**Terminal Action Analysis**

The terminal has to decides either to proceed the transaction offline, to go online or to reject the transaction. The Terminal will send the decision with a Generate AC command to the card.

The decision is based on the Transaction Verification Results. There are several lists called Issuer Action Code (IAC) and Terminal Action Code (TAC) which give a directive to evaluate the TVR.

**Structure**

IAC, TAC and TVR have the same structure.

Source: [EMV Book 3](http://www.emvco.com/specifications.aspx?id=155)

Byte 1:

| **b8** | **b7** | **b6** | **b5** | **b4** | **b3** | **b2** | **b1** | **Meaning** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | x | x | x | x | x | x | x | Offline data authentication was not performed |
| x | 1 | x | x | x | x | x | x | SDA failed |
| x | x | 1 | x | x | x | x | x | ICC data missing |
| x | x | x | 1 | x | x | x | x | Card appears on terminal exception file |
| x | x | x | x | 1 | x | x | x | DDA failed |
| x | x | x | x | x | 1 | x | x | CDA failed |
| x | x | x | x | x | x | 0 | x | RFU |
| x | x | x | x | x | x | x | 0 | RFU |

Byte 2:

| **b8** | **b7** | **b6** | **b5** | **b4** | **b3** | **b2** | **b1** | **Meaning** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | x | x | x | x | x | x | x | ICC and terminal have different applicatioin versions |
| x | 1 | x | x | x | x | x | x | Expired application |
| x | x | 1 | x | x | x | x | x | Application not yet effective |
| x | x | x | 1 | x | x | x | x | Requested service not allowed for card product |
| x | x | x | x | 1 | x | x | x | New Card |
| x | x | x | x | x | 0 | x | x | RFU |
| x | x | x | x | x | x | 0 | x | RFU |
| x | x | x | x | x | x | x | 0 | RFU |

Byte 3:

| **b8** | **b7** | **b6** | **b5** | **b4** | **b3** | **b2** | **b1** | **Meaning** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | x | x | x | x | x | x | x | Cardholder verification was not successful |
| x | 1 | x | x | x | x | x | x | Unrecognised CVM |
| x | x | 1 | x | x | x | x | x | PIN Try Limit exceeded |
| x | x | x | 1 | x | x | x | x | PIN entry required and PIN pad not present or not working |
| x | x | x | x | 1 | x | x | x | PIN entry required, PIN pad present, but PIN was not entered |
| x | x | x | x | x | 1 | x | x | Online PIN entered |
| x | x | x | x | x | x | 0 | x | RFU |
| x | x | x | x | x | x | x | 0 | RFU |

Byte 4:

| **b8** | **b7** | **b6** | **b5** | **b4** | **b3** | **b2** | **b1** | **Meaning** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | x | x | x | x | x | x | x | Transaction exceeds floor limit |
| x | 1 | x | x | x | x | x | x | Lower consecutive offline limit exceeded |
| x | x | 1 | x | x | x | x | x | Upper consecutive offline limit exceeded |
| x | x | x | 1 | x | x | x | x | Transaction selected randomly for online processing |
| x | x | x | x | 1 | x | x | x | Merchant forced transaction online |
| x | x | x | x | x | 0 | x | x | RFU |
| x | x | x | x | x | x | 0 | x | RFU |
| x | x | x | x | x | x | x | 0 | RFU |

Byte 5:

| **b8** | **b7** | **b6** | **b5** | **b4** | **b3** | **b2** | **b1** | **Meaning** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | x | x | x | x | x | x | x | Default TDOL used |
| x | 1 | x | x | x | x | x | x | Issuer authentication failed |
| x | x | 1 | x | x | x | x | x | Script processing failed before final GENERATE AC |
| x | x | x | 0 | x | x | x | x | RFU |
| x | x | x | x | 0 | x | x | x | RFU |
| x | x | x | x | x | 0 | x | x | RFU |
| x | x | x | x | x | x | 0 | x | RFU |
| x | x | x | x | x | x | x | 0 | RFU |

**Issuer Action Code - Online, Denial, Default**

There are three kinds of every IAC/TAC list: Online, Denial and Default.

**IAC - Online**

This specifies the issuer's conditions to approve a transaction online.

Example:

Issuer Action Code - Online: FC68BC9800

Byte 1:

Offline data authentication was not performed (b8)

SDA failed (b7)

ICC data missing (b6)

Card appears on terminal exception file (b5)

DDA failed (b4)

CDA failed (b3)

Byte 2:

Expired application (b7)

Application not yet effective (b6)

New card (b4)

Byte 3:

Cardholder verification was not successful (b8)

PIN Try Limit exceeded (b6)

PIN entry required and PIN pad not present or not working (b5)

PIN entry required, PIN pad present, but PIN was not entered (b4)

Online PIN entered (b3)

Byte 4:

Transaction exceeds floor limit (b8)

Transaction selected randomly for online processing (b5)

Merchant forced transaction online (b4)

Byte 5:

TVR byte two b7 is set to 1 (New Card). This match with byte two b7 from the Issuer Action Code - Online.  
As a Result of this the Terminal will decide to proceed the transaction online.

**IAC - Denial**

This specifies the issuer's conditions to reject a transaction.

Example:

Issuer Action Code - Denial: 0010180000

Byte 1:

Byte 2:

Requested service not allowed for card product (b5)

Byte 3:

PIN entry required and PIN pad not present or not working (b5)

PIN entry required, PIN pad present, but PIN was not entered (b4)

Byte 4:

Byte 5:

The transaction will be rejected, if byte three b5 is set to 1 in the TVR and IAC.

**IAC - Default**

If the Terminal has no online ability, the IAC - Default list specifies the issuers's conditions to reject a transaction.

Example:

Issuer Action Code - Default: FC40AC8000

Byte 1:

Offline data authentication was not performed (b8)

SDA failed (b7)

ICC data missing (b6)

Card appears on terminal exception file (b5)

DDA failed (b4)

CDA failed (b3)

Byte 2:

Expired application (b7)

Byte 3:

Cardholder verification was not successful (b8)

PIN Try Limit exceeded (b6)

PIN entry required, PIN pad present, but PIN was not entered (b4)

Online PIN entered (b3)

Byte 4:

Transaction exceeds floor limit (b8)

Byte 5:

If TVR and IAC both have byte four b8 set to 1 the transaction will be rejected.

**Terminal Action Code - Online, Denial, Default**

The TAC specifies the terminal's conditions. It is similar to the IAC.

**Generate AC**

If the terminal made an decision, it will send with a Generate AC command to the card. Depending on the decision, the terminal requires different Application Cryptograms from the card.

Source: [EMV Book 3](http://www.emvco.com/specifications.aspx?id=155)

|  |  |  |
| --- | --- | --- |
| **Type** | **Abbrevation** | **Meaning** |
| Application Authentication Cryptogram | AAC | Transaction declined |
| Application Authorisation Referral | AAR | Referral requested by the card |
| Authorisation Request Cryptogram | ARQC | Online authorisation requested |
| Transaction Certificate | TC | Transaction approved |

The Command Message has the following structure:

|  |  |
| --- | --- |
| **Code** | **Value** |
| CLA | '80' |
| INS | 'AE' |
| P1 | Reference control parameter (see table below) |
| P2 | '00' |
| Lc | Var. |
| Data | Transaction-related data |
| Le | '00' |

Coding of P1:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **b8** | **b7** | **b6** | **b5** | **b4** | **b3** | **b2** | **b1** | **Meaning** |
| 0 | 0 |  |  |  |  |  |  | AAC |
| 0 | 1 |  |  |  |  |  |  | TC |
| 1 | 0 |  |  |  |  |  |  | ARQC |
| 1 | 1 |  |  |  |  |  |  | RFU |
|  |  | x |  |  |  |  |  | RFU |
|  |  |  | 0 |  |  |  |  | CDA signature not requested |
|  |  |  | 1 |  |  |  |  | CDA signature requested |
|  |  |  |  | x | x | x | x | RFU |

The transaction-related data is depending on a Card Risk Management Data Objetct List 1(CDOL1).  
This CDOL is given by the card. It contains the tagname and length of the expected data.

**Example**

Card Risk Management Data Object List 1 (CDOL1):

9F02069F030695055F2A029A039C019F37049F4C089F4502

// Tag - Length - Meaning

9f02 - 06 - Authorised amount of the transaction (excluding adjustments)

9f03 - 06 - Secondary amount associated with the transaction representing a cashback

amount

95 - 05 - Terminal Verification Results

5f2a - 02 - Transaction Currency Code

9a - 03 - Transaction Date

9c - 01 - Transaction Type

9f37 - 04 - Unpredictable Number

9f4c - 08 - ICC Dynamic Number

9f45 - 02 - Data Authentication Code

First we create an ByteString which corresponds to the CDOL1 above.  
To obtain the ICC Dynamic Number we send a Get Challenge command to the card. The card will return an 8-byte unpredictable number.

var authorisedAmount = new ByteString("000000000001", HEX);

var secondaryAmount = new ByteString("000000000000", HEX);

var tvr = new ByteString("0000000000", HEX);

var transCurrencyCode = new ByteString("0978", HEX);

var transDate = new ByteString("090730", HEX);

var transType = new ByteString("21", HEX);

var unpredictableNumber = crypto.generateRandom(4);

var iccDynamicNumber = card.sendApdu(0x00, 0x84, 0x00, 0x00, 0x00);

var DataAuthCode = e.cardDE[0x9F45];

var Data = authorisedAmount.concat(secondaryAmount).concat(tvr)

.concat(transCurrencyCode).concat(transDate)

.concat(transType).concat(unpredictableNumber)

.concat(iccDynamicNumber).concat(DataAuthCode);

Then we set P1 to '40', to request an Transaction Certificate (offline transaction) and execute the Generate AC command.

var p1 = 0x40;

var generateAC = card.sendApdu(0x80, 0xAE, p1, 0x00, Data, 0x00);

The Generate AC command was succesful if the card returns SW1/SW2=9000.

96 C: 00 84 00 00 - GET CHALLENGE Le=0

R: SW1/SW2=9000 (Normal processing: No error) Lr=8

0000 8D 51 F4 6C 9F 40 5F 71 .Q.l.@\_q

96 C: 80 AE 40 00 - UNKNOWN\_INS Lc=37

0005 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 ................

0015 00 09 78 09 07 30 21 2C 76 4F 65 8D 51 F4 6C 9F ..x..0!,vOe.Q.l.

0025 40 5F 71 D1 79 @\_q.y

Le=0

R: SW1/SW2=9000 (Normal processing: No error) Lr=32

0000 77 1E 9F 27 01 80 9F 36 02 02 13 9F 26 08 2D F3 w..'...6....&.-.

0010 83 3C 61 85 5B EA 9F 10 07 06 84 23 00 31 02 08 .<a.[......#.1..