le cnam

Les Cartes SIM/USIM

Samia Bouzefrane
samia.bouzefrane@cnam.fr
Laboratoire CEDRIC
CNAM
http://cedric.cnam.fr/~bouzefra

Les réseaux cellulaires

samia.bouzefrane@lecnam.net

Il y a eu le GSM/1

- Dans les années 80, plusieurs réseaux cellulaires ont vu le jour en Europe
- Les systèmes sont incompatibles d'un pays à un autre
- Conséquences : - équipements mobiles limités aux frontières du pays
  - marché limité

-Création du « Groupe Spécial Mobile » pour :

- Améliorer la qualité de la transmission
- support international : roaming
- rajout de nouvelles fonctionnalités
- offrir des terminaux et des services à coûts accessibles

samia.bouzefrane@lecnam.net

Il y a eu le GSM/2

➢Normalisation 1982 : Baptisé « Groupe Spécial Mobile »

➢Depuis 1989, l'ETSI (European Telecommunications 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.

➢1991 : devenu une norme internationale nommée « Global System for Mobile communications »

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.

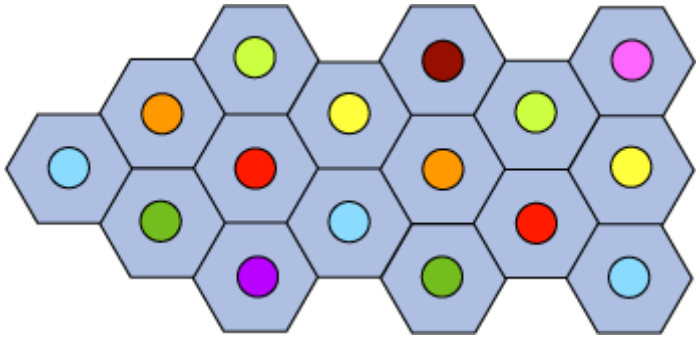
Tri-bande : les téléphones portables pouvant fonctionner en Europe et aux Etats-Unis
Bi-bande : les téléphones fonctionnant uniquement en Europe.

➢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*).

samia.bouzefrane@lecnam.net

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.

samia.bouzefrane@lecnam.net

Éléments du réseau cellulaire GSM

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

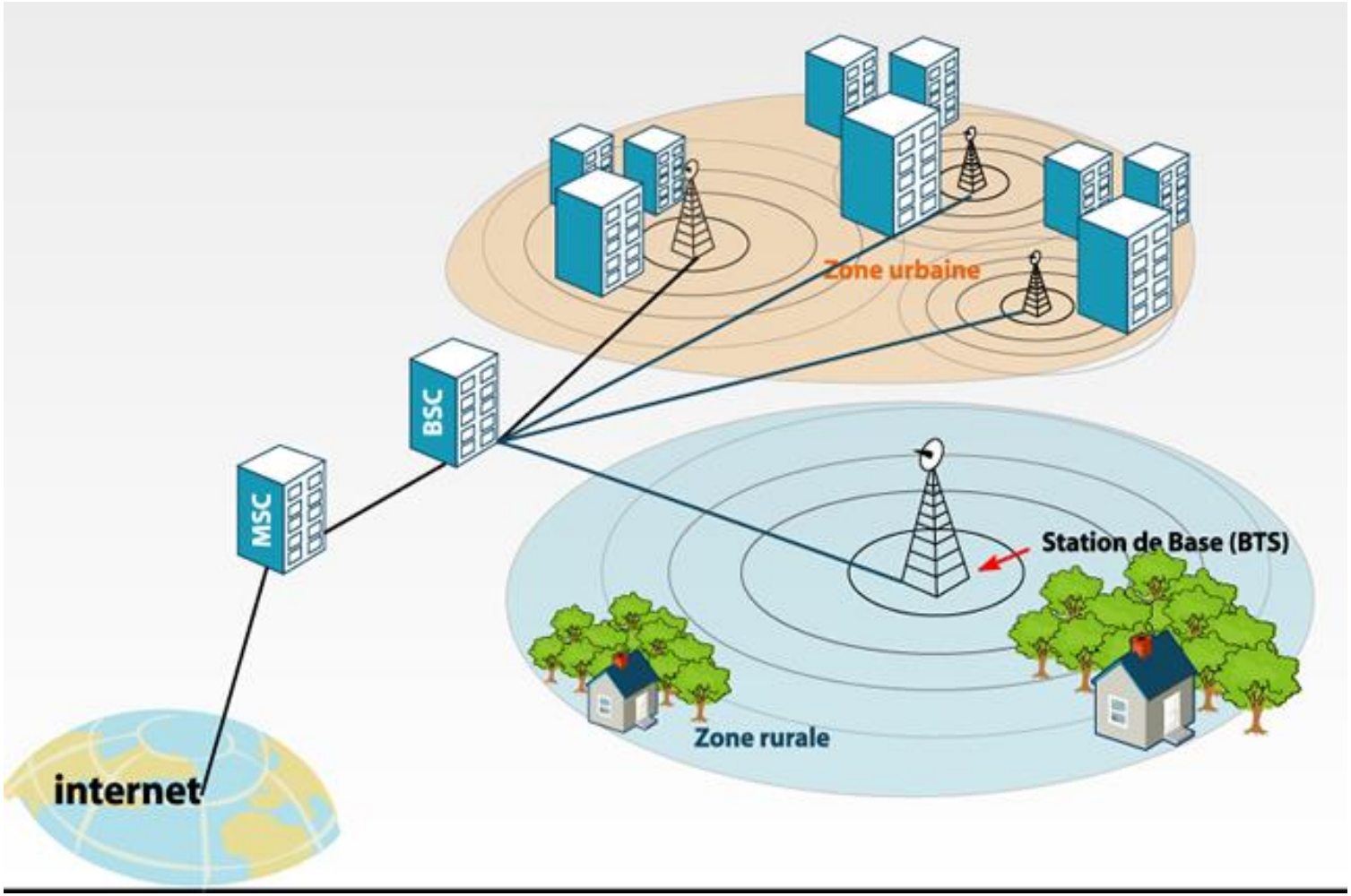
➢**Sous-système radio** (en anglais **BSS** pour *Base Station Subsystem*) =
contrôleur de stations + les stations de base.

➢**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.

samia.bouzefrane@lecnam.net

Architecture du réseau GSM



samia.bouzefrane@lecnam.net

Bases de données manipulées

- **Le registre des abonnés locaux** (**HLR,** *Home Location Register*): base de données contenant des informations (position géographique, informations administratives, etc.) sur les abonnés inscrits dans la zone du commutateur (MSC).

- **Le registre des abonnés visiteurs** (**VLR,** *Visitor Location Register*): base de données contenant des informations sur les autres utilisateurs que les abonnés locaux. Le VLR rapatrie les données sur un nouvel utilisateur à partir du HLR correspondant à sa zone d'abonnement. 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*) : élément chargé de vérifier l'identité des utilisateurs.

samia.bouzefrane@lecnam.net

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.

samia.bouzefrane@lecnam.net

Les stations mobiles

Station mobile

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

➢**Station mobile** composée de :

- Une carte **SIM** (*Subscriber Identity Module*), pour identifier l'usager de façon unique.

- Un équipement mobile 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 appelée *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**.

samia.bouzefrane@lecnam.net

Carte SIM

- **Notion introduite en 1988**
- **Plus de 5 milliards de cartes SIM fabriquées en 2015**
- **Rôle fonctionnel dans le réseau :**

  - Contient les détails concernant l'abonnement de l'utilisateur de téléphone mobile

  - Détient les secrets nécessaires pour prouver l'authenticité du mobile et pour chiffrer les échanges

  - Chargement de nouveaux services

samia.bouzefrane@lecnam.net

Carte SIM : Mobilité

- **Détails d'abonnement mémorisés sur la carte :**

  - Identité unique de l'abonné (IMSI)
  - Numéro de téléphone de l'abonné (MSISDN)
  - Identité de l'équipement mobile (IMEI)
  - Code de service (opérateur)

  etc.

samia.bouzefrane@lecnam.net

Carte SIM : Services sécuritaires

➢ **La carte SIM stocke des informations sensibles** :

➢ Codes secrets :

- Authentification de l'utilisateur : Code PIN (Personal Identification Code) Code PUK (Personal Unlock Code)
- Authentification de l'opérateur : Code PIN (Personal Identification Code) Code PUK (Personal Unlock Code)

➢ Clés secrètes :

- Pour l'authentification de la carte SIM par le réseau
- Pour la communication chiffrée

samia.bouzefrane@lecnam.net

Carte SIM : Services téléchargeables

➢**La carte SIM est un environnement d'exécution pour les applications de confiance**

- Capables d'interagir avec le mobile
  - * Affichage d'infos sur l'écran du mobile
  - * Récupérer les infos de l'utilisateur
  - * etc.

- Capables d'interagir avec le réseau :
  - * envoyer et recevoir des messages (SMS, GPRS, etc.)
  - * géolocalisation

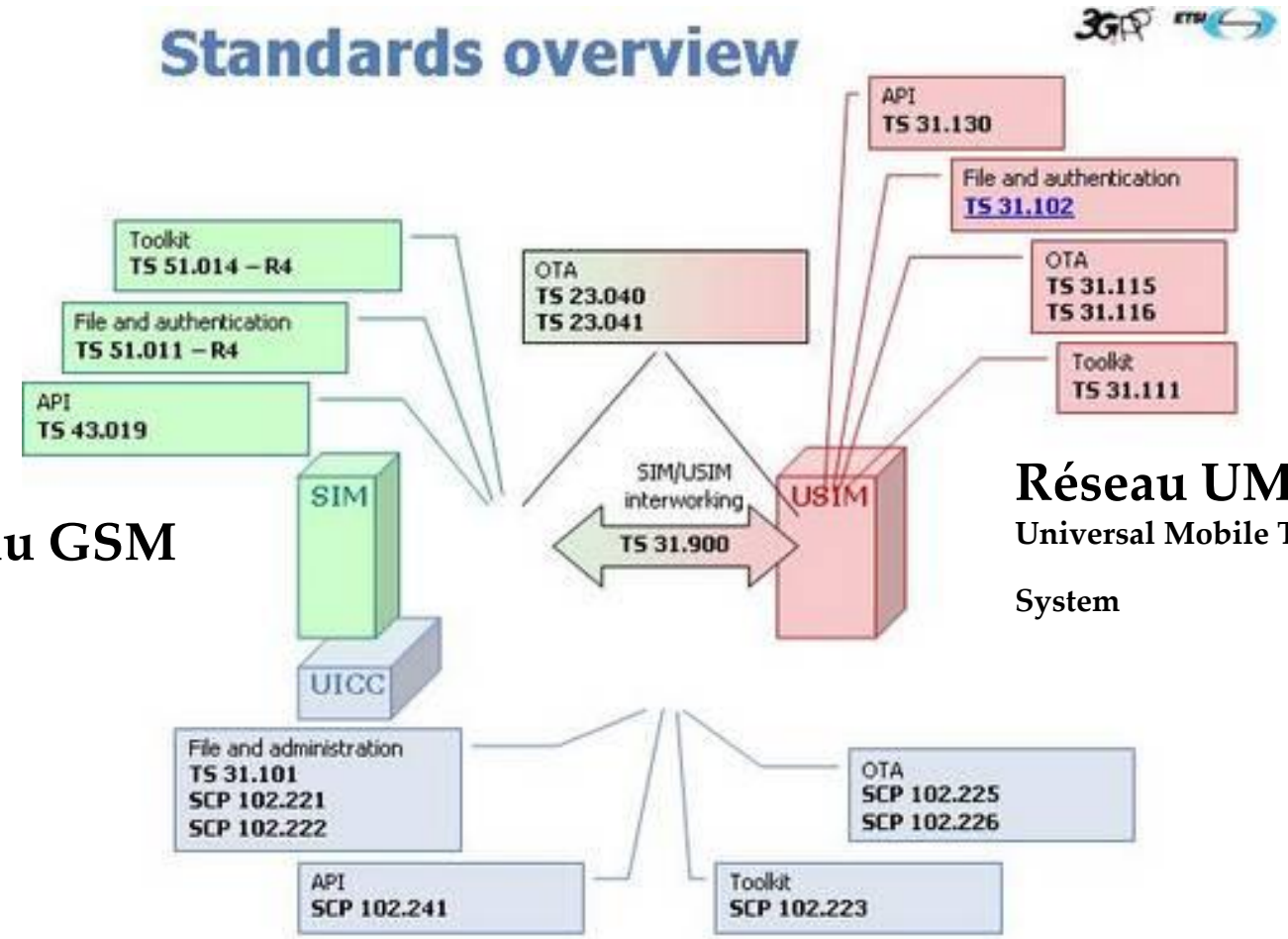
-Capables d'interagir avec le système fichiers de la carte SIM
  - * écrire/lire des fichiers de la SIM

samia.bouzefrane@lecnam.net

La normalisation et la sécurité

samia.bouzefrane@lecnam.net

Les standards



Réseau GSM

Réseau UMTS

Universal Mobile Telecommunications System

UICC: Universal Integrated Circuit Card

samia.bouzefrane@lecnam.net

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

samia.bouzefrane@lecnam.net

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 TMSI (*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".

samia.bouzefrane@lecnam.net

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 à l'aide du code PIN :

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

samia.bouzefrane@lecnam.net

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

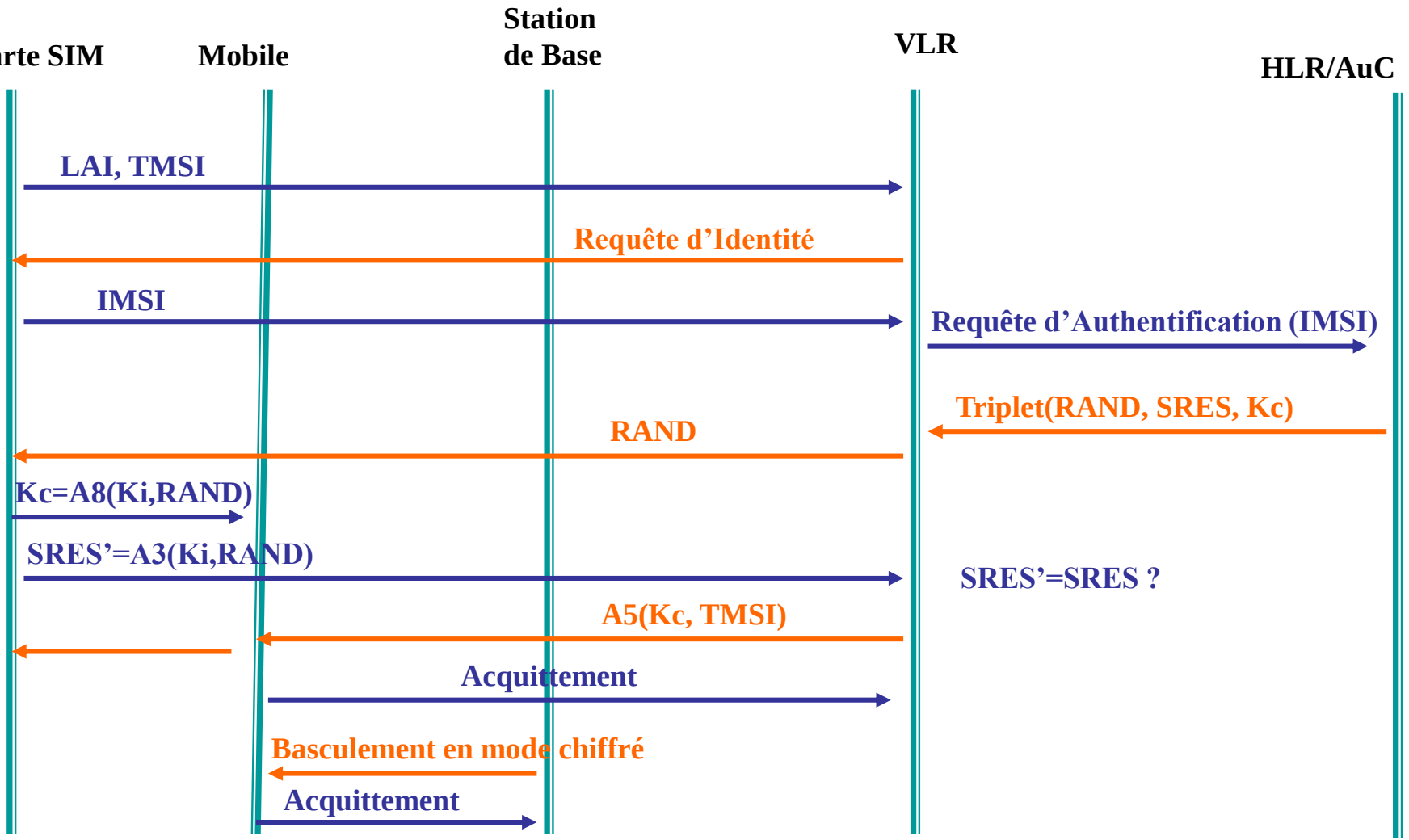
-Le centre d'authentification (AuC*, Authentication Center*).

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).

samia.bouzefrane@lecnam.net

Principes de sécurité d'un réseau GSM/1



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).

samia.bouzefrane@lecnam.net

Principes de sécurité d'un réseau GSM/2

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.

samia.bouzefrane@lecnam.net

Algorithmes cryptographiques

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

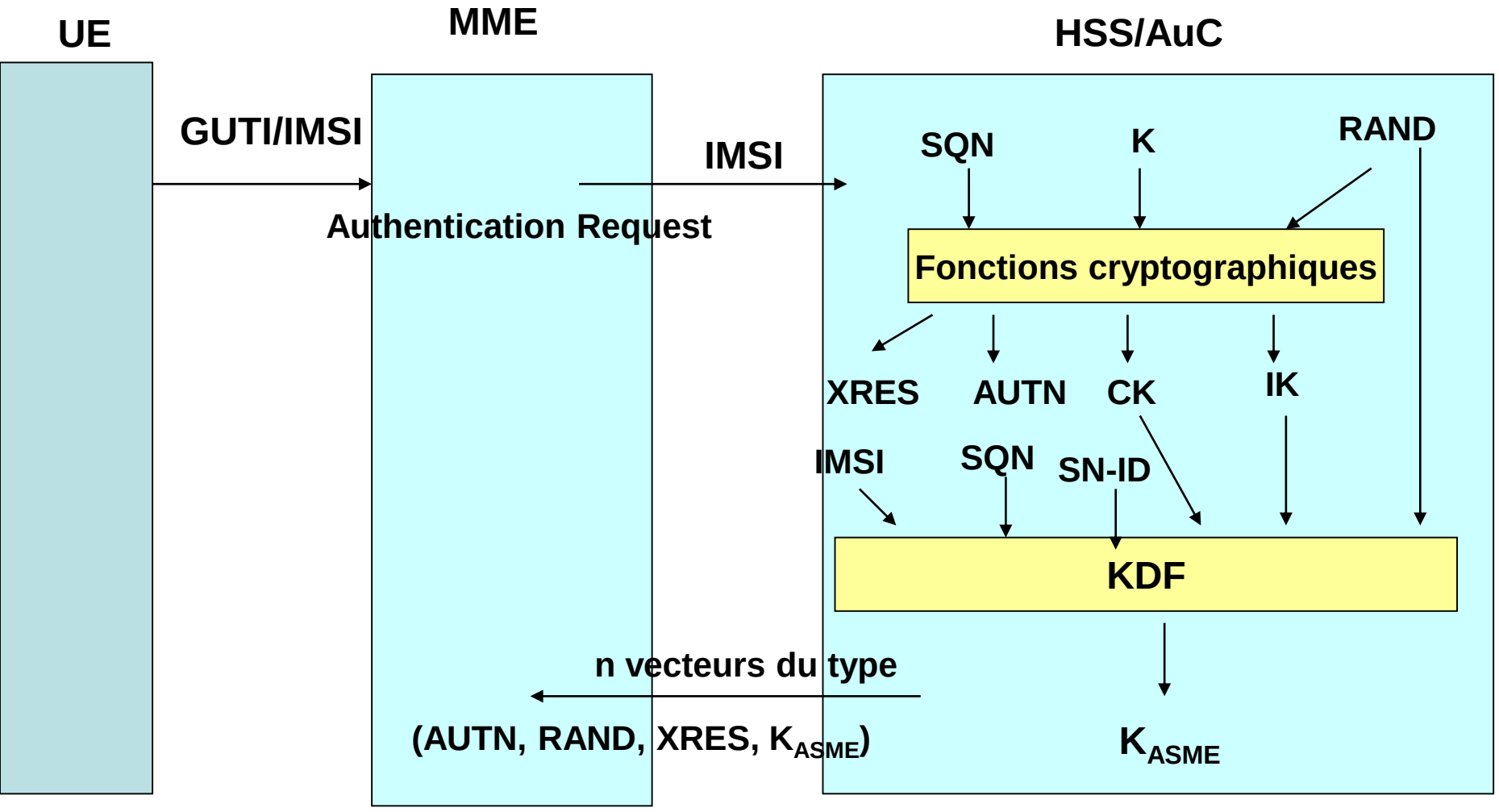
- En 1998, Mark Briceno, Ian Goldberg et David Wagner (chercheurs à l'université de Berkeley) ont cassé l'algorithme A3A8.

- 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.

samia.bouzefrane@lecnam.net

Authentification EPS-AKA (réseau LTE/4G)



Génération de n vecteurs selon ce calcul

samia.bouzefrane@lecnam.net

Le système de fichiers

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).

Aujourd'hui :
Une carte SIM de grande capacité : un CPU (32 bits), RAM (16 Ko), ROM (512 Ko), EEPROM/FLASH (512 Ko), processeur dédié au calcul cryptographique.

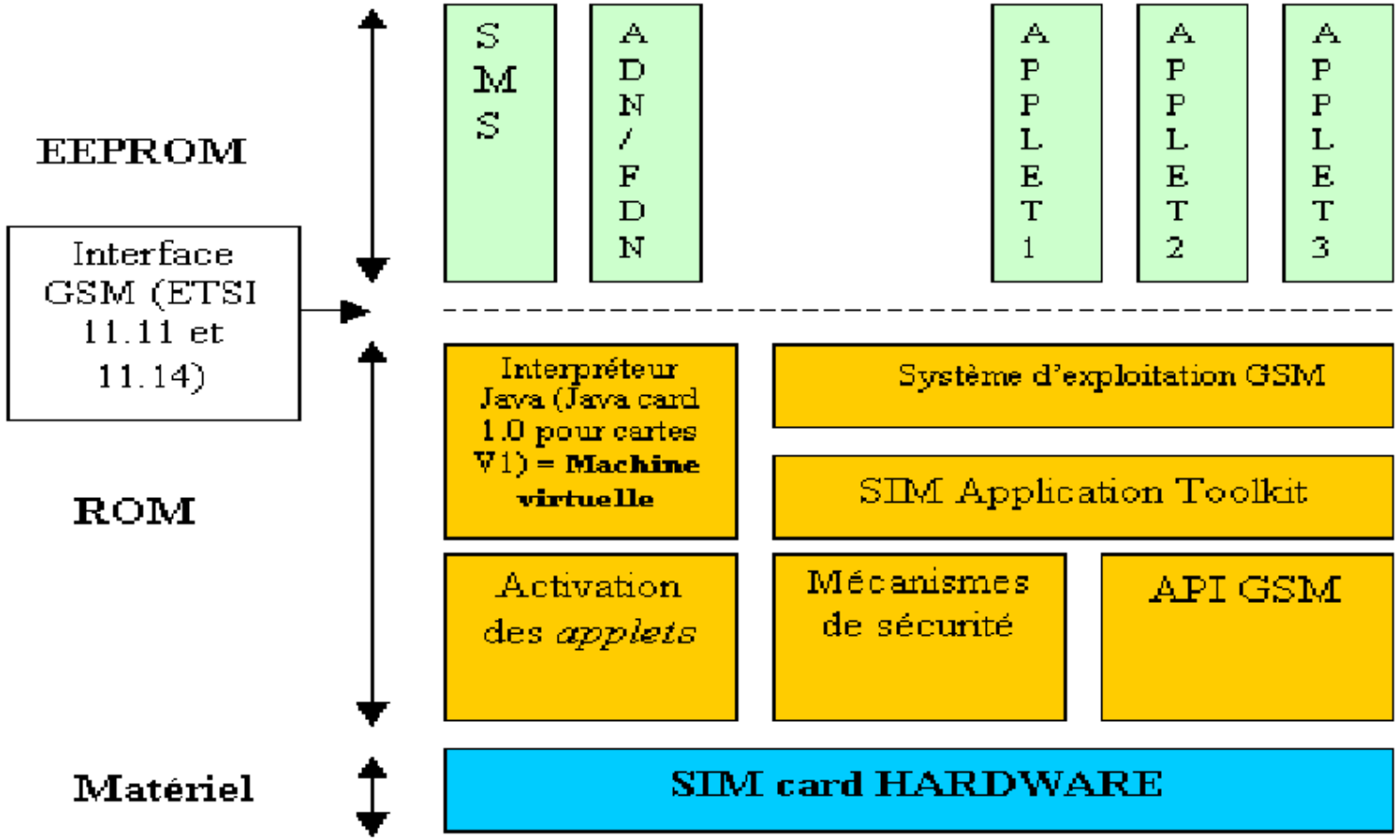
➢**La ROM** (Read Only Memory) contient le système d'exploitation de la carte, les mécanismes de sécurité (algorithmes spécifiques (API GSM).

➢**l'EEPROM** (Electrically Erasable Programmable Read Only Memory) contient des répertoires définis par la 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.

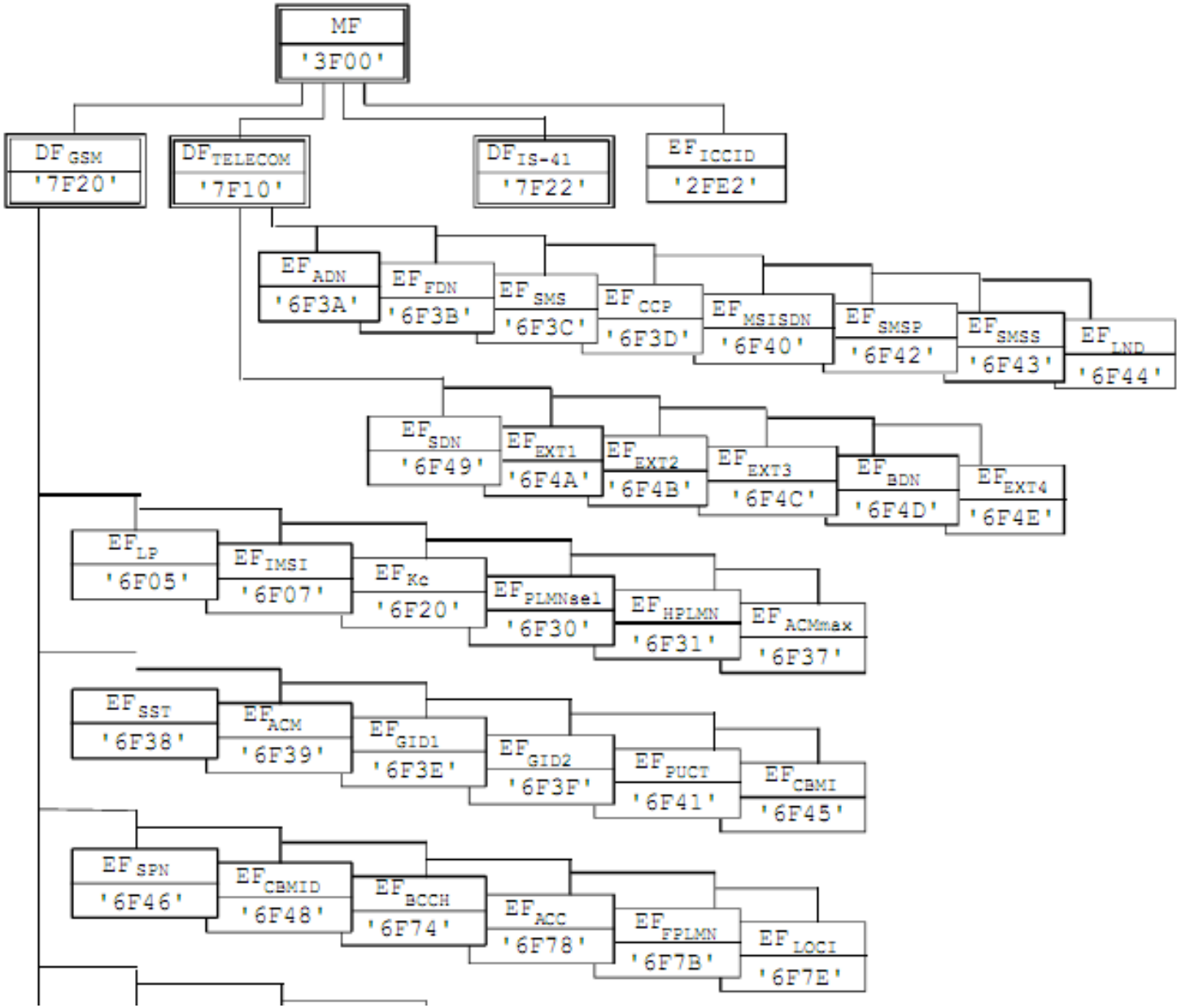
samia.bouzefrane@lecnam.net

Structure d'une carte SIM



samia.bouzefrane@lecnam.net

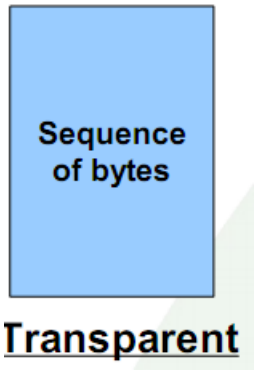
Système de Fichiers selon la norme 3GPP TS 51.011

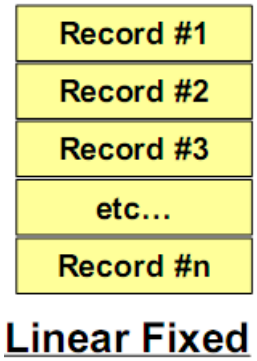


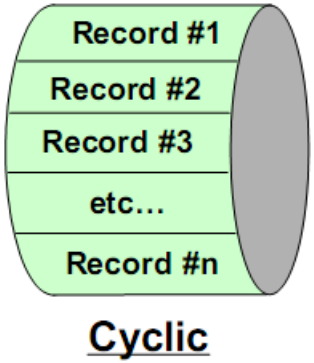
samia.bouzefrane@lecnam.net

Le système de fichiers de la SIM

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







samia.bouzefrane@lecnam.net

Les répertoires/fichiers

- **Répertoire racine** : 3F 00

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

- **identité sur deux octets, 1er octet :**
  - '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.

samia.bouzefrane@lecnam.net

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_{MSISDN} (MSISDN): contient le numéro de l'abonné MSISDN.

samia.bouzefrane@lecnam.net

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,

etc.

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

samia.bouzefrane@lecnam.net

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**

samia.bouzefrane@lecnam.net

Conditions d'accès aux fichiers

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

(**Card Holder Verification 1**) : l'action est possible seulement si une des trois conditions suivantes est remplie :

- Une valeur de CHV1 correcte a déjà été présentée à lu SIM durant la session
- L'indicateur enabled/disabled de CHV1 est défini à « disabled »
- UNBLOCK CHV1 a été successivement exécuté durant la session courante.

CHV2 : l'action est seulement possible si une des deux conditions suivantes est remplie :

- Une valeur correcte CHV2 a déjà été présentée à la SIM durant la session courante,
- UNBLOCK CHV2 a été successivement exécuté durant la session courante.

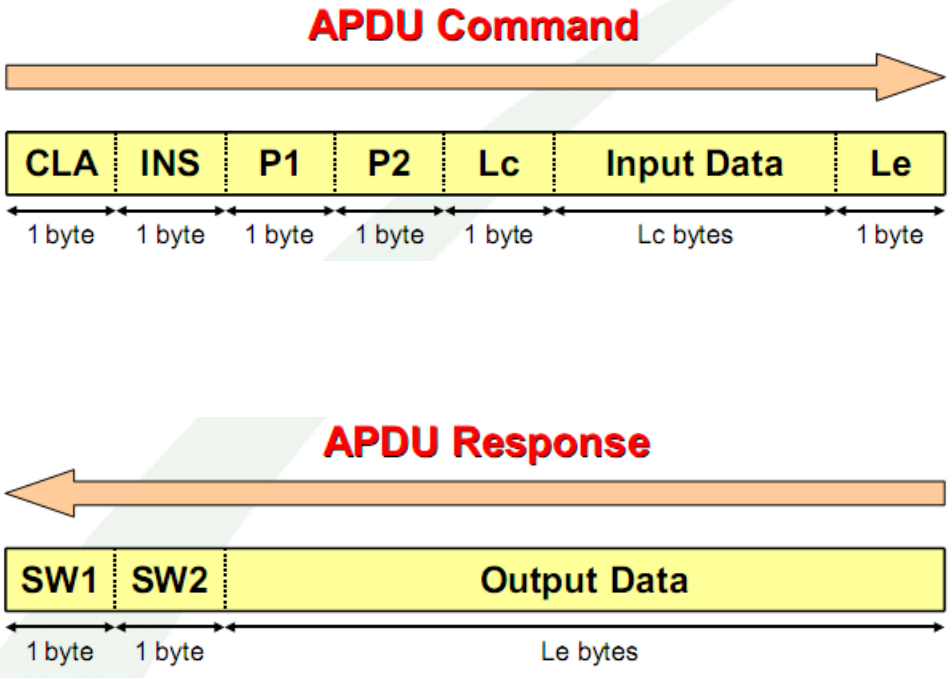
ADM : l'allocation de ces niveaux est de la responsabilité de l'autorité administrative appropriée.

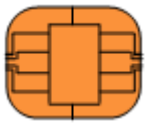
NEVER : l'action ne peut être exécutée au dessus de l'interface SIM/ME.

samia.bouzefrane@lecnam.net

Les commandes APDU

Mobile





SIM

samia.bouzefrane@lecnam.net

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.

samia.bouzefrane@lecnam.net

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

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.

samia.bouzefrane@lecnam.net

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 TMSI suivis de 5 octets pour LAI, ..)

samia.bouzefrane@lecnam.net

Algorithme d'authentification

➢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).

➢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).

samia.bouzefrane@lecnam.net

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).

samia.bouzefrane@lecnam.net

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 (SELECT EF-ADN)
Rép: 9F 0F (la carte souhaite envoyer 0F données)
Cmd : A0 C0 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.

samia.bouzefrane@lecnam.net

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 08 **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).

samia.bouzefrane@lecnam.net

SIM Toolkit

SIM Application Toolkit (SAT)

- 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).

samia.bouzefrane@lecnam.net

Applications SIM Toolkit

➢ **Les applications STK de la carte :**

- initient des actions (dites commandes pro-actives)

- peuvent être déclenchées par des actions externes (gestion d'événements)

- peuvent obtenir les caractéristiques du mobile (profil du mobile)

samia.bouzefrane@lecnam.net

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.)

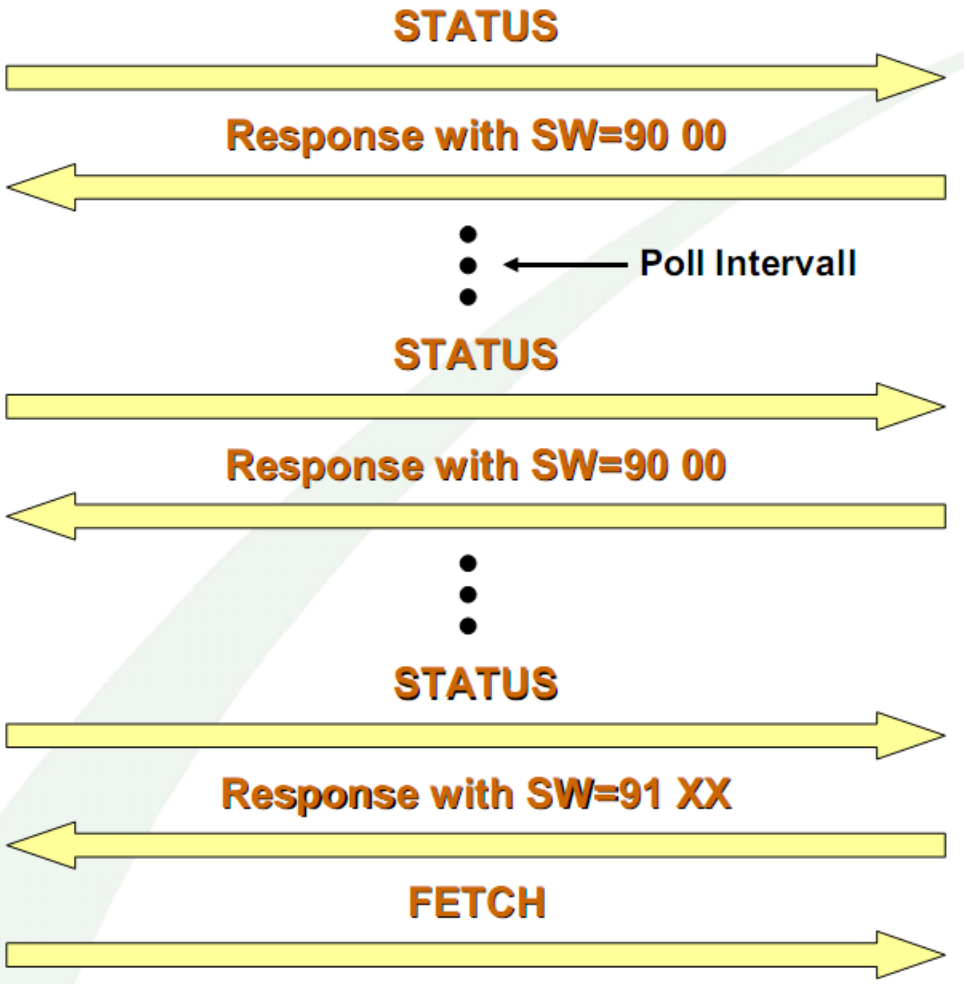
- **Avec l'écran du mobile** (**`DISPLAY TEXT`**, **`SET UP MENU`**, **`PLAY TONE`**, etc.)

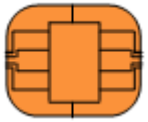
- **Avec le clavier du mobile** (**`GET INKEY`**, **`GET INPUT`**, etc.)

samia.bouzefrane@lecnam.net

Mode Polling

ME





SIM

samia.bouzefrane@lecnam.net

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

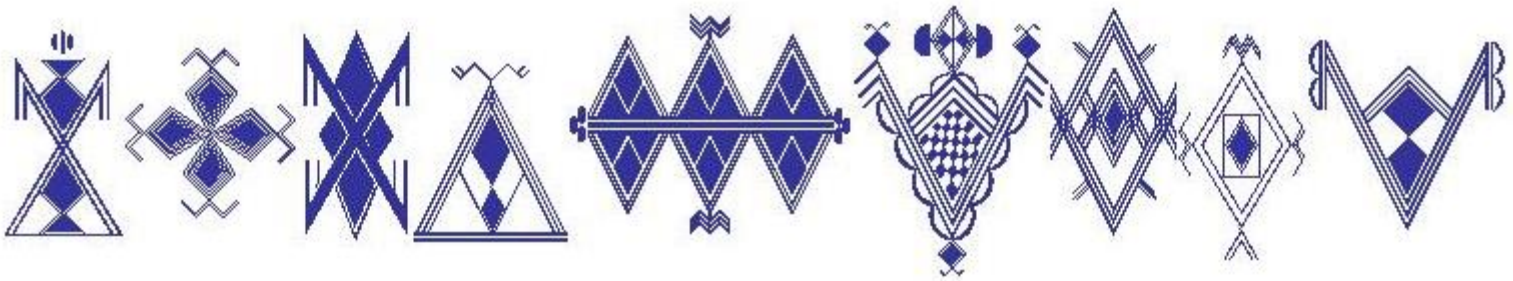
3GPP TS 51.014 V4.5.0 (2004-12), Technical Specification, 3rd Generation Partnership Project; Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (Release 4)

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).

Fin



samia.bouzefrane@lecnam.net