EMV mode: TTQ-driven kernels

Processing Restrictions, ODA and CVM

Practical exercises

1. Looking at Trace 01 (in file “01-06. Processing Restrictions, ODA and CVM - Trace 01.txt”):
   a. What application was selected in this transaction?

      _____

   b. What is the card decision on the outcome of the transaction?

      _____

   c. What is the transaction date?

      _____

   d. What is the application expiration date?

      _____

Consider the coding of tag 9F6C (Card Transaction Qualifiers), from EMV Book C-3:

Byte 1

- bit 8: 1 = Online PIN Required
- bit 7: 1 = Signature Required
- bit 6: 1 = Go Online if Offline Data Authentication Fails and Reader is online capable.
- Bit 5: 1 = Switch Interface if Offline Data Authentication fails and Reader supports contact chip.
- Bit 4: 1 = Go Online if Application Expired
- bit 3: 1 = Switch Interface for Cash Transactions
- bit 2: 1 = Switch Interface for Cashback Transactions
- bit 1: RFU (0)

Byte 2

- bit 8: 1 = Consumer Device CVM Performed
- bit 7: 1 = Card supports Issuer Update Processing at the POS
- bits 6-1: RFU (0,0,0,0,0,0)

e. Should you expect this transaction to be approved offline?

_____

2. Now looking at Trace 02 (in file "01-06. Processing Restrictions, ODA and CVM - Trace 02.txt"):

   a. What application was selected in this transaction?

   _____

   b. What is the card decision on the outcome of the transaction?

   _____

   c. What should you expect that the actual outcome be if fDDA fails?

   _____

3. Still looking at Trace 02 (in file "01-06. Processing Restrictions, ODA and CVM – Trace 02.txt").

Consider the coding of tag 9F66 (Terminal Transaction Qualifiers), from EMV Book C-3:

Byte 1
- bit 8: 1 = Mag-stripe mode supported
- bit 7: RFU (0)
- bit 6: 1 = EMV mode supported
- bit 5: 1 = EMV contact chip supported
- bit 4: 1 = Offline-only reader
- bit 3: 1 = Online PIN supported
- bit 2: 1 = Signature supported
- bit 1: 1 = Offline Data Authentication for Online Authorizations supported.

Byte 2
- bit 8: 1 = Online cryptogram required
- bit 7: 1 = CVM required
- bit 6: 1 = (Contact Chip) Offline PIN supported
- bits 5-1: RFU (0,0,0,0,0)

Byte 3
- bit 8: 1 = Issuer Update Processing supported
- bit 7: 1 = Consumer Device CVM supported
- bits 6-1: RFU (0,0,0,0,0,0)

Byte 4
- RFU (0,0,0,0,0,0,0,0)

a. What CVM method does the reader indicate is supported?

_____

b. Does the terminal require that the cardholder be verified?

_____

c. What CVM does the card require that the terminal process?

_____

4. Now looking at Trace 03 (in file "01-06. Processing Restrictions, ODA and CVM - Trace 03.txt"):

   a. What application was selected in this transaction?

   _____

   b. What is the card decision on the outcome of the transaction?

   _____

   Consider the coding of tag 9F71 (Card Processing Requirements), from EMV Book C-6:

BYTE 1: Transient Data		
Bit	**Value**	**Meaning**
b8	1	Online PIN required
b7	1	Signature required
b6	1	RFU
b5	1	Consumer Device CVM Performed
b4	0	RFU
b3	0	RFU
b2	0	RFU
b1	0	RFU

BYTE 2: Permanent Data		
Bit	**Value**	**Meaning**
b8	1	Switch other interface if unable to process online
b7	1	Process online if CDA failed
b6	1	Decline/switch to other interface if CDA failed
b5	1	Issuer Update Processing supported
b4	1	Process online if card expired
b3	1	Decline if card expired
b2	1	CVM Fallback to Signature allowed
b1	1	CVM Fallback to No CVM allowed

   c. What should you expect that the actual outcome be if CDA fails?

   _____

5. Now looking at Trace 04 (in file “01-06. Processing Restrictions, ODA and CVM - Trace 04.txt”):

   a. What application was selected in this transaction?

      _____

   b. What is the card decision on the outcome of the transaction?

      _____

   c. What CVM method does the reader indicate is supported?

      _____

   d. Does the terminal require that the cardholder be verified?

      _____

   e. What CVM does the card require that the terminal process?

      _____

6. Now looking at Trace 05 (in file “01-06. Processing Restrictions, ODA and CVM - Trace 05.txt”):

   a. What application was selected in this transaction?

      _____

   b. What is the card decision on the outcome of the transaction?

      _____

   c. What is the transaction date?

      _____

   d. What is the application expiration date?

      _____

   e. What should the reader do about this?

      _____

7. Now looking at Trace 06 (in file "01-06. Processing Restrictions, ODA and CVM - Trace 06.txt"):

   a. What application was selected in this transaction?

   _____

   b. What is the card decision on the outcome of the transaction?

   _____

   c. What is the value given by the reader to the card for the transaction type?

   _____

   This value means 'Purchase with cashback'.

   d. In what country does the transaction take place?

   (Codes for ISO 3166 can be found at https://en.wikipedia.org/wiki/ISO_3166-1_numeric)

   _____

   e. In what country was the card issued?

   _____

Consider the coding of the Application Usage Control tag from EMV Book3:

Application Usage Control Byte 1 (Leftmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Valid for domestic cash transactions
x	1	x	x	x	x	x	x	Valid for international cash transactions
x	x	1	x	x	x	x	x	Valid for domestic goods
x	x	x	1	x	x	x	x	Valid for international goods
x	x	x	x	1	x	x	x	Valid for domestic services
x	x	x	x	x	1	x	x	Valid for international services
x	x	x	x	x	x	1	x	Valid at ATMs
x	x	x	x	x	x	x	1	Valid at terminals other than ATMs

Application Usage Control Byte 2 (Rightmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Domestic cashback allowed
x	1	x	x	x	x	x	x	International cashback allowed
x	x	0	x	x	x	x	x	RFU
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

   f. Will this transaction be accepted by the reader?

   _____

Answers

1.a. A VISA application with AID "A0000000031010" was selected. This tells us that Kernel 3 is activated.

1.b. The CID has value 40 (from the GPO response, tag 9F27). The card approved the transaction offline.

1.c. From the PDOL (tag 9F38 from SELECT) and the data passed to GPO, we can associate value 181206 to tag 9A. The transaction date is December 6th, 2018.

1.d. From tag 5F24, the application expiration date is December 31st, 2017. You could also get the information from tag 57. The application is expired.

1.e. The CTQ has value 6840 (from tag 9F6C). Byte 1 bit 4 = 1, so the reader will force the transaction online, because it is expired.

2.a. A VISA application with AID "A0000000031010" was selected. This tells us that Kernel 3 is activated.

2.b. The CID has value 40 (from the GPO response, tag 9F27). The card approved the transaction offline.

2.c. The CTQ has value 6840 (from tag 9F6C). Byte 1 bit 6 = 1, so the reader will force the transaction online if fDDA fails.

3.a. From the PDOL (tag 9F38 from SELECT) and the data passed to GPO, we can associate value B2004000 to tag 9F66 (TTQ). In terms of CVM, this means:

Byte 1 bit 3 = 0 – Online PIN not supported

Byte 1 bit 2 = 1 – Signature supported

Byte 3 bit 7 = 1 – Consumer Device CVM supported

3.b. Still from the TTQ, Byte 2 bit 7 = 0, so the reader does NOT require that the cardholder be verified for this transaction.

3.c. The CTQ has value 6840 (from tag 9F6C). In terms of CVM, this means:

Byte 1 bit 8 = 0 – Online PIN not required

Byte 1 bit 7 = 1 – Signature required

The card therefore requires that the terminal processes the signature CVM.

4.a. A Discover or Diners Club application with AID "A0000001523010" was selected. This tells us that Kernel 6 is activated.

4.b. The CID has value 40 (from the GPO response, tag 9F27). The card approved the transaction offline.

4.c. The CPR has value 40BB (from tag 9F71).

Byte 2 bit 7 = 0, so the reader will NOT force the transaction online if CDA fails.

Byte 2 bit 6 = 1, so the reader will switch to the contact interface if CDA fails. If it isn't possible to switch to the contact interface, the reader will decline the transaction.

5.a. A Discover or Diners Club application with AID "A0000001523010" was selected. This tells us that Kernel 6 is activated.

5.b. The CID has value 80 (from the GPO response, tag 9F27). The card is requesting that the transaction be sent online for authorisation.

5.c. From the PDOL (tag 9F38 from SELECT) and the data passed to GPO, we can associate value B6808000 to tag 9F66 (TTQ). In terms of CVM, this means:

Byte 1 bit 1 = 1 – Online PIN supported

Byte 1 bit 2 = 1 – Signature supported

Byte 3 bit 7 = 0 – Consumer Device CVM is NOT supported

5.d. Still from the TTQ, Byte 2 bit 7 = 0, so the reader does NOT require that the cardholder be verified for this transaction.

5.e. The CPR has value 807F (from tag 9F71). In terms of CVM, this means:

Byte 1 bit 8 = 1 – Online PIN required

Byte 1 bit 7 = 0 – Signature not required

The card therefore requires that the terminal processes online PIN verification.

6.a. A Discover or Diners Club application with AID "A0000001523010" was selected. This tells us that Kernel 6 is activated.

6.b. The CID has value 80 (from the GPO response, tag 9F27). The card is requesting that the transaction be sent online for authorisation.

6.c. From the PDOL (tag 9F38 from SELECT) and the data passed to GPO, we can associate value 181127 to tag 9A. The transaction date is November 27th, 2018.

6.d. From tag 57, the application expiration date is December 31st, 2015. The application is expired.

6.e. The CPR has value 00B7 (from tag 9F71). In terms of expired application:

Byte 2 bit 4 = 0 – The reader will not force the transaction online

Byte 2 bit 3 = 1 – The reader will decline the transaction

7.a. A Discover or Diners Club application with AID "A0000001523010" was selected. This tells us that Kernel 6 is activated.

7.b. The CID has value 40 (from the GPO response, tag 9F27). The card approved the transaction offline.

7.c. From the PDOL (tag 9F38 from SELECT) and the data passed to GPO, we can associate value 09 to tag 9C. This is a purchase with cashback.

7.d. From the PDOL (tag 9F38 from SELECT) and the data passed to GPO, we can associate value 0372 to tag 9F1A. The transaction takes place in Ireland.

7.e. From tag 5F28 in the records, the card was issued in the USA. This is an international transaction.

7.f. From tag 9F07 in the records, the Application Usage Control has value FF80. Looking at the second byte, domestic cashback is allowed, but international cashback isn't.

The reader will therefore decline the transaction.