Partie Irek Tobor

10 points

1. Questions du cours (hardware)

1. Pourquoi on dit qu'une carte ISO communique un mode « half-duplex » ?
2. Quelle est la différence entre un « Cold Reset » et « Warm Reset » ? Quelles sont les conséquences sur le contenu des mémoire(s) ?

2. Contraintes sur le champ INS

Il s'agit ici d'analyser l'aspect bas niveau de la communication utilisant le protocole T=0

Extraits de spécifications nécessaires (ISO 7816-3 et ISO 7816-4) :

- ISO 7816-4
  - INS indicates the command to process. Due to specifications in ISO/IEC 7816-3, the values '6X' and '9X' are invalid.
  - SW1-SW2 indicates the processing state. Due to specifications in ISO/IEC 7816-3, any value different from '6XXX' and '9XXX' is invalid ; any value '60XX' is also invalid.
- ISO 7816-3
  - The interface device initiates every command by transmitting a five-byte header that tells the card what to do. The command processing continues with the transfer of a variable number of data bytes in one direction under the control of *procedure byte* (see below) transmitted by the card.
  - The header consists of five bytes denoted CLA, INS, P1, P2 and P3. The values of CLA, INS, P1 and P2 shall be as specified in ISO/IEC 7816-4. P3 encodes the number of data bytes to be transferred during the command.
  - After transmitting the header as a string of five characters, the interface device shall wait for a character conveying a *procedure byte*.
    - If the value is '60', it is a NULL byte. It requests no action on data transfer. The interface device shall wait for a character conveying a procedure byte.
    - If the value is '6X' or '9X', it is a SW1 byte. It requests no action on data transfer. The interface device shall wait for a character conveying a SW2 byte. There is no restriction on SW2 value
    - If the value is the value of INS, [...], it is an ACK byte. All remaining data bytes if any bytes remain shall be transferred subsequently. Then the interface device shall wait for a character conveying a procedure byte.

Questions :

1. Pourquoi le champ INS d'une commande APDU doit être différent de 6X et 9X ?
2. Quels pourraient être les problèmes liées à la direction de communication de la ligne IO si cette contrainte n'est pas respectée ?

3. Analyse de log d'une transaction bancaire

Contexte :

- Deux lecteurs différents,
- Même carte, (même application bancaire, même personnalisation),
- Même code du côté de PC (Terminal).

Log :

- Lecteur 1

```
[connection] -- Trying OMNIKEY CardMan 5x21 0 using T0|T1 protocol
[connection] -- Connected to OMNIKEY CardMan 5x21 0 using T0 protocol
[connection] -- Cold Reset
ATR:   3b 65 00 00 20 63 cb a3 20

Send:  00 a4 04 00 05
       a0 00 00 00 42
Resp:  61 31

Send:  00 c0 00 00 31
Resp:  6f 2f 84 07 a0 00 00 00 42 10 10 a5 24 50 02 43
       42 87 01 01 9f 11 01 01 9f 12 02 43 42 5f 2d 04
       66 72 65 6e bf 0c 0a df 60 02 0b 28 9f 4d 02 0b
       28 90 00

Send:  80 a8 00 00 02
       83 00
Resp:  61 18

Send:  00 c0 00 00 18
Resp:  77 16 82 02 39 00 94 10 10 02 03 01 18 01 01 00
       20 01 01 00 28 01 01 00 90 00

Send:  00 b2 02 14 00
Resp:  6c 9b

Send:  00 b2 02 14 9b
Resp:  70 81 98 57 13 51 31 62 33 75 72 68 41 d1 61 02
       01 60 06 78 64 56 02 9f 5f 25 03 13 10 01 5f 24
       03 16 10 31 5a 08 51 31 62 33 75 72 68 41 5f 34
       01 00 9f 07 02 ff 00 8e 10 00 00 00 00 00 00 00
       00 42 01 44 03 01 03 02 03 9f 0d 05 bc 60 ac 00
       00 9f 0e 05 00 10 50 00 00 9f 0f 05 bc 60 ac 88
       00 5f 28 02 07 24 8c 21 9f 02 06 9f 03 06 9f 1a
       02 95 05 5f 2a 02 9a 03 9c 01 9f 37 04 9f 35 01
       9f 45 02 9f 4c 08 9f 34 03 8d 0c 91 0a 8a 02 95
       05 9f 37 04 9f 4c 08 9f 4a 01 82 90 00

Send:  00 b2 03 14 00
Resp:  6c 45

Send:  00 b2 03 14 45
Resp:  70 43 5f 20 1a 54 4f 42 4f 52 2f 49 52 45 4e 45
       55 53 5a 2e 4d 52 20 20 20 20 20 20 20 20 20 9f
       1f 18 30 30 30 30 30 30 30 30 30 30 30 30 30 30
       30 36 34 35 30 30 30 30 30 30 9f 08 02 00 02 9f
       49 03 9f 37 04 90 00

Send:  00 b2 01 1c 00
Resp:  6c c3

Send:  00 b2 01 1c c3
Resp:  70 81 c0 8f 01 06 9f 32 01 03 92 24 b1 3d 0c f5
       52 c3 8b 2a e6 e5 ff 1a 75 8d a3 7b a0 94 5b 4d
       fe 7f f9 21 ed 9d f4 5f 13 3d 40 6a 52 3e 68 d7
       90 81 90 ad 3a 01 4d 15 6d 1f 1b 19 24 9e de 61
       f8 69 21 2f 48 da 24 b1 50 30 3b bf 2f 00 96 4c
       17 fb 06 32 cb f2 e6 62 43 04 5a e8 19 56 c4 50
       14 78 21 3c f6 dc 9e 3a 76 d7 d1 57 1c 98 73 49
       d5 ea be d8 fc 06 c7 bd 2f ea 26 43 f4 20 26 8f
       bf d9 62 9c 62 13 a5 a7 44 a2 ba b5 66 9e fa 38
       44 e4 5f 28 f2 57 79 e4 12 63 8d af d4 ee f7 3f
       a5 29 46 4c fe 95 ad f7 61 77 c5 9b f6 f3 c4 07
       86 ec 82 db ff 52 4a 80 24 bd 8d 42 fb 05 40 a8
       e1 77 05 90 00

Send:  00 b2 01 24 00
Resp:  6c 23

Send:  00 b2 01 24 23
Resp:  70 21 9f 47 01 03 9f 48 1a 1f e0 25 12 a6 b0 66
       c8 ca 74 a2 1a af 72 78 a9 b1 dd fa 6c 86 41 8a
       4a 65 15 90 00

Send:  00 b2 01 2c 00
Resp:  6c 97
```

```
 77:
 78:  Send:  00 b2 01 2c 97
 79:  Resp:  70 81 94 9f 46 81 90 52 56 4d cb 60 1b a2 81 ef
 80:         e9 ac 85 37 c6 69 d5 eb ba 52 76 71 87 30 f8 f4
 81:         2e bb 4d ee 5f b1 9c 93 cc cc 06 a3 3c 73 fe 31
 82:         9e ea 31 c2 52 db 50 0d 40 30 bf 5d 8a 5d 76 14
 83:         c6 b0 df 70 12 33 7e c7 82 97 d1 c7 27 06 e1 4e
 84:         50 65 26 2d 1d 0d 86 aa a4 27 46 fd f2 44 16 f5
 85:         d3 7a 66 03 bf a1 aa e0 13 55 20 5f c7 ca 26 74
 86:         0d 18 78 be 86 88 40 63 17 72 1b 33 f5 05 43 f6
 87:         31 88 b1 15 ed 5e fd 3b f1 42 63 88 31 c3 ba ee
 88:         e5 92 8a 39 60 7c 5a 90 00
 89:
 90:  Send:  00 b2 01 14 00
 91:  Resp:  69 85
 92:
 93:  Send:  00 b2 08 14 00
 94:  Resp:  6a 83
 95:
 96:  Send:  00 b2 02 0c 00
 97:  Resp:  6a 82
 98:
 99:  Send:  00 b2 02 18 00
100:  Resp:  6a 86
101:
102:  Send:  00 b2 00 5c 0f
103:  Resp:  6a 86
104:
105:  Send:  00 b2 01 5c 0f
106:  Resp:  00 00 00 00 35 20 40 07 24 09 78 16 10 29 00 90
107:         00
108:
109:  Send:  00 b2 02 5c 0f
110:  Resp:  00 00 00 00 10 79 40 07 24 09 78 16 10 29 00 90
111:         00
112:
113:  Send:  00 b2 03 5c 0f
114:  Resp:  00 00 00 00 19 99 40 02 50 09 78 16 10 24 01 90
115:         00
116:
117:  Send:  00 b2 04 5c 0f
118:  Resp:  00 00 00 01 20 00 40 02 50 09 78 16 10 22 01 90
119:         00
120:
121:  Send:  80 ca 9f 4f 13
122:  Resp:  9f 4f 10 9f 02 06 9f 27 01 9f 1a 02 5f 2a 02 9a
123:         03 9c 01 90 00
```

- Lecteur 2 (seulement le fragment nécessaire pour répondre aux questions)

```
  1:  [connection] -- Trying OMNIKEY CardMan 5x21 0 using T0|T1 protocol
  2:  [connection] -- Trying OMNIKEY CardMan 5x21-CL 0 using T0|T1 protocol
  3:  [connection] -- Connected to OMNIKEY CardMan 5x21-CL 0 using T1 protocol
  4:  [connection] -- Cold Reset
  5:  ATR:   3b 85 80 01 20 63 cb a3 20 0f
  6:
  7:  Send:  00 a4 04 00 05
  8:         a0 00 00 00 42 00
  9:  Resp:  6f 29 84 07 a0 00 00 00 42 10 10 a5 1e 50 02 43
 10:         42 87 01 01 9f 11 01 01 9f 12 02 43 42 5f 2d 04
 11:         66 72 65 6e bf 0c 04 df 61 01 04 90 00
 12:
 13:  Send:  80 a8 00 00 02
 14:         83 00 00
 15:  Resp:  77 12 82 02 19 80 94 0c 10 01 01 01 18 01 01 00
 16:         20 01 02 00 90 00
 17:  ...
```

Extraits de spécifications nécessaires (EMVCo, ISO7816-4) :

- GET PROCESSING OPTIONS Command, Data Field Returned in the Response Message
    - The data field of the response message consists of a BER-TLV coded data object. The coding of the data object shall be according to one of the following two formats.
        - Format 1 : […] *(pas nécessaire)*
        - Format 2 : The data object returned in the response message is a constructed data object

with tag equal to '77'. The value field may contain several BER-TLV coded objects, but shall always include the AIP and the AFL.

- The AFL is a list identifying the files and records to be used in the processing of a transaction. The terminal is to read only the records named in the AFL. Each element of the list corresponds to a file to be read and is structured as follows:
  - The five most significant bits of the first byte indicate the SFI. The three least significant bits of the first byte shall be set to zero.
  - The second byte indicates the first (or only) record number to be read for that SFI. The second byte shall never be set to zero.
  - The third byte indicates the last record number to be read for that SFI. Its value is either greater than or equal to the second byte. When the third byte is greater than the second byte, all the records ranging from the record number in the second byte to and including the record number in the third byte shall be read for that SFI. When the third byte is equal to the second byte, only the record number coded in the second byte shall be read for that SFI.
  - The fourth byte indicates […] *(pas nécessaire)*
- Data Elements Dictionary *(la table n'est pas entière mais elle est suffisante pour répondre aux questions)*

Name	Description	Tag
Amount, Authorised	Authorised amount of the transaction	9F02
Application Effective Date	Date from which the application may be used (format BCD, YYMMDD)	5F25
Application Expiration Date	Date after which application expires (format BCD, YYMMDD)	5F24
Application File Locator (AFL)	Indicates the location (SFI, range of records) related to a given application	94
Application Interchange Profile (AIP)	Indicates the capabilities of the card to support specific functions in the application	82
Application Transaction Counter (ATC)	Counter maintained by the application	9F36
Certification Authority Public Key Index	Identifies the certification authority‘s public key in conjunction with the RID	8F
Log Format	List (in tag and length format) of data objects representing the logged data elements that are passed to the terminal when a transaction log record is read	9F4F
Issuer Country Code	Indicates the country of the issuer according to ISO 3166	5F28
Terminal Country Code	Indicates the country of the terminal, represented according to ISO 3166	9F1A
Transaction Currency Code	Indicates the currency code of the transaction according to ISO 4217	5F2A
Transaction Date	Local date that the transaction was authorised	9A

- GET DATA Command, Command Message

Code	Value
CLA	80
INS	CA
P1P2	Tag number : 9F36, 9F13, 9F17, or 9F4F
Lc	Not present
Data	Not present
Le	00

- GET PROCESSING OPTIONS Command, Command Message

Code	Value
CLA	80
INS	A8
P1	00
P2	00
Lc	02
Data	8300
Le	00

- READ RECORD Command, Command Message

<table>
<tr><th>Code</th><th>Value</th></tr>
<tr><td>CLA</td><td>00</td></tr>
<tr><td>INS</td><td>B2</td></tr>
<tr><td>P1</td><td>Record number</td></tr>
<tr><td>P2</td><td>Reference control parameter:<table>
<tr><th>b8-b4</th><th>b3-b1</th><th>Meaning</th></tr>
<tr><td>xxxxx</td><td></td><td>SFI</td></tr>
<tr><td></td><td>100</td><td>P1 is a record number</td></tr>
</table></td></tr>
<tr><td>Lc</td><td>Not present</td></tr>
<tr><td>Data</td><td>Not present</td></tr>
<tr><td>Le</td><td>00</td></tr>
</table>

- STATUS WORD :
    - 9000 Normal processing, no further qualification
    - 6985 Conditions of use not satisfied
    - 6A82 File or application not found
    - 6A83 Record not found
    - 6A86 Incorrect parameters P1-P2

Questions :

1. Pourquoi la commande GPO envoie des réponses différentes sur deux lecteurs différents ? *(Attention, il ne s'agit pas ici de différencier les protocoles T=0 et T=1, SW=61xx et commande Get Response 00 c0 00 00, il faut expliquer les différences des réponses 77 … 90 00).*
2. Expliquez les raisons de différents Status Word obtenus avec la commande READ RECORD (5 cas).
3. Quels sont les fichiers (SFIs) / records lisibles sur la carte dans les deux cas (de deux lecteurs) ?
4. Pourquoi certaines réponses de la commande READ RECORD ne sont pas en format TLV ?
5. Quelle est la date d'expiration de la carte ?
6. En analysant les logs de transaction validées par la carte, si on considère que la carte a été délivrée dans un pays P1, quelles transactions ont été effectuées dans un pays étranger P2 (par rapport à P1) ? *Attention, encore une fois, les informations données dans l'énoncé sont suffisantes pour pouvoir répondre à cette question.*