JR

FINANCIAL INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.240.40

A 11

Registration number:

JR/T 0025.10-2013

Replacing JR/T 0025.10-2010

China financial integrated circuit card specifications - Part 10: Debit/credit card personalization guide

中国金融集成电路（IC）卡规范 - 第 10 部分：借记/贷记应用个人化指南

Issued on: February 05, 2013 **Implemented on: February 05, 2013**

Issued by: People's Bank of China

Table of Contents

Foreword

JR/T 0025 “China financial integrated circuit card specifications” is divided into the following parts:

- Part 1: Electronic purse/electronic deposit application card specification (abolished);
- Part 2: Electronic purse/electronic deposit application specification (abolished);
- Part 3: Specification on application independent ICC to terminal interface requirements;
- Part 4: Debit/credit application overview;
- Part 5: Debit/credit application card specification;
- Part 6: Debit /credit application terminal specification;
- Part 7: Debit/credit application security specifications;
- Part 8: Contactless specification independent of application;
- Part 9: Electronic purse comprehensive application guide (abolished);
- Part 10: Debit/credit card personalization guide;
- Part 11: Contactless integrated circuit card communication specification;
- Part 12: Contactless integrated circuit card payment specification
- Part 13: Low-value payment specifications based on debit/credit application;
- Part 14: Comprehensive application specification based on contactless low-value payment application;
- Part 15: Electronic cash dual-currency payment specification;
- Part 16: IC card internet terminal specification;
- Part 17: Enhanced debit/credit application security specification.

This part is part 10 of JR/T 0025.

This part was drafted in accordance with the rules given in GB/T 1.1-2009.

China financial integrated circuit card specifications - Part 10: Debit/credit card personalization guide

1 Scope

This part of JR/T 0025 describes the personalization command unique to China financial IC card debit/credit application, the definition of a unique data grouping identifier (DGI), and the security-related requirements for personalization.

This part is intended for China financial integrated circuit (IC) card debit/credit cards issued or accepted by banks, to provide guidance to data preparation system providers and personalization centers in defining the data preparation phase requirements. At the same time, it can also provide reference for the designer to design default files and record structure. This part can also be referred to when personalizing other applications.

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 document.

JR/T 0025.5 China financial integrated circuit card specifications - Part 12: Debit/credit application card specification

JR/T 0025.12 China financial integrated circuit card specifications - Part 12: Contactless Integrated Circuit Card Payment Specification

JR/T 0025.17 China financial integrated circuit card specifications - Part 17: Enhanced debit/credit application security specification

GM/T 0002 SM4 block cipher algorithm

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

GM/T 0004 SM3 password hashing algorithm

GM/T AAAA SM2 password algorithm using specifications

HSM: Hardware Security Module

IAC: Issuer Action Code

IC: Integrated Circuit

ICC: Integrated Circuit (s) Card

ISO: International Organization for Standardization

ISS: Issuer

KEK/TK: Key Exchange Key / Transport Key - Shared by data preparation system and personalization device

KEK_{ISS}: Key Exchange Key - Shared by issuer and data preparation system

K_{ENC}: Card unique key, used to generate encrypted session key

K_{DEK}: Card unique key, used to generate a symmetric key or other optional secret data session key

K_{MAC}: Card unique key, used to generate C-MAC session key

KMC: Symmetric master key, used to generate K_{ENC}, K_{DEK}, and K_{MAC} by dispersing key during personalization

KMCID: Symmetric Master Key Identifier

MAC: Message Authentication Code

MAC MDK: Message Authentication Code Master Key

MAC UDK: Message Authentication Code Unique Key

MDK: Master Key

PAN: Primary Account Number

PEK/TK: PIN Encryption Key - A transmission key dedicated to PIN transmission

PIN: Personal Identification Number

RSA: An asymmetric key algorithm proposed by Rivest, Sharmir and Adleman

SAD: Signed static Application Data

SDA: Static Data Authentication

c) Initialization processing of IC card: The IC card will receive the initialization command and related data from the initialization device, and create the corresponding application and necessary file structure and write certain data in accordance with the initialization command, to make preparation for the subsequent personalization. After initial processing, the IC card will be partially locked so that only personalization commands and application commands will be received, and the file or application structure cannot be modified again.

See clause 5 and clause 8 for a further description of initialization.

4.2 Data preparation

Data preparation is the program responsible for creating the application data stored on the IC card. Some of the data is the same for each card, others are different for each card. Some data may be encrypted throughout the personalization process, such as the key.

For further descriptions of data preparation, see clauses 6 and 8.

4.3 Personalization device processing

Personalization devices are chip readers that send personalized data to an IC card. For most IC card applications that use a common method for personalization, the device must be connected to a security module to encrypt and decrypt data and MAC checks when sending commands to the application.

Personalization devices shall be stand-alone and application-independent.

See clause 7 and clause 8 for further descriptions of personalization device processes.

4.4 Debit/credit application processing

The IC card must be able to receive personalized application data from personalization devices and store it for later use.

China financial integrated circuit (IC) card debit/credit application shall be locked by the key set before the personalization process.

create all the data. In other cases, the data will come from a variety of sources. Data can be divided into the following three types:

a) Issuer master key and its related data;

b) Application key and certificate;

c) Application data.

6.2.1 issuer master key and its related data

The personalization process usually requires the creation of a card issuer master key and related data. Some data may be implanted in the card during personalization. The master key is used to generate a card or application key.

Other processes may also use one or more master keys provided for the personalization process. For example, a key exchange key used between data preparation and personalization. To ensure that the master key can be securely shared between processes, there is a need for a way to import and export the master key.

6.2.2 Application key and certificate

If card supports the card authentication, issuer certification or issuer script processing, the card key must be generated by the dispersion of issuer master key in accordance with the method defined in JR/T 0025.5 based on PAN and PAN serial number.

If the card supports offline data authentication and the card supports only a single algorithm, the issuer needs to generate an SM2 public-private key pair and the public key must be signed by a payment system certificate authority and the generated issuer public key certificate must be placed in the card. If DDA is supported as the offline data authentication method, each card must generate a pair of public and private keys, and the ICC public key must be signed by the issuer's private key. The generated ICC public key certificate and corresponding private key must also be included in the card.

If the card supports offline data authentication and the card supports dual algorithms, the issuer needs to generate at the same time an SM2 public-private key pair and an RSA public-key pair again, and both the SM2 public key and the RSA public key must be signed by the payment system certificate authority, and the generated issuer SM2 public key certificate and RSA public key certificate must be placed on the card. If DDA is supported as an offline data authentication method, each card must generate a pair of SM2 public-private key pairs and a pair of RSA public- private key, and both the ICC SM2 public key and the ICC RSA public key must be signed by the issuer's

K_{ENC} : = DES3 (KMC) [KEYDATA’s 6 least significant bytes II "F0" II "01"] II DES3 (KMC) [KEYDATA’s 6 least significant bytes II “0F” II "01"].

A check key dispersion key (K_{MAC}) must be generated for each IC card and written to the corresponding IC card. This key is used to verify the C-MAC used by the EXTERNAL AUTHENTICATE command. At the same time, when the data in the cryptogram security level of the STORE DATA command requires the data in the command to be MAC, the key is also used to verify the C-MAC used by the STORE DATA command.

K_{MAC} is a 16-byte (112 bits plus parity check bit) DES key.

K_{MAC} shall be derived using the following methods:

K_{MAC} : = DES3 (KMC) [KEYDATA’s 6 least significant bytes II "F0" II "02"] II DES3 (KMC) [KEYDATA’s 6 least significant bytes II “0F” II "02"].

A key encryption dispersion key (K_{DEK}) must be generated for each IC card and written to the corresponding IC card. This key is used to decrypt the confidential data received by the STORE DATA command in ECB mode.

K_{DEK} is a 16-byte (112 bits plus parity check bit) DES key.

KDEK shall be derived using the following methods:

K_{DEK} : = DES3 (KMC) [KEYDATA’s 6 least significant bytes II "F0" II "03"] II DES3 (KMC) [KEYDATA’s 6 least significant bytes II “0F” II "03"].

K_{ENC} is a 16-byte SM4 key if using the SM4 algorithm.

K_{ENC} key is derived using the following method:

K_{ENC} : = DES3 (KMC) [KEYDATA’s 6 least significant bytes II "F0" II "01"] II SM3 (KMC) [KEYDATA’s 6 least significant bytes II “0F” II "01"].

A check code dispersion key (K_{MAC}) must be generated for each IC card and written to the corresponding IC card. This key is used to verify the C-MAC used by the EXTERNAL AUTHENTICATE command. At the same time, when the cryptogram security level of the STORE DATA command requires the data in the command to be MAC, the key is also used to verify the C-MAC used by the STORE DATA command.

K_{MAC} is a 16-byte SM4 key.

K_{MAC} shall be derived using the following methods:

- K_{DEK} - Used to encrypt confidential data that is written into a card during personalization process.

KMC is unique to each card issuer, while K_{MAC}, K_{ENC} and K_{DEK} are unique to each card.

b) Master key (MDK) - Used to export: UDK - for online card authentication and issuer authentication.

For each BIN (bank identification number), the MDK is usually unique, and the UDK must also be unique for each card.

c) Public-private key pair of issuer - Usually generated by the issuer, and the public key shall be transmitted to the China financial integrated circuit (IC) card certificate authority for the purpose of creating the issuer public key certificate. The private key is stored in the issuer's HSM (host security module).

d) Key exchange key (KEK) - Used to encrypt confidential data in the personalization input file of the issuer. The KEK of each issuer must be unique.

e) Transmission key (TK) - Used to encrypt the confidential data in the issuer personalization input file transmitted by the data preparation system to the personalization system.

Alternatively, these keys can also be generated using the issuer public-private key pair.

f) ICC public-private key pair - The IC card uses this pair of keys to perform DDA and CDA/AC cryptogram generation algorithms. Among them, the public key must be signed by the private key of the issuer before obtaining the public key certificate from the issuer.

The ICC public-private key pair for each card must be unique.

g) MDK ENC - Used to derive: UDK ENC - to encrypt the script confidential information of the issuer.

h) MDK MAC - Used to check the issuer's script information.

MDK EC and MDK MAC are unique to at least each BIN, whilst the UDK ENC and UDK MAC must be unique for each card.

If the issuer generates its own key, it must create a ZMK to transmit those keys online.

- The SM2/RSA private key (signature) may be temporary to the physically secure device;

- Key generation will utilize a random or pseudo-random process to make it impossible to predict any key or to determine that some key in the key space is more likely than any other keys;

- Personal computers or other similar insecure devices, i.e., devices that are untrusted, will never be used to generate SM2/RAS public-private key pairs.

Key transmission and storage

In order to protect the integrity of public-private key pairs, it is very important for the issuer to ensure that such key data use the following steps:

- Public keys shall be secured and transmitted in a way that guarantees their integrity. The recommended public key is always transmitted in a data structure such as a certificate or it can be assured of integrity with a message authentication code (MAC) that is obtained by applying a key used only for that purpose in accordance with the algorithm as defined in ISO 9807 to the public key and related data. It is also recommended that dual control techniques be used to ensure that the recipient of the public key has a way of verifying its sender and integrity, by implementing separate and independent transmissions of a check value on the public key;

- Private keys must be guaranteed of security and transmission in a way that guarantees their integrity and privacy. Transmission mechanisms may include:

  • A security encryption device;

  • Decrypt the private key of the protected key using a symmetric algorithm that is at least as powerful as encryption;

  • As a few parts (secure on the IC card) and use a symmetric algorithm to decrypt it.

b) Symmetric key management

The symmetric key in JR/T 0025 is used for special transactional functions. Symmetric keys are derived from a Master Derivation Key during personalization. The final card level key is unique.

Issuer master key includes:

- Symmetric keys can be safely transferred under the protection of a security token or smart card for transmission and storage;

- Symmetric keys can only be transmitted or stored within the protected memory of a security token or smart card in the following manner:

Using the principle of dual control and separation of confidentiality, two or more parts are used as passwords, which are created using a transmission or storage key that is securely established by all parties.

8.4.2.2 Saving root key plaintext data

The requirements for saving root key plain data are as follows:

a) Upon receipt of the key data, the responsible key management personnel must immediately check whether the packet has been tampered with and must verify the content;

b) If the receiving administrator has any uncertainties about the integrity of the key data, the sender must be notified immediately. The sender and receiver negotiate the future status of the key data. The basis of any decision on the continued use of key material must be documented and retained by both parties;

c) If hard copy data is to be retained for any length of time, each hard copy component, security token or smart card must be kept in a serialized, confidential envelope;

d) This serialized, confidential envelope must continue to be stored in a physically secure container that is only accessible to the designated key administrator or standby staff. Every access to key data must be logged, including time, date, envelope serial number, purpose, and signature. These logs will be available to any appropriate requesting agency;

e) Key data can never remain outside the confidential envelope and their physically secure environment after the required time for the task is exceeded.

8.4.2.3 Saving other key data

Here are some general guidelines on key storage issues that apply to asymmetric and symmetric key storage:

a) Use of PC board

The issuer must receive and securely save one or more CA public keys. These public keys must be transmitted in a way that enables the issuer to verify their integrity and data source. The CA public key will be used to verify the issuer's public key certificate.

d) Request and receive issuer public key certificate

For the issuer public key, the issuer must obtain the corresponding issuer public key certificate. For this purpose, each issuer's public key must be transmitted to the CA certificate authority (PBOC CA), which in turn, the issuer receives the issuer's public key certificate. The issuer's public key must be transmitted to the CA certificate authority in a manner that enables it to verify the integrity of the public key and the data source. When receiving the public key certificate sent by the CA certificate authority, the issuer can verify the certificate by using the CA public key.

e) Transfer “Issuer Encryption Key”

If the issuer wishes to authorize a third party to generate and verify the ICC password, the issuer must securely transmit the issuer encryption key used to calculate the ICC key to a third party.

8.4.3 Management practices

8.4.3.1 Personnel management

Personnel responsible for managing encryption keys and key elements and other key data devices must be assigned by different parties (i.e., issuer, third party processor, and/or IC card personalization vendor).

When assigning a person to monitor the key data, adequate security controls must be implemented to ensure that no individual or unauthorized individual has any chance of reading the data component of the key.

The key keepers must be formally appointed staff and must not be temporary servants or advisors.

In addition, to ensure continuity of service, candidates may be considered "backups" of the major key keepers. The criteria for choosing a "backup" administrator shall be the same as choosing a master key administrator.

The key administrator is responsible for a great deal and is an essential part of the security agreement of the issuer. The key data they will administrate is the most important encrypted opcode in the issuer's issuing process. Each issuer shall verify the role of the internal key management procedures and the persons involved in the following operations:

8.5 Security module

Tampering prevention requirements: Prevention of tampering can be divided into two areas: physical and logical security areas.

8.5.1 Physical security attributes

Physical security includes the following attributes:

- Protection against intrusion, including erasing of sensitive data;
- Protection against unauthorized modifications that will result in the disclosure of sensitive information;
- Protection against the monitoring of electromagnetic radiation brought by the operation of the device.

8.5.2 Logical security attributes

Logical security features include the following attributes:

- Verification of authenticity
- The design of equipment function sets ensures that no single or combination of device functions will result in the disclosure of sensitive information;
- Mechanism existed to ensure the key segmentation;
- Sensitive state operation requires double control;
- Tips contained to verify software downloads.

8.5.3 Functional requirements

The minimum requirements for an HSM shall be around the support for:

- Key value generation;
- Key value exchange;
- Key configuration profile separation (logically split key attributes);
- Key value output and input;
- Secure storage of key values.

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

About Us (Goodwill, Policies, Fair Trading…): https://www.chinesestandard.net/AboutUs.aspx

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: https://www.linkedin.com/in/waynezhengwenrui/

------ The End ------