Corrigé du TP Carte SIM

Outil GScriptor

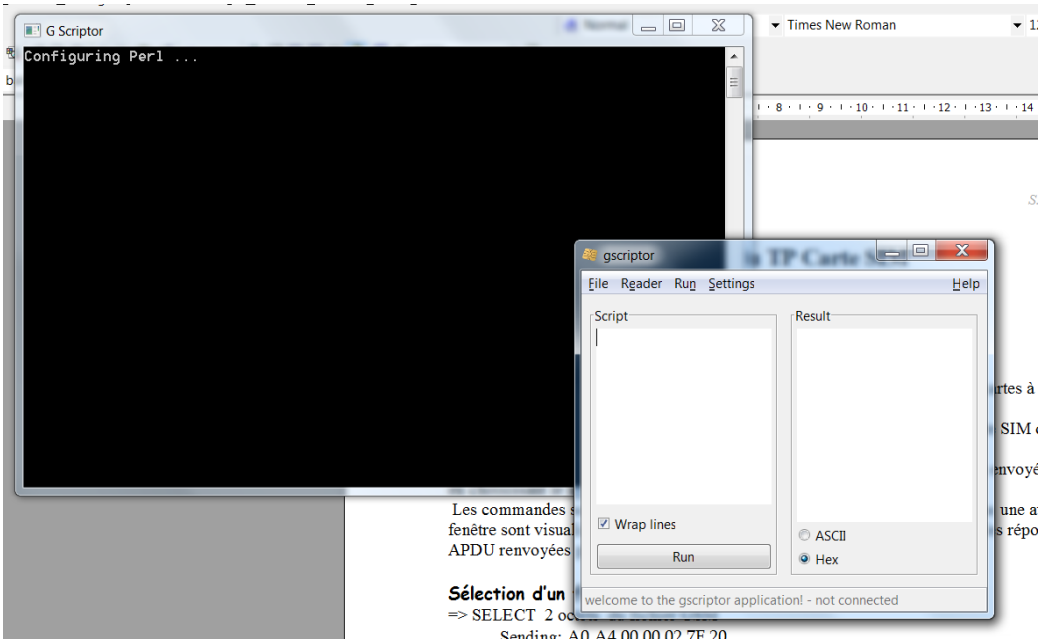
Il faut d'abord télécharger GScriptor : http://cedric.cnam.fr/~bouzefra/cours/gscriptor.exe
et l'installer sous Windows.
Depuis Windows 7, il n'est pas nécessaire d'installer le driver du lecteur de cartes à puce.

Après connexion du lecteur de cartes sur un port USB et l'insertion de la carte SIM dans le lecteur, on lance l'exécution de Pro-Active/Gscriptor.

Dans ces figures, vous avez le type de lecteur de cartes SIM utilisé en TP.

Lecteur de cartes SIM usb inséré dans le PC.

Avant le lancement de toute commande APDU, on vérifie que la carte a bien envoyé son ATR en choisissant le menu Reader/Status de l'outil Gscriptor. Si ce n'est pas le cas, il faut réinsérer la carte en lui changeant de sens.



Les commandes sont saisies en Hexadécimal dans la fenêtre SCRIPT. Dans la fenêtre RESULT sont visualisées les commandes APDU envoyées à la carte ainsi que les réponses APDU renvoyées par la carte.

Rappel du format des commandes APDU

Commande APDU						
Entête obligatoire				Corps optionnel		
CLA	INS	P1	P2	Lc	Data field	Le

- CLA (1 octet): Classe d'instructions : indique la structure et le format pour une catégorie de commandes et de réponses APDU.
- INS (1 octet): code d'instruction: spécifie l'instruction de la commande.
- P1 (1 octet) et P2 (1 octet): paramètres de l'instruction.
- Lc (1 octet): nombre d'octets présents dans le champ données de la commande.
- Data field (octets dont le nombre est égal à la valeur de Lc): une séquence d'octets dans le champ données de la commande.

Rappel du format des réponses APDU

Réponse APDU		
Corps optionnel	Partie obligatoire	
Data field	SW1	SW2

- Data field (longueur variable): une séquence d'octets reçus dans le champ Data de la réponse.
- SW1 (1 octet) et SW2 (1 octet): Status words (Mots d'état) état de traitement par la carte.

Dans toute la suite, le paragraphe qui commence avec le symbole => contient la commande en Héxa saisie dans la fenêtre SCRIPT. Dans la sélection du répertoire GSM, la commande est en rouge. Le paragraphe qui commence avec le symbole <= contient la réponse en Héxa

retournée par la carte et qui s'affiche dans la fenêtre RESULT. Dans la sélection du répertoire GSM, la réponse est en bleu.

Sélection d'un répertoire GSM :

=> SELECT 2 octets du répertoire GSM

Sending (commande envoyée vers la carte): **A0 A4 00 00 02 7F 20**

<= Received (données reçues de la carte): **9F 1A**

Lorsque la carte désire envoyer des données, elle envoie SW=9F XX au terminal pour lui dire qu'elle souhaite lui envoyer XX octets. La valeur XX est en Héxadécimal.

=> GET RESPONSE 1A octets

Sending: **A0 C0 00 00 1A**

<= Received: **00 00 04 7A 7F 20 02 00 00 00 00 00 0D 91 00 12 08 00 83 8A 83 8A 00 00 83 83 90 00**

Normal processing.

Analyse de la réponse : 00 00 04 7A 7F 20 02 00 00 00 00 00 0D 91 00 12 08 00 83 8A 83 8A 00 00 83 83 90 00

Suite d'octets	**Signification**
00 00	Sans signification
04 7A	Taille mémoire non utilisée (1146 octets)
7F 20	Le nom du répertoire
02	Type répertoire
00 00 00 00 00	Sans signification
0D	13 octets de données GSM
91	= 10010001 (bit de poids fort à 0 implique la présentation du code PIN, 1 sinon)
00	Nombre de sous-répertoires
12	Nombre de fichiers
08 00	Octets non commentés
83	Code CHV1 (PIN utilisateur) initialisé, 3 essais de PIN1 possibles
8A	Code initialisé, 10 essais PUK1 possibles
83	Code CHV2 (PIN admin) initialisé, 3 essais PIN2 possibles
8A	Code initialisé, 10 essais PUK2 possibles
00 00 83 83	Octets non commentés
90 00	Status word (succès de la commande)

Vérification du code PIN :

=> VERIFY code PIN=0000 (transmis en code ASCII, le chiffre 0 est codé à l'aide de la valeur 30. Le code PIN est complété par des FF pour faire 8 chiffres)

A0 20 00 01 08 30 30 30 30 FF FF FF FF

<= Réponse : **90 00** (en cas d'erreur on obtient 98 04 pour authentication failed).

Lecture de l'IMSI:

Le fichier EF-IMSI (6F 07) est de type transparent, localisé dans le répertoire GSM.

sélection du fichier EF-IMSI
=> A0 A4 00 00 02 6F 07 (SELECT)
<= 9F 0F
=> A0 C0 00 00 0F (GET RESPONSE)
<= 00 00 00 09 6F 07 04 00 1B 00 1B 01 02 00 00 90 00 (taille du fichier : 09 octets)
=> A0 B0 00 00 09 (READ BINARY)
<= 08 29 80 10 36 60 04 81 80 90 00 (IMSI)

On peut interpréter le code IMSI comme suit :
- inverser les quartets de chaque octet IMSI, ensuite omettre le quartet le plus à gauche, prendre les 3 quartets les plus à gauche qui donnent le numéro du pays (voir liste des Mobile Country Code sur wikipedia) : http://fr.wikipedia.org/wiki/Mobile_country_code

- saisir le code IMSI ainsi modifié sans le chiffre le plus à gauche pour retrouver les informations codées dans l'IMSI en utilisant ce lien:
https://www.numberingplans.com/?page=analysis&sub=imsinr

Exemple :
IMSI = 29 80 20 57 20 38 65 32
IMSI inversé = 92 08 02 75 02 83 56 23
IMSI à saisir pour analyse = 208027502835623
(208: Mobile Country Code de la France).

Information on IMSI number range 20801XXXXXXXXX

Country or destination	France
Network operator	Orange France
Network name	Orange F
Network status*	active

Lecture de TMSI et LAI:

Le fichier EF-LOCI (6F 7E) contient une liste d'attributs (TMSI sur 4 octets, LAI sur 5 octets, TMSI-TIME sur 1 octet et Location-Update Status sur 1 octet) :
=> A0 A4 00 00 02 6F 7E (SELECT)
<= 9F 0F
=> A0 C0 00 00 0F (GET RESPONSE)
<= 00 00 00 0B 6F 7E 04 00 11 FF 15 01 02 00 00 90 00 (taille du fichier : 0B= 11 octets)
=> A0 B0 00 00 0B (READ BINARY)
<= 78 08 8F 48 02 F8 10 38 00 00 00 90 00 (TMSI sur 4 octets et LAI sur 5 octets)

Exécution de l'algorithme d'authentification du GSM:

La commande RUN-GSM-ALGO (INS=88) exécute la fonction A3/A8 du GSM. Son argument d'entrée est un nombre aléatoire de 16 octets (RAND). Elle retourne une liste de deux valeurs : la signature SRES (4 octets) et la clé Kc (8 octets) :
=> A0 88 00 00 10 01 23 45 67 89 AB CE DF 01 23 45 67 89 0A BC DE (=RAND)
<= 9F 0C
=> A0 C0 00 00 0C (GET RESPONSE)
<= 11 02 60 F1 67 F0 E8 FE F2 BC 60 00 90 00 (SRES sur 4 octets, Kc sur 8 octets)

Mise à jour du fichier EF-Kc:

La carte SIM ne met pas à jour automatiquement le fichier EF-Kc (6F 20) à la fin de l'exécution de la procédure RUN-GSM-ALGO. Cette opération est réalisée par le mobile grâce à la commande UPDATE-BINARY (INS= D6). La valeur stockée dans le fichier EF-Kc est une liste de deux valeurs, la clé Kc et un octet de validation (00 lorsque le contenu est valide et 07 dans le cas contraire).
=> A0 A4 00 00 02 6F 20 (SELECT)
<= 9F 0F
=> A0 C0 00 00 0F (GET RESPONSE)
<= 00 00 00 09 6F 20 04 00 11 00 BB 01 02 00 00 00 90 00 (taille du fichier : 09 octets)
=> A0 B0 00 00 09 (READ BINARY)
<= FF FF FF FF FF FF FF FF 07 80 90 00
=> A0 D6 00 00 09 01 23 45 67 89 AB CD EF 00 (UPDATE BINARY Kc + octet de validation)
<= 90 00
=> A0 B0 00 00 09 (READ BINARY)
<= 01 23 45 67 89 AB CD EF 00 90 00

Lecture de la table de services SIM:

Le fichier EF-SIM-Service-Table (6F 38) est la liste des services offerts par la carte SIM. Chaque service, identifié par son ordre d'apparition (n°1, n°2, etc.) est associé à deux bits : le premier de poids fort renseigne l'existence du service (1 pour présent), le deuxième de poids faible indique son activation (1 pour actif).
=> A0 A4 00 00 02 6F 38 (SELECT)
<= 9F 0F
=> A0 C0 00 00 0F (GET RESPONSE)
<= 00 00 00 0D 6F 38 04 00 1B 00 BB 01 02 00 00 90 00 (taille du fichier 0D)
=> A0 B0 00 00 0D (READ BINARY)
<= FF 3C 3F 03 00 3C 03 00 0C 00 00 00 90 00

FF = 11 .11 .11. 11, les services 1, 2, 3 et 4 sont présents sur la SIM et sont actifs.
3C = 00.11.11.00 ; les services 5 et 8 sont absents et inactifs.

Le service n°1 permet la désactivation du code PIN utilisateur (CHV1).
Le service n°2 notifie la présence d'un annuaire de numéros abrégés (ADN).
Le service n°3 est un annuaire de numéros non abrégés (FDN).
Le service n°4 indique l'existence d'un fichier EF-SMS réalisant le stockage des SMS.

Les fichiers EF-ADN, EF-FDN et EF-SMS occupent un espace mémoire de l'ordre de plusieurs Ko. Ils sont localisés dans le répertoire DF-TELECOM (7F 10).

Sélection du répertoire DF-TELECOM

=> A0 A4 00 00 02 7F 10 (SELECT)
<= 9F 1A
=> A0 C0 00 00 1A (GET RESPONSE)
<= 00 00 04 7A 7F 10 02 00 00 00 00 00 0D 11 00 09 08 00 83 8A 83 8A 00 00 83 83 90 00

Lecture et écriture des SMS dans la SIM:

Le fichier EF-SMS (6F 3C) est un fichier cyclique.

=> A0 A4 00 00 02 6F 3C (SELECT)
<= 9F 0F
=> A0 C0 00 00 0F (GET RESPONSE)
<= 00 00 14 A0 6F 3C 04 00 11 00 BB 01 02 01 B0 90 00

Taille du fichier : 14 A0 = 5280 octets, taille de l'enregistrement : B0 = 176 octets. Donc, il y a 30[1] enregistrements (5280/176).
Les conditions d'accès sont définies dans les octets 9, 10 et 11 (11 00 BB) :

- les commandes READ, SEEK et UPDATE sont contrôlés par CHV1
- les commandes REHABILITATE et INVALIDATE sont contrôlées par ADM

READ RECORD (INS=B2) permet de lire des enregistrements :
=> A0 B2 01 04 B0 (lit l'enregistrement 1)
<= 01 07 91 33 86 09 40 00 F0 04 05 85 02 09 F4 00 F1 70 90 92 91 63 90 80 96 CD A7 … FF FF FF FF 90 00

Suite d'octets	**Signification**
01	Indication de présence d'un SMS (00 sinon)
07	Longueur de l'attribut SMS information
91 33 86 90 40 00 F0	Numéro du centre de SMS
04	Le premier octet d'un message SMS deliver
05	La longueur du numéro de l'émetteur du SMS
85	Type du numéro de l'émetteur 1000 0101
02 09 F4	Numéro de l'émetteur
00	L'octet TP-PID (Protocol Identifier)
F1	L'octet TP-DCS (Date Coding Scheme)
70 90 92 91 63 90 80	TP-SCTS (time stamp, l'heure d'émission)
96	TP-UDL (User Date Length), longueur du message 150 octets

La taille maximale d'un SMS est de 176 octets.

La commande UPDATE-RECORD (INS=DC) permet d'écrire un SMS dans le fichier EF-SMS :

[1] En héxa 1E

=> A0 DC 01 04 B0 [176 octets]
<= 90 00

Lecture de l'annuaire des numéros ADN :

Le fichier cyclique EF-ADN (6F 3A) est un annuaire téléphonique.

=> A0 A4 00 00 02 6F 3A (SELECT)
<= 9F 0F
=> A0 C0 00 00 0F (GET RESPONSE)
<= 00 00 1B 58 6F 3A 04 00 11 00 22 01 02 01 1C 90 00

Taille du fichier : 1B 58 = 7000 octets, taille d'un enregistrement : 1C (28 octets)
D'où : 7000/28= 250 enregistrements.

Lecture du 1er enregistrement :
=> A0 B2 01 04 1C
<= 11 53 65 72 76 2E 20 43 6C 69 65 6E 74 FF 03 81 23 53 FF FF FF FF FF FF FF FF FF FF 90 00

Suite d'octets	**Signification**
11 53 65 72 76 2E 20 43 6C 69 65 6E 74 FF	Service client (étiquette de 14 octets associée au numéro de téléphone)
03	Longueur en octets des attributs TON/NPI et numéro de téléphone (3=1+2)
81	Type de numéro de téléphone, 81 pour le GSM
25 53	Numéro de téléphone
FF	Capability/configuration identifier, attribut non utilisé
FF	Extension1 record identifier, attribut non utilisé

En général, un numéro de téléphone comporte 10 chiffres (soit 5 octets). Par exemple le numéro 06 22 58 63 78 sera inscrit dans l'annuaire sous la forme : 06 22 58 63 78

Lecture de l'annuaire de service FDN :

Le fichier cyclique EF-FDN (6F 3B) est un annuaire des services.

=> A0 A4 00 00 02 6F 3B (SELECT)
<= 9F 0F
=> A0 C0 00 00 0F (GET RESPONSE)
<= 00 00 03 48 6F 3B 04 00 12 00 BB 01 02 01 1C 90 00

Taille du fichier : 03 48 = 840 octets, taille d'un enregistrement : 1C (28 octets)
D'où : 840/28= 30 enregistrements.

Lecture du 1er enregistrement :
=> A0 B2 01 04 1C

<= 6 D 6F 62 69 63 61 72 74 65 FF FF FF FF FF 02 81 22 FF FF FF FF FF FF FF FF FF FF FF 90 00

Opérations liées au code PIN :

Un code PIN comporte 8 octets, représentant des chiffres au format ASCII. Les octets insignifiants sont codés par FF.
La commande **VERIFY CHV** permet de présenter le code PIN (CHV1) du propriétaire du mobile à la carte SIM. Elle est codée sous la forme : A0 20 00 P2 08 [PIN]. P2 = 01 dans le cas de CHV1 (PIN utilisateur) et égal à 02 si CHV2.

=> A0 20 00 01 08 30 30 30 30 FF FF FF FF
<= 90 00

L'usage du code PIN utilisateur est annulée grâce à la commande **DISABLE PIN (A0 26 00 01 08 [PIN]).** La commande **ENABLE PIN (A0 28 01 08 [PIN])** réalise l'opération inverse.

Activation du code PIN :
=> A0 28 00 01 08 30 30 30 30 FF FF FF FF
<= 90 00

Annulation de code PIN
=> A0 26 00 01 08 30 30 30 30 FF FF FF FF
<= 90 00

La modification du code est possible grâce à la commande **CHANGE CHV (A0 24 00 01 10 [Ancien_PIN] [Nouveau_PIN]).**
=> A0 24 00 01 10 30 30 30 30 FF FF FF FF 31 32 33 34 FF FF FF FF
<= 90 00

Au terme de 3 essais infructueux de présentation du code PIN utilisateur, la carte est bloquée. La commande **UNBLOCK CHV (A0 2C 00 01 10 [PUK] [PIN]** annule cet état et permet au module d'être à nouveau opérationnel. Le code PUK est un code unique de 8 chiffres associé à la SIM.

=> A0 2C 00 01 10 31 32 33 34 35 36 37 38 30 30 30 30 FF FF FF FF
<= 90 00