Les Cartes SIM/USIM

Samia Bouzefrane & Hai Binh LE

samia.bouzefrane@cnam.fr & hai-binh.le@cnam.fr
Laboratoire CEDRIC
CNAM
http://cedric.cnam.fr/~bouzefra

GSM

- En Europe, les équipements mobiles limités à des frontières nationales car les systèmes sont incompatibles
- D'où: création du "Groupe Spécial Mobile" (GSM) qui propose :
  - une bonne qualité de la voix
  - des terminaux pas très chers
  - un support pour le roaming international
  - etc.

1989: la responsabilité de GSM est transférée vers ETSI (European Telecommunication Standards Institute)
1990: Publication des spécifications GSM phase I
1991: Démarrage du service commercial
1993: 36 réseaux GSM dans 22 pays
1995: 114 réseaux GSM dans 66 pays
1998: 304 réseaux GSM dans 120 pays
2001: 445 réseaux GSM dans 170 pays
…

GSM

➢Depuis 1989, l'ETSI (European Telcommunications Standard Institute) édite les spécifications du GSM et de l'UMTS (*Universal Mobile Telecommunications System*, réseau de 3éme génération).
Siège de l'ETSI à Sophia Antipolis.

➢ En Europe, le standard GSM utilise les bandes de fréquences 900 MHz et 1800 MHz. Aux Etats-Unis, la bande de fréquence utilisée est la bande 1900 MHz.

Tri-bande : les téléphones portables pouvant fonctionner en Europe et aux Etats-Unis
Bi-bande : les téléphones fonctionnant uniquement en Europe.

➢La norme GSM autorise un débit maximal de 9,6 kbps
=> transmission de la voix, des données numériques de faible volume, des messages textes (**SMS**, pour *Short Message Service*) ou des messages multimédias (**MMS**, pour *Multimedia Message Service*).

3

Les services fournis par le GSM

➢**Services de téléphonie**

➢**Services de données**
Services Fax
SMS (Short Message Service)

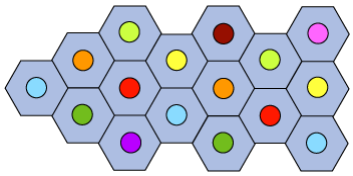
➢**Service d'échange de données (GPRS)**

➢**Services supplémentaires**
itinérance (roaming)
conversation multi-parties

4

Notion de réseau cellulaire

Un réseau de téléphonie mobile est basé sur la notion de **cellules**,
Une cellule : est une zone circulaire qui couvre une zone géographique.
Une cellule : centaine de mètres (zone urbaine), une trentaine de kms (zone rurale).



Chaque cellule dispose d'un émetteur-récepteur central appelé « **station de base** »
(en anglais *Base Transceiver Station*, **BTS**).
Plus le rayon d'une cellule est petit, plus la bande passante disponible est élevée.
Chaque cellule est entourée de 6 cellules voisines.
Les cellules adjacentes ne peuvent pas utiliser la même fréquence.

5

Éléments du réseau cellulaire

➢ Un **contrôleur de stations** (**BSC**, *Base Station Controller*)
qui relie toutes les stations de base, chargé de gérer la répartition des ressources.

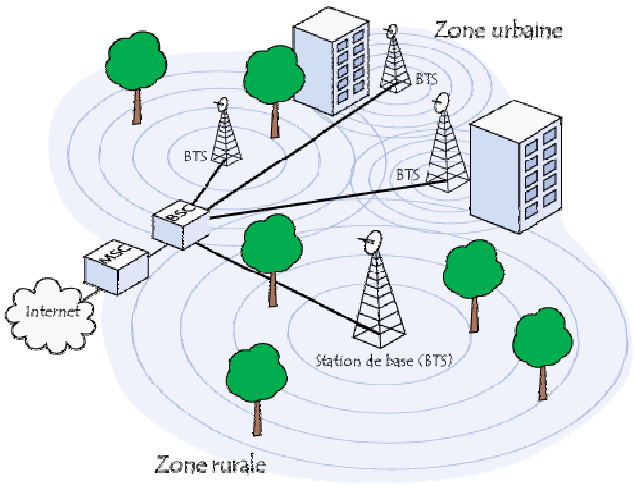
➢**Sous-système radio** (en anglais **BSS** pour *Base Station Subsystem*) =
contrôleur de stations + les stations de base.

➢**Centre de commutation du service mobile** (**MSC,** *Mobile Switching Center*),
géré par l'opérateur téléphonique, relie les contrôleurs de stations
au réseau téléphonique public et à internet.

➢**Sous-système réseau** (**NSS,** *Network Station Subsystem*) auquel appartient le MSC,
chargé de gérer les identités des utilisateurs, leur localisation et l'établissement
de la communication avec les autres abonnés.

6

Architecture du réseau GSM



7

Bases de données manipulées

- **Le registre des abonnés locaux** (**HLR,** *Home Location Register*): base de données contenant des informations (position courante, informations administratives, etc.) sur les abonnés du réseau GSM.
  Un seul HLR par réseau GSM.

- **Le registre des abonnés visiteurs** (**VLR,** *Visitor Location Register*): base de données contenant des informations sur les abonnés se trouvant dans la zone contrôlée par le VLR. Le VLR rapatrie les données de l'abonné à partir du HLR.
  Les données sont conservées pendant tout le temps de sa présence dans la zone et sont supprimées lorsqu'il la quitte ou après une longue période d'inactivité (terminal éteint).

- **Le registre des terminaux** (**EIR,** *Equipement Identity Register*) : base de données répertoriant les terminaux mobiles.

- **Le centre d'authentification** (**AuC**, *Autentication Center*) : est chargé de vérifier l'identité des utilisateurs, contient une copie de chaque clé stockée sur une SIM, utilisé pour l'authentification et le cryptage via le réseau cellulaire.

8

Mobilité

➢Le réseau cellulaire supporte la mobilité grâce à la gestion du *handover*, c-à-d le passage d'une cellule à une autre.

➢Les réseaux GSM supportent aussi la notion d'**itinérance** (*roaming*), c-à-d le passage du réseau d'un opérateur à un autre.

Station mobile

➢**Station mobile** : terminal de l'utilisateur

➢**Station mobile** composée de :

- Une carte **SIM** (*Subscriber Identity Module*), pour identifier l'usager de manière unique et d'un terminal mobile (en général un téléphone portable).
- Un terminal est identifié par un numéro d'identification unique de 15 chiffres appelé **IMEI** (*International Mobile Equipment Identity*).

➢Chaque carte SIM possède un numéro d'identification unique (et secret) : **IMSI** (*International Mobile Subscriber Identity*), qui peut être protégé à l'aide d'une clé de 4 chiffres appelés *code PIN*.

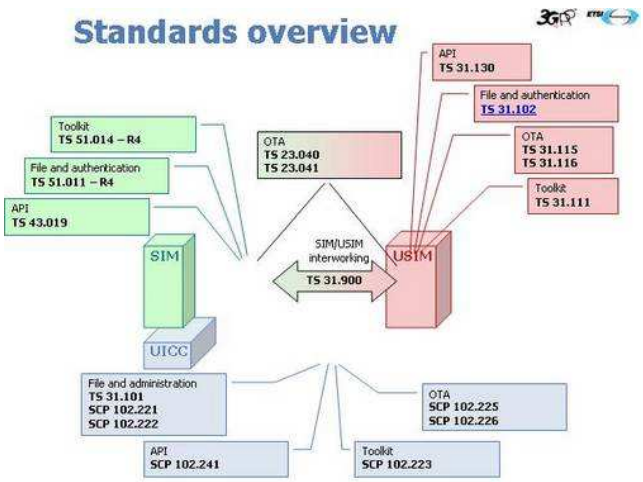
➢La communication entre une station mobile et la station de base se fait par l'intermédiaire d'un lien radio, généralement appelé **interface air**.

Carte SIM

- Notion introduite en 1988
- Rôle de la carte SIM (Subscriber Identity Module) :
  - contient les détails de l'abonnement :
    IMSI, Ki clé secrète d'authentification,
    langage de préférence, carnet d'adresses, etc.
  - contient les secrets permettant de prouver que l'utilisateur est bien lui :
    - codes secrets PIN (Personal Identification Code)
    et PUK (Personal Unlock Code)
    - clés secrètes pour l'authentification ou le cryptage.
  - permet le chargement de services sur la carte dans un environnement sécurisé permettant : l'interaction avec le mobile, l'affichage d'infos sur l'écran, la saisie des données par l'utilisateur, composer des appels, interagit avec le réseau via l'envoi/réception de messages SMS, GPRS, obtient des infos de localisation, capable d'interagir avec le système de fichiers de la SIM.
- Code 3 milliards de cartes SIM fabriquées en 2007

11

Normalisation



12

Les standards ETSI

SIM

- Gestion des Fichiers et Authentification : 3 GPP TS 51.011 (ETSI GSM 11.11)
- SIM Toolkit Applet Management : 3 GPP TS 51.014 (ETSI GSM 11.14)
- SIM API for Java Card : 3 GPP TS 43.019

USIM

- Gestion des Fichiers et Authentification : 3 GPP TS 31.102
- USIM Toolkit Applet Management : 3 GPP TS 31.111
- USIM API for Java Card : 3 GPP TS 31.130

13

Méthodes de protection proposées dans GSM 02.09/1

1. La protection de l'identité d'un abonné :

L'abonné possède un identifiant (IMSI : *International Mobile Subscriber Identity*) permettant de retrouver les paramètres d'abonnement dans le HLR (Host Location Register) : base de données des comptes client.
Le réseau délivre un TIMSI (*Temporary Mobile Subscriber Identity*) une identité temporaire qui change à chaque appel pour interdire la traçabilité des communications.

2. L'authentification d'un abonné :

Une authentification forte est réalisée à l'aide de l'algorithme A3 associé à une clé Ki de 128 bits.

GSM 02.09: "Digital cellular telecommunications system (Phase 2+); Security Aspects".

14

Méthodes de protection proposées dans GSM 02.09/2

3. La confidentialité des données utilisateur :

Dans un réseau cellulaire radio, l'information est transmise par des ondes électromagnétiques (Over The Air) entre le téléphone mobile et la station de base. Les échanges entre mobile et station de base sont chiffrés à l'aide de l'algorithme A5 qui utilise une clé de chiffrement Kc. Kc est mise à jour à chaque appel (authentification) avec l'algorithme A8 de génération de clés. A3 et A8 sont souvent confondus (nommés A38 ou A3A8).

4. La protection de certaines informations telles que :

IMSI, numéros appelés ou appelants, le numéro de série du téléphone (IMEI : *International Mobile Equipment Identity*).

15

Infrastructures d'authentification du GSM

Il existe cinq entités :

-La carte SIM

-Le mobile

-VLR (*Visitor Location Register*) : entité associée à plusieurs entités de base

-HLR (*Host Location Register*) : base de données clients

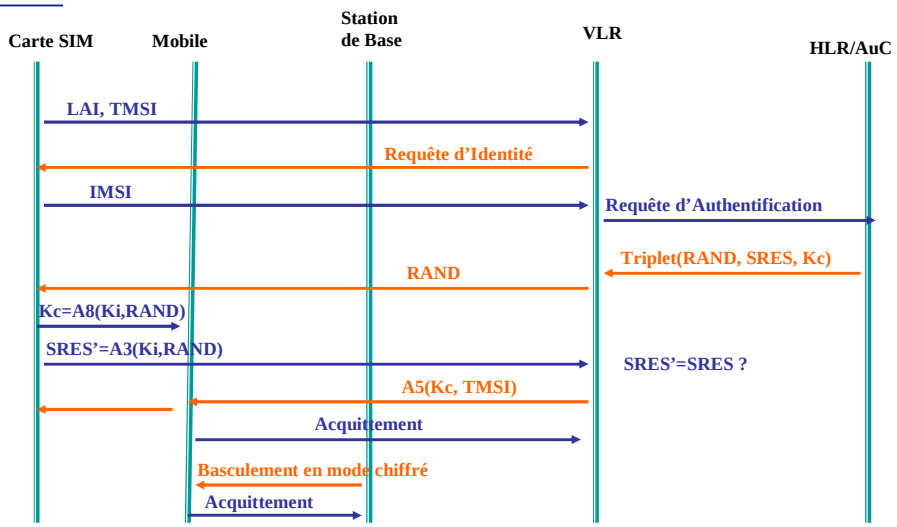
-Le centre d'authentification (AuC, *Authentication Center*).

La norme 3GPP TS 43.020 identifie une cellule ou un ensemble de cellules à l'aide de l'étiquette LAI (*Location Area Identity*).

3GPP TS 43.020 – Technical Specification Group Services & System Aspects; Security Related Network Functions (Release 5, 2002).

16

Services d'authentification



RAND : nb aléatoire de 16 octets
SRES (Signed RESponse) : réponse signée SRES=A3(Ki, RAND)
Kc : clé de chiffrement des communications, Kc=A8(Ki, RAND).

17

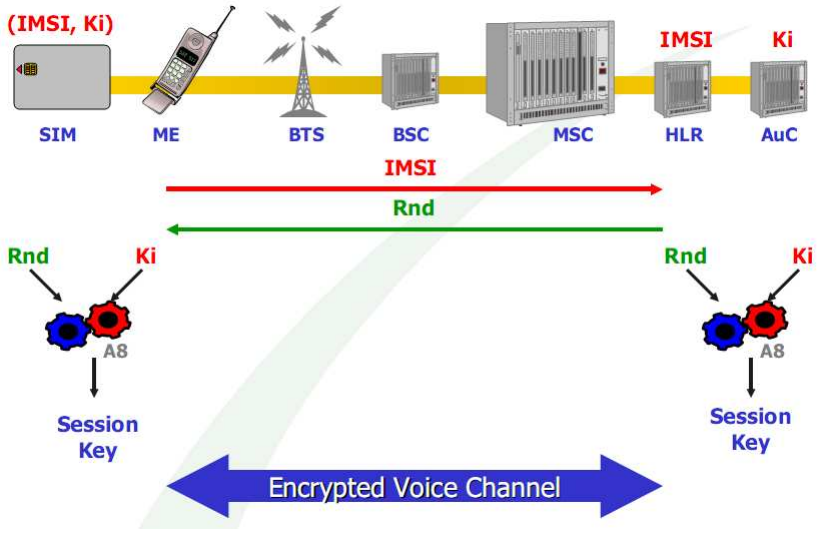
Services d'authentification

1. L'abonné dispose des valeurs (LAI, TMSI) stockées dans le module SIM, suite à un appel précédent.
2. Le mobile transmet au VLR les valeurs (LAI, TMSI).
3. Si le VLR échoue pour retrouver l'IMSI, il envoie une requête d'identification au mobile
4. Le VLR récupère l'IMSI mémorisé dans la carte SIM
5. Le VLR envoie au HLR/AuC une demande d'authentification
6. AuC produit un triplet GSM (RAND, SRES, Kc)
7. A la réception du triplet, le VLR transmet au mobile RAND
8. La carte SIM calcule SRES'= A3(Ki, RAND) qui est envoyé au HLR.
9. Le HLR vérifie l'égalité entre SRES et SRES'=> authentification de l'abonné en cas de succès.
10. Le VLR choisit un nouveau TMSI, le chiffre avec l'algorithme A5 et la clé Kc et l'envoie au mobile qui le déchiffre.

Les opérations de chiffrement et de déchiffrement appliqués aux signaux radio sont réalisées par le mobile (et non la carte SIM). Au-delà des stations de base, dans le réseau câblé de l'opérateur, il n'y a aucune garantie de confidentialité.

18

Services de cryptage



19

Algorithmes cryptographiques/attaques

➢La carte SIM réalise le calcul A3A8 dans un espace sûr.

➢En 1998, Mark Briceno, Ian Goldberg et David wagner (chercheurs à l'université de Berkeley) ont cassé l'algorithme A3A8.

➢Même si GSM ne recommande aucun algorithme, les opérateurs utilisent la procédure secrète COMP128-1.
Ces chercheurs ont aussi cassé cet algorithme en retrouvant la clé Ki en 219 calculs (environ 500 000 essais). Pour cette raison, les composants qui intègrent COMP128-1 sont munis d'un compteur limitant le nombre d'appels à 100 000.

➢Les modules SIM sont aujourd'hui basés sur l'algorithme COMP128-2 dont l'algorithme est pour le moment secret.

20

Caractéristiques physiques d'une carte SIM

Début des années 90:
Une carte SIM : un CPU (8 bits), RAM (128 octets), ROM (7 Ko), EEPROM (3 Ko).

Année 2008 :
Une carte SIM : un CPU (32 bits), RAM (16 Ko), ROM (512 Ko), EEPROM/FLASH (512 Ko), processeur dédié au calcul cryptographique.

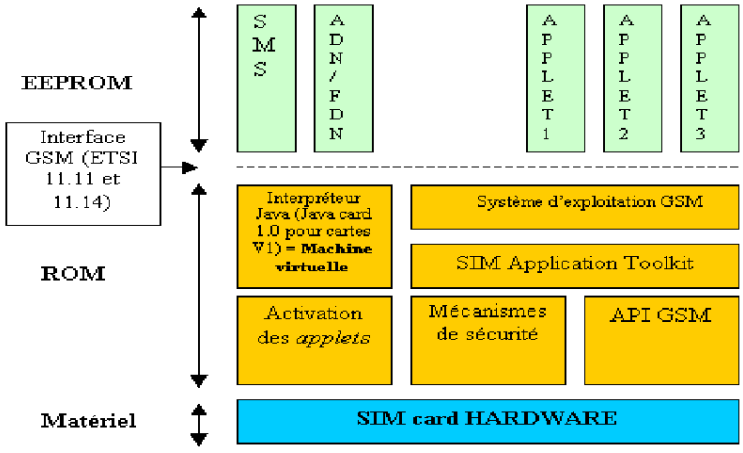
➢**La ROM** (Read Only Memory) contient le système d'exploitation de la carte, les mécanismes de sécurité (algorithmes spécifiques (API GSM).

➢**l'EEPROM** (Electrically Erasable Programmable Read Only Memory) contient des répertoires définis par norme GSM (tels que les numéros de téléphones l'abonné…) et des données liées aux applets (service de messages courts et applications spécifiques).

➢**la RAM** (Random Access Memory) permet d'effectuer des calculs ou de charger des instructions et les exécuter.

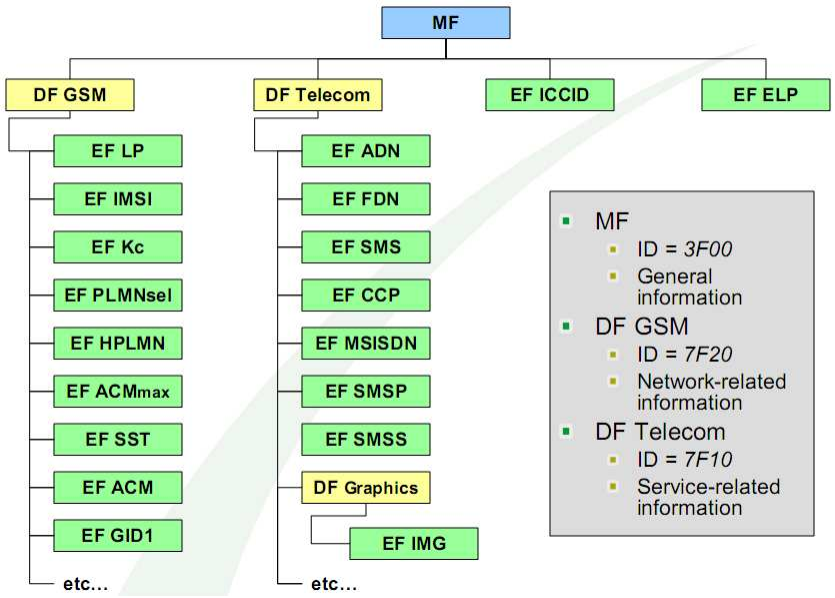
21

Structure d'une carte SIM



22

Système de Fichiers selon la norme 3GPP TS 51.011

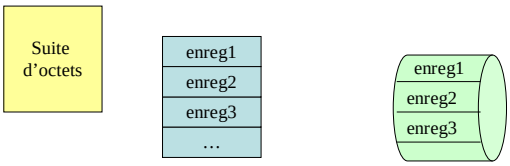


23

Le système de fichiers de La SIM

➢ ***Dedicated*** File

➢ ***Elementary*** File
- Fichier transparent
- Fichier linéaire fixe
- Fichier cyclique



Répertoire racine : 3F 00

Sous répertoires importants : GSM (DF_{GSM}, 7F20) et TELECOM ($DF_{TELECOM}$, 7F10).

- '3F': Master File;
- '7F': 1st level Dedicated File;
- '5F': 2nd level Dedicated File;
- '2F': Elementary File under the Master File;
- '6F': Elementary File under a 1st level Dedicated File;
-'4F': Elementary File under 2nd level Dedicated File.

Après la réception de l'ATR (*Answer To Reset*), le master file (MF) est implicitement sélectionné.

24

EF ICCID (Integrated Circuit Card Identification)

➢ EF_{ICCID} fournit le numéro de série de la carte SIM.

Identifier: 2FE2	**Structure:** Transparent	Mandatory
File size: 10 bytes	**Update activity:** low	

Access Conditions	***Read***	Always
	Update	Never
	Invalidate	ADM
	Rehabilitate	ADM

Bytes	Description	M/O	Length
1 - 10	Identification number	M	10 bytes

25

EF ELP (Extended Language Preference)

EF_{ELP} contient les langages dans l'ordre de préférence par l'utilisateur, fixé par l'utilisateur ou bien par l'opérateur.

Identifier: 2F05	**Structure:** Transparent	Optional
File size: 2n bytes	**Update activity:** low	

Access Conditions	***Read***	ALW
	Update	CHV1
	Invalidate	ADM
	Rehabilitate	ADM

Bytes	Description	M/O	Length
1 - 2	First language code (highest priority)	O	2 bytes
3 - 4	Second language code	O	2 bytes
2n-1 - 2n	n^{th} language code (lowest priority)	O	2 bytes

26

Répertoire GSM

- Le fichier EF_{IMSI} (6F07) contient le paramètre IMSI.
- Le fichier EF_{LOCI} (6F 7E) contient principalement les paramètres : TMSI, LAI.
- EF_{LP} (Language preference)
- EF_{Kc} (Ciphering key Kc) contient la clé Kc et le numéro de séquence de la clé.
- EF_{SST} (SIM service table) : dresse la liste des services disponibles dans la carte.
  - Service n°1 : CHV1 disable function
  - Service n°2 : Abbreviated Dialling Numbers (ADN)
  - Service n°3 : Fixed Dialling Numbers (FDN)
  - Service n°4 : Short Message Storage (SMS)
  - etc.
- EF_{ACM} (Accumulated call meter): contient le nombre total d'unités pour l'appel courant et les appels précédents.
- EF_{SPN} (Service Provider Name) contient le nom de l'opérateur.

27

Répertoire TELECOM

Le répertoire TELECOM comporte plusieurs fichiers :

- EF_{ADN} (6F3A) contient un annuaire abrégé,
- EF_{FDN} (6F3B) contient un annuaire téléphonique,
- EF_{SMS} (6F3C) contient la liste des SMS émis et reçus,
- EF_{MSISDN} : contient le numéro de téléphone de l'abonné MSISDN,
- EF_{LDN} (Last Dialed Numbers): derniers numéros de téléphone appelés,
- etc.

Ces fichiers sont accessibles en lecture/écriture et sont protégés par le code PIN de l'utilisateur.

28

Conditions d'accès aux fichiers

5 niveaux de priorités :
ALWays (code 0) : le fichier est toujours accessible
CHV1 (code 1) : fichier protégé par le code PIN du porteur
CHV2 (code 2) : fichier protégé par le code PIN de l'émetteur de la SIM
ADM (codes de 4 à E) : fichier géré par une autorité administrative
NEVER (code F) : fichier inaccessible.

Niveau	Conditions d'accès
0	ALWays
1	CHV1
2	CHV2
3	Réservé
4 à 14	ADM
15	NEver

29

Conditions d'accès aux fichiers

ALWAYS : l'action peut être exécutée sans aucune restriction.

(**Card Holder Verification 1**) : la valeur de CHV1 doit être présentée.

CHV2 : la valeur de CHV2 doit être présentée.

ADM : l'allocation de ces niveaux est de la responsabilité de l'autorité administrative appropriée.

NEVER : pas d'accès.

30

Les commandes APDU

La norme 3GPP TS 11.11 (ancien GSM 11.11) définit 22 commandes APDU classées en 4 groupes :

- Six commandes de gestion de fichiers de la SIM : SELECT, READ, WRITE
- Cinq commandes de gestion de code PIN : vérification, modification, activation, suppression ou déblocage à l'aide du code PUK.
- Exécution de l'algorithme A3A8 grâce à la commande RUN GSM ALGORITHM.
- Dix commandes à utilisation variée, dont des commandes définies dans le modèle SIM Tool Kit permettant à un programme exécuté sur la SIM d'avoir accès au clavier et à l'écran du mobile, ou de communiquer avec le monde extérieur via des messages SMS.

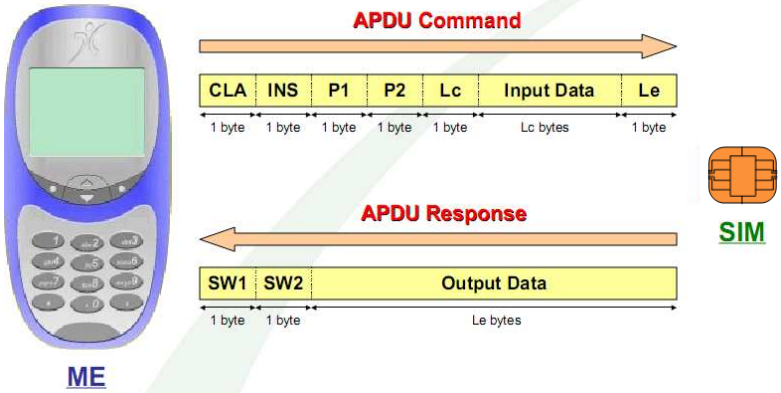
31

Les commandes APDU

COMMANDE	INS	P1	P2	P3
SELECT STATUS	A4 F2	00 00	00 00	02 Lgth
READ BINARY UPDATE BINARY READ RECORD UPDATE RECORD SEEK INCREASE	B0 D6 B2 DC A2 32	Offset high Offset high Rec N° Rec N° 00 00	Offset low Offset low Mode Mode Type/mode 00	lgth lgth lgth lgth lgth 03
VERIFY CHV CHANGE CHV DISABLE CHV ENABLE CHV UNBLOCK CHV	20 24 26 28 2C	00 00 00 00 00	CHV N° CHV N° 01 01 Voir note	08 10 08 08 10
INVALIDATE REHABILITATE	04 44	00 00	00 00	00 00
RUN GSM ALGORITHM	88	00	00	10
SLEEP	FA	00	00	00
GET RESPONSE TERMINAL PROFILE ENVELOPE FETCH TERMINAL RESPONSE	C0 10 C2 12 14	00 00 00 00 00	00 00 00 00 00	Lgth Lgth Lgth Lgth Lgth

32

Format des commandes APDU



33

La commande SELECT

A0 A4 00 00 02 XX XX (XX XX : FID du fichier/répertoire à sélectionner).

La sélection d'un répertoire entraîne une réponse qui peut inclure des informations telles que :

- la taille mémoire non utilisée
- le nom du répertoire sélectionné
- le type du répertoire (MF ou non)
- présentation du code PIN
- nombre de sous répertoires
- nécessité éventuelle de présentation du code PIN, avec le nombre d'essais possibles.

34

La commande SELECT

COMMAND

CLA	INS	P1	P2	Length In	Length Out
A0	A4	00	00	2	13+

INPUT DATA

Byte(s)	Description	Length
1 - 2	File ID	2

OUTPUT DATA (in case of an MF or DF)

Byte(s)	Description	Length
1 - 2	RFU	2
3 - 4	Total amount of free memory of the selected directory	2
5 - 6	File ID	2
7	Type of file (MF, DF, EF, RFU)	1
8 - 12	RFU	4
13	Length of the following data (from byte 14 to the end)	1
14 - 34	GSM specific data (file characterictics, nb. of child DF, nb. of child EF, nb. Of CHVs & unblock CHVs, status of CHVs, etc…)	21

35

Lectures de Fichiers

➢Lecture de l'IMSI

Le fichier EF_{IMSI} (6F07) du répertoire GSM est de type transparent, il contient l'IMSI. La sélection du fichier retourne la taille du fichier.

A0 B0 00 00 09 (READ BINARY 9 octets, taille de l'IMSI).

➢Lecture de TMSI et LAI

Ces paramètres sont lus à partir du fichier EF_{LOCI} (6F 7E)

A0 B0 00 00 B (READ BINARY 11 octets, 4 octets pour TSMI suivis de 5 octets pour LAI, ..)

36

Ecriture de fichiers

Mise à jour du fichier EF_{Kc}

Le fichier EF_{Kc} est mis à jour par le mobile grâce à la commande UPDATE BINARY . Deux valeurs sont stockées dans le fichier : la clé et un octet de validation (=00 si clé valide et 07 sinon).

COMMAND

CLA	INS	P1	P2	Length In	Length Out
A0	D6	Offset high	Offset low	lgth	00

INPUT DATA

Byte(s)	Description	Length
1 - lgth	Data	lgth

OUTPUT DATA

Byte(s)	Description	Length
N/A	N/A	N/A

37

Algorithme d'authentification

➢ **Algorithme GSM A3/A8 utilisé pour :**

- Authentification (A3)
- Cryptage (A8)

➢ **Exécution de l'algorithme d'authentification du GSM**

RUN-GSM-ALGORITHM exécute la fonction A3A8 avec comme argument le nb aléatoire RAND de 16 octets. La commande retourne la signature SRES (4 octets) et la clé Kc (8 octets).

38

RUN-GSM-ALGORITHM

COMMAND

CLA	INS	P1	P2	Length In	Length Out
A0	88	00	00	10	0C

INPUT DATA

Byte(s)	Description	Length
1 - 16	Randon number	16

OUTPUT DATA

Byte(s)	Description	Length
1 - 4	SRES (SIM result)	4
5 - 12	Cipher Key Kc (session key)	8

39

Lecture de la tables des Services

Le fichier $EF_{SIM\text{-}Service\text{-}Table}$ (6F 38) contient la liste des services offerts par la SIM.
Chaque service est associé à deux bits (bit1 =1 si service présent, bit2 =1 si service actif).

Exemple :
Service n°1 permet la désactivation du code PIN de l'utilisateur,
Service n°2 signale la présence d'un annuaire de numéros abrégés (fichier EF_{ADN}),
Service n°3 notifie la présence d'un annuaire de numéros non abrégés (fichier EF_{FDN}),
Service n°4 signale la présence du fichier des SMS (fichier EF_{SMS}),
etc.

Les fichiers EF_{ADN}, EF_{FDN}, EF_{SMS} appartiennent au répertoire $DF_{TELECOM}$ (7F 10).

40

Les fichiers Annuaire et SMS

Fichier des SMS :

- noté EF_{SMS}, possède 6F 3C comme FID,
- un fichier cyclique,
- permet la lecture et l'écriture des SMS dans la SIM.

Fichier de l'annuaire des numéros ADN

– noté EF_{ADN} avec 6F 3A comme FID,
- est un annuaire téléphonique.

Cmd: A0 A4 00 00 02 6F 3A (READ BINARY EF-ADN)
Rép: 91 0F (indique qu'il y a 0F données à envoyer)
Cmd : A0C0 00 00 0F (GET RESPONSE 0F octets)
Rép: 00 00 **1B 58** 6F 3A 00 11 00 22 01 02 01 **1C** 90 00.

Taille du fichier : 1B 58 (7 000 octets) et taille de l'enregistrement (1C : 28 octets). D'où le nb d'enregistrements : 7000/28=250 octets).

Chaque numéro contient une étiquette qui s'obtient en soustrayant 14 de la taille de l'enregistrement (28-14=14). L'étiquette a son bit de poids fort à 0.

41

Opérations sur les codes PIN

Le code PIN tient sur 8 octets. Les octets non significatifs sont codés par FF.

➢**VERIFY CHV** : présentation de code PIN
A0 20 00 P2 0B **PIN** (P2=01 pour CHV1 : code PIN utilisateur, = 02 pour CHV2).

➢**DISABLE PIN** annule l'utilisation du code PIN.
A0 26 00 01 08 **PIN**

➢**ENABLE PIN** permet l'utilisation du code PIN
A0 28 00 01 08 **PIN**

➢**CHANGE CHV** permet de modifier le code PIN
A0 24 00 01 10 **Ancien_PIN Nouveau_PIN**

➢**UNBLOCK CHV** permet de débloquer une carte bloquée après trois essais infructueux du code PIN (CHV1).
A0 2C 00 01 10 **PUK PIN** (**PUK** est un code unique de 8 chiffres associé à la SIM).

42

SIM Toolkit (STK)

- Spécifié par le standard 3GPP TS 11.14
- Environnement qui fournit des mécanismes permettant aux applications de la SIM d'interagir et d'inter-opérer avec tout terminal mobile (ME) supportant les mécanismes spécifiques requis par ces applications.
- Mécanismes dépendants des commandes et protocoles relevant de la norme 3 GPP TS 51.011.
- Identifié grâce au fichier EF_{SST}
- L'application est déclenchée par des actions externes (gestion des événements).

43

SIM Toolkit (STK)

Permet aux applications de la SIM d'interagir avec le mobile

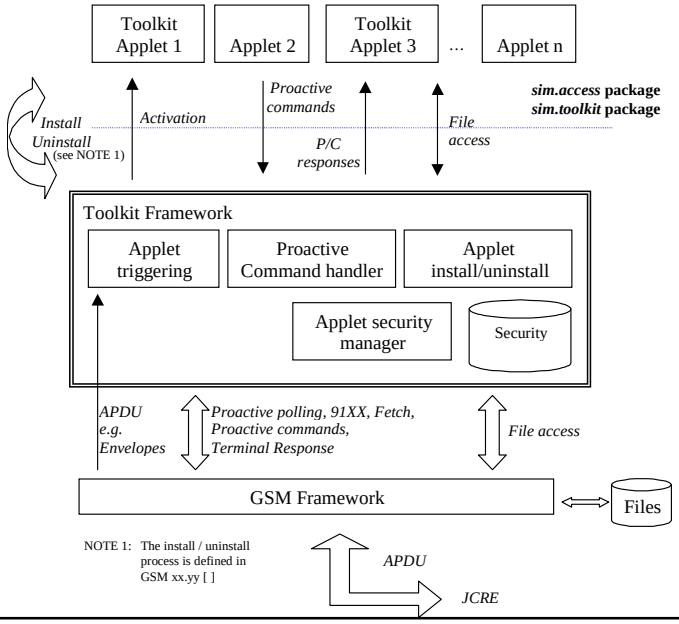
Le standard ETSI GSM 11.14 définit l'interopérabilité la SIM et le mobile

Les applications STK peuvent :

- initier des actions (commandes pro-actives)
- déclencher des actions externes (gestion d'événements)
- obtenir les caractéristiques du mobile (profile du mobile).

44

Framework SIM Toolkit



45

Carte SIM proactive

La carte SIM proactive peut dialoguer avec tous les éléments du terminal mobile à l'aide de commandes proactives spécifiques :

-Avec l'interface radio du mobile (via les commandes proactives **`SET UP`**, **`SEND SHORT MESSAGE`**, **`SEND SUPPLEMENTARY SERVICES`**, etc.)

- Avec l'écran du mobile (**`DISPLAY TEXT`**, **`SET UP MENU`**, **`PLAY TONE`**, etc.)

- Avec le clavier du mobile (**`GET INKEY`**, **`GET INPUT`**, etc.)

46

Commandes de SIM Toolkit

Interface utilisateur	Interface réseau	Interface mobile	Divers
DISPLAY TEXT	SETUP CALL	PROVIDE LOCAL INFORMATION	TERMINAL PROFILE
GET INPUT	SEND SHORT MESSAGE	POLLING INTERVAL	CALL CONTROL
SELECT ITEM	SEND USSD	POLLING OFF	EVENT TRIGGERING
DISPLAY IDLE MODE TEXT	ENVELOPE (SMS-PP DOWNLOAD)	TIMERS	LAUNCH BROWSER
GET INKEY		MORE TIME	BEARER INDEPENDENT PROTOCOL

47

Fonctionnement en mode proactif/1

La carte SIM qui veut envoyer une commande pro-active :

- doit attendre la réception d'une commande **STATUS** par le ME
  (envoyée toutes les secondes, mode polling)

- ou bien répondre à une toute autre commande en remplaçant
SW1 SW2 = 91 XX (**XX** le nb d'octets à envoyer).
  - Le ME répond alors avec la commande **FETCH** à la SIM pour qu'elle émette la commande proactive.

  - Le ME répondra à la commande proactive par l'envoi de la commande **TERMINAL RESPONSE**.

48

Gestion des fonctions de STK

Quatre commandes APDU sont définies pour la gestion des fonctions SIM Toolkit :

➢**FETCH** : utilisée pour transférer une commande Toolkit de la SIM au ME :
Entrée : vide
Sortie : la commande STK (proactive) envoyée vers le ME.

➢**TERMINAL RESPONSE** : sert à envoyer du ME à la SIM la réponse à la commande SAT précédemment exécutée :
Entrée : données constituant la réponse
Sortie : vide

➢**ENVELOPE** : utilisée pour envoyer des données aux applications STK :
Entrée : données
Sortie : la structure des données est définie dans TS 11.14.

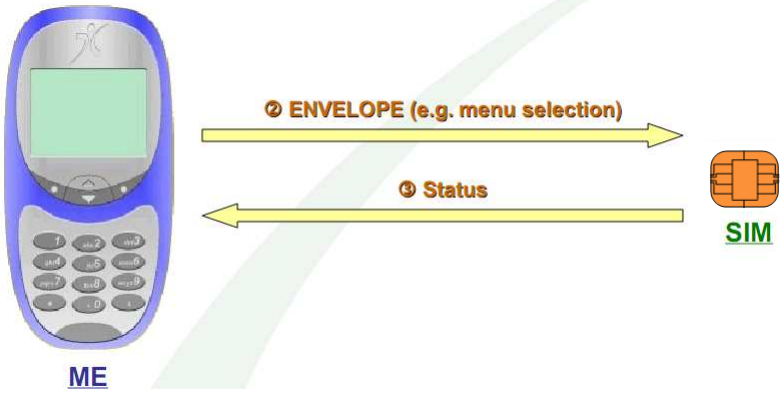
➢**TERMINAL PROFILE** : utilisée par le ME pour transmettre à la SIM, son profil :
Entrée : terminal profile
Sortie : vide

49

Fonctionnement en mode proactif/2

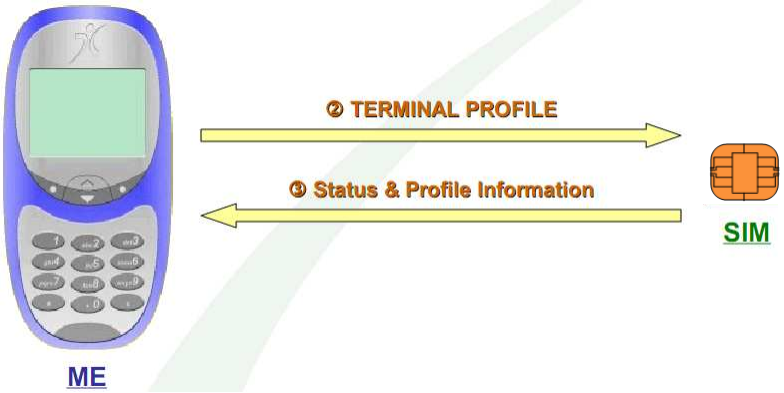
50

Gestion d'événements



51

Chargement du profile



52

La commande TERMINAL PROFILE

Le service SIM proactif doit être activé dans la table de services SIM (TS 11.11).

Un ME qui supporte le mode proactif est identifié lorsqu'une commande TERMINAL PROFILE est envoyée durant l'initialisation de la SIM.

Le ME doit alors envoyer une commande STATUS à la SIM à des intervalles réguliers.

53

Polling proactif

54

Structure des commandes proactives

- Les commandes et réponses SAT sont envoyées via l'interface de données BER-TLV.
- Chaque commande APDU doit contenir un objet BER-TLV.
- TLV = (Tag, Length, Value).
- Le tag est une valeur constante, de 1 octet, indiquant que c'est une commande SAT.

BER-TLV data object	**T**	**L**	**V 1..n SIMPLE-TLV objects**

SIMPLE-TLV data object	**T**	**L**	**V 1..m elements**		**T**	**L**	**V**

Longueur	**Octet 1**	**Octet 2**
0-127	Longueur ('00' à '7F')	Non présent
128-255	'81'	Longueur ('80' à 'FF')

55

Liste des commandes proactives

- Display Text
- Get Inkey
- Get Input
- More Time
- Play Tone
- Poll Intervall
- Refresh
- Set Up Menu
- Select Item
- Send Short Message
- Send SS
- Send USSD
- Set Up Call
- Polling Off
- Provide Local Information
- Set Up Event List
- Perform Card APDU
- Power Off Card
- Power On Card
- Get Reader Status
- Timer Management
- Set Up Idle Mode Text
- Run AT Command
- Send DTMF
- Language Notification
- Launch Browser
- Open Channel
- Close Channel
- Receive Data
- Send Data
- Get Channel Status

56

API Java Card SIM (3GPP TS 43.019 API)

-Extensions des classes de l'API Java Card 2.1.1.

-Permettent l'accès aux fonctions et données décrites dans TS 51.011 et TS 51.014.

L'API utilisée par la carte contient deux paquetages :

➢**sim.access** : fournit les moyens aux applets d'accéder aux données et systèmes de fichiers de l'application GSM définie dans le standard TS 51.011.

➢**sim.toolkit** : fournit les moyens aux applets de s'enregistrer aux événements du framework toolkit, à gérer les informations sous format TLV et à envoyer les commandes proactives selon la spécification 3GPP TS 51.014.

57

Algorithmes d'authentification SIM /USIM

➢**Algorithmes d'authentification GSM sont secrets : exemple de COMP128 qui a été attacké et qui n'est pas recommandé pour l'utilisation.**

➢**ETSI a adopté l'algorithme (rendu publique) : « Milenage » basé sur l'algorithme AES.**

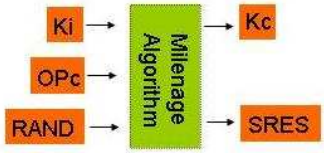
58

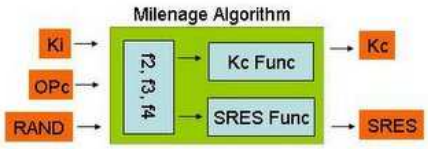
Comparaison de l'authentification SIM/USIM

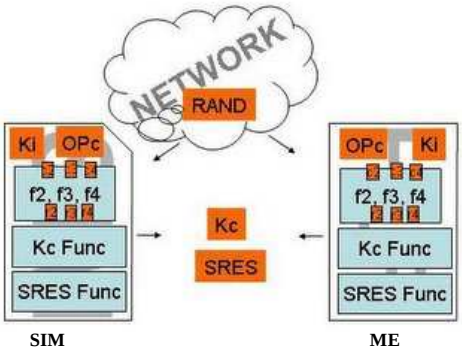
GSM			UMTS		
Description	**Bits**	**Alg**	**Description**	**Bits**	**Alg**
Ki Subscriber authentication key	128		K Subscriber authentication key	128	
RAND random challenge	128		RAND random challenge	128	
XRES exepected result	32	A3	XRES expected result	32-128	f2
Kc cipher key	64 max	A8	Ck cipher key	128	f3
			IK integrity key	128	f4
			AK anonimity key	48	f5
			SQN sequence number	48	
			AMF authentication management field	16	
			MAC message auth. Code	64	f1
Example : algorithm COMP128-1			Example : algorithm Milenage		

59

« Milenage » Algorithme







60

Comparaison Usage SIM/USIM

Caractéristique	SIM	USIM
Classe utilisée	CLA='A0'	CLA='00'
Répertoire racine	MF (3F 00)	ADF USIM (7F FF)
Support de canaux multiples	Non	Oui
Commande d'authentification	RUN GSM ALGORITHM	AUTHENTICATE
Peut être utilisé pour l'accès au GSM	Oui	Oui
Peut être utilisé pour l'accès 3G	Oui	Oui
Support SIM Toolkit	Oui	Oui
Développement de standards	Gelé	En cours
Spécifié dans les versions	Release 1 à Release 4	Release 99 à Release 7

61

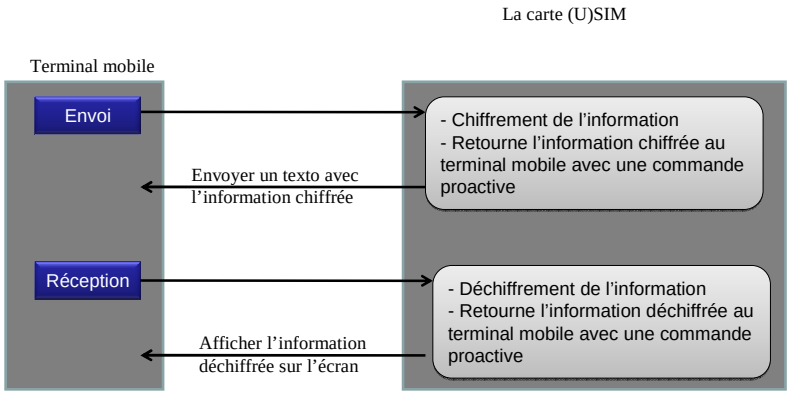
Exemple de l'application sur la carte (U) SIM

- Description de l'application
  - On va construire une application qui nous permet d'enregistrer des données personnelles confidentielles, per exemple: coordonnées bancaires, mots de passe etc.
- Les éléments de base
  - Une applet sur la carte (U)SIM
  - Une Midlet sur le téléphone mobile
  - Communication à effectuer:
    - Entre Midlet et Applet
    - Entre Midlet (Téléphone mobile) et le réseau mobile

62

La logique de l'exemple

Exemple proposé par Serge Chaumette et Jonathan Ouoba, voir:
http://www.labri.fr/perso/chaumett/papers/misc2008/usim



L'Applet

```
public class Applet_Misc extends javacard.framework.Applet implements toolkitInterface,
uicc.toolkit.ToolkitConstants
{
      public Applet_Misc(byte[] bArray, short bOffset, byte bLength)
      public static void install(byte[] bArray, short bOffset, byte bLength)
      public void processToolkit(short event)
      public void process(APDU apdu)
      private void initCrypto()
      private void padUserData (byte[] smsUserData, short len, short pad)
      private void appendUserData (byte[] smsUserData, byte inputData, short offset)
      private void sendSMS(byte[] smsUserData)
}
```

1- Le constructeur Applet_Misc

- Enregistrer l'applet auprès de la plateforme JavaCard
- L'utilisation du paquetage uicc.toolkit de Gemalto
  - reg = ToolkitRegistrySystem.getEntry(): registrer l'applet auprès de SIM Toolkit Framework
  - uiccView = UICCSystem.getTheUICCView(JCSystem.CLEAR_ON_RESET);
- L'invocation de la méthode **initCrypto** pour créer et initier une instance de l'objet de crypto

L'Applet

```
public class Applet_Misc extends javacard.framework.Applet implements toolkitInterface,
uicc.toolkit.ToolkitConstants
{
        public Applet_Misc(byte[] bArray, short bOffset, byte bLength)
        public static void install(byte[] bArray, short bOffset, byte bLength)
        public void processToolkit(short event)
        public void process(APDU apdu)
        private void initCrypto()
        private void padUserData (byte[] smsUserData, short len, short pad)
        private void appendUserData (byte[] smsUserData, byte inputData, short offset)
        private void sendSMS(byte[] smsUserData)
}
```

2- La méthode Install()

☛ Appelée par la plateforme JavaCard dans le processus de l'installation pour créer une instance de l'applet

65

L'Applet

```
public class Applet_Misc extends javacard.framework.Applet implements toolkitInterface,
uicc.toolkit.ToolkitConstants
{
        public Applet_Misc(byte[] bArray, short bOffset, byte bLength)
        public static void install(byte[] bArray, short bOffset, byte bLength)
        public void processToolkit(short event)
        public void process(APDU apdu)
        private void initCrypto()
        private void padUserData (byte[] smsUserData, short len, short pad)
        private void appendUserData (byte[] smsUserData, byte inputData, short offset)
        private void sendSMS(byte[] smsUserData)
}
```

3- La méthode Process()

☛ Chargée de manipulation des commandes APDU

☛ La commande APDU dont le champ INS est de type 0xC1, l'information confidentielle est chiffrée avec d'être retournée dans la réponse APDU:

- ☛ Formatage de l'information avec padUserData
- ☛ Chiffrer l'information avec la méthode cipher3DESEnc.doFinal()
- ☛ L'information chiffrée est retournée dans le tableau apduDataEncrypted

66

L'Applet

```
public class Applet_Misc extends javacard.framework.Applet implements toolkitInterface,
uicc.toolkit.ToolkitConstants
{
        public Applet_Misc(byte[] bArray, short bOffset, byte bLength)
        public static void install(byte[] bArray, short bOffset, byte bLength)
        public void processToolkit(short event)
        public void process(APDU apdu)
        private void initCrypto()
        private void padUserData (byte[] smsUserData, short len, short pad)
        private void appendUserData (byte[] smsUserData, byte inputData, short offset)
        private void sendSMS(byte[] smsUserData)
}
```

3- La méthode Process()

☛ La commande APDU dont le champ INS est de type 0xC3, l'information confidentielle contenue dans le champ de données de la commande est déchiffrée avant d'être retournée dans la réponse APDU:

- ☛ Déchiffrer l'information avec la méthode cipher3DESDec.doFinal()
- ☛ L'information chiffrée est renvoyée en réponse APDU avec la méthode apdusendBytesLong()

67

L'Applet

```
public class Applet_Misc extends javacard.framework.Applet implements toolkitInterface,
uicc.toolkit.ToolkitConstants
{
        public Applet_Misc(byte[] bArray, short bOffset, byte bLength)
        public static void install(byte[] bArray, short bOffset, byte bLength)
        public void processToolkit(short event)
        public void process(APDU apdu)
        private void initCrypto()
        private void padUserData (byte[] smsUserData, short len, short pad)
        private void appendUserData (byte[] smsUserData, byte inputData, short offset)
        private void sendSMS(byte[] smsUserData)
}
```

4- La méthode processToolkit()

☛ L'applet reste inactive jusqu'à quand elle est activée par un événement

☛ Cette méthode prend en charge des opérations liées aux événements définis par le développeur.

☛ L'utilisation du paquetage uicc.toolkit et uicc.access

68

L'Applet

```
public class Applet_Misc extends javacard.framework.Applet implements toolkitInterface,
uicc.toolkit.ToolkitConstants
{
        public Applet_Misc(byte[] bArray, short bOffset, byte bLength)
        public static void install(byte[] bArray, short bOffset, byte bLength)
        public void processToolkit(short event)
        public void process(APDU apdu)
        private void initCrypto()
        private void padUserData (byte[] smsUserData, short len, short pad)
        private void appendUserData (byte[] smsUserData, byte inputData, short offset)
        private void sendSMS(byte[] smsUserData)
}
```

5- La méthode initCrypto()

- Initialiser tous les éléments nécessaires à l'utilisation d'une clé 3DES
- Elle est chargée de l'initialisation des objets cipher3DESEnc et cipher3DESDec qui contiennent respectivement les méthodes pour chiffrer et déchiffrer les données

69

L'Applet

```
public class Applet_Misc extends javacard.framework.Applet implements toolkitInterface,
uicc.toolkit.ToolkitConstants
{
        public Applet_Misc(byte[] bArray, short bOffset, byte bLength)
        public static void install(byte[] bArray, short bOffset, byte bLength)
        public void processToolkit(short event)
        public void process(APDU apdu)
        private void initCrypto()
        private void padUserData (byte[] smsUserData, short len, short pad)
        private void appendUserData (byte[] smsUserData, byte inputData, short offset)
        private void sendSMS(byte[] smsUserData)
}
```

6- La méthode sendSMS()

- l'envoi de l'information confidentielle par SMS
- C'est fait par une commande proactive pour le terminal mobile

70

Bibliographie

http://www.commentcamarche.net/contents/telephonie-mobile/gsm.php3

http://discobabu.blogspot.com/2006/02/gsm-milenage-implementing-it-at.html

Normes GSM : http://www.etsi.org

Article de Pascal Urien, « La carte SIM ou la sécurité du GSM par la pratique », Magazine MISC, hors Série « Cartes à puce », Nov. /Dec. 2008.

Article de Serge Chaumette et Jonathan Ouoba, « Java Card (U)SIM et Applications sécurisées sur téléphones mobiles », Magazine MISC, hors Série « Cartes à puce », Nov. /Dec. 2008.

Description des SMS : http://www.dreamfabric.com/sms/

Smart Card Handbook, Third Edition, Wolfgang Rankl and Wolfgang Effing, Giesecke & Devrient GmbH, Munich, Germany, Translated by Kenneth Cox, John Wiley & Sons, 2002.

Rapport de stage Niang Souleymane réalisé chez Trusted Logics, Master SEM, septembre 2008.

Keith E. Mayes and Konstantinos Markantonakis, Smart Cards, Tokens, Security and Applications, Springer, 2008, 392 pages.

3 GPP TS 11.14. Specification of the SIM Application Toolkit for the Subscriber Identity Module-Mobile Equipement interface (Release 1999).

3 GPP TS 11.11. Technical Specification Group Terminals Specification of the Subscriber Identity Module-ME interface (Release 1999).

3GPP TS 43.019 V6.0.0 (2004-12), Technical Specification, 3rd Generation Partnership Project; Technical Specification Group Terminals; Subscriber Identity Module Application Programming Interface, (SIM API) for Java Card™, Stage 2, (Release 6), http://www.3gpp.org

3GPP TS 51.014 V4.5.0 (2004-12), Technical Specification, 3rd Generation Partnership Project; Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (Release 4)

3GPP TS 51.011 V5.0.0 (2001-12), Technical Specification, 3rd Generation Partnership Project; Technical Specification Group Terminals; Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface, (Release 5)

ETSI SAGE Task Force for 3GPP, Authentication Function Algorithms, VERSION 1.0, Security Algorithms Group of Experts (SAGE); General Report on the Design, Specification and Evaluation of The MILENAGE Algorithm Set: An Example Algorithm Set for the 3GPP, Authentication and Key Generation Functions, 2000 (http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_10/Docs/PDF/SP-000630.pdf).

3GPP TS 43.020 – Technical Specification Group Services & System Aspects; Security Related Network Functions (Release 5, 2002).

SIM Toolkit training, Cours dispensé par Patrick Biget, Trusted Logics, Janvier 2009.

Fin