GSM : Global System for Mobile Communications
Architecture, Interfaces et Identités

EFORT
http://www.efort.com

La définition de la norme GSM remonte au début des années 80. A l'origine, la prise de conscience par les opérateurs que le marché du radiotéléphone en Europe était morcelé du fait de la multiplicité des systèmes analogiques alors en place et des bandes de fréquence correspondantes. La conséquence était l'impossibilité pour l'usager d'utiliser son terminal ailleurs que dans son réseau d'origine. De ce constat est né le concept de système de radiotéléphonie européen permettant d'abolir les frontières du réseau et de constituer un véritable marché européen pour les équipements d'infrastructure et de terminaux.
En 1982, le CEPT (Conférence Européenne des Postes et Télécommunications) décide alors de constituer le Groupe Spécial Mobile (dont est issu le nom GSM) avec pour mission de développer un standard paneuropéen pour les communications mobiles. L'acronyme GSM correspond à Global System for Mobile Communications.
D'ailleurs, le réseau radiomobile GSM représente le premier système standardisé qui utilise une technique de transmission numérique pour le canal radio: Ce point représente une caractéristique particulière du réseau, parce que tous les systèmes radio cellulaires précédents utilisaient des techniques de transmission analogiques. Une autre caractéristique essentielle du système est le roaming (itinérance), c'est à dire la possibilité offerte à l'utilisateur mobile d'accéder aux services GSM même dans le cas où il se trouve à l'extérieur de la zone de couverture de son réseau de souscription, en tant qu'utilisateur visiteur.
Le GSM acquiert une influence majeure dans le monde des télécommunications : de nombreux pays européens et non-européens l'ont adopté. Le GSM constitue pour l'utilisateur européen la première pierre de la future Europe des télécommunications. Aujourd'hui, il existe plus de 690 opérateurs GSM répartis dans 213 pays.

Le paragraphe 1 présente l'architecture GSM à travers ses entités et ses interfaces. Le paragraphe 2. introduit les interfaces de l'architecture GSM et le paragraphe 3 présente les identités utilisées dans un réseau GSM pour une meilleure compréhension des procédures de gestion de la mobilité, de transfert intercellulaire et de contrôle d'appel. Ces trois procédures sont présentées dans le tutoriel EFORT « Mobilité et Contrôle d'appel dans le réseau GSM ».

1. Architecture GSM

L'appellation GSM (Global System for Mobile Communications) regroupe deux types de réseaux cellulaires numériques de télécommunications pour abonnés mobiles :
- Le réseau GSM900 : il utilise des fréquences porteuses dans la gamme des 900 MHz et il a été le premier type de réseau mobile cellulaire numérique européen,
- Le réseau DCS1800 (Digital Cellular Telecommunications System) qui utilise des fréquences porteuses dans la gamme des 1800 MHz.

Les réseaux GSM/DCS permettent d'offrir au public des services de télécommunication avec une couverture continue sur un vaste territoire.
Cette disponibilité du service est obtenue par la localisation automatique de la station mobile et par des accords d'itinérance (roaming) entre opérateurs.
L'offre de services est comparable à celle du RNIS grâce à l'utilisation d'une norme proche de la recommandation Q.931 de l'ITU-T pour le contrôle de l'appel.

Pour que le système puisse offrir les services prévus, un ensemble de fonctions a été défini. Ces fonctions sont celles requises dans tout réseau mobile comme la numérotation, l'acheminement vers un usager mobile, le transfert de cellules, etc. Ces fonctions sont regroupées en entités fonctionnelles. Le système GSM est constitué des entités suivantes (Figure 1):

- La station mobile (MS) : La station mobile est l'équipement physique utilisé par l'usager du réseau GSM pour accéder aux services de télécommunication offerts.
- Le sous-système radio (BSS, Base Station Subsystem) : il assure la couverture de zones géographiques données appelées cellules et qui contiennent les matériels et logiciels nécessaires pour communiquer avec les stations mobiles.
- Le sous-système d'acheminement appelé couramment sous-système réseau (NSS, Network Sub-System) : il comprend l'ensemble des fonctions nécessaires à l'établissement des appels et à la mobilité.
- Le sous-système d'exploitation et de maintenance (OMC, Operations and Maintenance Centre) : il permet à l'exploitant d'administrer son réseau GSM.

Le BSS comprend :
- Les BTS (Base Transceiver Station), émetteurs-récepteurs ayant un minimum "d'intelligence",
- le BSC (Base Station Controller) qui contrôle un ensemble de BTS,

Le NSS comprend des bases de données et des commutateurs :
- Les MSC (Mobile Switching Center), commutateurs mobiles associés en général aux bases de données VLR (Visitor Location Register), fichier des abonnés visiteurs,
- le HLR (Home Location Register), base de données de localisation et de caractérisation des abonnés,
- l'AUC (Authentication Centre), base de données qui génère des paramètres sur demande du HLR pour protéger le réseau des utilisateurs frauduleux.
- L'EIR (Equipment Identity Register) qui vérifie l'identification de l'équipement mobile.

L'OMC peut être scindé en deux parties :
- L'OMC-R (Operations and Maintenance Centre Radio), qui a pour fonction de gérer les éléments du BSS,
- l'OMC-S (OMC Switching), qui a pour fonction de gérer les éléments du NSS.

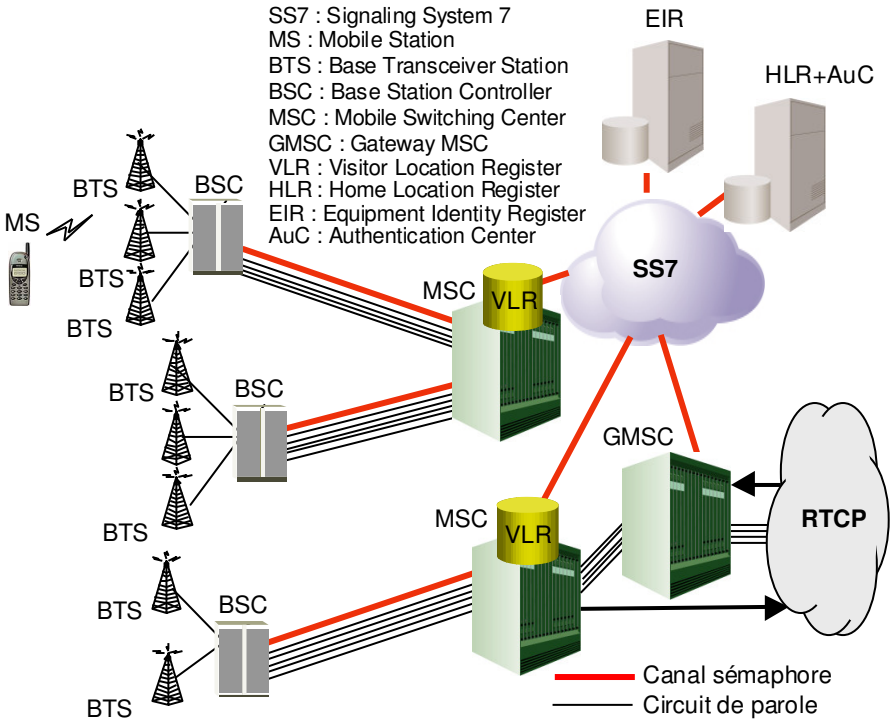


Figure 1 : Architecture du réseau GSM

1.1. Station Mobile (MS, Mobile Station)

Le but d'un réseau GSM/DCS est d'offrir des services de télécommunication à des abonnés, quels que soient leurs déplacements à l'intérieur d'une zone de service, desservie par un opérateur ou éventuellement par plusieurs opérateurs ayant passé des accords mutuels. Pour ce faire, l'abonné mobile utilise une station mobile (MS, Mobile Station) qui est constituée de deux éléments séparables :

- Un équipement mobile qui fournit les capacités radio et logicielles nécessaires au dialogue avec le réseau et demeure indépendant de l'abonné utilisateur.
- Une carte SIM (Subscriber Identification Module) qui contient les caractéristiques de l'abonné et de ses droits.

Lorsque la carte n'est pas présente dans le terminal, le seul service que peut accepter le réseau de la part de l'abonné mobile est le service d'urgence.

1.2. Sous-système Radio (BSS, Base Station Subsystem)

1.2.1. Base Transceiver Station (BTS)

La BTS (Base Transceiver Station) relie les stations mobiles à l'infrastructure fixe du réseau. La BTS est composée d'un ensemble d'émetteur / récepteurs. Elle assure :

- La gestion du multiplexage temporel (une porteuse est divisée en 8 slots dont 7 sont alloués aux utilisateurs), et la gestion des sauts de fréquence.
- Des opérations de chiffrement.
- Des mesures radio permettant de vérifier la qualité de service ; ces mesures sont transmises directement au BSC.
- La gestion de la liaison de données (données de trafic et de signalisation) entre les mobiles et la BTS.
- La gestion de la liaison de trafic et de signalisation avec le BSC.

La capacité maximale typique d'une BTS est de 16 porteuses, soit 112 communications simultanées. En zone urbaine où le diamètre de couverture d'une BTS est réduit, cette capacité peut descendre à 4 porteuses soit 24 communications.

1.2.2. Base Station Controller (BTS)

Un BSC gère un ou plusieurs BTS et n'est relié qu'à un seul MSC. Pour le trafic abonné venant des BTS, le BSC joue le rôle de concentrateur. Pour le trafic venant du commutateur, il joue le rôle d'aiguilleur vers la BTS dont dépend le destinataire.
Un BSC utilise les mesures radio des BTS pour gérer la signalisation des "Handover" entre les cellules dont il a la responsabilité.

1.3. Sous-système réseau (NSS, Network Subsystem)

1.3.1. Mobile Switching Center (MSC)

Un MSC (Mobile Switching Center) est un commutateur qui réalise les fonctions de connexion et de signalisation pour les mobiles localisés dans une zone géographique appelée zone de localisation du MSC. La différence principale entre un MSC et un commutateur d'un réseau fixe est qu'un MSC doit prendre en compte l'impact de l'allocation des ressources radio aux mobiles et la mobilité des mobiles. Il doit posséder des ressources suffisantes pour réaliser au moins les procédures suivantes :

- Procédures pour l'enregistrement des localisations.
- Procédures requises pour les handovers.

Un MSC constitue l'interface entre le système radio et les réseaux fixes. Il réalise toutes les fonctions nécessaires à la mise en œuvre des appels de et vers les mobiles.
Dans la pratique, un MSC intègre les fonctionnalités d'un VLR.

1.3.2. Gateway MSC (GMSC)

Si le Réseau Téléphonique Commuté (RTC) doit router un appel vers un abonné mobile, l'appel est routé vers un MSC. Ce MSC interroge le HLR concerné, puis route l'appel vers le MSC sous lequel le mobile est localisé (il peut s'agir du même MSC). Un MSC qui reçoit un appel d'un autre réseau et qui assure le routage de cet appel vers la position de localisation d'un mobile est appelé Gateway MSC (GMSC).

1.3.3. Home Location Register (HLR)

Le HLR (Home Location Register) contient les informations relatives aux abonnés du réseau. Un réseau peut posséder plusieurs bases pour mettre en œuvre le HLR en fonction des capacités de ces bases de données. Dans un HLR, chaque abonné est décrit par un enregistrement contenant le détail des options d'abonnement et des services complémentaires accessibles à l'abonné. A ces informations statiques se rajoutent des informations dynamiques telles que la dernière localisation connue du mobile (localisation permettant la taxation et le routage des appels vers le MSC sous lequel le mobile est localisé) et son état. Le HLR contient par ailleurs la clé secrète de l'abonné qui permet au service d'authentifier l'abonné. Cette clé est inscrite sous un format codé que seul l'AUC (Authentication Center) peut décrypter.

1.3.4. Visitor Location Register (VLR)

Le VLR (Visitor Location Register) est une base de données généralement associée à un commutateur MSC. Il est aussi possible de considérer un VLR partagé par plusieurs MSCs. Sa mission est d'enregistrer des informations dynamiques relatives aux abonnés actuellement connectés. Le réseau doit connaître à chaque instant la localisation des

abonnés présents. Dans le VLR, chaque abonné est décrit en particulier par un identifiant et une localisation. Grâce à ces informations, le réseau est apte à acheminer un appel vers un abonné mobile. A chaque changement de zone de localisation d'un abonné, le VLR du MSC auquel est rattaché le mobile doit être mis à jour ainsi que l'enregistrement de cet abonné dans le HLR. Lorsqu'un appel doit être délivré, c'est le HLR qui est le premier interrogé afin de connaître la dernière localisation connue de l'abonné.

1.3.5. Authentication Center (AUC)

L'AUC (Authentication Center) est associé à un HLR et sauvegarde une clé d'identification pour chaque abonné mobile enregistré dans ce HLR. Cette clé est utilisée pour fabriquer :

- Les données nécessaires pour authentifier l'abonné dans le réseau GSM.
- Une clé de chiffrement de la parole (Kc) sur le canal radio entre le mobile et la partie fixe du réseau GSM.

L'AuC est une fonctionnalité généralement intégrée dans le HLR.

1.3.6. Equipment Identity Register (EIR)

Un EIR sauvegarde toutes les identités des équipements mobiles utilisés dans un réseau GSM. Cette fonctionnalité peut être intégrée dans le HLR.

Chaque poste mobile est enregistré dans l'EIR dans une liste :

- Liste "blanche" : poste utilisable sans restriction.
- Liste "grise" : poste sous surveillance (traçage d'appels).
- Liste "noire" : poste volé ou dont les caractéristiques techniques sont incompatibles, avec la qualité requise dans un réseau GSM (localisation non autorisée).

1.4. Le réseau d'exploitation et maintenance

Le réseau d'exploitation et maintenance comprend les centres d'exploitation maintenance (OMC : Operations and Maintenance Center) qui sont les entités fonctionnelles permettant à l'opérateur du réseau de contrôler son système. Un OMC-R (OMC-Radio) prend en charge la supervision et le contrôle d'un ensemble de BSC et BTS. Un OMC-S (OMC-Switching) permet de superviser et contrôler un ensemble de MSC/VLR. Au-delà des OMC-R et OMC-S, on peut trouver, si l'importance du réseau le justifie, un NMC (Network Management Centre) qui assure l'administration générale centralisée du réseau. Les fonctions suivantes peuvent être spécifiquement identifiées :

- Fonctions liées à la gestion commerciale ou administrative du réseau :
- Gestion de la sécurité,
- Gestion des performances,
- Gestion de la configuration,
- Maintenance, gestion des alarmes.

1.5. Réseau Sémaphore Numéro 7 appliqué au GSM

Le mode associé est utilisé entre les BSCs et les MSCs. Le protocole de signalisation utilisé est BSSAP (Base Station Subsystem Application Part).
Le mode quasi-associé s'applique au sous-système réseau (NSS, Network Subsystem). Les MSCs, GMSCs, HLR et EIR sont considérés comme des SPs (Signaling Point) rattachés à des STPs (Signaling Transfer Point). Les protocoles de signalisation considérés sont ISUP, MAP (Mobile Application Part), INAP (Intelligent Network Application Part) et CAP (CAMEL Application Part.

2. Interfaces GSM

Le système GSM normalise un ensemble d'interfaces entre les entités afin de permettre l'interfonctionnement entre équipements de fournisseurs différents (Figure 2).
Le BSC et le MSC disposent de l'interface A basée sur l'utilisation d'une ou plusieurs liaisons numériques à 2Mbit/s qui supportent le trafic ainsi que la signalisation nécessaire. L'interface A est définie à la sortie du MSC et le débit du canal de parole y est égal à 64 kbit/s. Or, le débit correspondant sur l'interface radio est égal au plus à 16 kbit/s. Une fonction de transcodage (TRAU, Transcoder / Rate Adaptor Unit) pour la parole ou de conversion de débit pour les canaux de données est donc nécessaire. L'interface A permet que ces fonctions soient géographiquement situées près du MSC ou du BSC ; cependant, fonctionnellement, le transcodeur est considéré comme faisant partie du BSS. Le protocole de signalisation sur l'interface A est BSSAP (Base Station Subsystem Application Part) qui s'appuie sur un transport SS7. Cette interface est parfaitement spécifiée et permet un réel interfonctionnement entre des MSC et des BSC provenant de différents fournisseurs.

Le BSC et la BTS partagent une interface Abis qui utilise au niveau physique des liens à 2 Mbit/s. le protocole LAPD (Link Access Protocol for the D channel) du RNIS est utilisé pour le transport de la signalisation. Cette interface devait à l'origine faire l'objet d'une spécification technique très stricte, afin de permettre l'interfonctionnement entre des BTS et des BSC de différents fournisseurs. En pratique, l'ouverture de cette interface s'est heurtée à la réticence des industriels et au peu d'intérêt des opérateurs mobiles qui préfèrent souvent acheter des solutions clé en main.

La station mobile (MS) communique avec la BTS par le biais de l'interface radio U_m qui utilise le protocole de signalisation LAPDm. Cela permet à la station mobile d'établir une connexion de niveau 2 avec la BTS pour fiabiliser le dialogue sur le canal dédié. Le sens montant désigne les activités radio de la station mobile vers le réseau; le sens descendant désigne les activités radio du réseau vers la station mobile.

Les interfaces B, C, D, E, F et G utilisent le protocole MAP (Mobile Application Part) qui s'appuie sur la pile de protocole SS7.

Lorsqu'un MSC nécessite des informations concernant une station mobile localisée dans sa zone de couverture radio, il interroge le VLR qui lui est dédié, par le biais de l'interface B. Lorsqu'un mobile démarre une procédure de mise à jour de sa localisation avec un MSC, le MSC en informe son VLR toujours à travers l'interface B qui sauvegarde les informations appropriées.

Le GMSC et le HLR disposent de l'interface C permettant au GMSC d'interroger le HLR contenant les caractéristiques d'abonnement d'un abonné mobile, afin d'établir un appel vers sa station mobile.

L'interface D est utilisée entre VLR et HLR pour échanger les données relatives à la localisation d'un mobile ainsi que pour la gestion des caractéristiques de l'abonné. Lorsqu'un mobile met à jour sa localisation auprès d'un nouveau MSC/VLR, le nouveau VLR envoie au HLR les données relatives à la dernière localisation du mobile; le HLR lui retourne toutes les informations afin de fournir le service à la station mobile. Le HLR demande ensuite au VLR ayant géré la précédente localisation d'effacer les informations de localisation qu'il possédait concernant ce mobile.

Lorsqu'une station mobile se déplace d'un MSC vers un autre pendant une communication, une procédure de transfert intercellulaire (handover) inter-MSC doit être exécutée afin de garantir la continuité de la communication. A cette fin, les MSCs doivent échanger des

données afin d'initier puis de réaliser l'opération. L'interface F utilisée entre MSCs et supportée par le protocole MAP est utilisée à cet effet.

L'interface F est utilisée entre MSC et EIR afin d'échanger des données pour que l'EIR puisse vérifier l'état de l'identité de l'équipement mobile.

Lorsqu'un abonné mobile se déplace d'une zone contrôlée par un MSC/ VLR à une autre sous la responsabilité d'un autre MSC/VLR, une procédure de mise à jour de localisation a lieu. Cette procédure peut comprendre l'échange de signalisation entre VLRs sur l'interface G afin que le nouveau VLR puisse obtenir de l'ancien VLR, l'IMSI et les triplets d'authentification concernant la station mobile.

Par ailleurs lors d'appels provenant du RTC, l'interface de signalisation entre un Class 5 Switch (Commutateur d'accès du RTC) et le GMSC est ISUP/SS7. La même interface est utilisée entre un MSC et le RTC pour des appels de la station mobile à destination d'un abonné du RTC.

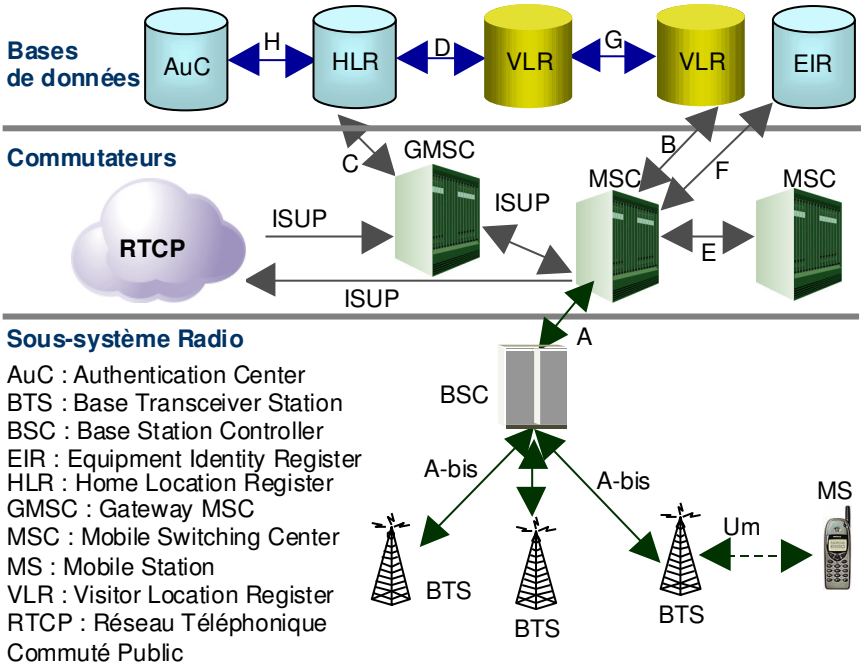


Figure 2 : Interfaces GSM

3. Identités dans un réseau GSM

3.1. IMSI

Lorsqu 'un abonné souscrit à un abonnement mobile auprès d 'un opérateur, un identifiant unique appelé IMSI (International Mobile Subscriber Identity) lui est affecté. Ce numéro d'IMSI a été préalablement stocké sur la carte SIM (Subcriber Identity Module). Un téléphone mobile ne peut être utilisé que si une carte SIM valide a été insérée dans l 'équipement mobile car c 'est la seule façon de facturer correctement un abonné mobile.
Cet IMSI est un concept d 'adressage spécifique au GSM ; il est différent du plan de numérotage RNIS.

Le numéro d 'IMSI n 'est pas connu de l 'abonné mobile et n 'est utilisé que par le réseau GSM.

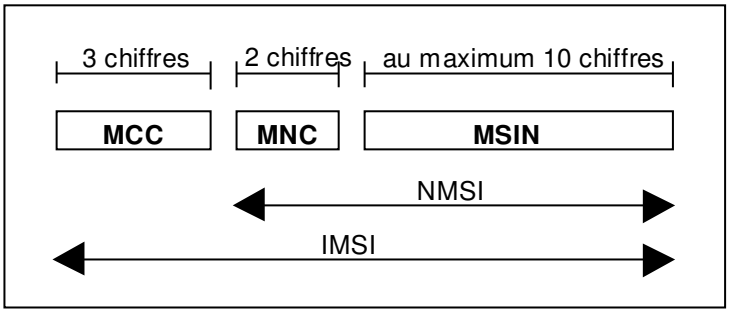
L'IMSI est constitué de trois sous-champs (Figure 3):

- MCC (Mobile Country Code) : Il s'agit du code du pays du réseau GSM (208 pour la France). Le 1er Chiffre du champ MCC identifie le continent. Europe: 2; Etats-Unis: 3; Asie: 4; Australie: 5; Afrique: 6; Amérique du Sud: 7. L'allocation des valeurs des codes de pays pour réseaux GSM est régie par l'ITU-T.
- MNC (Mobile Network Code) : Il s'agit du code du réseau mobile. Il est codé sur 2 chiffres et identifie de manière unique le réseau GSM à l'intérieur d'un pays. Le code réseau Orange France est 01. Le code réseau SFR est 10. Enfin, le code réseau Bouygues Telecom est 20.
- MSIN (Mobile Subscriber Identification Number) : il s'agit du numéro d'identification du mobile. Il identifie l'abonné mobile à l'intérieur du réseau mobile.

Les deux champs MCC et MNC permettent de déterminer de façon unique dans le monde le réseau mobile de l'abonné.

Les deux premiers chiffres du champ MSIN donnent l'indicatif du HLR de l'abonné au sein de son réseau mobile. Les MSC/VLR sont capables, à partir d'un IMSI quelconque, d'adresser le HLR de l'abonné correspondant.

A titre d'exemple, les codes MCC et MNC des opérateurs au Royaume Uni et en Belgique sont les suivants :
UK-CELLNET : 234-10; UK-VODAFONE : 234-15; UK-ONE2ONE : 234-30; UK-ORANGE : 234-33.
B-PROXIMUS : 206-01; B-MOBISTAR : 206-10; B-ORANGE : 206-20.



MCC : Mobile Country Code
MNC : Mobile Network Code
MSIN : Mobile Subscriber Identification Code
NMSI : National Mobile Subscriber Identity
IMSI : International Mobile Subscriber Identity

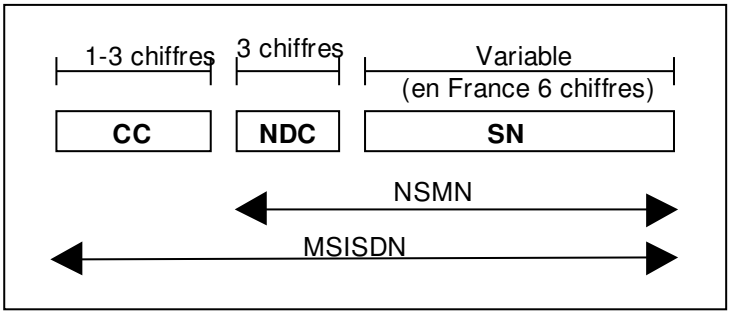
Figure 3 : Format de l'IMSI

3.2. MSISDN

Le numéro de téléphone associé à la station mobile est le MSISDN (Mobile Station ISDN Number).
Le MSISDN consiste en trois sous-champs (Figure 4) :

- CC (Country Code) : Il s'agit du code du pays dans lequel l'abonné mobile a souscrit un abonnement (e.g., Code CC France = 33)
- NDC (National Destination Code) : Il s'agit du numéro national du réseau GSM dans lequel un client a souscrit un abonnement. (Orange France = 607, 608; SFR = 611 entre autres)
- SN (Subscriber Number) : En France le numéro MSISDN a la forme 33 6 AB PQ MCDU. 6 regroupe tous les abonnées mobiles. AB est l'indicatif Mobile GSM. PQ est le numéro

de HLR logique dans le réseau GSM (à l'intérieur d'un même HLR physique, peuvent exister plusieurs HLR logiques identifiés par des valeurs PQ différentes). MCDU est le numéro de l'abonné dans le HLR.



CC : Country Code
NDC : National Destination Code
SN : Subscriber Number
NSMN : National Significant Mobile Number

Figure 4 : Format du MSISDN

3.3. IMEI

L 'IMEI (International Mobile Equipment Identity) identifie de façon unique un terminal mobile au niveau international. Il s 'agit d 'un numéro de série. Ce numéro est alloué par le constructeur du terminal mobile. L'IMEI est utilisé de manière optionnelle par les opérateurs GSM pour lutter contre les vols de terminaux ou pour interdire l'accès au réseau à des terminaux qui auraient un comportement perturbant ou non conforme aux spécifications. A cet effet, l'opérateur dispose de la base de données EIR (Equipment Identity Register). Lorsque la station mobile, suite à sa mise sous tension, s'enregistre au réseau, le réseau a la possibilité de demander son IMEI au terminal et peut par conséquent refuser l'accès à un mobile identifié dans l'EIR comme suspect ou volé.

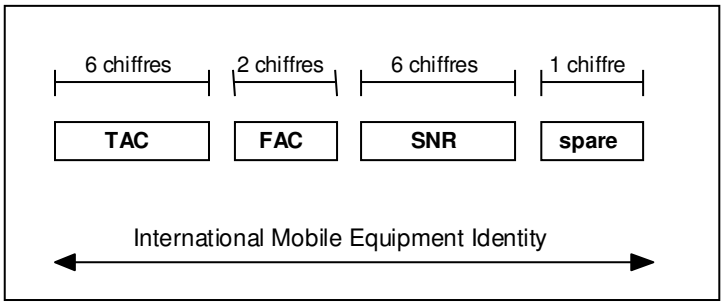


Figure 5 : Format de l'IMEI

L'IMEI est composé des éléments suivants (Figure 5) :

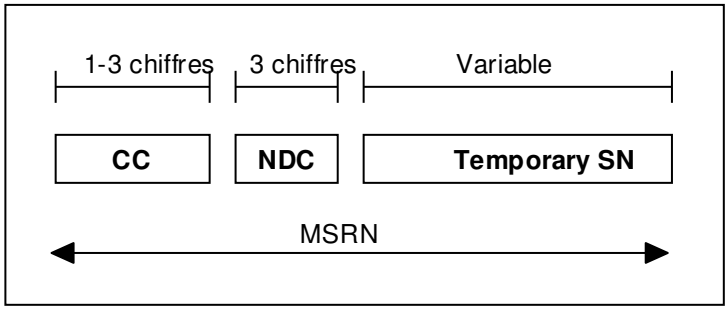
- TAC (Type Approval Code) : Il s'agit d'un numéro indiquant la version de validation du matériel.
- FAC (Final Assembly Code) : Il s'agit du numéro qui identifie l'usine où a été assemblé le poste.
- SNR (Serial Number) : Il s'agit du numéro de série de l'appareil dans le TAC et le FAC.
- Spare (en réserve) : Ce chiffre doit être codé à "0" lorsqu'il est transmis par le mobile.

3.4. TMSI

De manière à conserver la confidentialité de l'identité de l'IMSI, le VLR alloue un numéro temporaire unique à chaque mobile se localisant dans sa zone de couverture ; ce numéro est appelé TMSI (Temporary Mobile Subscriber Identity). Le VLR est capable de corréler l'IMSI d'un mobile et son identité temporaire courante (TMSI).
A l 'intérieur d 'une zone gérée par un VLR, un abonné dispose donc d'un TMSI, attribuée au mobile de façon locale, c 'est à dire pour la zone gérée par le VLR courant du mobile. Le TMSI est utilisé pour identifier le mobile lors des interactions station mobile ←→ réseau.
Le TMSI n 'est connu que sur la partie MS ←→ MSC/VLR. Le HLR n 'en n'a jamais connaissance. A chaque changement de VLR, un nouveau TMSI est attribué. L 'utilisation du TMSI est optionnelle. On peut avoir recours à l 'IMSI uniquement.
La structure et le codage du TMSI sont laissés à la discrétion d'accords entre l'opérateur GSM et les fabricants des postes mobiles utilisés par les abonnés du réseau de l'opérateur. Le TMSI est codé sur 4 octets.
Lorsqu'un mobile reçoit une identité temporaire (TMSI) d'un VLR (suite à une procédure d'authentification), il stocke cette identité sur sa carte SIM.

3.5. MSRN

Un numéro de roaming (numéro de réacheminement) est utilisé pour router les appels vers un mobile. Le MSRN (numéro de réacheminement) est un numéro PSTN (E164) attribué temporairement à la MS et qui permet d'acheminer l'appel vers le MSC dans l'aire duquel se trouve la MS ; tout se passe comme si la MS était un abonné du MSC. A la demande d'un GMSC au HLR concerné, un MSRN (Mobile Station Roaming Number) est alloué temporairement par le VLR qui possède les dernières informations de localisation de ce mobile.
Un numéro de réacheminement (MSRN) doit avoir la même structure que les MSISDN relatifs à une zone de localisation donnée, dans un réseau GSM et dans un pays donné (Figure 6).



CC : Country Code
NDC : National Destination code
SN : Subscriber Number

Figure 6 : Format du MSRN

3.6. LAI

Un réseau GSM est divisé en aires de service. Chaque MSC/VLR dans un réseau GSM contrôle une aire de service, composée d'un ensemble de zones de localisation (LAs, Location Areas), chaque LA représentant un ensemble de cellules. La figure 7 décrit de manière simplifiée un exemple de réseau GSM avec deux aires de services, celles du MSC/VLR1 et du MSC/VLR2. Le réseau est divisé en cinq zones de localisation.

- Les zones de localisation LA1 et LA2 sont sous le contrôle du MSC/VLR1. Elles constituent l'aire de service 1.
- Les zones de localisation LA3, LA4 et LA5 sont sous la responsabilité du MSC/VLR2. Elles forment l'aire de service 2.

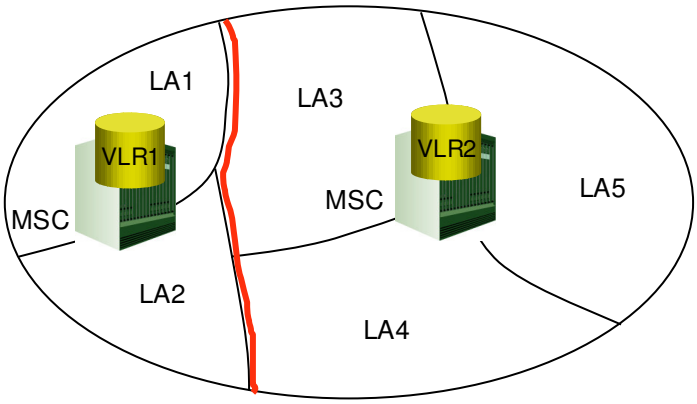
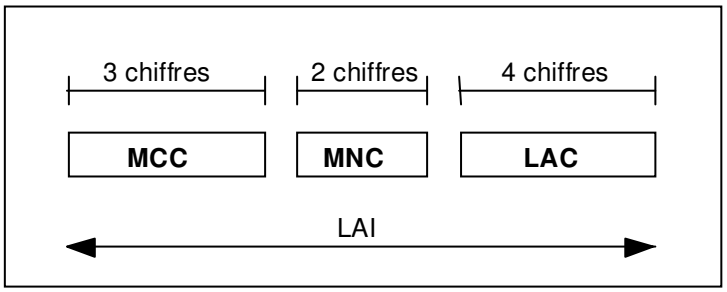


Figure 7 : Aire de service et zone de localisation

Une zone de localisation est identifiée par l'adresse LAI (Location Area Identification) composée des champs suivants (Figure 8) :

- MCC : Il s'agit du code du pays du réseau GSM (208 pour la France), champ également présent dans l'IMSI.
- MNC : Il s'agit du code du réseau mobile, champ également présent dans l'IMSI.
- LAC (Location Area Code) : il s'agit du code de la zone de localisation librement affecté par l'opérateur. 208 01 12 est un exemple de zone de localisation dans le réseau d'Orange France.



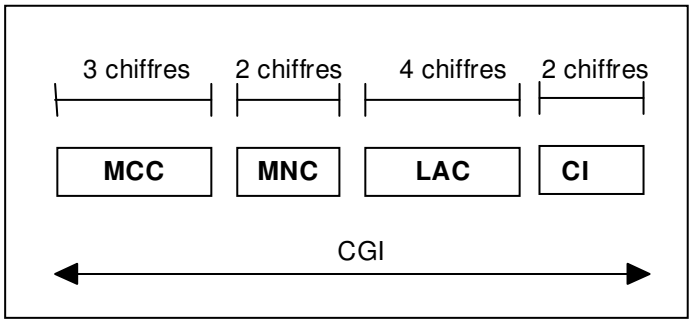
MCC : Mobile Country Code. Champ également présent dans l 'IMSI.
MNC : Mobile Network Code. Champ également présent dans l 'IMSI.
LAC : Location Area Code
LAI : Location Area Identification

Figure 8 : Format du LAI

A la mise sous tension et ensuite lorsqu'il se déplace, la MS se met à l'écoute du canal BCCH de la cellule la plus puissante ; le BCCH (Broadcast Control Channel) diffuse l'identité de la LA. Le MS compare l'identité de la LA avec celle qui est mémorisée sur sa carte SIM. Si les identités sont identiques, la MS est correctement localisée et il ne se passe rien. Dans le cas contraire, la MS initie une procédure de mise à jour de localisation en signalant au réseau (VLR) l'identité de la nouvelle LA et son identité IMSI (ou TMSI).
Après localisation, la MS se met à l'écoute du canal de recherche PCH (Paging Channel) afin de pouvoir recevoir d'éventuels appels. En effet, lors d'un appel entrant, le VLR ne connaît que la LA courante du mobile. C'est la raison pour laquelle un avis de recherche (Paging) est émis sur cette LA.

3.7. CGI

La cellule au sein d'une zone de localisation est identifiée en rajoutant un numéro de cellule (CI, Cell Identity) à l'identification de la zone de localisation (Figure 9). L'identification globale de la cellule (CGI, Cell Global Identification) qui est unique, est donc la concaténation LAI+CI.



MCC : Mobile Country Code
MNC : Mobile Network Code
LAC : Location Area Code
CI : Cell Identity
CGI : Cell Global Identity

Figure 9 : Format du CGI

3.8. Identités pour l'authentification et le chiffrement

La sécurité GSM est adressée sur deux plans : authentification et chiffrement.
L'authentification empêche l'accès frauduleux par une station mobile clonée. Le chiffrement empêche l'écoute par un usager non autorisé.
Après que l'usager se soit identifié au réseau, il doit être authentifié. Pour ce faire, une clé d'authentification individuelle Ki et un algorithme d'authentification A3 sont utilisés. L'AuC et la carte SIM contiennent Ki et A3. Pour initier le processus d'authentification, le réseau nominal d'un usager mobile génère un nombre aléatoire, RAND, d'une longueur de 128 bits. Ce nombre est envoyé à la station mobile. En appliquant l'algorithme d'authentification A3, le réseau (AuC) et la station mobile (Carte SIM) utilisent la clé Ki et le nombre RAND afin de produire un résultat (SRES) comme cela est montré à la figure 10.
Le résultat SRES généré par la station mobile est envoyé au réseau nominal et comparé au résultat SRES généré par l'AuC. S'ils ne sont pas égaux, la demande d'accès de la station mobile est rejetée par le réseau. SRES et RAND générés par l'AuC sont envoyés au MSC/VLR qui les compare aux résultats soumis par la station mobile. L'algorithme d'authentification A3 est spécifique à un opérateur GSM donné.
Si la station mobile est acceptée, une clé de chiffrement Kc est produite par un algorithme de génération de clé de chiffrement A8 à partir de la clé Ki et du nombre RAND. Comme A3, A8 est spécifique au réseau nominal. Le système nominal (AuC) ayant généré Kc, l'envoie au MSC/VLR. Kc est une clé de chiffrement utilisée pour chiffrer / déchiffrer les données de signalisation et de trafic sur la voie radio entre la station mobile et la BTS.
Un algorithme de chiffrement A5 présent sur la station mobile et la BTS est alors utilisé pour chiffrer / déchiffrer les données de signalisation et de trafic en utilisant Kc. Cet algorithme A5 est normalisé et est le même pour tous les opérateurs mobiles.
La carte SIM contient les informations Ki, A3, A8. L'AuC contient les informations A3, A8, IMSI/Ki. La station mobile et la BTS contiennent l'algorithme A5.

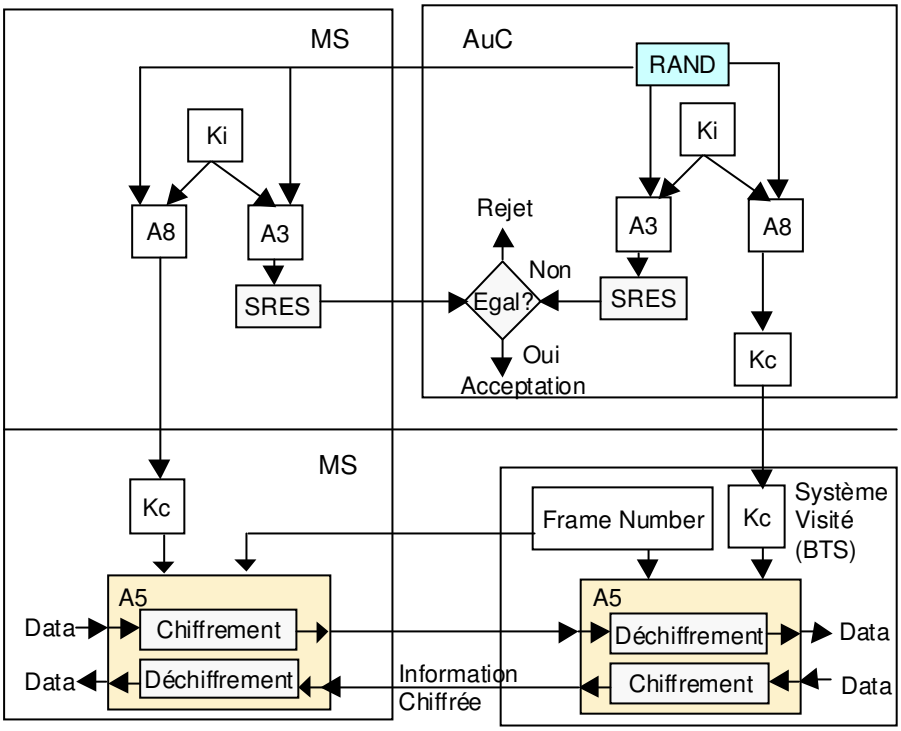


Figure 10 : Authentification et Chiffrement

3.9. Organisation des informations de l'abonné mobile

Les données de l'abonné sont stockées dans trois entités :

- L'entité HLR qui contient toutes les informations permanentes de souscription et certaines informations temporaires des usagers enregistrés sur ce HLR.
- L'entité VLR qui contient toutes les informations nécessaires pour le traitement d'appel et autres procédures pour les abonnés mobiles actuellement dans l'aire de localisation contrôlée par ce VLR.
- La carte SIM qui contient des informations permanentes liées aux services souscrits par l'abonné ainsi que des informations temporaires modifiées par le réseau au cours de la vie de la carte SIM.

L'IMSI est une information permanente. Elle est stockée dans le HLR, le VLR, et la carte SIM.
Le MSISDN est une information permanente présente dans les entités HLR et VLR.
Le TMSI est une information temporaire qui n'est stockée que dans le VLR et la carte SIM.
Le MSRN est une information temporaire générée et stockée dans le VLR.
Le LAI est une information temporaire présente sur le VLR et la carte SIM.
Le numéro de MSC/VLR est une information temporaire qui permet au HLR de connaître la localisation courante de la station mobile. Cette information est stockée dans le HLR.
La clé Ki est une information permanente stockée dans l'AuC et la carte SIM, l'AuC étant intégrée dans le HLR.
Le triplet (RAND, SRES, Kc) qui correspond à une information temporaire est calculé par l'AuC, et stocké dans le HLR et le VLR.