JR

FINANCIAL INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.240.40

A 11

Filing No.:

JR/T 0025.16-2013

China financial integrated circuit card specifications -

Part 16: IC card internet terminal specification

中国金融集成电路（IC）卡规范

第 16 部分：IC 卡互联网终端规范

Issued on: February 5, 2013 **Implemented on: February 5, 2013**

Issued by: The 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 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 Part is Part 16 of JR/T 0025.

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

China financial integrated circuit card specifications - Part 16: IC card internet terminal specification

1 Scope

This Part describes the requirements and regulations for IC card internet terminals in terms of hardware requirements, interface protocols, command sets, personalization and security systems.

This Part **is applicable to** the financial IC card internet terminal equipment defined conforming to the JR/T 0025 specification. Such equipment is mainly used in the departments (authorities) related to the application design, manufacturing, management and acceptance as well as the development, integration and maintenance of the application systems associated with the IC card internet terminal applications.

All the terminals mentioned in this Part, unless otherwise specified, refer to the IC card internet terminals.

This Part describes the rules of using IC card internet terminals on personal computers. For the rules of use in other application environments (such as smart phones, tablets, etc.), REFER to the provisions of this Part.

2 Normative references

The following documents are essential to the application of this document. For dated references, only the editions with the dates indicated are applicable to this document. For undated references, only the latest editions (including all the amendments) are applicable to this document.

JR/T 0025.3 *China financial integrated circuit card specifications - Part 3: Specification on application independent ICC to terminal interface requirements*

JR/T 0025.6 *China financial integrated circuit card specifications - Part 6: Debit / Credit application terminal specification*

JR/T 0025.7 *China financial integrated circuit card specifications - Part 7: Debit / Credit application security specification*

JR/T 0025.8 *China financial integrated circuit card specifications - Part 8: Contactless specification independent of application*

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

ISO/IEC 8859-1 ~ ISO/IEC 8859-10 *Information technology - 8-bit single-byte coded graphic character sets*

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

3 Terms and definitions

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

3.1 Application

Application protocols and related data sets between cards and terminals.

3.2 Asymmetric cryptographic technique

Cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation.

3.3 Authentication

Measures for conforming the identity claimed by an entity.

3.4 Certificate

Unforgeable data formed by the certification authority issuing the certificate using its private key to sign the entity's public key, identity information and other related information.

3.5 Certification authority

A trusted third party that certifies that the public key and other related information are associated with their owners, which is hereinafter referred to as CA certification center or CA center.

3.6 Certification authority root certificate

Unforgeable public key information of an entity signed by the certification authority.

3.26 Load

The process of increasing the EC balance in the card.

3.27 Record Protocol

It is based on a reliable transmission protocol for providing the application layer protocol with the support for basic functions such as data encapsulation, compression, encryption, etc.

3.28 Response

The message returned to the terminal after the IC card processes the received command message.

3.29 Secure channel

A secure communication channel established between the IC card internet terminal and the process center.

3.30 Script

Commands or command sequences sent by the issuer to the terminal, for continuous command input into the IC card.

3.31 Secure channel command

The command for the terminal to performing the operations such as establishing secure channel between the terminal and the process center, managing the digital certificates, etc.

3.32 Symmetric cryptographic technique

Cryptographic technique using the same secret key for both the sender's and the recipient's data transformation. In the absence of a secret key, it is impossible to derive the data transformation of the sender or the recipient.

3.33 Terminal certificate

A unique digital certificate conforming to the X.509 format and used for identifying the terminal devices, which is written into each terminal device during pre-personalization.

3.34 Transaction command

The terminal's secure storage space shall at least meet the secure storage requirements for certificates and keys required for the transactions involved in this Part.

5.2 Requirements for trusted platform module

The terminal shall adopt the trusted platform module with the capability of key generation and digital signature operation, so as to ensure that sensitive operations are carried out within the trusted platform module, without revealing sensitive information or affecting security functions.

The trusted platform module shall have a separate unreadable area, used for storing the terminal private key, terminal key and other important information representative of the unique terminal. There shall be no mechanism for outputting plaintext private keys, plaintext keys or plaintext PINs. In addition, the keys or PINs shall not be encrypted using a key that might already be compromised.

The random numbers involved in the key operation shall be generated by the trusted platform module. Its random index shall conform to the general international standard for hardware random number generation.

5.3 Hardware composition

5.3.1 IC card reader module

The terminal shall be equipped with an IC card reader module, which can carry out command data communication with IC card and support contact and contactless IC cards. This module shall include mechanical, electrical and logical protocols and shall be consistent with the provisions of JR/T 0025.3 and JR/T 0025.11.

The terminal shall be provided with a tab indicating how to insert contact IC cards and to induce contactless IC cards.

5.3.2 Display

The terminal shall be equipped with a display for monitoring transaction process, performing data input and option settings or confirming transaction data. The terminal shall support the basic character sets of ISO 8859. The display shall be capable of displaying Chinese, English and figures.

5.3.3 Keyboard

The terminal shall be equipped with a key pad for entering the transaction amount and personal identification numbers (PINs), selecting commands and

the online PINs by selecting the corresponding PIN encryption certificate according to the DN field in the trusted server certificate. For specific method, REFER to Annex D.

7.2 Terminal public and private keys

The terminal's public and private keys are produced by the terminal in the process of downloading the terminal certificate. The public key generated by the terminal commits the CA to participate in making a certificate, while the terminal's private key shall be stored in the trusted platform module of the terminal and is not allowed to be exported.

7.3 Terminal personalization process

Terminal personalization is the process of writing terminal personalization data in advance into the terminal before the terminal exits factory. The CA root certificate, terminal certificate and PIN encryption certificate need to be downloaded from the CA center server.

The specific steps are as follows:

— Write terminal data information to a terminal;

— Install a terminal certificate to a terminal device;

— Install a CA root certificate to a terminal device;

— Install a PIN encryption certificate to a terminal device.

7.4 Certificate application and issuance process

The certificates with relation to the IC card internet terminals include the trusted server certificate, terminal certificate, CA root certificate and PIN encryption certificate.

7.4.1 CA root certificate

The CA root certificate is used for verifying the authenticity of the trusted server certificate, terminal certificate and PIN encryption certificate to distinguish legitimate identities, which needs to be written into IC card internet terminals and security devices in the process center during personalization. The CA root certificate download shall be negotiated by the CA center and the terminal authority.

7.4.2 Terminal certificate

6) After R3 and R2 are connected, R3 is obtained. The terminal first performs a digest algorithm on R3 to get H1, then performs a signature operation on H1 using the terminal private key to get S1.
7) The terminal sends S1, E1 and terminal certificate to the process center.
8) The process center uses the CA root certificate to verify the validity of the terminal certificate. If the terminal certificate verification fails, an error message will be sent to end the chain. If the terminal certificate verification passes, the terminal certificate will be used to verify S1. If S1 verification fails, an error message will be sent to end the chain. Otherwise, the shared master key M1 will be decrypted from E1.
9) The process center performs digest operation on the trusted server certificate and terminal certificate to get H2 and H3, respectively. T1 (T1 = R1 || R2 || H2 || H3 || S1 || E1) is obtained by connecting R1, R2, H2, H3, S1 and E1. Then, PERFORM a digest operation on T1 to get H4. After ASCII code “SERVER” and H4 are connected, D1 is obtained. USE the first 16 bytes of M1 to perform HMAC operation on D1 to get F1 (for HMAC calculation method, SEE B.2).
10) The process center sends a Handshake Verification Completed message F1 to the terminal.
11) The terminal verifies the F1 received from the process center. If the verification fails, an error message will be sent to end the chain. Otherwise, SEND a terminal handshake verification message F2 to the process center. The F2 operation is the same as the F1 operation method. It only needs to change the ASCII code “SERVER” in F1 operation into the ASCII code “CLIENT”.
12) The terminal sends Handshake Verification Completed message F2 to the process center.
13) The process center uses the same calculation method to verify the received F2 message. If the verification fails, an error message will be sent to end the chain.
14) After the above handshake process is successful, both parties use the following method to calculate the session key:
    X = HMAC (M1, key_label || r1 || r2) (M1 takes the first 16 bytes)
    where key_label is a 3-byte ASCII code “KEY”. REFER to Annex B.2 for the HMAC algorithm. LET X1X2 ... X20 be the 1st to 20th bytes of X, respectively. Then the encryption key SKey is SKey = X1X2 ... X16, and the MAC key MKey is MKey = X5X6 ... X20.
15) The handshake process is over.

8.2.2 Operating principle of Record Protocol

After the handshake is successful, both parties can perform data transmission over the established secure channel.

Data encryption method of Record Protocol

The data block length, Length (2 bytes), is added in front of the data to be transmitted, Data, to form a data block, D = (Length || Data). USE the session key, SKey, to encrypt D in accordance with the encryption algorithm agreed between the terminal and the process center, which is:

$EData = E_{SKey}(D)$

Data integrity protection method of Record Protocol

During the transmission of Record Protocol, a record serial number is designated for each double-ended transmission and reception record. The initial value, Seq0, is generated as follows:

TAKE the first 8 bytes of the terminal random number as Random1, and the first 8 bytes of the process center as Random2. Then Seq0 = Random1 || Random2.

After each transmission or reception of a frame of record information, record serial number plus 1, that is, $Seq_i = Seq_{i-1} + 1$. It shall be noted that both ends should maintain synchronous transmission and reception of the serial number.

The integrity of the application data exchanged by both parties is protected by using the Message Authentication Codes (MACs). MACs are generated according to the following method:

DataMAC = MAC (MKey, Seq_i || EData) (MKey takes the first 16 bytes),

where EData is the transmitted encrypted application data, and Seq_i is the current record serial number. REFER to Annex B.1 for the calculation method of MAC. After receiving the data, the terminal or the process center first verifies the correctness of the MAC. If MAC is correct, the data will be processed; otherwise, an error message will be sent to end the current chain.

9 Terminal transaction process

This clause describes the online transaction process of IC card internet terminals, which is the transaction processing flow after mutual authentication of the internet terminal and the process center to establish a secure channel.

9.1 Start of transaction

After a secure channel is established between the terminal and the process center, the terminal performs analysis and processing according to the transaction commands received from the process center. The debit / credit

Annex A

(Normative)

Terminal command set

A.1 Overview on terminal command set

The terminal command APDU format and the response APDU format comply with the provisions of JR/T 0025.3.

The terminal command set includes two parts: a specific command set and a common command set.

— Specific command set: All APDU commands of 7E or 7F Class Byte of the Command Message (CLA) in this Part, where 7E represents the data transmission in plaintext and 7F represents the encrypted data transmission. The key includes the session (data encryption) key and the MAC key. The key is produced by negotiation between both parties of the secure channel. The terminal-specific commands are divided into five categories according to their functions, namely management commands, secure channel commands, transaction commands, issuer retention commands, and commands reserved in this specification. The terminal-specific command is defined in Table A.1.

— Common command set: APDU commands other than the terminal-specific commands defined in this Part.

Note 1: Management commands: DEFINE the management commands for obtaining terminal parameter information, controlling terminal prompts, etc.

Note 2: Secure channel commands: DEFINE the secure channel commands for establishing secure channels between terminals and process centers and managing digital certificates.

Note 3: Transaction commands: DEFINE the transaction commands for performing transaction initiation and online processing on partial debit / credit application process.

Note 4: Issuer retention commands: Defined by the issuer.

Note 5: Commands reserved in this specification: Reserved for use by this specification.

key of the trusted server certificate.

A.3.10.2 Command message

The EXPORT MASTERKEY command message is coded in Table A.29.

Table A.29 -- EXPORT MASTERKEY Command Message

Code	Value
CLA	7E
INS	29
P1	00
P2	00
Lc	Does not exist
Data	Does not exist
Le	00

A.3.10.3 Command message data field

The command message data does not exist.

A.3.10.4 Response message data field

The shared master key's ciphertext encrypted using the public key of the trusted server certificate.

A.3.10.5 Response message status code

The status code for successful execution of this command is '9000'.

The error message that the command may return is shown in Annex A.5.

A.3.11 HMAC command

A.3.11.1 Definition and scope

The HMAC command is used for:

1) taking the HMAC value generated after the completion of handshake during the protocol, and sending it to the process center for verification.
2) entering the HMAC value generated after the completion of handshake in the process center during the protocol, and sending it to the terminal for verification.
3) generating a session key in the terminal through the HMAC algorithm.

For the above contents, SEE the definitions in Subclauses 8.2.1 and 8.2.2 of this Part.

The TRANSMIT ENCRYPTED COMMAND is used for the encrypted transmission between the process center and the terminal.

A.3.12.2 Command message

The TRANSMIT ENCRYPTED COMMAND message is coded in Table A.32.

Table A.32 -- TRANSMIT ENCRYPTED COMMAND Message

Code	Value
CLA	7F
INS	2B
P1	00
P2	00: non-cascade mode; 01: cascade mode
Lc	Input data length
Data	Input data
Le	00

When P2 = 0x00, the secure channel message is transmitted in non-cascade mode, or the message has reached the last frame of the cascade data.

When P2 = 0x01, the secure channel message is transmitted in cascade mode, followed by data.

A.3.12.3 Command message data field

SKey encrypted command data and MKey calculated MAC issued by the process center.

A.3.12.4 Response message data field

Encrypted command response data and MAC.

A.3.12.5 Response message status code

The status code for successful execution of this command is ‘9000’.

The error message that the command may return is shown in Annex A.5.

Remark:

1) The transaction command can only be transmitted to the terminal equipment through this encrypted command, that is, the terminal cannot perform transaction until the secure channel is established.
2) The terminal commands transmitted through this command are executed after decryption. The execution result and the return code need to be sent back to the process center after encryption. In addition, the return code

A.4 Transaction commands

A.4.1 CREDIT FOR LOAD command

A.4.1.1 Definition and scope

The CREDIT FOR LOAD command is used for supporting the online load transaction of the financial IC card, allowing to credit the primary account funds of the financial IC card to an EC account, and completing the operation of updating the EC balance in the IC card. The load amount is input in the terminal. During the transaction, the terminal shall automatically query the load limit and prompt the cardholder for the maximum load amount.

A.4.1.2 Command message

The CREDIT FOR LOAD command message is coded in Table A.34.

Table A.34 -- CREDIT FOR LOAD Command Message

Code	Value
CLA	7E
INS	40
P1	00 / 01
P2	When P1 = 00, P2 = 00, START transaction, READ the data defined in Table A.36; When P1 = 00, P2 = 01, READ the data defined in Table A.37; When P1 = 01, P2 = 00, RETURN data online
Lc	Data length in the Data field
Data	SEE the description on command message data field
Le	00

A.4.1.3 Command message data field

When P1 = 00, P2 = 00:

START load transaction. Table A.35 describes the command message data field.

Table A.35 -- Command Message Data Field for Start of Load Transaction

Data	Length (byte)	Remark
Transaction amount	6	Fixed to 0
Transaction date YYMMDD	3	Current date of process center
Transaction time HHMMSS	3	Current time of process center
Other transaction data	Variable (VAR)	SEE the Note below the table

Note: Other transaction data refers to the data of the process center, which needs to be sent back to the pre-processing system in the exception (reversal, script notification) transaction message. The terminal does not need to parse this data. Other transactions are handled in the same way.

A.4.1.5 Response message status code

The status code for successful execution of this command is '9000'.

The error message that the command may return is shown in Annex A.5.

A.4.2 DEBIT FOR PURCHASE command

A.4.2.1 Definition and scope

The DEBIT FOR PURCHASE command is used for supporting the online purchase transactions of the financial IC cards, and allowing the cardholders to use the financial IC cards for internet shopping and access to related services.

A.4.2.2 Command message

The DEBIT FOR PURCHASE command message is coded in Table A.40.

Table A.40 -- DEBIT FOR PURCHASE Command Message

Code	Value
CLA	7E
INS	41
P1	00 / 01
P2	When P1 = 00, P2 = 00, START transaction, READ the data defined in Table A.42; When P1 = 00, P2 = 01, READ the data defined in Table A.43; When P1 = 01, P2 = 00, RETURN data online
Lc	Data length in the Data field
Data	SEE the description on command message data field
Le	00

A.4.2.3 Command message data field

When P1 = 00, P2 = 00:

START online purchase transaction. Table A.41 describes the command message data field.

Table A.41 -- Command Message Data Field

Data	Length (byte)	Remark
Transaction amount	6	Purchase amount
Transaction date YYMMDD	3	Current date of process center
Transaction time HHMMSS	3	Current time of process center
Other transaction data	Variable (VAR)	SEE the Note below the table

Note: Other transaction data refers to the data of the process center, which needs to be sent back to the process center in the exception (reversal, script notification) transaction message. The terminal does not

The status code for successful execution of this command is '9000'.

The error message that the command may return is shown in Annex A.5.

A.4.3 GET ELECTRONIC CASH BALANCE command

A.4.3.1 Definition and scope

The GET ELECTRONIC CASH BALANCE command is used for checking the IC card EC balance through the terminal. This transaction is offline.

A.4.3.2 Command message

The GET ELECTRONIC CASH BALANCE command message is coded in Table A.46.

Table A.46 -- GET ELECTRONIC CASH BALANCE Command Message

Code	Value
CLA	7E
INS	42
P1	00: DISPLAY EC balance
P2	00
Lc	Does not exist
Data	Does not exist
Le	00

A.4.3.3 Command message data field

The command message data field does not exist.

A.4.3.4 Response message data field

For EC balance of financial IC cards, the response message data field is described in Table A.47.

Table A.47 -- GET ELECTRONIC CASH BALANCE Response Message Data Field

Description	Length (byte)	Remark
EC balance	6	BCD code

A.4.3.5 Response message status code

The status code for successful execution of this command is '9000'.

The error message that the command may return is shown in Annex A.5.

A.4.4 GET PRIMARY BALANCE command

contents according to the input data object list.

A.4.5.2 Command message

The GET DOL VALUE command message is coded in Table A.54.

Table A.54 -- GET DOL VALUE Command Message

Code	Value
CLA	7E
INS	45
P1	00
P2	00
Lc	Data length in the Data field
Data	SEE the description on command message data field
Le	00

A.4.5.3 Command message data field

The format of the input data object list is shown in Table A.55.

Table A.55 -- Format of GET DOL VALUE Command Message Data Field

Tag 1	Length 1	Tag 2	Length 2	…	Tag n	Length n

Note: The length refers to the length of the tag value to be obtained.

A.4.5.4 Response message data field

The data field of the response message is a BER-TLV encoded data object. This data object needs to be encoded according to the following format:

Table A.56 -- Format of GET DOL VALUE Response Message Data Field

Tag 1	Length 1	Value 1	Tag 2	Length 2	Value 2	…	Tag 3	Length 3	Value 3

A.4.5.5 Response message status code

The status code for successful execution of this command is ‘9000’.

The error message that the command may return is shown in Annex A.5.

A.4.6 GET REVERSAL INFO command

A.4.6.1 Definition and scope

The GET REVERSAL INFO command is used for obtaining the reversal information or the script execution result notification information saved by the financial IC card when the online transaction is abnormal.

(Tag 9F26)		
Issuer application data (Tag 9F10)	35 for maximum	TLV format

When P1 = 01, P2 = 01:

There is no data field in the command message.

A.4.6.5 Response message status code

The status code for successful execution of this command is '9000'.

The error message that the command may return is shown in Annex A.5.

A.4.7 VERIFY OFFLINE PIN command

A.4.7.1 Definition and scope

The VERIFY OFFLINE PIN command is used by the terminal to initiate a card verification of offline card PIN. The verification command initiates the IC card to verify the transaction PIN data in the command message data field with the reference PIN data related to the application. The verification method is determined by the application in the IC card.

A.4.7.2 Command message

The VERIFY OFFLINE PIN command message is coded in Table A.60.

Table A.60 -- VERIFY OFFLINE PIN Command Message

Code	Value
CLA	7E
INS	4A
P1	00
P2	00
Lc	Does not exist
Data	Does not exist
Le	00

A.4.7.3 Command message data field

The command message data field does not exist.

A.4.7.4 Response message data field

The response message data field does not exist.

A.4.7.5 Response message status code

Annex B

(Normative)

Calculation method of Message Authentication Code (MAC)

B.1 MAC based on block algorithm

According to the ISO/IEC 9797-1 specification, the MAC algorithm uses CBC mode to compute 8-byte MAC values for messages of any length using a symmetric encryption algorithm with a key length of 128 bits.

Table B.1 -- Parameter Description for MAC Algorithm

M	Plaintext message
C	Ciphertext message
M_{AC}	Message authentication code
K	MAC key
IV	Initial vector
$E_K(M)$	USE key K to encrypt M
$D_K(C)$	USE key K to decrypt C

Padding blocks:

APPEND 0x80 to plaintext M. Then FILL in the right side with a minimum of 0x00 so that the length of the message M = (M||80||00||00||…||00) after padding is an integer multiple of 8. M is divided into 16-byte blocks M_1, M_2, …, M_n.

MAC calculation

USE the left half of the key K, 8-byte KL, to encrypt the blocks M_1, M_2, …, M_n through 3DES algorithm in CBC mode, where the initial vector IV = (00 || 00 || 00 || 00 || 00 || 00 || 00 || 00).

The encryption process in CBC mode is as follows:

$$C_0 = IV$$

$$C_i = E_{KL} (M_i \oplus C_{i-1}), i = 1, 2, \ldots, n$$

The method for MAC calculation using the last data block is as follows:

$M_{AC} = E_{KL} (D_{KR} (C_n))$

Annex C

(Informative)

Example of secure channel setup process

The host sends a GET CLIENT HELLO command to the terminal. The terminal returns a 1-byte algorithm identifier and a 32-byte random number.

The host obtains a list of symmetric and asymmetric algorithms supported by the terminal from a 1-byte algorithm identifier. This identifier will be sent to the process center which will check whether the algorithm list contains the signature algorithm and symmetric algorithm used by the process center's trusted server certificate, based on the algorithm list.

The random number is used in subsequent verification and generation of authentication information

The process center sends the trusted server certificate, an algorithm identifier and a 32-byte random number to the terminal.

At this point, the terminal shall first check the validity of the trusted server certificate, that is, HASH SERVER CERTIFICATE command and VERIFY SERVER CERTIFICATE command.

The HASH SERVER CERTIFICATE command is used for performing hash operation on the subjects of the trusted server certificate, and for saving the hash operation results in the terminal.

The VERIFY SERVER CERTIFICATE command uses the CA root certificate in the terminal to decrypt the signature value of the trusted server certificate, and makes comparison with the hash results of HASH SERVER CERTIFICATE to check the validity of the trusted server certificate.

After verifying the validity of the trusted server certificate, the terminal generates a 48-byte random number as the shared master key, and uses the trusted server certificate to perform public key encryption on this shared master key. The EXPORT MASTERKEY command is to encrypt the shared master key using the trusted server certificate and to return a 128-byte cryptogram.

The terminal certificate is read out using the READ CERTIFICATE command and the GET CERT RESPONSE command. Considering that the size of a certificate is greater than the maximum number of bytes transmitted by a single

CCID command, it is not possible to read the terminal certificate through a single command. The GET CERT RESPONSE command can be called multiple times until the terminal certificate is completely read. For a detailed explanation of the command, SEE Annex A.3.

During the terminal authentication carried out by the process center, it is necessary to verify the signature of the terminal private key. The terminal uses the CLIENT SIGN command to perform hash and signature operations on the incoming random number of the process center and the connection values of the terminal's random number, and returns 128 bytes of signature data.

The terminal sends the cryptogram of a 128-byte shared master key, the terminal certificate and a 128-byte signature value to the process center.

The process center uses the root certificate to verify the validity of the terminal certificate. If the terminal certificate is valid, the terminal public key will be used for verifying the signature value to determine the validity of the terminal. After the authentication of the terminal is completed, the private key of the trusted server certificate is used for decrypting the cryptogram of the shared master key to obtain a 48-byte shared master key. Here you need to send a message authenticated by the process center, so as to prevent this message from being counterfeited. This message is calculated by means of HMAC. Its key is the first 16 bytes of a 48-byte shared master key. The data includes the ASCII "SERVER", terminal's random number, process center's random number, trusted server certificate's hash value, terminal certificate's hash value, signature value sent by the terminal to the process center, and cryptogram information of the shared master key.

The process center sends Handshake Completed message, that is, HMAC value calculated by the process center, to the terminal.

After receiving the HMAC, the terminal uses HMAC (P2 = 0x01) to command the terminal to verify the HMAC value generated after the handshake completion of the process center. Then USE HMAC (P2 = 0x00) to command to return the HMAC value generated after the handshake completion of the terminal. This command calculates the HMAC value in the same way as the process center generates the HMAC value, just changing the ASCII "SERVER" into "CLIENT".

The terminal sends Handshake Completed message, that is, the HMAC value calculated by the terminal, to the process center.

The terminal generates a session key through the HMAC (P2 = 0x02) command. This session key is only stored in the terminal. It is not allowed to be exported and needs to be regenerated in the case of power outage.

Figure D.1 -- Terminal Program Processing Flow

1) The cardholder starts online transaction.
2) A secure channel is established between the process center and the terminal.
3) The terminal determines the identity of the process center to which the terminal is connected, according to the content of the generic name in the DN domain of the trusted server certificate obtained in the establishment of the secure channel. In case of the trusted server certificate of the process center system A, ENTER the terminal application (business) process of the process center A. In case of the trusted server certificate of the process center system B, ENTER the terminal application (business) process of the process center B.
4) DETERMINE the implementation of the process center's terminal application (business) process (including the use of the corresponding process center's PIN encryption certificate for PIN encryption, reversal mechanism, display of information tips, etc.) according to Step 3).
5) The transaction process is completed, and the transaction is over.

D.2 Differences in terminal personalization

The terminal data and certificate system for the terminals supporting the dual process center are the same as the single process center terminal. However, there are differences in the number of certificates for terminal personalization. The differences between the number of personalized certificates are shown in Table D.2.

Table D.1 -- Number of Personalized Certificates

Terminal capability / Certificate type	Single process center terminal	Dual process center terminal
Terminal certificate	1	1
CA root certificate	1	1
PIN encryption certificate	1	2
Trusted server certificate	No need for personalization	No need for personalization

Note: The trusted server certificate is sent by the process center to the terminal for verification during the establishment of the secure channel.

END

This is an excerpt of the PDF (Some pages are marked off intentionally)

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