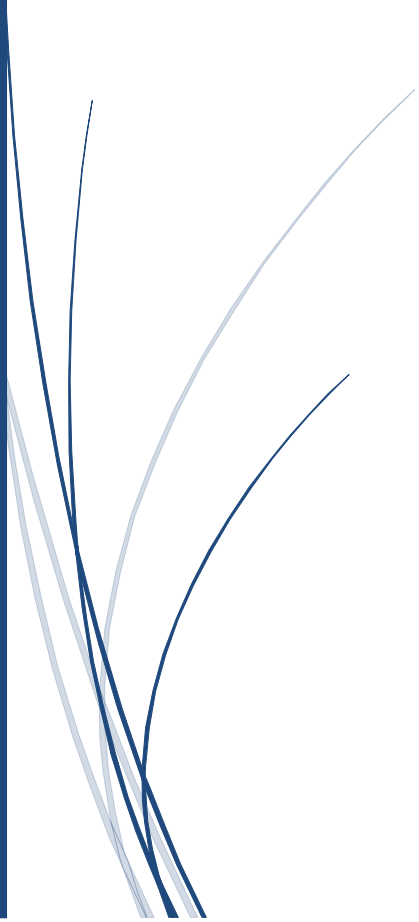
Master 2 – ITLC
Université de M'sila

Chapitre I : Infrastructure d'un réseau GSM



KETFI Mohammed Elamin

Sommaire

1 Infrastructure d'un réseau GSM

1.1 Présentation de l'infrastructure d'un réseau

Le réseau GSM a pour premier rôle de permettre des communications entre abonnes mobiles (GSM) et abonnes du réseau téléphonique commute (RTC –réseau fixe).

Le réseau GSM s'interface avec le réseau RTC et comprend des commutateurs.

Le réseau GSM se distingue par un accès spécifique : la liaison radio.

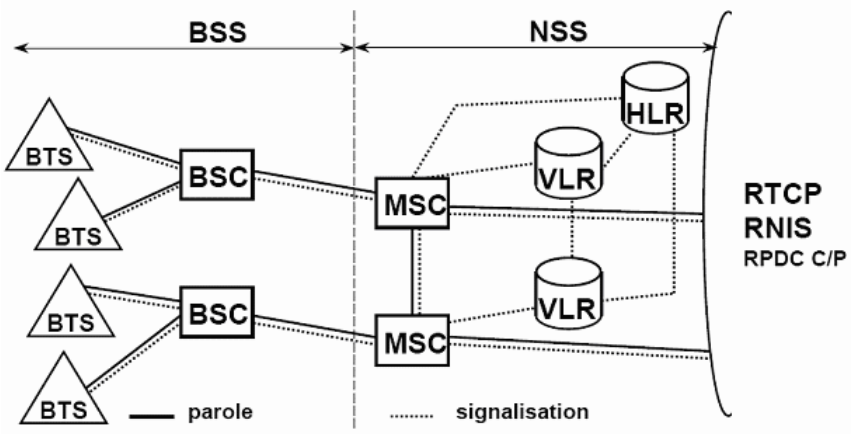
Le réseau GSM est compose de trois sous-ensembles :

• **Le sous-système radio – BSS** Base Station Sub-system assure et gère les transmissions radios

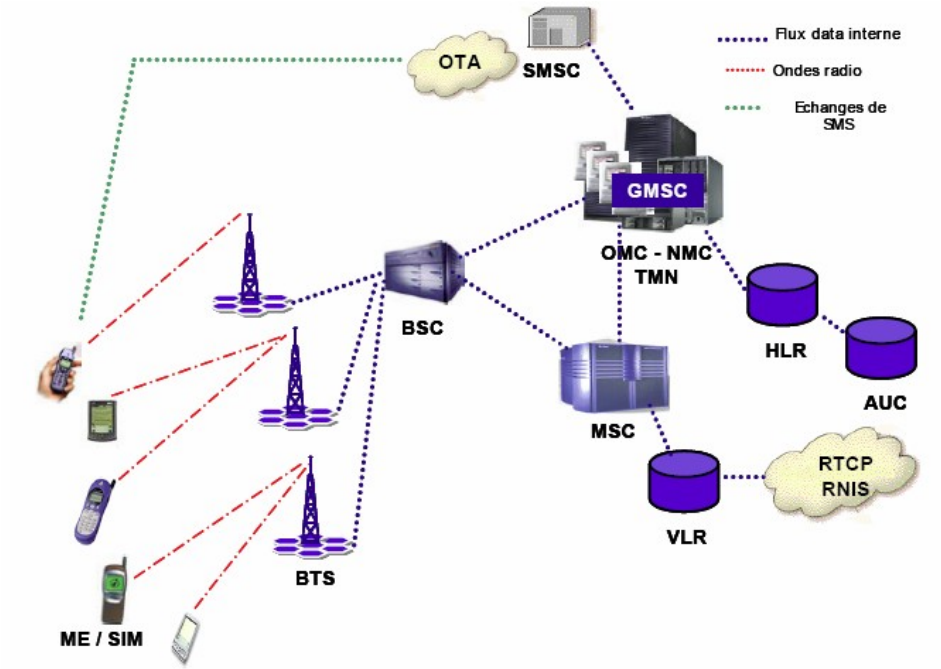
• **Le sous-système d'acheminement – NSS** Network Sub System (on parle aussi de

SMSS Switching and Management Sub-System pour parler du sous-système d'acheminement). Le NSS comprend l'ensemble des fonctions nécessaires pour appels et gestion de la mobilité.

• **Le sous-système d'exploitation et de maintenance – OSS** Operation Sub-System) qui permet à l'opérateur d'exploiter son réseau.



La mise en place d'un réseau GSM (en mode circuit) va permettre à un opérateur de proposer des services de type « Voix » à ses clients en donnant accès à la mobilité tout en conservant un interfaçage avec le réseau fixe RTC existant.



1.2 Les équipements d'un réseau GSM

- **BTS** : Base Transceiver Station (Station de base) assure la réception les appels entrant et sortant des équipements mobiles.

- **BSC** : Base Station Controller (Contrôleur station de base) assure le contrôle des stations de bases.

- **MSC** : Mobile Switching Centre (Centre de commutation de mobile) assure la commutation dans le réseau

- **HLR** : Home Location Register (Enregistrement de localisation normale). Base de données assurant le stockage des informations sur l'identité et la localisation des abonnées.

- **AUC** : Authentification Center (centre d'authentification). Assure l'authentification des terminaux du réseau - VLR Visitor Location Register (Enregistrement de localisation pour visiteur). Base de données assurant le stockage des informations sur l'identité et la localisation des visiteurs du réseau.

1.3 Architecture matérielle du sous-système radio BSS

Le BSS comprend les BTS qui sont des émetteurs-récepteurs ayant un minimum d'intelligence et les BSC qui contrôlent un ensemble de BTS et permettent une première concentration des circuits.

1.3.1 Fonctions de la BTS

La BTS est un ensemble d'émetteurs-récepteurs appelés TRX. Elle a pour fonction la gestion :

- Des transmissions radios (modulation, démodulation, égalisation, codage et correcteur d'erreurs).

- De la couche physique des réseaux.

- De la couche liaison de données pour l'échange de signalisation entre les mobiles et l'infrastructure réseau de l'opérateur.

- De la liaison de données avec le BSC

L'exploitation des données recueillies par la BTS est réalisée par le BSC.

La capacité maximale d'une BTS est de **16 porteuses** (limite technique rarement atteinte pour des raisons de fiabilité). Ainsi une BTS peut gérer au maximum une centaine de communications simultanées.

On distingue deux types de BTS :

• Les BTS dites « normales »'

• Les micros – BTS.

On distingue ensuite différentes classes de BTS normales et micro, en fonction de la nature du réseau (GSM 900 ou DCS 1800) et de la puissance recherchée (puissance exprimée en W).

Les BTS normales sont les stations de base classiques utilisées dans les systèmes cellulaires avec des équipements complémentaires installes dans des locaux techniques et des antennes sur les toits.

Les micro-BTS sont utilisées pour couvrir les zones urbaines denses avec des microcellules. Il s'agit d'équipements de faible taille, de faible coût qui permet de mieux couvrir un réseau dense comme le quartier d'une ville à forte densité de population.

Le rayon d'une cellule varie entre 200m en milieu urbain et 30 km en milieu rural. Une cellule est au minimum couverte par la triangulation de trois BTS.

L'exploitation de la BTS se fait soit en local soit par télécommande au travers de son contrôleur de station (BSC).

1.3.2 Fonctions du BSC

Le BSC est l'organe intelligent du sous-système radio. Le contrôleur de stations de base gère une ou plusieurs stations et remplit différentes fonctions

de communication et d'exploitation. Pour le trafic abonné venant des BTS, le BSC jour un rôle de concentrateur. Il a un rôle de relais pour les alarmes et les statistiques émanant des BTS vers le centre d'exploitation et de maintenance Pour le trafic issu du concentrateur, le BSC joue le rôle d'aiguilleur vers la station de base destinataire. Le BSC est une banque de données pour les versions logicielles et les données de configuration téléchargées par l'opérateur sur les BTS.

Le BSC pilote enfin les transferts entre deux cellules ; il avise d'une part la nouvelle BTS qui va prendre en charge l'abonne « mobile » tout en informant le back end system – ici le HLR – de la nouvelle localisation de l'abonné.

Les BTS sont « contactées » par le centre de maintenance et d'exploitation par le biais des BSC qui jouent ce rôle de relais.

1.4 Architecture matérielle du sous-système fixe NSS

Le NSS comprend des bases de données et des commutateurs.

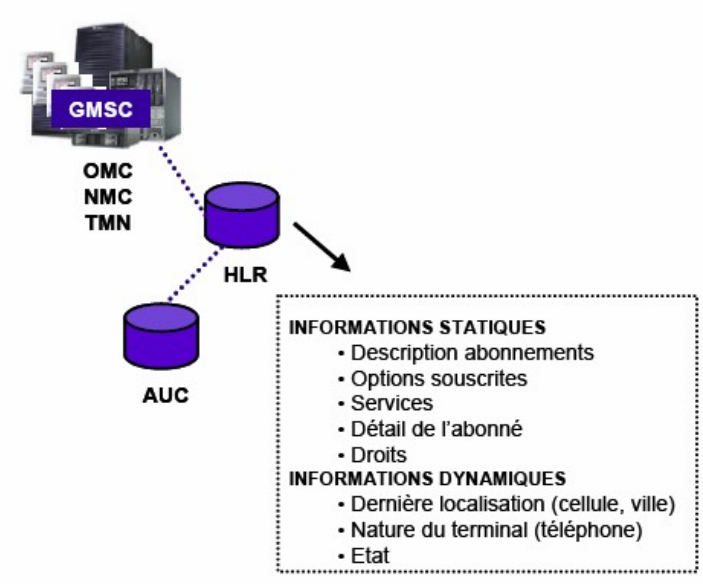
1.4.1 Fonctions du HLR

Le HLR est une base de données de localisation et de caractéristiques des abonnes. Un réseau peut posséder plusieurs HLR selon des critères de capacité de machines, de fiabilité et d'exploitation. Le HLR est I ‘enregistreur de localisation nominale par opposition au VLR (voir partie 1.4.3) qui est I ‘enregistreur de localisation des visiteurs.

Le schéma ce dessous décrit les informations gérées par le HLR.

Une base de données qui conserve des données statiques sur l'abonne et qui administre des données dynamiques sur le comportement de l'abonné.

Les informations sont ensuite exploitées par l'OMC. L'AUC est une base de données associée au HLR.



La carte SIM qui transmet deux informations importantes. L'IMSI (International Mobile Subscriber Identity) qui est gère par le HLR (l'IMSI donne des informations sur le réseau d'origine et le pays entre autre) et le KI (clé de cryptage) qui est géré par la base de données AUC

Prenons un exemple.

IMSI + KI : Identification de l'abonné x

MSISDN : Numéro de téléphone de x (Mobile Station ISDN Number) Le HLR vérifie que le couple IMSI + KI = MSISDN

L'AUC vérifie que le couple IMSI + KI est valide

Les informations dynamiques relatives à l'état et à la localisation d'un abonné sont actualisées en permanence. Ces informations sont particulièrement utiles lorsque le réseau achemine un appel vers l'abonné.

Le réseau commence par interroger le HLR pour prendre connaissance de la dernière localisation connue, de l'état du terminal (On / Off) et de la date de ces données avant toute action. La mobilité constitue la différence essentielle entre le réseau filaire et le réseau de radiotéléphonie.

Ainsi sur le réseau mobile, l'opérateur doit interroger les différentes bases de données (HLR) afin de localiser un abonné pour établir une connexion.

1.4.2 Fonction du MSC

Les MSC sont des commutateurs de mobiles généralement associes aux bases de données VLR. Le MSC assure une interconnexion entre le réseau mobile et le réseau fixe public. Le MSC gère l'établissement des communications entre un

mobile et un autre MSC, la transmission des messages courts et l'exécution du handover si le MSC concerné est impliqué. (Le handover est un mécanisme grâce auquel un mobile peut transférer sa connexion d'une BTS vers une autre

(handover inter BTS) ou, sur la même BTS d'un canal radio vers un autre (handover intra BTS). On parle de transfert automatique inter/intra cellule Le commutateur est un noeud important du réseau, il donne un accès vers les bases de données du réseau et vers le centre d'authentification qui vérifie les droits des abonnes. En connexion avec le VLR le MSC contribue à la gestion de la mobilité des abonnés (à la localisation des abonnés sur le réseau) mais aussi à la fourniture de tous les télé services offerts par le réseau : voix, données, messageries ... Le MSC peut également posséder une fonction de passerelle, GMSC (Gateway MSC) qui est activée au début de chaque appel d'un abonné fixe vers un abonné mobile.

Un couple MSC / VLR gère généralement une centaine de milliers d'abonnés. Les commutateurs MSC sont souvent des commutateurs de transit des réseaux téléphoniques fixes sur lesquels ont été implants des fonctionnalités spécifiques au réseau GSM.

1.4.3 Fonctions du VLR

L'enregistreur de localisation des visiteurs est une base de données associée à un commutateur MSC. Le VLR a pour mission d'enregistrer des informations dynamiques relatives aux abonnes de passage dans le réseau, ainsi l'opérateur peut savoir à tout instant dans quelle cellule se trouve chacun de ses abonnés. Les données mémorisées par le VLR sont similaires aux données du HLR mais concernent les abonnés présents dans la zone concernée.

A chaque déplacement d'un abonné le réseau doit mettre à jour le VLR du réseau visite et le HLR de l'abonné afin d'être en mesure d'acheminer un appel vers l'abonné concerné ou d'établir une communication demandée par un abonné visiteur.

Pour ce faire un dialogue permanent est établit entre les bases de données du réseau.

La mise à jour du HLR est très importante puisque lorsque le réseau cherche à joindre un abonné, il interroge toujours le HLR de l'abonné pour connaître la dernière localisation de ce dernier, le VLR concerné est ensuite consultés afin de tracer le chemin entre le demandeur et le demandés pour acheminer l'appel.

1.5 Sous système d'exploitation et de maintenance OSS

1.5.1 L'administration de réseau

L'administration du réseau comprend toutes les activités qui permettent de mémoriser et de contrôler les performances d'utilisation et les ressources de manière à offrir un niveau correct de qualité aux usagers.

On distingue 5 fonctions d'administrations :

• **L'administration commerciale**

La déclaration des abonnés et des terminaux, la facturation, les statistiques ...

• **La gestion de la sécurité**

La détection des intrusions, le niveau d'habilitation ...

• **L'exploitation et la gestion des performances**

L'observation du trafic et de la qualité (performance), les changements de configuration pour s'adapter à la charge du réseau, la surveillance des mobiles de maintenance ...

• **Le contrôle de configuration du système**

Les mises à niveau de logiciels, les introductions de nouveaux équipements ou de nouvelles fonctionnalités ...

• **La maintenance**

Les détections de défauts, les tests d'équipements ...

Le système d'administration du réseau GSM est proche du concept TMN qui à pour objet de rationaliser l'organisation des opérations de communication et de maintenance et de définir les conditions techniques d'une supervision économique et efficace de la qualité de service.

1.5.2Architecture de TMN (Télécommunications Management Network)

L'administration des premiers réseaux se faisait de manière individuelle sur chaque équipement à partir d'un terminal simple directement connecté. Ainsi les fonctions disponibles étaient liées à la structure matérielle de l'équipement. Ce niveau d'administration est encore utilisable mais il est peu à peu remplacé par des terminaux déplaces et relies aux équipements par l'intermédiaire d'un réseau de données. Le réseau X.25 Transpac (réseau lancé par France Télécom et basé sur la transmission des données par paquet) est une option possible.

1.5.3 Fonctions de l'EIR (Equipement Identity register)

L'EIR est une base de données annexe contenant les identités des terminaux. Un terminal est identifié par un numéro de série dénommé IMEI (IMEI = numéro

d'homologation (série). Numéro d'identifiant. Numéro du terminal). La base EIR est consulté lors des demandes de services d'un abonné pour vérifier si le terminal utilise est autorisé à fonctionner sur le réseau. Ainsi l'accès au réseau peut être refuse si le terminal n'est pas homologue, si le terminal perturbe le réseau ou si ce même terminal a fait l'objet d'une déclaration de vol. Dans la réalité ces bases de données EIR sont peu utilisées faute d'accords entre les opérateurs d'un même pays. La création d'une liste noire des terminaux volés pour en interdire leur utilisation pourra décourager les vols de téléphones portables.

1.5.4Fonctions de l'AUC

Le centre d'authentification AUC (AUthentification Center) mémorise pour chaque abonné une clé secrète utilisée pour authentifier les demandes de services et pour chiffrer (crypter) les communications. L'AUC de chaque abonne est associe au HLR. Pour autant le HLR fait partie du « sous-système fixe » alors que l'AUC est attaché au « sous-système d'exploitation et de maintenance ». L'AUC avec l'IMSI et le MSISDN fait partie des données clé insérées dans la carte SIM de chaque abonné.

1.5.5 Présentation de l'OMC et du NMC

Deux niveaux de hiérarchie sont définis dans la norme GSM. Les OMC

(Operations and Maintenance Center) et le NMC (Network and Management Centre).

Cette organisation a été définie afin de permettre aux opérateurs télécoms de gérer la multiplicité des équipements (émetteurs, récepteurs, bases de données, commutateurs ...) et des fournisseurs.

Le NMC permet l'administration générale de l'ensemble du réseau par un contrôle centralisé.

Les OMC permettent une supervision locale des équipements (BSC /MSC / VLR) et transmettent au NMC les incidents majeurs survenus sur le réseau. Les différents

OMC assurent une fonction de médiation.

NB : Plus généralement dans les schémas présentés dans cette partie, l'OMC désigne l'ensemble du sous-système d'exploitation et de maintenance (OSS) TMN compris, et ce dans un souci de clarté et de simplification des représentations graphiques.

1.6 Présentation des interfaces

Les interfaces désignées par des lettres de A à H dans le tableau ci-après ont été définies par la norme GSM. Bien souvent, le découpage des fonctions entre les éléments du réseau (VLR et MSC) par exemple est effectue par les constructeurs (Ericsson, Nokia ...) qui ne respectent pas forcement celles définies dans le tableau.

Deux normes sont néanmoins imposées :

• L'interface D qui permet au couple MSC/VLR de dialoguer avec le HLR afin d'assurer l'itinérance internationale que I'on dénomme « roaming ». (Un abonné d'un réseau camerounais quitte le Cameroun pour se rendre en Espagne et se connecter au réseau espagnol. Ce cas présent est un cas de roaming).

• L'interface A qui sépare NSS et BSS. Ainsi les opérateurs peuvent avoir un multisourcing de BSC et MSC (avoir plusieurs fournisseurs différents pour leur infrastructure).

• L'interface Abis supporte les transmissions de communication entre BSC et BTS.

En réalité, la plupart des messages de signalisation sont changé entre le BSC ou le MSC et le MS : la BTS n'a qu'une simple fonction de relais.

NB : Le handover est l'ensemble des opérations mises en œuvre pour permettre qu'une station

mobile puisse changer de cellule sans interruption de service. Cette notion est traitée à la

séquence 4 intitulé "gestion de la mobilité" de ce cours.

1.7 Architecture réseau en couches (modéle OSI)

La recommandation GSM établit un découpage des fonctions et une répartition de celles ci sur divers équipements. La structuration en couches reprend ce découpage en respectant la philosophie générale des couches du modèle OSI.

1.7.1 Couches réseaux gérées par le sous-système radio (BSS)

Dans le BSS on retrouve les 3 couches de base du modèle OSI :

• La couche physique définit l'ensemble des moyens de transmission et de réception physique de l'information.

• La couche liaison de données a pour objet de fiabiliser la transmission entre deux équipements par un protocole.

• La couche réseau a pour fonction d'établir, de maintenir et de libérer des circuits commutés (voix ou données) avec un abonné du réseau fixe. Cette couche est ensuite divisée en trois sous couches :

La sous couche RR (Radio Ressource) pour les aspects purement radio. Cette couche gère le l'établissement d'un canal dédié et le rétablissement des canaux lors du changement de cellules. Il ne peut y avoir qu'une seule connexion RR active. C'est un pré requis nécessaire avant toute connexion réseau.

La sous couche MM (Mobility management) qui assure la gestion de la mobilité ce qui génère des échanges entre la MS et le réseau mise à jour de localisation).

Elle assure aussi les fonctions de sécurité, ce qui va provoquer des échanges de messages particuliers lors de la plupart des demandes de services.

Cette couche permet à la couche CM de faire abstraction des problèmes de l'aspect itinérant et radio de la MS et de se ramener au cas d'un accès terminal fixe au réseau RNIS. Une telle connexion est établit sur demande del la couche CM(sur envoi d'appel ou SMS) non pas par envoi de message d'établissement mais implicitement par le premier message CM

La sous couche CM (Connection Management). Elle assure la gestion des usagers, l'acheminement et l'établissement des appels d'un abonné. Elle est découpée en quatre entités :

L'entité CC (Call Control) qui traite la gestion des connections de circuit avec le destinataire final.

L'entité SMS (Short Message Service) qui assure la transmission et la réception de messages courts.

L'entité SS (Supplementary Services) qui gère les services supplémentaires.

L'entité GCC (Group Call Control) qui a pour objet de contrôler les appels de groupes. (Attention seulement téléphone compatible SIM phase 2+) L'entité BCC (Broadcast Call Control) qui a pour objet de contrôler les appels diffusés. (Attention seulement téléphone compatible SIM phase 2+)

NB : Une entité de gestion de données par paquets devrait également être définie par la suite

Ce sont des premiers pas vers l'approche GPRS.

La couche 1 — physique et la couche 2 — liaison de données sont gérées dans leur intégralité dans le BSS. En revanche, concernant la couche 3 — réseau, seul la sous couche RR est gérée au sein du BSS, les sous couches CM et MM ne font que « transiter » par le BSS sans être analysées.

1.7.2 Couches réseaux gérées par le sous système fixe (NSS)

Le réseau fixe NSS que nous avons vu précédemment regroupe ensuite les 4 couches complémentaires du modèle OSI. Le réseau NSS en GSM est relie et géré avec le réseau RTC (Réseau Téléphonique Commuté) — réseau de téléphonie fixe initial. Les 4 couches complémentaires sont ainsi regroupées au sein de cet ensemble qui permet de gérer les connexions entre abonnes mobiles et abonnes fixes.

1.8 La station mobile de l'utilisateur final

1.8.1 Le mobile

Le terme station mobile désigne un terminal équipé d'une carte SIM. Chaque terminal reste muni d'une identité particulière IMEI (Voir séquence 3 intitulé gestion de l'itinérance de la sécurité et des appels dans les réseaux mobile). La norme définit pour les terminaux plusieurs classes suivant leur puissance maximale d'émission. En GSM 800, deux catégories, 2W en téléphone mobile portable et 8W en téléphone mobile embarqué dans les véhicules. En DCS 1800, de manière générale 1W pour l'ensemble des terminaux.

1.8.2La carte SIM

La carte SIM telle que définit dans la norme GSM permet aux abonnes une mobilité personnelle indépendante du terminal utilise. Il existe initialement deux types de cartes SIM :

• La carte SIM ID-1 : carte à la taille d'une carte de crédit.

• La carte SIM plug in : de petite taille. L'objet de cette carte est d'être utilisée de façon quasi permanente dans un terminal portatif donné.

La carte IM contient de nombreux paramètres de sécurité. Comme toute carte à puce elle possède un ensemble de clés permettant de sécuriser les étapes de personnalisation par les différents intervenants (fabricants, opérateurs, distributeurs, utilisateurs). A chaque intervenant est associe un code, nous connaissons le code PIN compose de 4 a 6 chiffres, également appelé CHIV1.

L'architecture d'une carte SIM est simple, il y a trois parties :

• La mémoire ROM (Read Only Memory) d'une taille de 16Koctets contient l'OS, des algorithmes et éventuellement des applications spécifiques. Voir NB1

• La mémoire EEPROM (E2 PROM – Electrical erasable Programmable Read Only

Memory) contient tous les champs de la norme GSM et des applications. Sa taille varie entre 8 KO et 64 KO aujourd'hui.

• La mémoire RAM (Random Access Memory) contient des données liées aux applications spécifiques, la taille est réduite, généralement quelques centaines d'octets.

NB 1 : L'OS de la carte est intègre au sein de la mémoire ROM. Initialement propriété des

SIM manufacturers, ces OS étaient développés en natif pour le compte des opérateurs.

Aujourd'hui les OS tendent à être développés en Java, ce qui ouvre des ouvertures pour des sociétés souhaitant développer des OS pour le compte de clients. Le SIM manufacture devient alors un fabricant industriel de cartes qui intègre des données (OS) développées pour une tierce partie.

NB 2 : Les SIM manufacturers parlent essentiellement de la taille de la E2PROM pour présenter leurs produits, on parlera ainsi de Cartes 32 Ko, 64 ko ...

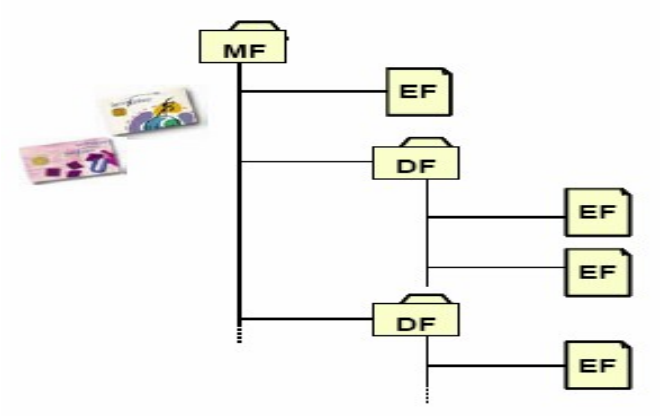
L'architecture d'une carte SIM respecte une organisation interne définie dans la norme GSM.

La racine est constituée par le dossier maître MF (Master File)

Le fichier MF peut contenir des fichiers élémentaires EF (Elementary File)

Le fichier MF contient des répertoires dédies DF (Dedicated Files)

Chaque répertoire DF peut contenir des fichiers élémentaires EF.



1.10 Conclusion sur le réseau GSM

La mise en place d'un réseau GSM représente un investissement considérable.

A l'heure actuelle les réseaux GSM ne cessent d'évoluer afin d'assurer une qualité de couverture toujours plus importante. La couverture du réseau est assurée par la multiplication des ensembles BTS – BSC. Nous verrons par la suite que le réseau GSM est une base pour la mise en place des réseaux GPRS et UMTS, même si pour le réseau UMTS au-delà du coût élevé d'achat des licences, nous verrons que ('ensemble BTS – BSC – MSC devra être changé ou modifié à la base.

Rappelons ici rapidement qu'une BTS couvre environ 500m de zone en ville et 10 km de zone en campagne. Cela donne un aperçu du coût et du temps nécessaires pour la mise en place de la simple architecture technique du mode UMTS. Ci-dessous un rappel de l'architecture GSM, en encadré bleu les éléments de couverture, en ellipse bleue les éléments de gestion du réseau, en ellipse rouge, les éléments du réseau GSM qui seront utiles pour les réseaux GPRS et UMTS.