**常用tag**

95 TVR （Terminal Verification Results） 终端验证结果

9F 38 Processing Options Data Object List (PDOL) 处理选项数据对象列表（PDOL）

9F 37 Unpredictable Number 不可预测数

94 Application File Locator (AFL) 应用文件定位器（AFL）

57 Track 2 Equivalent Data 轨道2等效数据

9F 1F Track 1 Discretionary Data 轨道1自主数据

9F 49 Dynamic Data Authentication Data Object List (DDOL) 动态数据认证数据对象列表（DDOL）

5A Application Primary Account Number (PAN) 应用主帐户号码（PAN）

5F 34 Application PAN Sequence Number 应用泛序列号

8C Card Risk Management Data Object List 1 (CDOL1)卡风险管理数据对象列表1（CDOL1）

8D Card Risk Management Data Object List 2 (CDOL2)卡风险管理数据对象列表2（CDOL2）

8E Cardholder Verification Method (CVM) List 持卡人验证方法（CVM）列表

9F 0D Issuer Action Code - Default 发行人操作码 - 默认

9F 0E Issuer Action Code - Denial 发行人操作码 - 否认

9F 0F Issuer Action Code - Online 发行人操作码 - 在线

9F 27 Cryptogram Information Data (CID) 密码信息数据（CID）

9F 26 Application Cryptogram (AC) 请求密文

**卡片与终端交互过程**

**1.启动**

**1.1应用选择**

决定终端和卡片共同支持的的应用，两种选择方法

·PSE选择方法 >> PSE选择方法（1PAY.SYS.DDF01），从PSE入口搜索其下的文件树结构，找到所有应用

·应用列表选择方法 >> 终端按照支持的的应用列表逐个发动SELECT命令

最终从候选列表中选出执行交易的应用

·没有匹配的应用IC卡退出

·有一个匹配应用，会被选择

·有多个匹配应用 提升持卡人选择或选择优先级最高的应用

**1.2应用初始化**

功能：获取交易应用信息，即卡片支持的功能和交易数据存放的文件记录

根据终端的要求卡片作初步的判断

给卡片发送取处理选项（Get Processing Options)命令

需要给卡片的终端数据（PDOL '9F38')

发送请求数据的案列：

Request : 80 A8 00 00 3E 83 3C 00 00 00 00 00 00 00 00 00 00 00 00 08 40 00 00 00 00 00 08 40 17 09 27 00 F4 19 DA 69 22 E0 F8 C8 F0 00 F0 A0 01 00 00 00 8C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

数据分析：

Tag 9F 02: Transaction Amount : 00 00 00 00 00 00

Tag 9F 03: Cashback Amount : 00 00 00 00 00 00

Tag 9F 1A: Terminal Country Code : 08 40

Country Code = 08 40 国家代码

Country Name = United States 美国

Tag 95 : Terminal Verification Results (TVR) : 00 00 00 00 00

数据认证

Byte 1 bit 8 = 0 Offline data authentication was performed 离线数据认证

bit 7 = 0 SDA passed or not performed 静态数据认证

bit 6 = 0 No ICC data missing

bit 5 = 0 Card does not appear on terminal exception file

bit 4 = 0 DDA passed or not performed （DDA）数据认证

bit 3 = 0 CDA passed or not performed （CDA）复合动态数据认证

bit 2 = 0 SDA not selected

bit 1 = 0 RFU

Byte 2 bit 8 = 0 ICC and terminal do not have different application versions

bit 7 = 0 No Expired application

bit 6 = 0 Application effective

bit 5 = 0 Requested service allowed for card product

bit 4 = 0 No New card

Byte 3 bit 8 = 0 Cardholder verification was successful or not performed

bit 7 = 0 Recognised CVM

bit 6 = 0 PIN Try Limit not exceeded

bit 5 = 0 No PIN entry required (PIN pad may or may not be present or may or may not be working)

bit 4 = 0 No PIN entry required (PIN pad may or may not be present)

bit 3 = 0 No Online PIN entered

Byte 4 bit 8 = 0 Transaction does not exceed floor limit

bit 7 = 0 Lower consecutive offline limit not exceeded

bit 6 = 0 Upper consecutive offline limit not exceeded

bit 5 = 0 Transaction not selected randomly for online processing

bit 4 = 0 Merchant did not force transaction online

Byte 5 bit 8 = 0 No Default TDOL used

bit 7 = 0 Issuer authentication passed or not performed

bit 6 = 0 Script processing passed before final GENERATE AC or no script received

bit 5 = 0 Script processing passed after final GENERATE AC or no script received

Tag 5F 2A: Transaction Currency Code : 08 40

Code (num) = 08 40

Code (an) = USD

Currency = US Dollar

Tag 9A : Transaction Date : 17 09 27

Year : 2017

Month: September

Day : 27

Tag 9C : Transaction Type : 00

Purchase (of goods or services)

Tag 9F 35: Terminal Type : 22

Terminal Type: 22

Attended

Merchant

Offline with online capability

Tag 9F 33: Terminal Capabilities : E0 F8 C8

Byte 1 bit 8 = 1 Manual key entry is supported

bit 7 = 1 Magnetic stripe is supported

bit 6 = 1 IC with contacts is supported

Byte 2 bit 8 = 1 Plaintext PIN for ICC verification is supported

bit 7 = 1 Enciphered PIN for online verification is supported

bit 6 = 1 Signature (paper) is supported

bit 5 = 1 Enciphered PIN for offline verification is supported

bit 4 = 1 No CVM Required is supported

Byte 3 bit 8 = 1 SDA is supported

bit 7 = 1 DDA is supported

bit 6 = 0 Card capture is NOT supported

bit 4 = 1 CDA is supported

Tag 9F 40: Additional Terminal Capabilities : F0 00 F0 A0 01

Byte 1 bit 8 = 1 Cash supported

bit 7 = 1 Goods supported

bit 6 = 1 Services supported

bit 5 = 1 Cashback supported

bit 4 = 0 Inquiry NOT supported

bit 3 = 0 Transfer NOT supported

bit 2 = 0 Payment NOT supported

bit 1 = 0 Administrative NOT supported

Byte 2 bit 8 = 0 CashBack Deposit NOT supported

Byte 3 bit 8 = 1 Numeric keys supported

bit 7 = 1 Alphabetic and special characters keys supported

bit 6 = 1 Command keys supported

bit 5 = 1 Function keys supported

Byte 4 bit 8 = 1 Print, attendant supported

bit 7 = 0 Print, cardholder NOT supported

bit 6 = 1 Display, attendant supported

bit 5 = 0 Display, cardholder NOT supported

bit 2 = 0 Code table 10 NOT supported

bit 1 = 0 Code table 9 NOT supported

Byte 5 bit 8 = 0 Code table 8 NOT supported

bit 7 = 0 Code table 7 NOT supported

bit 6 = 0 Code table 6 NOT supported

bit 5 = 0 Code table 5 NOT supported

bit 4 = 0 Code table 4 NOT supported

bit 3 = 0 Code table 3 NOT supported

bit 2 = 0 Code table 2 NOT supported

bit 1 = 1 Code table 1 supported

Tag 5F 36: Transaction Currency Exponent : 00

Tag 9F 7A: VLP Terminal Support Indicator [VSDC] : 00

Tag 9F 09: Terminal Application Version Number : 00 8C

Tag 9F 15: Merchant Category Code : 00 00

Tag 9F 66: Terminal Transaction Qualifiers [qVSDC VCPS 2.0.2] : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

卡片返回AIP和应用文件定位器AFL，

举例发送指令：C0 80 0E 7C 00 08 01 01 00 10 01 03 00 18 01 02 01 90 00

Tag 80 : GPO Response Message Template Format 1

Tag 82 : Application Interchange Profile [VSDC] : 7C 00

Byte 1 bit 8 = 0 RFU

bit 7 = 1 Offline static data authentication is supported

bit 6 = 1 Offline dynamic data authentication is supported

bit 5 = 1 Cardholder verification is supported

bit 4 = 1 Terminal risk management is to be performed

bit 3 = 1 Issuer authentication is supported using the EXTERNAL AUTHENTICATE command

bit 1 = 0 Combined DDA / GENERATE AC NOT supported

Byte 2 bit 8 = 0 Mag-stripe mode is NOT supported

bit 7 = 0 NOT Mobile phone

Tag 94 : Application File Locator (AFL) : 08 01 01 00 10 01 03 00 18 01 02 01

AFL (1) = 08 01 01 00

SFI (decimal) = 1

Start record = 1

End record = 1

for offline data authentication = 0

AFL (2) = 10 01 03 00

SFI (decimal) = 2

Start record = 1

End record = 3

for offline data authentication = 0

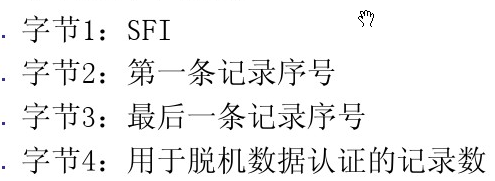
AFL (3) = 18 01 02 01

SFI (decimal) = 3

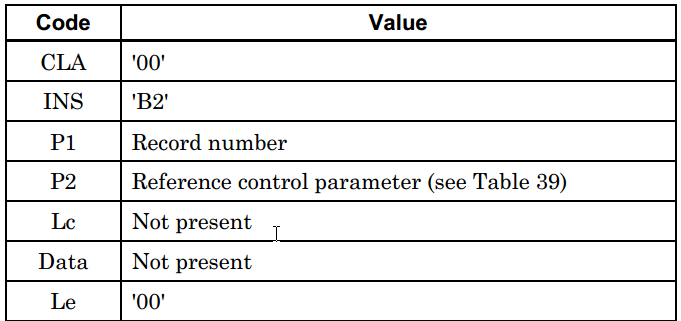
Start record = 1

End record = 2

for offline data authentication = 1



**1.3读取应用数据**



根据AFL发送 READ RECORD，读取对应数据信息

Request : 00 B2 01 0C 00

Response: B2 70 45 57 11 47 61 73 90 01 01 00 10 D2 21 22 01 11 43 84 44 89 5F 20 1A 56 49 53 41 20 41 43 51 55 49 52 45 52 20 54 45 53 54 2F 43 41 52 44 20 30 36 9F 1F 12 31 31 34 33 38 38 39 30 30 34 34 34 30 30 30 30 30 30 90 00

Tag 70 : Application Elementary File (AEF) Data Template

Tag 57 : Track 2 Equivalent Data : 47 61 73 90 01 01 00 10 D2 21 22 01 11 43 84 44 89

PAN = 4761739001010010

Separator field = D

Expiry Date (YY/MM) = 22/12

Service Code = 201

Discretionary Data = 1143844489

(may be padded with one 'F')

Tag 5F 20: Cardholder Name : 56 49 53 41 20 41 43 51 55 49 52 45 52 20 54 45 53 54 2F 43 41 52 44 20 30 36

Text value = VISA ACQUIRER TEST/CARD 06

Tag 9F 1F: Track 1 Discretionary Data : 31 31 34 33 38 38 39 30 30 34 34 34 30 30 30 30 30 30

Request : 00 B2 01 14 00

Response

Tag 70 : Application Elementary File (AEF) Data Template

Tag 90 : Issuer Public Key Certificate

Tag 8F : Certification Authority Public Key Index : 92

Tag 92 : Issuer Public Key Remainder : 50 DA 20 DD A8 95 3B 69 3F ED 84 36 68 31 BA 1E EA 97 F7 8F 79 2A CF 8C B9 8F DF 01 49 A7 B7 8F DA 1C 49 67

Tag 9F 32: Issuer Public Key Exponent : 03

Tag 9F 47: ICC Public Key Exponent : 03

Tag 9F 49: Dynamic Data Authentication Data Object List (DDOL) : 9F 37 04

Request : 00 B2 02 14 00

Response

Tag 70 : Application Elementary File (AEF) Data Template

Tag 9F 46: ICC Public Key Certificate

Tag 9F 69: Unknown Data Element : 01 00 00 00 00

Request : 00 B2 03 14 00

Response

Tag 93 : Signed Static Application Data

Request : 00 B2 01 1C 00

Response: B2 70 0E 5A 08 47 61 73 90 01 01 00 10 5F 34 01 01 90 00

Tag 5A : Application Primary Account Number (PAN) : 47 61 73 90 01 01 00 10

Tag 5F 34: Application PAN Sequence Number : 01

Request : 00 B2 02 1C 00

Response: B2 70 7D 5F 24 03 22 12 31 5F 25 03 09 07 01 5F 28 02 08 40 5F 30 02 02 01 8C 15 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04 8D 17 8A 02 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04 8E 0E 00 00 00 00 00 00 00 00 1E 03 02 03 1F 00 9F 07 02 FF 00 9F 08 02 00 8D 9F 0D 05 F0 40 00 88 00 9F 0E 05 00 10 00 00 00 9F 0F 05 F0 40 00 98 00 9F 42 02 08 40 90 00

Tag 5F 24: Application Expiration Date : 22 12 31

Year : 2022

Month: December

Day : 31

Tag 5F 25: Application Effective Date : 09 07 01

Year : 2009

Month: July

Day : 01

Tag 5F 28: Issuer Country Code : 08 40

Country Code = 08 40

Country Name = United States

Tag 5F 30: Service Code : 02 01

Position 1 (2): Interchange: International; Technology: ICC

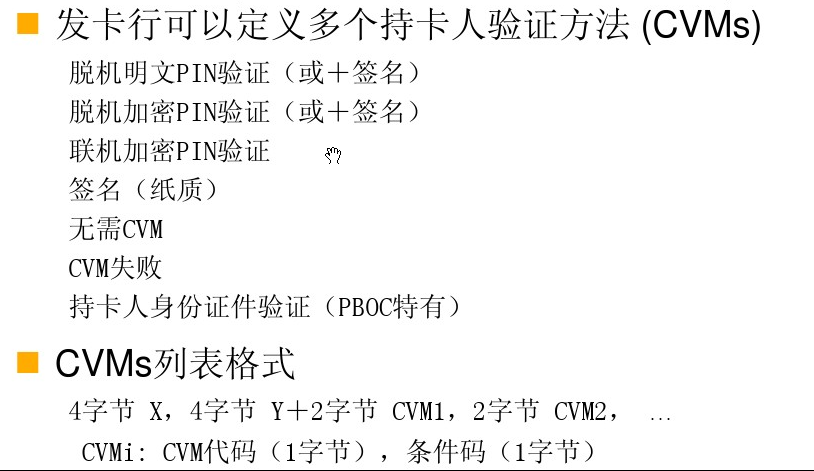
Position 2 (0): Authorization processing: Normal

Position 3 (1): Range of services: No restrictions; PIN requirements: -

Tag 8C : Card Risk Management Data Object List 1 (CDOL1) : 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04

Tag 8D : Card Risk Management Data Object List 2 (CDOL2) : 8A 02 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04

Tag 8E : Cardholder Verification Method (CVM) List : 00 00 00 00 00 00 00 00 1E 03 02 03 1F 00



Tag 9F 07: Application Usage Control : FF 00

Byte 1 bit 8 = 1 Valid for domestic cash transactions

bit 7 = 1 Valid for international cash transactions

bit 6 = 1 Valid for domestic goods

bit 5 = 1 Valid for international goods

bit 4 = 1 Valid for domestic services

bit 3 = 1 Valid for international services

bit 2 = 1 Valid at ATMs

bit 1 = 1 Valid at terminals other than ATMs

Byte 2 bit 8 = 0 Domestic cashback NOT allowed

bit 7 = 0 International cashback NOT allowed

Tag 9F 08: Application Version Number : 00 8D

Tag 9F 0D: Issuer Action Code - Default : F0 40 00 88 00

Byte 1 bit 8 = 1 Reject if unable to process online and if Offline data authentication was not performed

bit 7 = 1 Reject if unable to process online and if Offline static data authentication failed

bit 6 = 1 Reject if unable to process online and if ICC data missing

bit 5 = 1 Reject if unable to process online and if Card appears on terminal exception file

bit 4 = 0 Do not reject if unable to process online and if Offline dynamic data authentication failed

bit 3 = 0 Do not reject if unable to process online and if Combined DDA/AC Generation failed

bit 2 = 0 Do not reject if unable to process online and if SDA selected

Byte 2 bit 8 = 0 Do not reject if unable to process online and if ICC and terminal have different application versions

bit 7 = 1 Reject if unable to process online and if Expired application

bit 6 = 0 Do not reject if unable to process online and if Application not yet effective

bit 5 = 0 Do not reject if unable to process online and if Requested service not allowed for card product

bit 4 = 0 Do not reject if unable to process online and if New card

Byte 3 bit 8 = 0 Do not reject if unable to process online and if Cardholder verification was not successful

bit 7 = 0 Do not reject if unable to process online and if Unrecognised CVM

bit 6 = 0 Do not reject if unable to process online and if PIN Try Limit exceeded

bit 5 = 0 Do not reject if unable to process online and if PIN entry required and PIN pad not present or not working

bit 4 = 0 Do not reject if unable to process online and if PIN entry required, PIN pad present, but PIN was not entered

bit 3 = 0 Do not reject if unable to process online and if Online PIN entered

Byte 4 bit 8 = 1 Reject if unable to process online and if Transaction exceeds floor limit

bit 7 = 0 Do not reject if unable to process online and if Lower consecutive offline limit exceeded

bit 6 = 0 Do not reject if unable to process online and if Upper consecutive offline limit exceeded

bit 5 = 0 Do not reject if unable to process online and if Transaction selected randomly for online processing

bit 4 = 1 Reject if unable to process online and if Merchant forced transaction online

Byte 5 bit 8 = 0 Do not reject if unable to process online and if Default TDOL used

bit 7 = 0 Do not reject if unable to process online and if Issuer authentication was unsuccessful

bit 6 = 0 Do not reject if unable to process online and if Script processing failed before final GENERATE AC

bit 5 = 0 Do not reject if unable to process online and if Script processing failed after final GENERATE AC

Tag 9F 0E: Issuer Action Code - Denial : 00 10 00 00 00

Byte 1 bit 8 = 0 Do not decline if Offline data authentication was not performed

bit 7 = 0 Do not decline if Offline static data authentication failed

bit 6 = 0 Do not decline if ICC data missing

bit 5 = 0 Do not decline if Card appears on terminal exception file

bit 4 = 0 Do not decline if Offline dynamic data authentication failed

bit 3 = 0 Do not decline if Combined DDA/AC Generation failed

bit 2 = 0 Do not decline if SDA selected

Byte 2 bit 8 = 0 Do not decline if ICC and terminal have different application versions

bit 7 = 0 Do not decline if Expired application

bit 6 = 0 Do not decline if Application not yet effective

bit 5 = 1 Decline if Requested service not allowed for card product

bit 4 = 0 Do not decline if New card

Byte 3 bit 8 = 0 Do not decline if Cardholder verification was not successful

bit 7 = 0 Do not decline if Unrecognised CVM

bit 6 = 0 Do not decline if PIN Try Limit exceeded

bit 5 = 0 Do not decline if PIN entry required and PIN pad not present or not working

bit 4 = 0 Do not decline if PIN entry required, PIN pad present, but PIN was not entered

bit 3 = 0 Do not decline if Online PIN entered

Byte 4 bit 8 = 0 Do not decline if Transaction exceeds floor limit

bit 7 = 0 Do not decline if Lower consecutive offline limit exceeded

bit 6 = 0 Do not decline if Upper consecutive offline limit exceeded

bit 5 = 0 Do not decline if Transaction selected randomly for online processing

bit 4 = 0 Do not decline if Merchant forced transaction online

Byte 5 bit 8 = 0 Do not decline if Default TDOL used

bit 7 = 0 Do not decline if Issuer authentication was unsuccessful

bit 6 = 0 Do not decline if Script processing failed before final GENERATE AC

bit 5 = 0 Do not decline if Script processing failed after final GENERATE AC

Tag 9F 0F: Issuer Action Code - Online : F0 40 00 98 00

Byte 1 bit 8 = 1 Go online if Offline data authentication was not performed

bit 7 = 1 Go online if Offline static data authentication failed

bit 6 = 1 Go online if ICC data missing

bit 5 = 1 Go online if Card appears on terminal exception file

bit 4 = 0 Do not go online if Offline dynamic data authentication failed

bit 3 = 0 Do not go online if Combined DDA/AC Generation failed

bit 2 = 0 Do not go online if SDA selected

Byte 2 bit 8 = 0 Do not go online if ICC and terminal have different application versions

bit 7 = 1 Go online if Expired application

bit 6 = 0 Do not go online if Application not yet effective

bit 5 = 0 Do not go online if Requested service not allowed for card product

bit 4 = 0 Do not go online if New card

Byte 3 bit 8 = 0 Do not go online if Cardholder verification was not successful

bit 7 = 0 Do not go online if Unrecognised CVM

bit 6 = 0 Do not go online if PIN Try Limit exceeded

bit 5 = 0 Do not go online if PIN entry required and PIN pad not present or not working

bit 4 = 0 Do not go online if PIN entry required, PIN pad present, but PIN was not entered

bit 3 = 0 Do not go online if Online PIN entered

Byte 4 bit 8 = 1 Go online if Transaction exceeds floor limit

bit 7 = 0 Do not go online if Lower consecutive offline limit exceeded

bit 6 = 0 Do not go online if Upper consecutive offline limit exceeded

bit 5 = 1 Go online if Transaction selected randomly for online processing

bit 4 = 1 Go online if Merchant forced transaction online

Byte 5 bit 8 = 0 Do not go online if Default TDOL used

bit 7 = 0 Do not go online if Issuer authentication was unsuccessful

bit 6 = 0 Do not go online if Script processing failed before final GENERATE AC

bit 5 = 0 Do not go online if Script processing failed after final GENERATE AC

Tag 9F 42: Application Currency Code : 08 40

**2.数据认证**

内部认证：

Request : 00 88 00 00 04 F4 19 DA 69

采用DDA(动态数据认证)来验证IC卡本身的真伪和数据的正确性

ICC dynamic number: D5 14 E9 D0 6A CE F3 CE

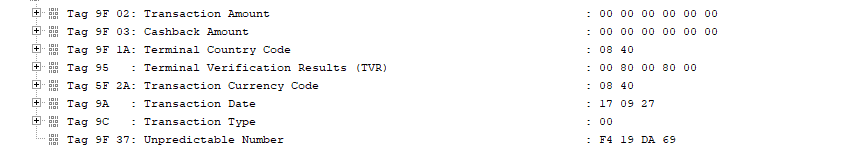
ICC private key: 85 35 90 12 28 07 9D 17 1D FC E0 3A CC 4B 8E 81 59 B6 D5 2D DD 09 3D 2B BE E6 07 8C B8 6E 7E 53 98 D7 EA D4 93 41 B4 3F 3A 5A C1 D0 E7 B3 CF B3 29 4B 84 97 12 13 80 1E 3F 92 EF FC A9 49 BD D6 DE 9E E0 48 D2 0F EC 65 15 44 79 9C 36 D9 41 C4 22 2D 0E F1 71 8F 92 77 53 D6 DA 95 66 0B 4F 7F 38 2F 0B 7D DA C0 5D 5F 13 D1 46 5E 96 4E 75 AB

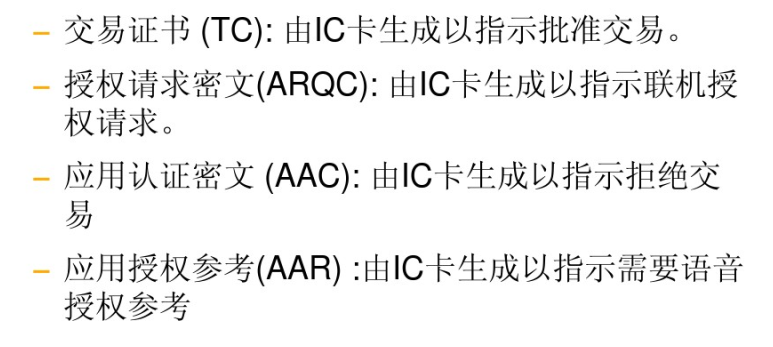
ICC public modulus: C7 D0 58 1B 3C 0B 6B A2 AC FB 50 58 32 71 55 C2 06 92 3F C4 CB 8D DB C1 9E 59 0B 53 14 A5 BD 7D 65 43 E0 3E DC E2 8E 5E D7 88 22 B9 5B 8D B7 8C BD F1 46 E2 9B 1D 40 2F 24 7F 80 61 CE 15 E5 61 15 8B 6D 54 56 70 FC A4 91 58 A6 32 1F E8 16 07 93 67 F3 4F 56 3C F0 6E 4B 16 E6 FE 38 16 49 26 D5 2F 2A 47 CE 7F 76 1C CB E8 1F 44 00 34 78 E9

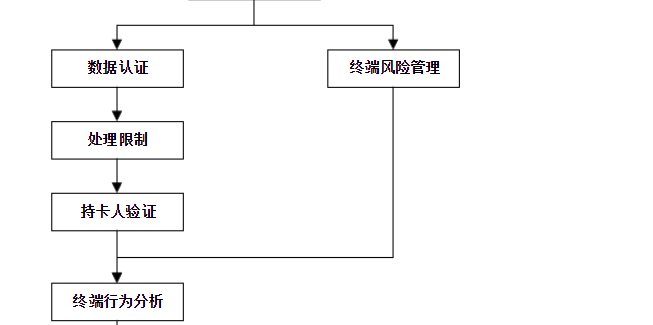
Terminal unpredictable number: F4 19 DA 69

（ARQC）

Request : 80 AE 80 00 1D 00 00 00 00 00 00 00 00 00 00 00 00 08 40 00 80 00 80 00 08 40 17 09 27 00 F4 19 DA 69







**3.终端行为分析**

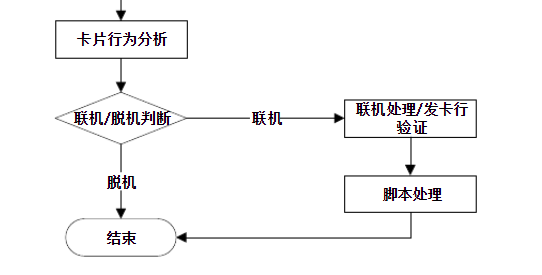
终端对脱机处理结果使用发卡行在卡片中设置的规则和支付系统在终端 中设置的规则来决定交易是接受、拒绝还是上送联机授权。

终端行为分析包括下面两个步骤：

步骤 1 ：检查脱机处理结果——终端通过检查脱机处理结果， 决定交易是联机上送、 接受脱机或 拒绝。这个处理过程中要考虑发卡行在卡片中定义的发卡行行为代码（ IAC ）以及终端中定 义的终端行为代码（ TAC）。

步 骤 2 ： 请 求 密 文 — — 终 端 请 求 卡 片 生 成 密 文 。 终端行为分析过程中做出的交易联机或接受并不是一个最终的结果。卡片进行卡片行为分 析处理时，卡片可能会推翻终端的决定。但是卡片不能推翻终端做出的交易拒绝的决定。

**4.卡片行为分析**



联机处理 联机处理允许发卡行使用发卡行主机系统中的风险管理参数对交易进行检查， 作出批准或拒绝交 易的决定。 除了执行传统的联机检查以外， 主机授权系统可以使用由卡片生成的动态密文执行联 机 卡 片 认 证 ， 并 且 在 作 出 授 权 决 定 时 可 以 考 虑 交 易 脱 机 处 理 的 结 果 。 发卡行的响应可以包括给卡片的二次发卡更新和一个发卡行生成的密文。 卡片验证密文确保响应 来自一个有效的发卡行。此验证叫发卡行认证。

交易结束 终端和卡片执行交易结束步骤决定交易处理结果。包括下列步骤：

——如果请求了联机处理但是终端不支持联机或者联机授权没有完成， 终端和卡片执行另外的风 险管理决定交易是接受还是拒绝；

——卡片可以根据发卡行认证的结果以及卡片内部的一些设置将一个发卡行作出的联机接受交 易改为拒绝；

——一些计数器和指示位要被设置用来记录交易过程中发生的各种情况；

——联机授权结束后，根据授权结果和卡片内部的一些设置，一些计数器和指示位复位。

联机授权请求，发送请求密文ARQC

联机授权响应，发送授权响应密文ARPC

结束

生成封装交易信息的密文

·批准 交易证书（TC)

·拒绝 应用认证密文 (AAC)