fact if the message has been altered during transmission.

MAC calculation is complied with ISO8731-1992 Approved Algorithms for Authentication.

5.2.1 Condition of MAC Usage

MAC is generally applicable to request message like 01xx, 02xx, 04xx, 05xx and successful response message like 01xx, 02xx, 04xx (the meaning of response code is

"Approved" and for details please see the response codes in *Part VI Annex*). Except for 08xx message for Key exchange, MAC is not applicable to other management messages (06xx) and network management messages (08xx).

MAC is optional for Participants. CUP and Participants shall discuss whether to use MAC.

5.2.2 Fields for MAC Calculation

The fields for MAC calculation are defined by CUP. The MAC calculation adopts a mode known as Cryptogram Block Connection (CBC).

Generally, the following data fields are involved in MAC calculation:

- Unique data fields, including trace number, date, time, etc.
- Data fields representing message features, including message type, transaction type, etc.
- Data fields relating to transaction, including card number, amount, response code etc.

5.2.2.1 Data Fields for Message of 01xx, 02xx, 04xx, 05xx

If the following data fields present or meet certain condition, they should be included in MAC calculation:

Table 8 Data Fields for MAC calculation of MTI in 01xx, 02xx, 04xx and 05xx

No	Field	Field Name	Attribute
1	0	Message-type-identifier[a]	n4
2	2	Primary-account-number[b]	n...19(LLVAR)
3	3	Processing-code	n6
4	4	Amount-of-Transactions	n12
5	7	Transmission- date-and - time	n10
6	11	System-trace-audit-number	n6
7	18	Merchants-type	n4
8	25	Point- of-service- condition- code	n2
9	28	Amount_transaction_fee	x+n 8
10	32	Acquiring –institution –identification -code[c]	n..11(LLVAR)
11	33	Forwarding- institution-identification-code[d]	n..11(LLVAR)
12	38	Authorization –identification -response	an6
13	39	Response-code	an2
14	41	Card-acceptor -terminal- identification	ans8
15	42	Card –acceptor –identification -code	ans15
16	90	Original-data-elements[e]	n42

[a]Message-type-identifier: 0100/0110, 0200/0210, 0220/0230, 0420/0430, 0422/0432)

[b]Primary-account-number: a PAN length of 2 bytes + PAN

[c]Acquiring-institution-identification-code: a length of 2 bytes length (n)+ institution ID with a maximum length of 11 bytes

[d]Forwarding- institution-identification-code: a length of 2 bytes length (n)+ institution ID with a maximum length of 11 bytes

[e]Original-data-elements: the first 20 positions only, Content：

org-message-type	n4	Original Message Type
org-system-trace-number	n6	Original Message Trace No.
org-transmission-date-time	n10	Original Message Transmission Time

5.2.2.2 Data Fields for Key Management Transaction Message

Key Management Message refers to Request for Key reset and its response message. The MAC is composed of the following fields:

Table 9 Data Field for Key Management Transaction Message

No	Field	Field Name	Attribute
1	0	Message-type[a]	n4
2	7	Transmission-date-and-time	n10
3	11	System-trace-audit-number	n6
4	39	Response-code	An2
5	53	Security-related-control-information[b]	n16
6	70	Network-management-information-code[c]	n3
7	100	Receiving-institution-identification-code[d]	n..11(LLVAR)

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

[b]For Security-related-control-information please refer to explanation in Field 53 as:

1000000000000000 —— Reset PIN Key PIK

2000000000000000 —— Reset MAC Key MAK

[c]Network-management-information-code: 101

[d]Receiving-institution-identification-code: a 2-position length (n) +a maximum 11-position institution ID

5.2.3 MAC Block Composition

5.2.3.1 MAC Character Selection

The selected MAC data fields shall be further processed as follows

- Data fields with length indicator should comprise the length value for MAC calculation
- Insert a blank between fields
- Replace all lowercases with capital letters
- Eliminate all characters except for letters A-Z, numbers 0-9, blank, comma, and

full stop

- Remove blanks at the beginning and ending of all fields
- Replace consecutive blanks with a single blank

5.2.3.2 Composition of MAC Block (MAB)

After picked up from a message, data should go through MAC character selection and then composes Message Authentication Block (MAB). The process is as below:

The data after MAC character selection will be divided into blocks of 64-bit. If the last block is less than 64 bits, binary “0” will be padded to 64 bits.

5.2.4 MAC Calculation

In case one of the following occurs, there is no need for the message receiver to check the MAC, and the corresponding error message shall be returned:

- Timestamp Field missing
- Invalid Time
- Message Identifier undefined
- Invalid Key

Prior to the delivery of the message, the message fields for MAC calculation shall be intercepted from the message. After MAC characters selection, MAB will be composed and its length will be calculated. The MAB, MAB length and MAK will be input into HSM to generate the MAC, which shall be delivered together with the message.

MAC verification shall be performed upon receiving the message. The message can only be accepted when the new MAC is identified as the same with the one received, otherwise the message will be declined.

5.2.4.1 MAC Calculation through MAB by HSM (DES)

5.2.4.1.1 Single Length Key Algorithm

MAB shall be divided into groups of eight bytes (pad 0X00 to the right if the last group contains less than eight bytes). The following operations will be performed with MAK as the single length key:

- Execute DES operation
- XOR the DES operation result with the eight bytes in the next group, and repeat to DES the XOR result and then XOR the DES result with the following group. An eight-byte encryption value can be obtained by performing DES operation on the last XOR result.

5.2.4.1.2 Double-Length Key Algorithm

According to ISO 9.19, MAB shall be divided into groups of eight bytes (padding 0X00 to the right if the last group contains less than eight bytes). The following will be performed with double-length key:

a. XOR the next group with the result generated by using the left 64 bits in the double length key to the first group.

b. XOR the result of the Step a with the rest groups repeatedly, until the last group.

c. An eight-byte encryption value can be obtained eventually by decrypting the last XOR result with the right 64 bits in the double length key and then encrypting the result of decryption with the left 64 bits in the double length key.

5.2.4.2 MAC Field Value of Online Message

5.2.4.2.1 General Transaction

MAC field (Field 128), which is the first half of the 8-byte binary digit (a 4-byte binary digit) calculated from DES operation, is presented in the form of a hex character string (eight hex characters).

5.2.4.2.2 Key Reset Transaction Initiated by CUP System

In the key reset request message initiated by CUP system and the corresponding response message, the MAK shall be the new distributed key. Additionally, the newly distributed PIN key shall be adopted as the MAK in MAC calculation during PIN key reset.

5.2.4.2.2.1 MAC Calculation in Request Message

MAC field (Field 128) of request message, an eight-byte binary number, is composed of two parts. The first part is the first half of the 8-byte binary number (a 4-byte binary number) obtained from a MAC calculation based on single length-key algorithm (refer to 5.2.4.1.1 for MAK reset algorithm) or double-length key algorithm (refer to 5.2.4.1.2 for PIK reset algorithm), and the second part is the first half of the 8-byte binary number (a 4-byte binary number) obtained from the Check Value calculation based on single-length key algorithm or double-length key algorithm.

5.2.4.2.2.2 MAC Calculation in Response Message

If MAK is to be reset, the algorithm of MAC calculation in response message is the same as that of the general transaction described in Section 5.2.4.1.1. There’s no need to calculate Check Value, but the key for the MAC calculation shall be the new distributed key.

If PIK is to be reset, the algorithm of PIK calculation in response message is the same as that described in Section 5.2.4.1.2. There’s no need to calculate Check

Value either, but the key used shall be the newly distributed key.

5.2.4.2.2.3 CHECH VALUE Calculation

Check Value can be obtained by performing single length key algorithm (refer to 5.2.4.1.1 for MAK reset algorithm) or double length key algorithm (refer to 5.2.4.1.2 for PIK reset algorithm)on eight binary “0” with the new distributed key.

5.2.4.2.3 MAC Calculation When Double-length PIN Key is Reset

A new PIN key may be a 128–byte-double-ength key when the PIN key is reset, double length key algorithm should be adopted to MAC calculation in both request message and response message. Similarly, double length key algorithm should be adopted to CHECK VALUE calculation in request message. For MAC calculation and CHECK VALUE calculation flow, please refer to Section 5.2.4.1.2

.5.2.5 MAC Error Processing

Please see Chapter 11: Flow of Transaction Abnormalities Processing in Part I Transaction Processing of Technical Specifications on Bankcard Interoperability.

5.3 MAC Calculation of Sequential File

Sequential file refers to the file with file header (000) and file trailer (001), such as Dual-message Settlement File and Risk Information Sharing File. Please refer to *Part III File Interface* of *Technical Specification on Bankcard Interoperability* for details. All sequential files must use MAC verification. This section describes the requirements on MAC verification.

5.3.1 Character Composition of MAC KEY and MAC

There are two fields in a file trailer: MAC KEY and MAC, with each of them presented in the form of a string of 16 characters. There are no separators inserted between fields and no concluding symbol attached to the end of them. Every character contained in these two strings shall be hex characters, i.e. numbers 0-9 and capital letters A-F, used to present the 8-byte MAC key and 8-byte MAC. This presentation guarantees a convenient display and eliminates any unprintable characters.

5.3.2 Generation of MAC KEY

MAC KEY is a key that is generated randomly with the generation of files. It is here referred to as a cryptograph encrypted with the master key of an institution. Meanwhile, MAC KEY shall fulfill odd check.

5.3.3 MAB Composition

The whole file (excluding MAC Key and MAC) shall be divided into groups of 256 bytes padding with binary ‘0’ for the last group containing less than 256 bytes; the MAC Block for sequential file is the result of performing XOR of each group.

5.3.4 MAC Calculation

MAC is divided into two parts: the first and the second. Its generation is as below:

The first half (4-byte binary data) of the result, which is obtained by performing DES operation on the first 128 bytes, is presented in the form of a hex character string (eight hex characters) and regarded as the first part of MAC field; the first half of the result, which is obtained by performing DES operation on the last 128 bytes of the 256-byte Data Block that is also presented in the form of a hex character string (eight hex characters) and regarded as the second part MAC field.

5.3.5 MAC Error Processing

In case MAC verification fails, the system will generate a reject file with reason clarified as MAC Verification Failure. For specific format please refer to *Chapter 5 Basic Stipulations* in *Part III File Interface* of *Technical Specifications on Bankcard Interoperability*.

5.4 Encryption and Decryption for Internet Payment PIN of Internet Transaction

The Internet Payment PIN of internet transaction is sent to issuer with online message. It must be transmitted in cryptograph to ensure the security of PIN. Sender performs encryption, while the receiver performs decryption.

The Internet Payment PIN is involved in encryption/decryption calculation in the form of 192-bit binary digit. The distribution of its plaintext in this digit is known as Internet Payment PIN Data Block, whose format among CUP and Participants is as follows:

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

Note 1: P means Password, F means filler

Note 2: N - length of Internet Payment PIN (8-bit)

Note 3: P - the 8-bit binary digits of Internet Payment PIN

Note 4: P/F - the 8-bit binary digits of Internet Payment PIN/FILLER

Note 5: F - 8-bit binary digits of internet payment PIN FILLER

Figure 4 Internet Payment PIN Data Block Format

5.4.1 Length of Internet Payment PIN

Length of Internet Payment PIN is 6 to 20 digits.

5.4.2 Character set for Internet Payment PIN

Internet Payment PIN must be ASCII coding character, including character, digit, or other symbol.

5.4.3 Data Block of Internet Payment PIN

The Internet Payment PIN should have the format as follows:

Table 10 Format of Internet Payment PIN

Position	Length	Description
1	2 Byte	Length of Internet Payment PIN
2	22 Bytes	Internet Payment PIN is 13-19 digits (each character is 1 byte digit with space padded to right if vacancy appears, i.e. 0xFF)

Example:

Plaintext of Internet Payment PIN is Hello!123

As Internet Payment PIN is displayed in plaintext, therefore it is needed to change to ASCII code.

Plaintext of Internet Payment PIN	H	e	l	l	o	!	1	2	3
ASCII code	72	101	108	108	111	33	49	50	51
Hex	0x48	0x65	0x6C	0x6C	0x6F	0x21	0x31	0x32	0x33

As the description in Figure 6, this Internet Payment PIN has 9 characters, so add '09' in the front of the PIN as the length, which ASCII code is 48 and 57, Hex code is 0x30 and 0x39. Then pad 13 spaces behind, which Hex code os 0xff. So, the result of Internet Payment PIN data block is as follows:

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

5.4.4 Encryption of Internet Payment PIN

Enter the Internet Payment PIN data block obtained as above into HSM, perform DES or 3DES operation with the single or double length PIK saved in HSM, and then obtain the cryptograph of 24 bytes for Internet Payment PIN.

Here are 2 points to be noted: 1. the key for calculating Internet Payment PIN is PIK; 2. Internet Payment PIN key should use double length key algorithm.

5.4.5 Error Processing

Same with the processing for PIN, including Error Processing Procedure and Error Response Code.

5.5 File Encryption and Decryption in Flow Transmission Mode

5.5.1 File Encryption Key Generation

Method of file encryption key generation is the same as that for MAC key. The file encryption key, encrypted by MMK and also in compliance with odd check, is generated randomly when the file is to be transmitted. The key is of eight-byte-length, and generated by HSM with double length key algorithm.

5.5.2 Encryption and Decryption for File

As for file encryption, a file is encrypted by using DES algorithm. Data in the file shall be divided into groups of eight-byte strings (padding F to the right if the last string contains less than eight bytes). Then a group of 8-bytes new strings are generated by encrypting these strings with DES algorithm and meanwhile connected in sequence, leading to the cryptograph of the file. The cryptograph of the file is generated by directly connecting these news strings, not considering if it can be displayed by visible characters.

As for file decryption, at first, a file key plaintext shall be generated by decrypting the file key cryptograph with MMK. Then the file data plaintext can be obtained by decrypting the file encrypted with the file key plaintext. Be aware that the last group of eight-byte-strings should be removed during the process of file decryption because it is the file key. MAC should be checked at last, if the file is a dual-message presentment file. A MAC value shall be calculated by the MAC key in the file plaintext and be compared with MAC at the end of file. If they are the same, it means the file transmitted is correct. MAC needn’t be checked for audit trailers.

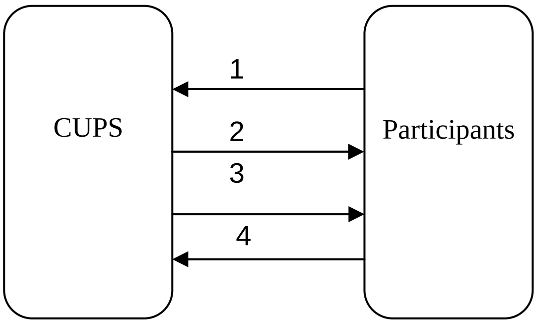
6 Key Reset

6.1 Key Reset Request Initiated from Participants

6.1.1 Transaction Flow

A Participant sends the request for Key Reset to CUP system. Upon receiving the request message CUP system shall reply immediately. Meanwhile, CUP system shall start up Key Renewal Module in generating a new key and send the Participant the new key in a Key Reset Message.

CUP will drop the message in case CUP system fails to reply the Key Reset Request or sends Key Reset to Participant.



1——Key Reset Request sent by a Participant to CUP system (0820)

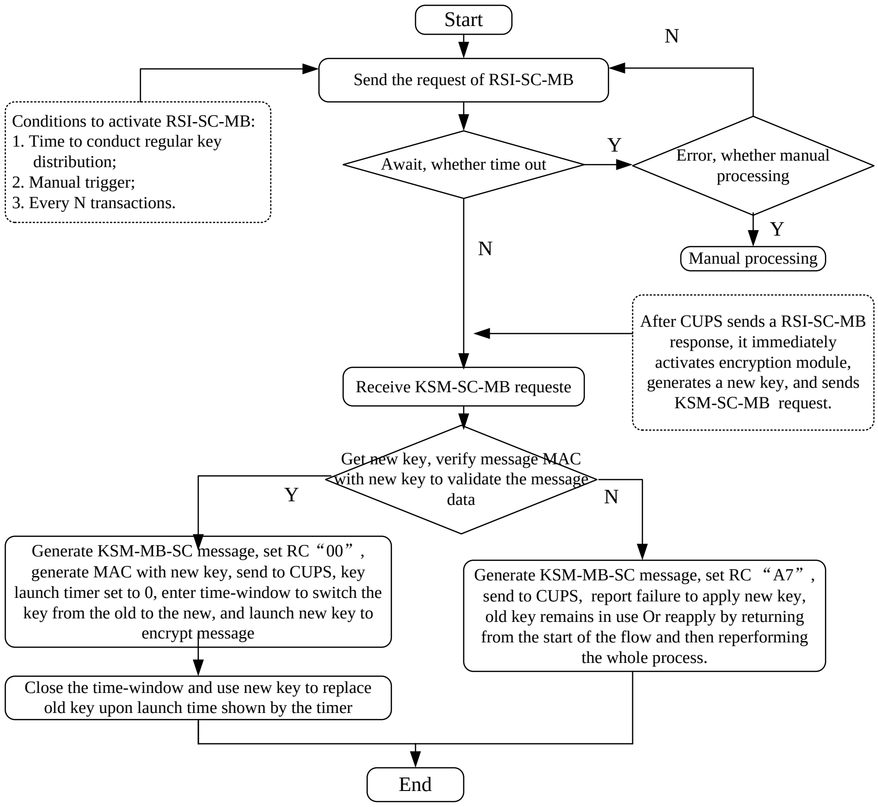
2——Response sent by CUP system to a Participant (0830)

3——Key Reset sent by CUP system to a Participant (0800)

4——Response sent by a Participant to CUP system (0810)

Figure 5 Flow of Key Exchange Request by a Participant

6.1.2 Flowchart


Start
Send the request of RSI-SC-MB
N
Conditions to activate RSI-SC-MB:
1. Time to conduct regular key distribution;
2. Manual trigger;
3. Every N transactions.
Await, whether time out
Y
Error, whether manual processing
Y
Manual processing
N
After CUPS sends a RSI-SC-MB response, it immediately activates encryption module, generates a new key, and sends KSM-SC-MB request.
Receive KSM-SC-MB requeste
Get new key, verify message MAC with new key to validate the message data
Y
N
Generate KSM-MB-SC message, set RC "00", generate MAC with new key, send to CUPS, key launch timer set to 0, enter time-window to switch the key from the old to the new, and launch new key to encrypt message
Generate KSM-MB-SC message, set RC "A7", send to CUPS, report failure to apply new key, old key remains in use Or reapply by returning from the start of the flow and then reperforming the whole process.
Close the time-window and use new key to replace old key upon launch time shown by the timer
End

Note 1: RSI－MB－SC : Key Reset Application Request Message sent by a Participant to CUP (0820)

Note 2: RSI－SC－MB: Key Reset Application Response Message sent by CUP to a Participant (0830)

Note 3: KSM－SC－MB: Key Reset Request Message sent by CUP to a Participant (0800)

Note 4: KSM－MB－SC: Key Reset Response Message sent by a Participant to CUP (0810)

Figure 6 Flow of Key Exchange Request by a Participant

6.1.3 Explanation on Key Reset request initiated from a Participant

Phase I: Send Key Reset Request to CUP

A Participant may send key reset request (RSI-MB-SC) (0820) to CUP when necessary, then wait for the response message of CUP system (RSI-SC-MB) (0830). The Participant may send the same message repeatedly if there is no response from CUP system within specified time limit. If there is still no response from CUP system, manual processing will be adopted.

Phase II: Receive the new key

Since CUP system has already applied new key in MAC calculation when delivering Key Reset message (KSM-SC-MB) (0800), a Participant shall extract the new key upon receiving the KSM-SC-MB and verify the MAC embedded in the message (refer to 5.2.4.2.2.1 for calculation of MAC in request message) and then it shall reply to CUP system with a response message (KSM-MB-SC) (0810) for Key Reset. The response message shall adopt MAC generated by the new key (refer to 5.2.4.2.2.2 for calculation of MAC in response message).

Upon successful receiving new key, a Participant shall add a start-up tag to the new key, and all messages delivered by the Participant shall be encrypted by using this new key. The shift window for new and old keys is defined as three minutes, during which new and old keys coexist. Within the time-window, the Participant performs decryption, conversion or verification for PIN and MAC information sent from CUP system by using the new key. This operation shall be repeated with old key in case errors occur in PIN format or MAC verification. If the errors still exist, it shall be regarded as material error and encryption/decryption failure. At that time, the Participant should try to reset key again. The Participant should take urgent measures to reset key manually in case of failure again (also contacting CUP technical support personnel by phone), while the Participant shall check the encryption and decryption program after the urgent measures are taken and may ask for help from CUP. The following operations shall be carried out beyond time window limit:

- To replace old key with new one
- To eliminate start-up tag attached to new key
- To finish Key Reset Application

The Participant should ask for help from CUP technical support personnel to look into the reason if the errors still occur during the operation of encrypting and decrypting with new keys beyond time window.

6.1.4 Message Format

The message format of Key Reset Request (RSI-MB-SC) by a Participant is as follows:

Table 11 Message Format of Key Reset Request

Position	Field Name	Description
	MESSAGE-TYPE－IDENTIFIER	Value ‘0820’
	BIT-MAP	b128
7	TRANSMISSION-DATE-AND-TIME	System Time
11	SYSTEM-TRACE-AUDIT-NUMBER	System Trace No.
33	FORWARDING-INSTITUTION-IDENTIFICATION-CODE	Forwarding institution identification code

Position	Field Name	Description
53	SECURITY-RELATED-CONTROL-INFORMATION	1st bit: Key Type (leftmost) 1 PIK 2 MAK 2nd bit: Encryption Algorithm Type 0 DES 6 3DES 3rd-16th bits: preserved , currently fill with ‘0’
70	NETWORK-MANAGEMENT-INFORMATION-CODE	Value ‘101’

The format of Key Reset Request response message (RSI-SC-MB) generated by CUP for a Participant is as follows:

Table 12 Message Format of Response for Key Reset Request by a Participant

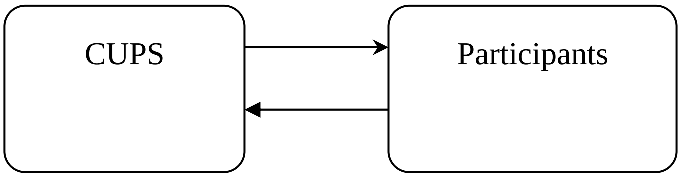
Position	Field Name	Description
	MESSAGE-TYPE－IDENTIFIER	Value ‘0830’
	BIT-MAP	b128
7	TRANSMISSION-DATE-AND-TIME	System Time
11	SYSTEM-TRACE-AUDIT-NUMBER	System Trace No.
33	FORWARDING-INSTITUTION-IDENTIFICATION-CODE	Forwarding institution ID
39	RESPONSE-CODE	Response Code
53	SECURITY-RELATED-CONTROL-INFORMATION	1st bit: Key Type (leftmost) 1 PIK 2 MAK 2nd bit: Encryption Algorithm Type 0 DES 6 3DES 3rd-16th bits: preserved, currently filled with ‘0’
70	NETWORK-MANAGEMENT-INFORMATION-CODE	Value ‘101’

A Participant shall send CUP system a key Reset application request right after the successful installation of MK and MMK. Due to the fact that each request can apply for only one DK, Participants shall send CUP system more than one request according to their own needs.

6.2 Key Reset initiated by CUP System

6.2.1 Transaction Flow

CUP system sends key reset to a Participant and the Participant replies to CUP system upon receiving the message. In case the Participant encounters a malfunction and CUP system does not receive any response, manual processing shall be directly adopted.



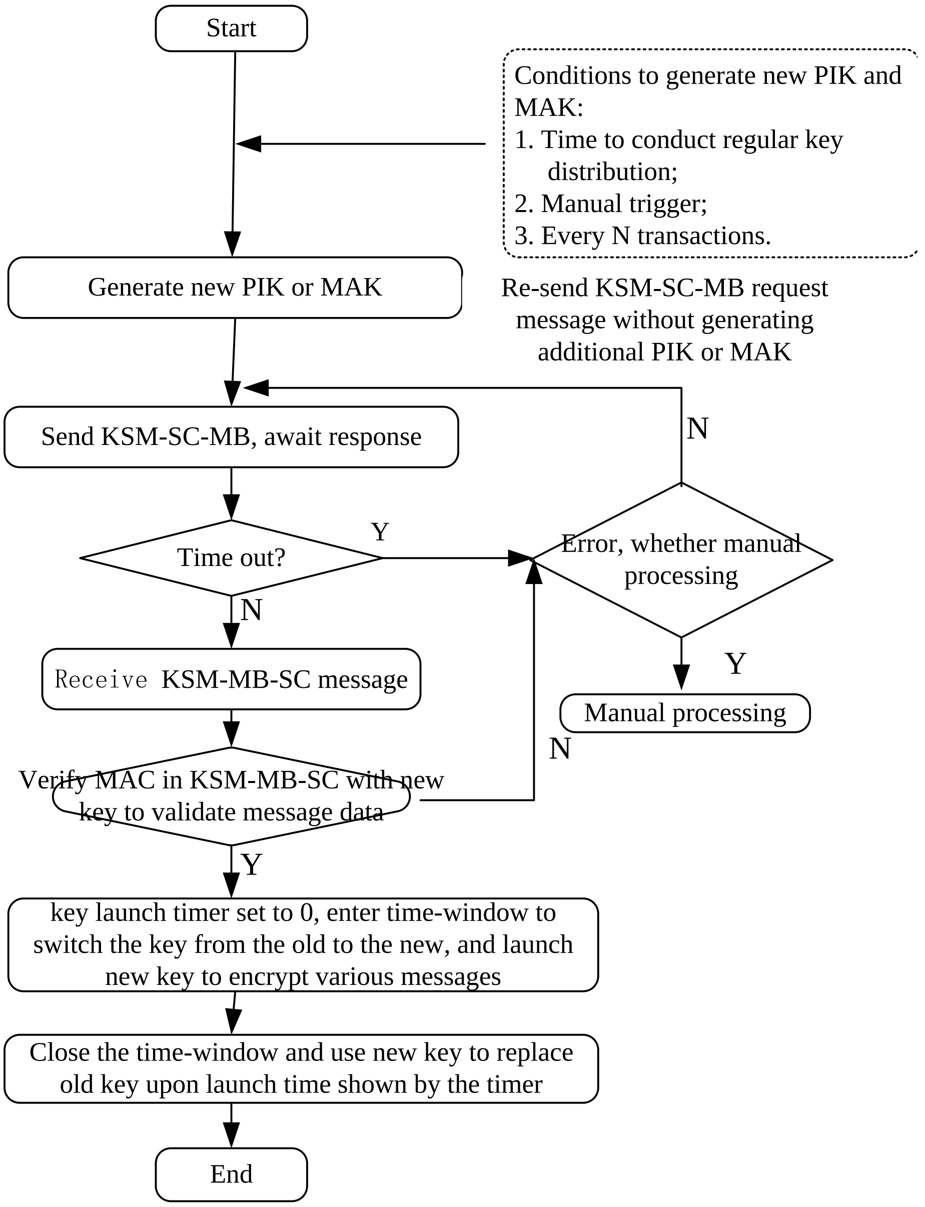
Messages involved in the above flow are as follows：

1—Key Reset sent by CUP system to Participant (0800) (referred to as KSM－SC－MB)

2—Response to Key Reset sent by a Participant to CUP system (0810) (referred to as KSM－MB－SC)

Figure 7 Flow of Key Reset initiated by CUP System

6.2.2 Flowchart


Start
Conditions to generate new PIK and MAK:
1. Time to conduct regular key distribution;
2. Manual trigger;
3. Every N transactions.
Generate new PIK or MAK
Re-send KSM-SC-MB request message without generating additional PIK or MAK
N
Send KSM-SC-MB, await response
Time out?
Y
Error, whether manual processing
N
Y
Receive KSM-MB-SC message
Manual processing
N
Verify MAC in KSM-MB-SC with new key to validate message data
Y
key launch timer set to 0, enter time-window to switch the key from the old to the new, and launch new key to encrypt various messages
Close the time-window and use new key to replace old key upon launch time shown by the timer
End

Note 1: RSI—MB—SC : Key Reset Application Request Message sent by a Participant to CUP (0820)

Note 2: RSI—SC—MB: Key Reset Application Response Message sent by CUP to a Participant (0830)

Note 3: KSM—SC—MB: Key Reset Request Message sent by CUP to a Participant (0800)

Note 4: KSM—MB—SC: Key Reset Response Message sent by a Participant to CUP (0810)

Figure 8 Flow of Key Reset initiated by CUP

6.2.3 Description on Key Reset Initiated by CUP System

CUP waits for Key Reset response message (KSM-MB-SC) (0810) from a Participant after sending Key Reset message (KSM-SC-MB) (0800)

If there is no response from the Participant within the time limit, , manual processing will be adopted directly.

Upon receiving successful key reset response message (KSM-MB-SC) from a Participant, CUP will check MAC with new key (Referto 5.2.4.2.2.2 for calculation of MAC in response message). If successful, CUP add a start-up tag to the new key, all message delivered shall be encrypted by using this new key. If failed, CUPS will use manual processing, contacting the Participant to offer advice and assistance as possible.

The shift window for new and old keys is defined as three minutes, during which new and old keys coexist. Within the time-window, CUP will perform decryption, conversion or verification for PIN and MAC information sent by the Participant with this new key. This operation shall be repeated with old key in case errors found in PIN format or MAC verification. If the errors still exist, it shall be regarded as material error and encryption/decryption failure, and CUPS will directly contact the Participant and try to offer assistance. The following operations shall be carried out beyond time window limit:

- To replace old key with new one
- To eliminate start-up tag attached to new key
- To finish Key Reset Application

CUPS will activate manual processing by contactting the Participant to look into the reason if the errors still occur during the operation of encrypting and decrypting with news key beyond time window.

6.2.4 Message Format

The format of Key Reset Message initiated by CUP system is as below:

Table 13 Format of Key Reset Message initiated by CUPS

Position	Field Name	Description
	MESSAGE-TYPE－IDENTIFIER	Value ‘0800’
	BIT-MAP	b128
7	TRANSMISSION-DATE-AND-TIME	System Time
11	SYSTEM-TRACE-AUDIT-NUMBER	System Trace No.
48	ADDITIONAL-DATA-PRIVATE	New Key Cryptogram
53	SECURITY-RELATED-CONTROL-INFORMATION	1st bit: Key Type (leftmost) 1 PIK 2 MAK 2nd bit: Encryption Algorithm Type 0 DES 6 3DES

Position	Field Name	Description
		3rd-16th bits: preserved, currently filled with ‘0’.
70	NETWORK－MANAGEMENT－INFORMATION－CODE	Value ‘101’
96	MESSAGE－SECURITY－CODE	New key cryptograph with maximum length of 8 bytes
100	RECEIVING-INSTITUTION-IDENTIFICATION-CODE	Receiving institution ID
128	M AC	Message Authentication Code

The format of Key Reset Response Message (KSM-MB-SC) initiated by Participants for CUP is as below:

Table 14 Format of Key Reset Response Message initiated by Participants

Position	Field Name	Description
	MESSAGE-TYPE－IDENTIFIER	Value ‘0810’
	BIT-MAP	b128
7	TRANSMISSION-DATE-AND-TIME	System Time
11	SYSTEM-TRACE-AUDIT-NUMBER	System Trace No.
39	RESPONSE-CODE	Response Code
53	SECURITY-RELATED-CONTROL-INFORMATION	1st bit: Key Type (leftmost) 1 PIK 2 MAK 2nd bit: Encryption Algorithm Type 0 DES 6 3DES 3rd-16th bits: Preserved, currently filled with‘0’
70	NETWORK－MANAGEMENT－INFORMATION－CODE	Value ‘101’
100	RECEIVING-INSTITUTION-IDENTIFICATION-CODE	Receiving Institution ID
128	MAC	Message Authentication Code

6.3 Switching between New/Old Key (Synchronous)

Switching between new and old keys (synchronous) refers to the effective time of the new key during the process of key reset.

Participants shall perform encryption or decryption with new key only if it has received KSM-SC-MB (Key Reset Request Message, 0800) and successfully decrypted the key. MAC value in KSM-MB-SC (Key Reset Response Message, 0810) shall be generated by using a new key after the new key is decrypted. CUP system shall perform encryption or decryption with new key only if it has received and authenticated KSM-MB-SC (Key Reset Response Message, 0810) sent from

Participants. There shall be a time difference if a Participant enables a key before CUPS does. The time difference is defined as time-window of Switching between New/Old Key'. There will be some transactions encrypted by the old key in the time window, with some transactions encrypted by the new key coexisting. The time-window is set as three minutes.

Within the three minutes time-window, the encryption and decryption of each transaction is as follows: a transaction needs be checked and authenticated with the new key, or if unsuccessful, it needs be checked and authenticated with the old key. Generally, one of two ways will work well at least. But if the checking with the old key way fails as well, it means key reset fails, leading to keys of both parties are asynchronous, under which manual processing may be adopted as soon as possible.

After the three minutes, the time–window shall be closed. Then encryption and decryption processing of all transactions should be processed with new key. If quite a few transaction fail in encryption and decryption processing with the new key means, it means key reset fails, leading to keys of both parties are asynchronous, under which manual processing may be adopted as soon as possible.

The key exchange time and event are as follows:

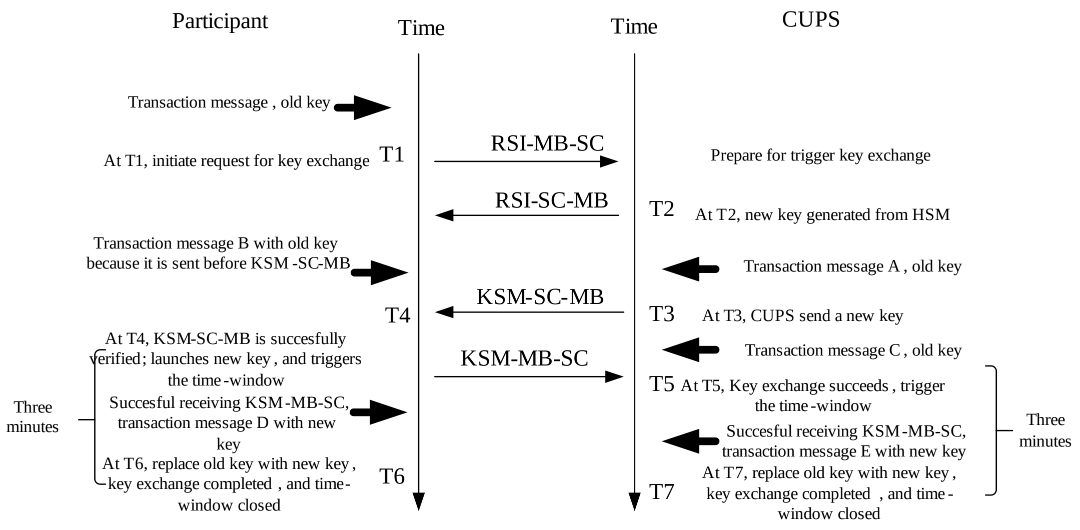

Participant
Time
Time
CUPS
Transaction message , old key
At T1, initiate request for key exchange
T1
RSI-MB-SC
Prepare for trigger key exchange
RSI-SC-MB
T2
At T2, new key generated from HSM
Transaction message B with old key because it is sent before KSM -SC-MB
Transaction message A , old key
KSM-SC-MB
T4
T3
At T3, CUPS send a new key
At T4, KSM-SC-MB is succesfully verified; launches new key , and triggers the time -window
KSM-MB-SC
Transaction message C , old key
T5
At T5, Key exchange succeeds , trigger the time -window
Three minutes
Succesful receiving KSM -MB-SC, transaction message D with new key
Succesful receiving KSM -MB-SC, transaction message E with new key
Three minutes
At T6, replace old key with new key , key exchange completed , and time-window closed
T6
T7
At T7, replace old key with new key , key exchange completed , and time - window closed

Figure 9 Key Reset Time and Event

THIS PAGE INTENTIONALLY LEFT BLANK.

7 Security Specification on CUPIC Debit/Credit Standard IC Card

7.1 Security Authentication Function

Security authentication is a key feature of IC card. There are two levels authentication existing in IC card online verification.

——Online Card Authentication (Issuer authentic the card)

The card creates an ARQC (Authorization Request Cryptogram) during the process of an online transaction, with which the Issuer can authenticate the validity of the card.

——Online Issuer Authentication (Card authentic the Issuer)

The Issuer creates an ARPC (Authorization Response Cryptogram) during the process of an online transaction, with which the card can authenticate the validity of the Issuer.

7.2 Algorithms of ARQC

7.2.1 Generation of ARQC

Unique Derivation Key (UDK) shall be initially calculated before ARQC can be obtained. A Session Key, which is finally used to calculate ARQC, can be computed through UDK.

7.2.2 Derivation Algorithms of Key (MDK creates UDK)

The IC card key is a derivate of the issuing key of Issuers which is unique to each other. The key of each IC card can be reckoned only if the root key and derivation algorithms are recorded.

- Data prescribed to be involved in derivation algorithms. Due to the fact that UDK is unique to each card, it shall be obtained derivatively from the unique data of card, including card number, card serial number and region code etc. Issuers themselves will determine the data elements, which shall be released to CUPS in case CUPS needs to perform stand-in ARQC authentication. Data elements involved in UDK calculation totally have eight bytes and it is prescribed that no more than five data elements shall be involved in derivation algorithms by Issuers.

- Data Block D1 (eight bytes, including sixteen hex digits) can be obtained by extracting the data prescribed to be involved in derivation algorithms with Issuers and array them one after another according the order stipulated by Issuers. If the data block does not contain 16 hex digits, so:

Flush right and pad 0x00 ahead in case the length less than 16

Quote the 16 rightmost hex digits if the length exceeds 16

D2 is obtained by reversing the above Data Block D1.

- To obtain a 8-byte UDK A by performing 3DES operation on D1 with MDK key; similarly, the 8-byte UDK B can be obtained through performing 3DES operation on D2 with MDK.

UDK B is put next to UDK A in getting UDK as shown in the following chart:

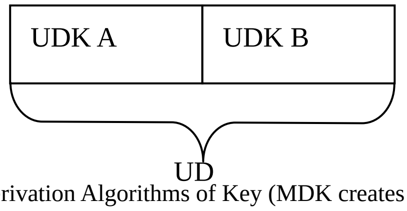


Figure 10 Derivation Algorithms of Key (MDK creates UDK)

7.2.3 Derivation Algorithms of Dual-length Key

- To calculate UDK based on MDK
- To pad hex ‘0’ to left of ATC (Field 137) in the message in expanding it to eight bytes and perform DES operation on the result with UDK to get the first eight bytes as Session Key A
- To XOR the 16-bit ATC with a hex value of FFFF (16bit) and pad to the left of the result with hex ‘0’ in expanding it to eight bytes, and then perform DES operation on the outcome with UDK to get the last eight bytes as Session Key B
- Session key (totally 16 bytes) can be obtained by combining the first eight bytes and the last eight bytes as depicted in the following chart:

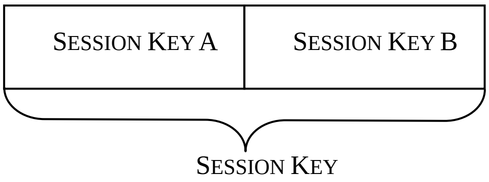


Figure 11 Derivation Algorithms of Dual-length Session Key

The Session key must meet requirements by odd parity.

7.2.4 Algorithms of ARQC

7.2.4.1 Data Source

Issuer may customize the data source and array order for ARQC calculation. The data source and array order, which are generally accepted, can be adopted if Issuer does not customize to define the arrangement. The following table gives the details:

Table 15 Data Source of ARQC

No.	Data Elements	Data from Terminals	Terminal Data involved in Terminal Field Hash value Computation	Data in Card	Corresponding Message Tag
1	Authorized Amount	√	√		9F02
2	Other Amount	√	√		9F03
3	Terminal Country Code	√	√		9F1A
4	Terminal Verification Result	√	√		95
5	Transaction Currency Code	√	√		5F2A
6	Transaction Date	√	√		9A
7	Transaction Type	√	√		9C
8	Unpredictable number	√	√		9F37
9	Applied Interactive Properties (AIP)			√	182
10	Applied Transaction Calculator (ATC)			√	9F36
11	Issuer applied Card Verification Result (CVR)			√	9F10

These three data sources, which named terminal field, Hash value for terminal field and data in card, shall be involved in ARQC calculation according to the universal algorithm

Hash value for terminal field will be obtained through SHA-1and comprises 20 bytes. In the wake of the Hash value is the terminal data, which can be arrayed one after another comply with the order presented in the above table without any process. Hence, the source data array for ARQC calculation is depicted as below:

Hash Result (20 bytes)	Terminal Data (length determined by actual content in message field)	Card Data (length determined by actual content in message field)

Figure 12 Source Data Array for ARQC Calculation

7.2.4.2 Approach for ARQC Calculation

- To divide the above mentioned data block into groups of 8 bytes: D1, D2, D3…
- If the length of last data block is eight bytes, an additional eight bytes shall be attached to the end of it and the data block is composed of data as: 0x80 0x00 0x00 0x00 0x00 0x00 0x00 0x00. In case the last data block falls short of eight

bytes, the vacancy shall be filled. A byte of 0x80 will be attached to the end of the data block if it contains seven bytes; two bytes of 0x80 0x00 will be attached to the end of the data block if it contains six byes, and so on, that is, if the data block falls short of eight bytes if a byte of 0x80 is attached to the end of it, the byte of 0x00 will be filled in till the data block contains eight bytes

- Session Key, as a double-length key, will carry out the following operations towards each group in turn:

Perform 3DES calculation

Perform XOR operation on the result with the eight bytes in the following group and replace the following group with the outcome and then carry on the operation. An 8-byte encryption value can be obtained by perform 3DES operation on the last group.

7.2.4.3 Data-Field Composition for Terminal Hash Value Calculation

TDOL data in the card denote the data-field involved in calculation of Hash Value for terminal field. The data name is read from TDOL and the relevant data is retrieved from the message. These data information are connected according to the following rules:

- If the tag for the data object denoted in TDOL cannot not be identified; or the data represented by the tag are not the optional static data in IC card; or the tag cannot represent the data applicable to the current transaction, the command field representing the data object shall be filled in with binary ‘0’;

- If the length denoted in TDOL entry is shorter than that of the actual data object, the data object shall be curtailed to the denoted length:

If the data object is presented in numeric format (n), bytes shall be curtailed starting from the leftmost of the data unit

If the data object is presented in other format, bytes shall be curtailed starting from the rightmost of the data unit

In case the denoted length is longer than that of the actual data, the actual data shall be filled to the denoted length:

If the data object is presented in numeric format (n), a hex 0 shall be padded starting from the leftmost of the data unit

If the data object is presented in other format, a hex FF shall be padded starting from the rightmost of the data unit

The sequence of data information link in messages shall be identical to the order of appearance of corresponding data objects in TDOL.

7.2.5 ARPC Calculation

ARPC is generated from ARQC. The detailed algorithm is shown as below:

- Perform XOR operation on applied cryptograph response code (Field 139.2) with authorization response cryptograph response code. The applied cryptograph which is populated in TAG9F26 in the uploaded request message, generally as ARQC or as AAC in some special circumstances, Prior to Xor, the response code of the authorization response cryptograph should be left justified with six bytes padding 0x00.

The result of the above mentioned is an 8-byte data block D1, which can lead to an 8-byte ARPC by perform 3DES operation on it with the session key.