Collection and summary of CPU card-related data

One line of Java   Posted on 2016-06-12 17:18:52   Reading: 5.9k   Collection 14   Likes 4   copyright

Category Column: Mobile development   Article Tags: CPU card   14443 protocol   Ministry of Housing and Urban-Rural Development Card Specifications   Recharge your bus card

APDU command error code

The command replies with an error description
Commonly used commands and analysis

The command replies with an error description

- 6200 "Warning Information Not Provided"
- 6281 "Warning Loopback Data Possible"
- 6282 "WARNING File Length Less Than Le"
- 6283 "Warning: Invalid Selected File"
- 6284 "Warning FCI Format Not Specified by P2"
- 6300 "Warning Identification Failed"
- 63Cx "Warning Check Failed (x - Number of Retries Allowed)"
- 6400 "Status Flag Unchanged"
- 6581 "Memory Failure"
- 6700 "Wrong Length"
- 6882 "Security messages are not supported"
- 6981 "The command is incompatible with the file structure, the current file is not the required file"
- 6982 "Operating Condition (AC) Not Met, No PIN Check"
- 6983 "Your card has been locked"
- 6984 "Invalid random number, invalid data referenced"
- 6985 "Conditions of use not met"
- 6986 "Command execution conditions not met (not allowed commands, INS is wrong)"
- 6987 "MAC Lost"
- 6988 "INCORRECT MAC"
- 698D "Reserved"
- 6A80 "Incorrect Data Field Parameters"
- The "6A81" feature is not supported; Creation is not allowed; The directory is invalid; App Lock"
- 6A82 "The file was not found"
- 6A83 "This record was not found"
- 6A84 "Not Enough File Reserve"
- 6A86 "P1 or P2 is incorrect"
- 6A88 "Reference Data Not Found"
- 6B00 "Parameter Error"
- 6Cxx "Le length is wrong, actual length is xx"
- 6E00 "Unsupported Class: CLA Error"
- 6F00 "Invalid Data"
- 6F01 "Connection Interrupted"
- 6D00 "Unsupported Instruction Code"
- 9301 "Your Card Balance Is Insufficient"
- 9302 "MAC2 Error"
- 9303 "App is permanently locked"
- 9401 "Your Card Doesn't Have Enough Balance"

- 9402 "Transaction Counter Maximized"

- 9403 "Key index not supported"

- 9406 "REQUIRED MAC IS NOT AVAILABLE"

- 6900 "Unprocessable"

- 6901 "Order Not Accepted (Invalid Status)"

- 61xx "Normal, GET RESPONSE command is required" read command 00C00000xx

- 6600 "Received Communication Timeout"

- 6601 "Receive Character Parity"

- 6602 "Checksum is Incorrect"

- 6603 "WARNING No FCI for Current DF File"

- 6604 "WARNING No SF or KF under current DF"

- 6E81 "Card Left"

Commonly used commands and analysis

> The following is the CPU card recharge process

- **Select the master file**
  00a40000023f00 (the main file of the Ministry of Housing and Urban-Rural Development card is generally this instruction)

- **Read file 05 00b0850000**

  The response packet is as follows:

byte	Data objects	length	format	illustrate
01-02	Issuer code	2	BCD	
03-04	City code	2	BCD	
05-06	Industry code	2	BCD	
07-08	obligate	2	HEX	Different cities have different meanings, depending on the situation
09-16	Apply the serial number	8		2: City code BCD 1: Card master type BCD 1: Card subtype BCD 4: Issuance flow HEX
17	Card master type	1	BCD	
18	Card subtype	1	BCD	
19-22	Release date	4	BCD	YYYYMMDD
23-28	Issue device information	6	BCD	
29-30	App version number	2	BCD	

- **Select the file ID**
  00a40000023f01
  00a4000002df01
  00a4000002df04
  00a4040009a00000000386980701
  ....
  Depending on the city, the documents you are in may be different

- **Read file 15 00b0950000**

The response packet is as follows:

byte	Data objects	length	format	illustrate
1-2	Issuer code	2	BCD	
3-4	City code	2	BCD	
5-6	Industry code	2	BCD	
7-8	deposit	2	BCD	
9	App Type Identifier (Enabled Flag)	1	BCD	00: Not enabled
01	enable			
10	App version	1	BCD	
11-12	Connectivity Logo (Logo of Participating Cities)	2	BCD	
13-20	Apply the serial number	8	BCD	2: City code BCD 1: Card master type BCD 1: Card subtype BCD 4: Issuance flow HEX
21-24	The date the app was launched	4	BCD	YYYYMMDD is enabled when it is enabled
25-28	The app expiration date	4	BCD	YYYYMMDD is enabled when it is enabled
29	Card master type	1	BCD	
30	Card subtype	1	BCD	
31-34	Business bitmap data	4	HEX	

- **Read balance**
  805c000204

The response packet is as follows:

byte	Data objects	length	format	illustrate
01-04	balance	4	HEX	

- **E-wallet transaction history**
  00b2xxc400 (Document 18)
  00b2xxd400 (Document 1a)

> It can be read according to different card types in different cities

xx identifies the first few records
read 01: the first article
02: the second article
....
0a: Article 10

The response packet is as follows:

byte	Data objects	length	format	illustrate
01-02	E-wallet consumption, recharge transaction serial number	HEX	2	
03-05	Overdraft limits	HEX	3	

byte	Data objects	length	format	illustrate
06-09	The amount of the transaction	HEX	4	
10-10	The type of transaction	BCD	1	
11-16	The trading terminal number	BCD	6	
17-20	The date of the transaction	BCD	4	YYYYMMDD
21-23	Trading hours	BCD	3	HHMMSS

- **Verify the PIN**

  Command parsing:

data	description
CLA	00
INS	20
P1	00
P2	00
LC	The length of the PIN
PIN	PIN
LE	not

0020000003123456 9000
is considered a success

> It is important to note that the card only has 3 attempts, and if the PIN verification fails 3 times, the card will be locked The card in some cities needs to verify the PIN after the file is selected before the balance query and transaction record can be checked

- **Initialize a trapped-up transaction**

  Command parsing:

data	description
CLA	80
INS	50
P1	00
P2	01: ED Trap 02: EP Trap
LC	0B
DATA	See the table below
LE	10

DATA

data	Length (bytes)
Key index	1
The amount of the transaction	4
Terminal number	6

805000020B010000000111 2233445566

Response packets:

byte	Data objects	length	format	illustrate
01-04	ED or EP balance	4		
05-06	ED or EP online transaction serial number	2		
07	Key Version Number (DLK)	1		
08	Algorithm Identifier (DLK)	1		
09-12 Pseudo-random number (IC card)	4			
13-16	MAC1	4		

- Deposit Confirmation
  Command Format:

data	description
CLA	80
INS	52
P1	00
P2	00
LC	0B
DATA	See the table below
LE	04

DATA：

data	Length (bytes)
Transaction Date (Host)	4
Trading Hours (Host)	3
MAC2	4

Response packets:

byte	Data objects	length	format	illustrate
01-04	TAC	4		

The above instructions, various situations are for reference only, all need to be adjusted according to different cities and different cards, the Ministry of Housing and Urban-Rural Development's card specifications are the same, but because the cos in different cities are not the same, there will be some differences in operation, and adjustments need to be made as appropriate.