PBOCEMV Transaction Process Explained - Analysis of the data interaction between POS and cards

 Johndos Posted on 2016-11-10 14:29:56 Reading: 1.2k collection Likes

Category Column: PBOC/EMV

Symbol description:

RFU: reserved for use

Recently, in the debugging PBOC transaction, I came up with the idea of analyzing all the data interactions, in order to throw bricks and stones, hoping that there will be a high finger to correct the mistakes in this article, or the incomprehension of the place.
Without further ado, here's the start of the PBOC transaction:

Detect the insert, after checking the existence of the card:
(1): Select the payment environment pse:1PAY.SYS.DDF01
Select (SSELECT) packet,00 a4 xx (select by command) xx (first or only one)
a4##
[IC LEN: 20]
[00] [a4] [04] [00].
[0e] [31] [50] [41] [59] [2e] [53] [59] [53] [2e] [44] [44] [46] [30] [31] [00]
SELECT SEND END dd
qwe###

##
[GET LEN : 40]
[6f] [24]
[84] [0e] [31] [50] [41] [59] [2e] [53] [59] [53] [2e] [44] [44] [46] [30] [31]
[a5] [12]
[88] [01] [01]
[5f] [2d] [08] [7a] [68] [65] [6e] [66] [72] [64] [65]
[9f] [11] [01] [01]
[90] [00] SELECT GET END dd
##
Response to PSE Payment Environment
6F: FCI Template
84: DF Name
A5: FCI-specific template
88: SFI of the basic file in the directory (the upper three digits are 0, followed by 100 to read the file data)
5F2D: Preferred language
9F11: Issuer code
BF0C: Issuer Custom Data -- (The card does not carry this data)

FCI (File Control Information) contains SFI (Short File Identifier) and lists one app for each app in the directory.

--At this point, the PSE selection is complete. If the card's response to the selected payment environment is not 90 00, the POS will need to try to select AID

(2) one by one: Select a basic file associated with the PSE that lists the supported payment applications.
READ RECORD 00 b2 xx (record number) xx (indicates read record number)
b2##
[IC LEN: 5].
[00] [b2] [01] [0c] [00] SELECT SEND END dd
##

asd###
[GET LEN : 49]
[70] [2d]

[61] [2b]
[4f] [07] [a0] [00] [00] [03] [33] [01] [01]
[50] [0b] [50] [42] [4f] [43] [20] [43] [72] [65] [64] [69] [74]
[87] [01] [01]
[9f] [12] [0f] [43] [41] [52] [44] [20] [49] [4d] [41] [47] [45] [20] [30] [30] [30] [31]
[90] [00] SELECT GET END dd
##
card response: 70 xx (length) xx (record template)
70: Basic data template
61: Application template, which only exists if there is PSE, contains data objects related to the application directory entry.
4F: Application Identifier = RID + PIX (Application Provider and Proprietary Application Identifier)
50: Application label, EMV is required data for application selection, easy-to-remember data related to AID Here is PBOC Credit
87: Application Priority Indicator, If the card has more than one app, indicate the priority of the apps in the same directory.
bit8=》1: The application cannot be selected without the cardholder's confirmation; 0: No cardholder confirmation can be applied
bit7-bit5: RFU
bit4-bit10000: No priority is specified. :xxxx:1-15,1 has the highest priority
9f12: App Preferred Name Here: CARD IMAGE 0001

Once you have an AID, you should be selected into the AID list

Continue to read the next record of the file

b2## [IC len: 5]
[00] [b2] [02] [0c] [00] SELECT SEND END dd
##

asd###
[GET LEN : 2]
[6a] [83] SELECT GET END dd
##
until there are no records to read

(3): Add the AID list according to the application identifier of the read record, and then select the application according to the user button or select the application according to the priority.
a4##
[IC LEN : 13]
[00] [a4] [04] [00] [07] [a0] [00] [00] [03] [33] [01] [01] [00] SELECT SEND END dd
qwe###

###
[GET LEN : 48]
[6f] [2c]
[84] [07] [a0] [00] [00] [03] [33] [01] [01] [a5] [21] [87] [01] [01]

[9f] [38] [0c]
[9f] [1a] [02]
[9f] [7a] [01]
[9f] [02] [06]
[5f] [2a] [02]

[5f] [2d] [08] [7a] [68] [65] [6e] [66] [72] [64] [65]
[9f] [11] [01] [01]
[90] [00] SELECT GET END dd
##
-- Select the ADF response packet
6F: FCI profile
84: DF name
9F38: PDOL data (9F1A: terminal country code; 9F7A: Electronic Cash Indicator, 9F02: Authorized Amount, 5F2A: Transaction Currency Code)
5F2D: Preferred Language

9F11: Issuer Code Table Index

Make the final selection, ask the user to enter the amount, judgeWhether the POS can take the electronic cash transaction path indicates the electronic cash indicator.

(4): Get Processing Option (GPO) notifies the card transaction to begin. Package according to PDOL options.
Transmission of GPO instructions 80 a8 00 00 xx (length) 83 (PDOL tag) xx (PDOL length) xx xx (data)
a8##
[IC LEN: 19].
[80] [a8] [00] [00] [0d]
[83] [0b]

[01] [56]
[01]
[00] [00] [00] [00] [00] [09]
[01] [56]
[00] SELECT SEND END ss
###

###
[GET LEN : 18]
[80] [0e]
[58] [00]
[08] [01] [01] [00]
[10] [01] [04] [01]
[18] [01] [03] [00]
[90] [00] SELECT GET END ss
The response format for the ##
GPO includes: 80 xx (length) xx (application interaction characteristics) xx (AFL)
As above, the application interaction characteristics are: 58 00
Analysis:
bit8: RFU;
bit7:1=SDA support;
bit6:1=Support DDA;
bit5: 1=Support cardholder authentication
bit4: Perform endpoint risk management
bit3: Support issuer authentication
bit2: RFU
bit1: 1=CDA
bytes supported2: RFU

AFL (Application File Locator), each AFL includes 4 bytes
Byte 1: bit8-bit4: SFI (Short File Identifier)
bit3-bit1:
Byte 2: The record number of the first record to be read in the file (cannot be 0) Byte
3: The record number of the last record to be read in the file (greater than or equal to byte 2)
Byte 4: Start with the record of byte 2, Number of static data records (starting from 0, no more than (byte 3) - (byte 2) + 1)

Read the file based on the AFL returned by the GPO. The format of the read file number is as follows: SFI is shifted by 3 bits to the left, and 100 is added to the right.
For example, the above 08 hexadecimal is 0000 1000 bit8-bit4 is SFI, so the real is: 0000 0001, when reading the file, the right complement 0100 (indicatesRead the specified record) to get 0000 1100, which is the 0x0c. Similarly, the 02 file is: 0x14
b2##
[IC LEN: 5]
[00] [b2] [01] [0c] [00] SELECT SEND END dd
###

asd###

[GET LEN : 66]
[70] [3e]
[5f] [20] [0f] [46] [55] [4c] [4c] [20] [46] [55] [4e] [43] [54] [49] [4f] [4e] [41] [4c]
[57] [11] [62] [28] [00] [01] [00] [00] [11] [17] [d1] [01] [22] [01] [01] [23] [45] [67] [89] [9f] [1f] [16] [30] [31] [30] [32] [30] [33] [30] [34] [30] [35] [30] [36] [30] [37]
[30] [38] [30] [39] [30] [41] [30] [42]
[90] [00]
SELECT GET END dd
##
70: template
5f20: Cardholder Name: FULL FUNCTIONAL
57: Track Equivalence Data (including Master Account Separator Expiration Date Service Code PIN Verification Domain Custom Data If not even, Supplement
F
)
9F1F: Track One Custom Data

b2##
[IC LEN : 5]
[00] [b2] [01] [14] [00] SELECT SEND END dd
##

asd###
[GET LEN : 18]
[70] [0e]
[5a] [08] [62] [28] [00] [01] [00] [00] [11] [17]
[5f] [34] [01] [01]
[90] [00]
SELECT GET END dd
##
5a: Application Principal Account (PAN)
5F34: Application Principal Account (serial number of Application PAN)

b2
[IC LEN : 5]
[00] [b2] [02] [14] [00] SELECT SEND END dd
##

asd###
[GET LEN : 89]
[70] [55]
[8c] [1d] [9f] [34] [03] [9f] [02] [06] [9f] [03] [06] [9f] [1a] [02] [95] [05] [9b] [02] [5f] [2a] [02] [9a] [03] [9f] [21] [03] [9c] [01] [9f] [37] [04]
[8d] [1c] [8a] [02] [9f] [02] [06] [9f] [03] [06] [9f] [1a] [02] [95] [05] [9b] [02] [5f] [2a] [02] [9a] [03] [9f] [21] [03] [9c] [01] [9f] [37] [04]
[9f] [0e] [05] [00] [00] [00] [00] [00]
[9f] [0f] [05] [00] [00] [00] [00] [00]
[9f] [0d] [05] [00] [00] [00] [00] [00]
[90] [00] SELECT GET END dd
##
8C: Card Risk Management Data Object List 1 CDOL1
8D: Card Risk Management Data Object List 2 CDOL2
9F0E: Issuer Behavior Code - Reject
9F0F: Issuer Behavior Code - Online
9F0D: Issuer Behavior Code - Default

b2##
[IC LEN : 5]
[00] [b2] [03] [14] [00] SELECT SEND END dd
##

asd###
[GET LEN : 53]
[70] [31]
[5f] [25] [03] [95] [07] [01]

[5f] [24] [03] [10] [12] [31]
[5f] [28] [02] [01] [56]
[9f] [07] [02] [ff] [c0]
[9f] [08] [02] [00] [8c]
[8e] [0a] [00] [00] [00] [00] [00] [00] [00] [00] [1f] [00]
[5f] [30] [02] [02] [01]
[9f] [42] [02] [01] [56]
[90] [00] SELECT GET END dd
##
5F25: Application Effective Date
5F24: Application Expiration Date
5F28: Issuer Country Code
9F07: Application Usage Control
9F08: Application Version Number
8e: Cardholder Verification Method
5F30: Service code
9F42: Apply currency code

b2##
[IC LEN: 5].
[00] [b2] [04] [14] [00] SELECT SEND END dd
##

asd###
[GET LEN : 13]
[70] [09]
[9f] [74] [06] [45] [43] [43] [31] [31] [31]
[90] [00] SELECT GET END dd
##
9F74: Electronic cash issuer authorization code (electronic cash transactions
cannot be made without 9F74
).
b2##
[IC LEN : 5]
[00] [b2] [01] [1c] [00] SELECT SEND END dd
##

asd###
[GET LEN : 139]
[70] [81]
[86]
[8f] [01] [80]
[90] [81]
[80] [22] [91] [03] [a5] [e3] [12] [0f] [2d] [28] [62] [09] [11] [76] [aa] [2b] [d4] [e2] [4d] [69] [e7] [ee] [f7] [b9] [19] [5c] [91] [ea] [00] [88] [ae] [cf] [f4] [7e] [df] [a0] [be]
[ef] [7c] [39] [1d] [f3] [b0] [5f] [71] [7d] [cc] [06] [ff] [c8] [ee] [ff] [90] [ba] [14] [21] [2b] [8a] [52] [ad] [48] [b3] [32] [77] [b2] [e2] [30] [d4] [0b] [3e] [76] [dc] [59] [77]
[89] [26] [f1] [d8] [73] [9e] [10] [6c] [d7] [41] [de] [06] [a7] [42] [3d] [fb] [a2] [5e] [02] [f1] [2e] [54] [3d] [13] [d1] [b4] [71] [80] [65] [26] [02] [49] [81] [b7] [d2] [6b]
[4b] [f6] [e5] [55] [86] [04] [cc] [c2] [89] [f5] [9e] [8a] [80] [2f] [45] [fb] [3d] [9e] [67]
[90] [00] SELECT GET END dd
##
8F: Public key index
90: Issuer public key certificate -- used in Offline Data Authentication

b2##
[IC LEN: 5]
[00] [b2] [02] [1c].] [00] SELECT SEND END dd
##

asd###
[GET LEN : 46]
[70] [2a]
[9f] [32] [01] [03]

[92] [24] [8b] [64] [3d] [1e] [af] [2e] [a7] [84] [ac] [20] [53] [03] [c9] [0e] [74] [5e] [a2] [ef] [a5] [cb] [f0] [2c] [c4] [7d] [47] [83] [3b] [b7] [b2] [7e] [cc] [69] [62] [38] [5a] [4b]
[90] [00] SELECT GET END dd
##
9F32: issuer public key index
92: issuer public key remainder

b2##
[IC LEN : 5]
[00] [b2] [03] [1c] [00] SELECT SEND END dd
##

asd##
[GET LEN : 136]
[70] [81]
[83]
[93] [81]
[80] [33] [5d] [0c] [c2] [4c] [19] [70] [a2] [69] [bc] [a7] [9b] [d9] [2c] [ad] [12] [68] [35] [9d] [10] [5f] [af] [a1] [d0] [c5] [29] [46] [f3] [64] [5f] [bc] [d4] [6a] [45] [e6] [23] [a4] [37] [f6] [1e] [d7] [b4] [5d] [8f] [32] [42] [76] [7e] [69] [53] [4d] [ee] [7b] [a0] [35] [cd] [c0] [64] [9e] [14] [95] [cf] [7a] [13] [89] [03] [ae] [4f] [28] [05] [e5] [18] [b1] [12] [31] [88] [ed] [cc] [74] [52] [42] [e5] [f4] [c5] [2e] [e9] [34] [d9] [57] [df] [0d] [79] [e1] [4c] [c6] [12] [62] [7c] [ab] [bd] [f5] [fd] [1b] [a1] [a5] [dd] [23] [4e] [0e] [54] [0b] [59] [74] [91] [dd] [b5] [cb] [77] [50] [85] [61] [0d] [75] [83] [77] [a7] [fe] [c3]
[90] [00] SELECT GET END dd
##
93: Signed static application data - the record in the SDA

file has been read The

POS has checked that it can do electronic cash transactions and read the available balance value: 9F79
9F4F##
[IC LEN : 5]
[80] [ca] [9f] [79] [00] SELECT SEND END EE
##
##
[GET LEN : 11]
[9f] [79] [06] [00] [00] [00] [01] [00] [00] [90] [00] SELECT GET END EE
##

POS has been checked to be able to do electronic cash transactions, reading the reset threshold: 9F6D
9F4F##
[IC LEN : 5]
[80] [ca] [9f] [6d] [00] SELECT SEND END EE
##
##
[GET LEN : 11]
[9f] [6d] [06] [00] [00] [00] [00] [15] [00] [90] [00] SELECT GET END EE
##
If the available balance minus the authorized amount is less than the reset threshold, the POS will force the user to go online, requiring the user to enter the back office account.

At this point, the random number is obtained, the offline data authentication (SDA/DDA) is performed, the card number information is obtained, the usage control is performed, the expiration date is checked, the effective date is checked, the CVM is executed, the terminal risk management is performed, the card behavior is analyzed, and various bull checks are performed.

(5): Generate AC (get application ciphertext) 80 AE xx (control parameters) 00
AE##
[IC LEN : 43]
[80] [ae] [40] [00]
[25]
[3f] [00] [01]

[00] [00] [00] [00] [00] [09]
[00] [00] [00] [00] [00] [00]
[01] [56]
[00] [00] [80] [00] [00] [c0] [00]
[01] [56]
[10] [04] [10] [20] [19] [02] [00]
[b8] [4f] [ba] [07]
[00]
SELECT SEND END oo
##
control parameter 40: bit8, bit7 :00=AAC--Reject
01=TC--Offline
10=ARQC--Online
11=RFU
Data Source for Generating Redaction: Part 5 Appendix D: Authorization Amount
##
[GET LEN : 34]
[80] [1e]
[40]
[00] [01]
[df] [db] [ca] [78] [4f] [f1] [54] [66]
[07] --Length
[01] --Dispersed key index
[01] --Ciphertext version number
[03] [94] [00] [00] --Card verification result CVR
[01] -- Algorithm identification
[0a] [01] [00] [00] [00] [08] [00] [11] [22] [33] [44] --Custom Data
[90] [00]
SELECT GETOUT OF PAPER. END oo
####################OUT#
#
L:1) + Apply Transaction Counter (L:2) + Apply Redaction (L:8) + Issuer App Data