

ICS 35.240.40
CCS A 11

JR

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

JR/T 0025.7-2013

**China financial integrated circuit card specifications. Part 7:
Debit/credit application security specification
(English Translation)**

Issued on: February 5, 2013

Implemented on: February 5, 2013

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

Table of Contents

Foreword...	3
Introduction...	5
1 Scope...	6
2 Normative references...	6
3 Terms and definitions...	7
4 Symbols and abbreviations...	12
5 Offline data authentication...	13
6 Application cryptogram and issuer authentication...	45
7 Security message...	47
8 Card security...	49
9 Terminal security...	56
10 Key management system...	64
11 Security mechanism...	74
12 Approved algorithms...	83
Bibliography...	87

Foreword

JR/T 0025 China Financial Integrated Circuit Card Specifications consists of the following parts.

- Part 1.Electronic Purse/Electronic Deposit Application Card Specification;
- Part 2.Electronic Purse/Electronic Deposit Application Specification;
- 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 Specification;
- Part 8.Contactless Specification Independent of Application;
- Part 9.Electronic Purse Extended Application Guide;

- 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 is the 7th Part of JR/T 0025.

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

This Part replaces JR/T 0025.7-2010 "China Financial Integrated Circuit Card Specifications - Part 7. Debit/Credit Application Security Specification".

China financial integrated circuit card specifications -

Part 7. Debit/credit application security specification

1 Scope

This Part of JR/T 0025 describes the requirements for debit/credit application security functions and the security mechanisms involved in implementing these security functions and the encryption algorithms allowed for use, including IC card offline data authentication method, communication security between IC card and issuer, and related symmetric and asymmetric key managements, as specified as follows.

- offline data authentication;
- application cryptogram and issuer authentication;
- security message;
- card security;
- terminal security;

- symmetric and asymmetric key management system.

In addition, it also includes the security mechanisms involved in implementing these security features and the specifications for the encryption algorithms approved for use.

This Part applies to the security related equipment, cards, terminal equipment and management of financial debit/credit IC card application issued or accepted by the bank. The users are mainly the research, development, integration, maintenance and other relevant departments (organizations) of design, manufacture, management, distribution and application systems of cards, terminals and encryption devices related to the financial debit credit IC card application.

2 Normative references

The following standards contain the provisions which, through reference in this Part, constitute the provisions of this Part. For dated references, subsequent amendments (excluding corrections) or revisions do not apply to this Part.

However, the parties who enter into agreement based on this Part are encouraged to investigate whether the latest versions of these documents are applicable. For undated reference documents, the latest versions apply to this Part.

GB/T 16649.4, Identification Cards - Integrated circuit cards - Part 4.

Organization, security and commands for interchange (GB/T 16649.4-2010, ISO/IEC 7816-4:2005, IDT)

GB/T 16649.5, Identification cards - Integrated circuit cards - Part 15.

Cryptographic information application (GB/T 16649.5-2002, ISO/IEC 7816-5:1994)

GB/T 20547.2, Banking - Secure cryptographic devices(retail) - Part 2.

Security compliance checklists for devices used in financial transactions (GB/T 20547.2-2006, ISO 13491-2:2005, IDT)

ISO 873-1, Intelligent transport systems - Cooperative ITS - Test architecture

ISO 8732, Banking - Key management (wholesale)

ISO/IEC 9796-2, Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2.Integer factorization based mechanisms

ISO/IEC 9797-1, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1.Mechanisms using a block cipher

ISO/IEC 10116, Information technology - Security techniques - Modes of operation for an n-bit block cipher

ISO 13491-1, Financial services - Secure cryptographic devices (retail) - Part

3 Terms and definitions

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

3.1 accelerated revocation

recover keys before the issued expired key expiry date

3.2 application

application protocols and related data sets between cards and terminals

3.3 asymmetric cryptographic technique

are not used for offline data authentication processing and all other data in the READ RECORD command response data field (except SW1, SW2) is participating in offline data authentication;

- for files with SFI from 11 to 30, the recorded Tag ('70') and recording length are used for offline data authentication processing so that all data in the READ RECORD command response data field (except SW1, SW2) is participating in the offline data authentication;

- if the tag for the record in the file for offline data authentication is not '70', the offline data authentication is considered to have been performed and failed; the terminal must set the TSI's "Offline Data Authentication