

ICS 35.240.40
CCS A 11

JR

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

JR/T 0025.17-2013

**China financial integrated circuit card specifications. Part 17:
Enhanced debit/credit application security specification
(English Translation)**

Issued on: February 5, 2013

Implemented on: February 5, 2013

Issued by: People's Bank of China

Table of Contents

Foreword...	4
Introduction...	6
1 Scope...	7
2 Normative references...	7
3 Terms and definitions...	8
4 Symbols and abbreviations...	10
5 Offline data authentication...	13
6 Application of cryptogram and issuer authentication...	25
7 Security message...	29
8 Security mechanism...	30
9 Approved algorithms...	36
10 Algorithm selection and transaction process...	36
11 PIN change/unlock command data calculation method...	45
Appendix A (Normative) Algorithm identifier...	47
References...	49

1 Scope

This part as an enhancement to JR/T 0025.7, mainly describes the debit/credit application security features requirements based on SM2, SM3, SM4 algorithm, and the security mechanism and approved encryption algorithm to achieve these security features, including IC card offline data authentication methods based on SM2 and SM3, communication security between SM4-based IC card and issuer, and security mechanisms and encryption algorithms involved in implementing these security features.

This part applies to the security-related equipment, card, terminal machine, and management, etc., of the financial debit/credit card application issued or accepted by the bank. The objective user is mainly the card, terminal and encryption device design, manufacture, management, issuance, application system research, development, integration and maintenance, and other departments (units) related to the application of the financial debit/credit IC card.

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this Standard.

JR/T 0025.4 China financial integrated circuit card specifications - Part 4.

Debit/credit application overview

JR/T 0025.5 China financial integrated circuit card specifications - Part 5.

Debit/credit application card specification

JR/T 0025.7 China financial integrated circuit card specifications - Part 7.

Debit/credit application security specification

GM/T 0002 SM4 block cipher algorithm

GM/T 0003 Public key cryptographic algorithm SM2 based on elliptic curves

3 Terms and definitions

The following terms and definitions apply to this document.

3.1

Application

Application protocols and related data sets between cards and terminals.

3.2

Command

A message sent from the terminal to the IC card that initiates an operation or requests a response.

3.3

Cryptogram

Encryption operation results.

3.4

Financial transaction

Information exchange, clearing and settlement of funds between cardholders, issuers, merchants and acquirers due to the exchange of goods or services between cardholders

and merchants.

3.5

Integrated circuit (IC)

Electronic devices with processing and/or storage capabilities.

4 Symbols and abbreviations

The following symbols and abbreviations apply to this document.

5.1.1 Key and certificate

The certificate authority uses the certificate authority private key SCA to sign the data specified in Table 1 using the SM2 algorithm to obtain the issuer public key certificate in the format shown in Table 4.

5.2.1 Key and certificate

The certificate authority uses the certificate authority private key SCA to sign the data specified in Table 1 using the SM2 algorithm, to obtain the issuer public key certificate in the format shown in Table 4.

5.2.2 Issuer public key acquisition

See 5.1.2.

5.2.3 IC card public key acquisition

The IC card public key certificate data as obtained by the terminal is as shown in Table 8. The public key of the IC card is included in the IC card public key certificate in the form of plain text, and the terminal verifies the signature field in the IC card public key certificate with the public key of the issuer. If the verification is passed, the public key information is extracted from the IC card public key certificate.

5.2.4.1 Dynamic signature generation

Use of SM2 algorithm to generate dynamic signature is in accordance with the following steps.

5.2.5 Combined dynamic data authentication/application cryptogram

generation (CDA)

5.2.5.1 Generation of dynamic signatures

IC card uses SM2 algorithm to generate dynamic signature, combined dynamic signature, and application cryptogram generation in accordance with the following steps.

6.1.1 Data Source Selection

See JR/T 0025.7.

6.1.2 Application cryptogram algorithm

Using a single 16-byte IC card application cryptogram (AC) unique key MKAC and the data source as described in clause 6.1.1 as the input, to calculate the

8-byte application cryptogram using the following two steps.

6.2 Issuer authentication

The method of generating an 8-byte authorized response cryptogram ARPC is to encrypt the 8-byte length ARQC and the 2-byte authorization response code

ACR which is generated in clause 8.1.2 in accordance with the symmetric encryption algorithm as specified in clause 11.1.2 using the 16-byte application cryptogram process key SKAC (see clause 8.1.2), and the encryption steps are as follows.

7.1.1 MAC process key generation

The first step in the security message MAC generation consists of dispersing a unique 16-byte security message authentication code (MAC) unique key and the 2-byte ATC from the IC card to obtain a unique 16-byte security message authentication code (MAC) process key. AND the process key generation method is as shown in clause 8.1.3.

7.2.1 Encryption process key generation

The first step in security message encryption/decryption consists of dispersing of the unique 16-byte encryption security message encryption unique key and the 2-byte ATC from the IC card to obtain a unique 16-byte encryption process key. And the process key generation method is as shown in clause 8.1.3.

8.1.1 Encryption and decryption

Encryption of data uses a 16-byte grouping encryption algorithm, either in electronic code book (ECB) mode or cipher block chaining (CBC) mode. JR/T

0025 uses ECB mode as encryption and decryption mode.

The procedure for encrypting message MSG of any length with encryption process key Ks