

JR

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

JR/T 0055.4-2009

**Technical specifications on bankcard interoperability - Part 4:
Data secure transmission control
(English Translation)**

Issued on: June 1, 2009

Implemented on: July 1, 2009

**Issued by: People's Bank of China 3. No action is required - Full-copy of
this standard will be automatically & immediate**

Table of Contents

Foreword...	3
1 Scope ..	4
2 Normative references...	4
3 Terms and definitions...	4
4 Key management and control...	5
5 Online message PIN encryption and decryption...	9
6 Calculation of online message MAC ..	11

Foreword

JR/T 0055 Technical specifications on bankcard interoperability consists of the following five parts.

- Part 1. Transaction processing;
- Part 2. Message interface;
- Part 3. File data format;
- Part 4. Data secure transmission control;
- Part 5. Communication interface.

This Part is Part 4 of JR/T 0055.

This Part was proposed by People's Bank of China.

This Part shall be under the jurisdiction of National Technical Committee on Finance of Standardization Administration of China.

Main drafting organizations of this Part. People's Bank of China Science and Technology Division, China UnionPay Co., Ltd.

The drafting organizations of this Part. Industrial and Commercial Bank of China, Agricultural Bank of China, Bank of China, China Construction Bank, HSBC Bank, China Financial Computerization Corporation, Bank Card Testing Center.

Main drafters of this Part. Jiang Yunbing, Du Ning, Huang Faguo, Li Jie, Wan Gaofeng, Lu Erdong, Shi Dapeng, Lin Song, Zeng Zheng, Deng Lifeng, Cao

Ying, Ma Xiaoqiong, Liu Zhigang.

Technical specifications on bankcard interoperability

- Part 4. Data secure transmission control

1 Scope

This Part of this Standard specifies the basic requirements of the key management mechanism and the safe transfer of transaction data in the process of bank card interbank transaction transmission, so as to ensure the security and integrity of transaction information.

This Part of this Standard applies to the switching center, the acquirer, the issuer who conduct the inter-bank transaction of bank card.

2 Normative references

The provisions in following documents become the provisions of this Standard through reference in this Standard. For dated references, the subsequent amendments (excluding corrigendum) or revisions do not apply to this Standard, however, parties who reach an agreement based on this Standard are encouraged to study if the latest versions of these documents are applicable. For undated references, the latest edition of the referenced document applies.

ANSI X9.8, Banking - Personal Identification Number Management and Security

JR/T 0025 (all parts), China Financial Integrated Circuit Card Specifications

3 Terms and definitions

For the purpose of this document, the following terms and definitions apply.

3.1 personal identification number (PIN)

i.e., personal password; the data information that identifies the legitimacy of cardholder in online transaction

3.2 message authentication code (MAC)

the data used to validate the source and content of information between sender and receiver

- b) encryption/decryption of key generation, storage, destruction and transaction information shall be performed in hardware cryptographic equipment;
- c) it shall comply with national standards and international standards related to data security;
- d) it shall strengthen the management requirements for operator;
- e) the key shall be changed regularly.

4.1.1 Basic requirements of data secure transmission control

The data secure transmission control requirements shall include, but not limited to, the following four aspects.

- a) key management mechanism. technically implement strict and reliable key distribution process;
- b) encryption-decryption and conversion mechanism of personal identification number (PIN). PIN plain code is not allowed to appear on communication line and on manually operable storage media;
- c) all agencies shall use hardware encryption;
- d) peer-to-peer data encryption and decryption network mechanism.

4.1.2 Basic requirements of hardware encryption machine

The main function of the hardware encryption machine is to encrypt and decrypt PIN, to verify the correctness of the message source and to store the key. All of these operations shall be completed in a hardware encryption machine to ensure that the key and PIN plain code only appear in the encryption machine to prevent the disclosure of key and PIN. The hardware encryption machine shall pass the national commercial password department safety certification. In

addition, it shall also meet the following requirements.

- a) support single-length (B64, used in single-length key algorithm) and double-length (B128, used in double-length key algorithm) keys;
- b) support the provisions of this Part on PIN, the ciphertext of PIN verification, conversion;
- c) support the provisions of this Part on MAC, verify and generate MAC;
- d) verify the key;
- e) in the event of an unlawful attack, the cryptographic key is automatically destroyed.

Then PIN data block shall be. 0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF

Exclusive OR. 0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67

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

5.4 Encryption and decryption of PIN

Input the PIN data block generated in 5.3 into the hardware encryption machine.

Then use double length key algorithm to calculate it and PIK that is stored in the hardware encryption machine. Then the PIN ciphertext shall be obtained.

When a message arrives at an inter-bank transaction network, the PIN has been encrypted by the recipient's PIK. The switching center decrypts the ciphertext of the PIN with the PIK of the recipient. After the issuer's PIK is encrypted, it shall be sent to the issuer.

6.1 Conditions for MAC use

MAC is usually used for request message of 01XX, 02XX, 04XX types as well as successful replay messages of 01XX, 02XX, 04XX (reply code category means "approved"). The parties involved in the transaction may agree whether to use the MAC during the online transaction.

6.2.1 Selection of message field

The information involved in forming a MAC data block generally includes the