Barème globale : 5 + 5 + 10= 20 points

Comme la note doit être sur 10, je divise le nb de points par 2 et j'arrondis vers le haut – par exemple 13 points sur 20 donne 7 sur 10 (mais 12,5 / 20 donne 6 / 10).

Exercice 1, Question de cours

Développez les sigles de la colonne 1. Associez-les avec les concepts de la colonne 2. Justifiez.

Sigle	Concept
ATR	Spécification de cartes bancaires
GPO	Commande de la carte bancaire Visa
ISO 7816-3	Cold Reset
EMV	Passeport électronique
BAC	Protocole T0

Réponse

Barème : 5 x (0.5 développent du sigle + 0.5 association) = 5 points

ATR – Answer To Reset – Cold Reset

GPO – Get Processing Options – Commande de la carte bancaire Visa

ISO – International Organization for Standardization – Protocole T0

EMV – Europay Mastercard Visa – Spécifications des cartes bancaires

BAC – Basic Access Control – Passeport électronique

Exercice 2, Entrée / sortie Java Card, différences entre 2 exécutions

La même commande de la même application Java Card chargée et exécutée sur 2 cartes différentes peut donner des résultats différents : (la ligne Send : correspond a ce qui est envoyé par le terminal et la linge Resp : indique la réponse de la carte)

Log 1

```
...
     52:   Send:  80 54 03 42 08
     53:          57 ff 45 be 10 3c 80 5d 00
     54:   Resp:  00 00 42 86 00 47 61 06 47 92 ff 02 00 77 04 d4
     55:          73 72 ed c5 c3 00 38 52 b7 90 e5 92 90 00
...
```

Log 2

```
...
     52:   Send:  80 54 03 42 08
     53:          57 ff 45 be 10 3c 80 5d
     54:   Resp:  61 1c
...
```

1. Pourquoi ces réponses sont différentes ?
2. Pourquoi il n'y a pas le même nombre d'octets envoyés à la carte (voir dans la ligne 53) ?
3. Parmi ces 4 lignes en Java Card, lesquelles sont nécessaires pour implémenter cette commande ? Pourquoi ?
    - `apdu.setIncomingAndReceive();`

- `apdu.setOutgoing();`
- `apdu.setOutgoingLength(...);`
- `apdu.sendBytes(…);`

Réponse

Barème : 1+1+3 = 5 points

1. La première carte est en T1, la seconde en T0
2. C'est Le=0x00 nécessaire en T1. En T0 en cas 4 on l'envoie pas, il faut Get Reponse derrière
3. Toutes les 4 sont nécessaires.

Exercice 3, Compréhension de spécifications

Voilà un fragment de log d'exécution d'un dialogue entre un terminal et une carte Java Card avec quelques applets déjà chargés.

```
...
      8:   [connection] --> Cold Reset
      9:   ATR:   3b dc 18 ff 81 91 fe 1f c3 80 73 c8 21 13 66 05
     10:          02 42 58 00 02 79
     11:
     12:   Send:  00 a4 04 0c 08
     13:          a0 00 00 01 51 00 00 00 00
     14:   Resp:  6f 10 84 08 a0 00 00 01 51 00 00 00 a5 04 9f 65
     15:          01 ff 90 00
     16:
...
     39:   ##############
     40:     Open SC GP
     41:   ##############
     42:   Send:  80 50 00 00 08
     43:          57 ff 45 be 10 3c 80 5d 00
     44:   Resp:  00 00 42 86 00 47 61 06 47 92 ff 02 00 77 04 d4
     45:          73 72 ed c5 c3 00 38 52 b7 90 e5 92 90 00
     46:
     47:   Send:  84 82 01 00 10
     48:          72 ff db 64 9c 96 ca fb 73 e6 a9 70 d7 5e e0 b9
     49:   Resp:  90 00
     50:
     51:   ##############
     52:     Get Status
     53:   ##############
...
    243:   Send:  84 f2 40 02 0a
    244:          4f 00 95 4d 30 2a 93 bd db 43 00
    245:   Resp:  e3 26 4f 06 a0 00 00 00 50 00 9f 70 01 07 c5 03
    246:          00 00 00 c4 05 a0 00 00 00 50 ce 02 01 09 cc 08
    247:          a0 00 00 01 51 00 00 00 e3 26 4f 06 a0 00 00 02
    248:          30 00 9f 70 01 07 c5 03 00 00 00 c4 05 a0 00 00
    249:          02 30 ce 02 02 03 cc 08 a0 00 00 01 51 00 00 00
    250:          90 00
```

Aujourd'hui les cartes Java Card contient un composant logiciel appelé Card Manager et conforme aux spécifications de GlobalPlatform. Son rôle est (parmi d'autres) de gérer le contenu de la carte (chargement, effacement). Il est vu de « l'extérieur » comme n'importe quelle autre application (appelée ISD – Issuer Security Domain). C'est avec ce composant le programme *gpshell* vu en TP communique, pour charger les applets sur la carte.

Voilà quelques fragments de spécification GlobalPlatform (version 2.2) concernant la commande Get Status :

Definition and Scope

The GET STATUS command is used to retrieve Issuer Security Domain, Executable Load File, Executable Module, Application or Security Domain Life Cycle status information according to a given match/search

criteria.

Command Message

The GET STATUS command message shall be coded according to the following table.

Code	Value	Meaning
CLA	'80' – '8F', 'C0' - 'CF' or 'E0' - 'EF'	
INS	'F2'	GET STATUS
P1	Reference control parameter P1	See below
P2	Reference control parameter P2	See below
Lc	Length of Data	
Data	Search criteria (and MAC)	See below
Le	'00'	

Reference Control Parameter P1

Reference control parameter P1 is used to select a subset of statuses to be included in the response message. It is coded as follows:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	-	-	-	-	-	-	-	Issuer Security Domain
-	1	-	-	-	-	-	-	Applications and Supplementary Security Domains only
-	-	1	-	-	-	-	-	Executable Load Files
-	-	-	1	-	-	-	-	Executable Load Files and Executable Modules
-	-	-	-	x	x	x	x	RFU

Reference Control Parameter P2

The reference control parameter P2 controls the number of consecutive GET STATUS command and indicates the format of the response message. It shall be coded according to the following table.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	x	-	-	RFU
-	-	-	-	-	-	-	0	Get first or all occurrence(s)
-	-	-	-	-	-	-	1	Get next occurrence(s)
-	-	-	-	-	-	0	-	Deprecated
-	-	-	-	-	-	1	-	Output format in TLV format, see below for Response data structure

Data Field Sent in the Command Message

...

The GET STATUS command message data field shall contain at least one TLV coded search qualifier: the AID (tag '4F'). It shall be possible to search for all the occurrences that match the selection criteria according to the reference control parameter P1 using a search criteria of '4F' '00'.

…

Response Data Structure

…

Based upon the search criteria of the GET STATUS command data field and the selection criteria of reference control parameter P1 and P2, multiple occurrences of the data structure in the following table may be returned.

Tag	Length	Name	Presence
'E3'	Variable	GlobalPlatform Registry related data	Conditional
'4F'	5-16	AID	Conditional
'9F70'	1	Life Cycle State	Conditional
'C5'	1 or 3	Privileges	Conditional
'C4'	5-16	Application's Executable Load File AID	Conditional
'CE'	1-n	Executable Load File Version Number	Conditional
'84'	5-16	First or only Executable Module AID	Conditional
'CC'	5-16	Associated Security Domain's AID	Conditional

...

Information supplémentaire: Les commandes dans les lignes 42 et 47 sont Initialize Update et External Authenticate qui servent à authentifier le terminal (seulement la personne qui connaît des clefs de gestion de la carte est autorisé de la faire) et activent le mode où chaque commande qui suit doit être complétée par un MAC – une somme de contrôle de 8 octets basée sur le chiffrement Triple DES.

Questions :

1. Que fait la commande de la ligne 12 ?
2. Et celle de la ligne 243 ?
3. La carte est en mode T0 ou T1 ?
4. Quelles sont les applications (i.e. leurs AIDs) sur la carte et combien il y en a ?
5. Quels sont les numéros de version des application présentes sur la carte ?
6. J'ai indiqué plus haut que l'application ISD est vue comme n'importe autre application. Quel est son AID ? Et pourquoi, à votre avis il n'apparaît pas dans la réponse de Get Status ? Et que faudrait-il modifier dans la commande Get Status pour l'avoir dans la réponse ?
7. GlobalPlatform n'est pas limité à la gestion des applications écrites en Java Card. Son terminologie (comme par exemple Executable Load File) est donc « générique ». Pourtant, dans le cadre de Java Card, et à partir de ce que vous avez vu en TP et aussi dans cet exercice, pouvez vous déduire que veut justement dire Executable Load File dans le cas de Java Card ?

Réponse

Barème : 1+1+1 + 2 + 2 + 2 + 1 = 10 points

1. Commande Select
2. Commande Get Status

3. T1
4. 2 applications (hors ISD évidemment): a0 00 00 00 50 00 et a0 00 00 02 30 00. On les retrouve dans le Tag 4F
5. 0109 et 0203. On les retrouve dans le Tag CE
6. AID de ISD est a0 00 00 01 51 00 00 00. On le voit dans la commande Select. Elle est pas listée dans le résultat de Get Status car P1 = 0x40 : « Applications and Supplementary Security Domains only ». Pour l'avoir il faut mettre le bit 8 de P1 à 1 (donc par exemple P1=0x80 ou P1=0xC0)
7. C'est le package JavaCard. Et/ou le .CAP chargé sur la carte.