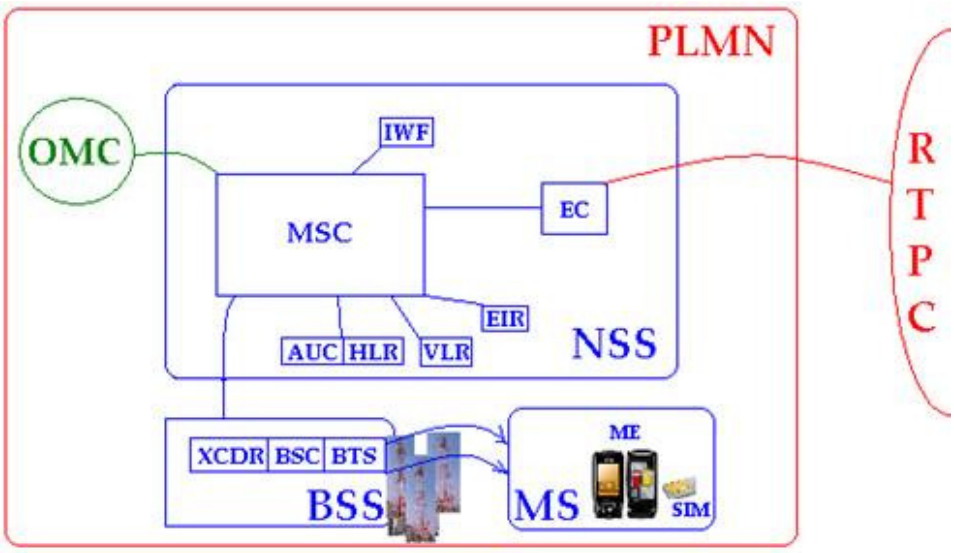
REDES GSM, GPRS, EDGE E UMTS

Ricardo Di Lucia Santos - DRE: 108038139

2.1 – Componentes



Componentes GSM.

2.1.1 – Estação móvel(MS)

A estação móvel é constituída de um equipamento móvel (*Mobile Equipment*- ME), e um módulo de identidade do assinante, (*Subscriber Identity Module* - SIM), geralmente um chip.

2.1.1.1 - Equipamento Móvel - ME
Cada equipamento móvel tem um número de identificação chamado identidade internacional do equipamento móvel (*International Mobile Equipment Identity* - IMEI). Esses números são armazenados no registro de identidade e equipamento (*Equipment Identity Register* - EIR), estudado mais a frente.É o próprio aparelho celular.
São três tipos :
- Veicular : geralmente uma antena na parte externa do veículo;
- Estação Móvel Portátil : Composto por uma maleta.
- Estação Móvel (*handset*) : Composto por um telefone de pequeno porte.
Esses três tipos possuem características diferentes que fazem a comunicação da MS com a BSS depender do tipo de aparelho. A BSS, portanto, precisa saber qual é o tipo de aparelho para implementar a comunicação. Para resolver esse problema, a MS envia uma mensagem inicial que carrega as seguintes informações :
- Revisão : identifica a fase do padrão GSM adotada. As fases mais recentes conseguem realizar todos os serviços das anteriores, mas o contrário não acontece. Logo, quando duas fases distintas se comunicam, os serviços implantados são os da fase mais antiga;
- Algoritmo de Criptografia : diz qual é o algoritmo de criptografia usado na MS. Na fase 1 há somente o algoritmo A5, enquanto na fase 2 existem os algoritmos A5/0 e A5/7;
- Capacitação de Freqüências : dependendo do padrão GSM adotado pela MS, o aparelho utiliza uma das faixas de freqüência - 850 MHz, 900 MHz, 1.800 MHz ou 1.900 MHz - , como citado no tópico "Padrão GSM". A mensagem inicial deve, portanto, indicar em que faixa de freqüências será feita a comunicação. Existem celulares que operam nas 4 faixas, num modo conhecido como modo quatro (*quadri-mode*);
- Capacitação do Serviço de Mensagens Curtas (*Short Message Service* – SMS) : informa se a MS está

preparada para receber ou enviar mensagens curtas;

2.1.1.2 - Módulo de Identidade do Assinante – SIM
Esse módulo consiste em um cartão inteligente (*smart card*) que carrega informações essenciais para a identificação do assinante. Geralmente é um chip que se conecta ao telefone celular. O processamento dos serviços e suas tarifações são realizados a partir das informações contidas nesse chip, e não no aparelho celular. Sendo assim, o assinante pode retirar seu chip, encaixar em outro aparelho e realizar uma chamada com seu próprio número, o que será tarifado em nome do dono do chip.
O SIM carrega as seguintes informações, cuja utilização será estudada mais adiante :
- Identidade internacional do assinante (*International Mobile Subscriber Identity* – IMSI);
- Identidade temporária do assinante (*Temporary Mobile Subscriber Identity* – TMSI);
- Identidade da área de localização (*Location Área Identity* – LAI);
- Chave de autenticação do assinante (*Subscriber Authentication Key* – Ki);
- Número internacional ISDN (*Integrated Service Digital Network*) da estação móvel (*Mobile Station Integrated Servicer Digital Network* – MSISDN).

2.1.2 – Sistema de estação base (BSS)

O sistema de estação base é responsável por conectar a MS com o sistema de comutação de rede (NSS). A MS envia um sinal à BSS, que o capta e dele extrai as informações. Essas informações são enviadas à rede. No outro sentido, a BSS recebe os dados vindos da rede, e constrói um sinal cujas informações a MS é capaz de extrair.
A BSS é formado por três elementos. Um para captar sinais da MS e enviar outros para a mesma, outro para comandar o primeiro e se comunicar com a rede. O terceiro auxilia o segundo na comunicação com a MSC. Os três estão detalhados abaixo :
2.1.2.1 – Estação transceptora base (BTS)
A BTS (*Base Transceiver Station*) implementa conexões com as MSs através da interface aérea. É formada por Hardware de radiofreqüência e antenas, basicamente.
Essas estações ficam sempre ligadas ao BSC, e ambos controlam gerenciam os canais de tráfego.

2.1.2.2 – Controlador de estação base (BSC)
O BSC (*Base Station Controller*) é responsável por controlar um grupo de estações transceptoras base (BTSs). Todas as operações de uma BTS são comandadas pelo respectivo BSC.
Através de uma matriz de comutação digital, as BSCs conectam os canais de RF com os circuitos terrestres provenientes da central de comutação celular (MSC), um componente do sistema de comutação de rede. Com essa técnica, o BSC é capaz de realizar handovers entre os canais de RF independente da MSC, o que otimiza o tráfego na interface aérea e reduz o trabalho da MSC.

2.1.2.3 – Transcodificador (XCDR)
A MSC envia sinais de voz a uma taxa de 64 Kbits/s. Se os canais de voz PCM a essa taxa fossem trasmitidos direto na interface aérea, sem modificação, iriam ocupar uma faixa muito extensa da banda de RF, o que diminuiria o número de possíveis canais de voz na interface aérea.
O XCDR é responsável por converter esses sinais de voz de 64 Kbits/s em sinais de 16 Kbits/s que podem ser enviados na interface aérea. A transmissão de dados não passa pelo processo de transcodificação, é apenas adaptada de 9,6 kbits/s para 16 Kbits/s, com 3 Kbits/s de controle.
Para isso, utiliza algoritmos de codificação, padronizados no GSM :
- Algoritmo de taxa plena : codifica o canal de voz de 64 Kbits/s em 13 Kbits/s, adicionando 3 Kbits/s para dados de controle (chamado TRAU - *Transcoder Rate Adaption Unit*).
- Algoritmo de taxa plena melhorado : presente apenas na fase 2 do GSM, codifica 64 Kbits/s em 12,2 Kbits/s, e usa 3,8 Kbits/s para controle.

2.1.3 – Sistema de comutação de rede (NSS)

O sistema de comutação de rede é reponsável por :
- Comutar os canais de comunicação entre duas BSSs;
- Controlar e gerenciar a mobilidade dos usuários;
- Armazenar e consultar a base de dados dos assinantes.

Os elementos desse sistema são estudados a seguir.

2.1.3.1 – Central de comutação celular (MSC)
A MSC (*Mobile services Switching Center*) é o "coração" do sistema de comutação de rede.
Possui as seguintes funções :
- Processar chamadas, ou seja, conectar e desconectar chamadas, promover handover entre BSSs e MSCs;
- Supervisionar, manter e operar as bases de dados.
- Gerenciar as interfaces entre a rede GSM e outras redes, como a RTCP (rede pública) e a Rede Digital de Serviços Integrados – RDSI;
- Tarifar os serviços.
Para realizar todas essas funções, a MSC precisa estar conectada aos bancos de dados de todas essas informações. Dois componentes contém grande parte dessas informações : o HLR e o VLR.

2.1.3.2 – Registro de localização local (HLR)
O registro de localização local administra, altera e atualiza a base de dados dos assinantes locais. Esses dados são acessados remotamente pelo MSC e pelo VLR. Os principais dados guardados pelo HLR são:
- Identidade internacional do assinante (*International Mobile Subscriber Identity* - IMSI);
- Localização corrente do assinante no VLR;
- Serviços suplementares aos quais o assinante tem direito, bem como informações adicionais sobre esses serviços;
- Estado do assinante (registrado ou não registrado);
- Chave de autenticação, que mencionaremos mais à frente.

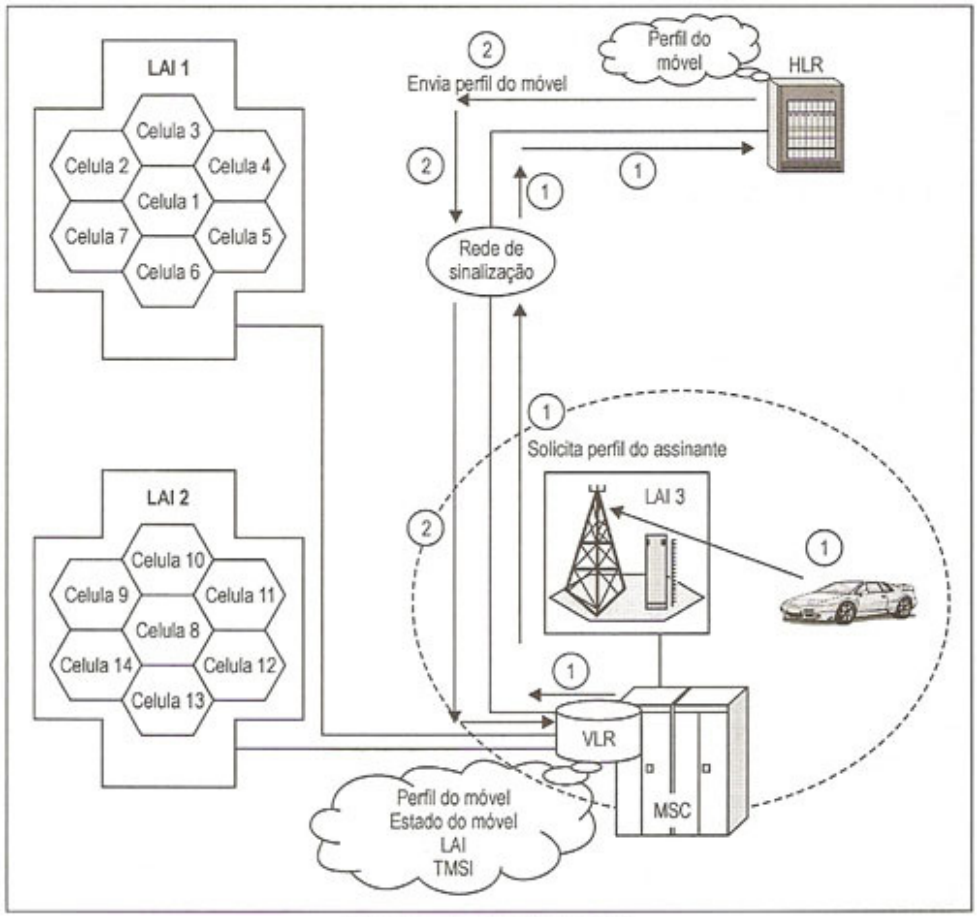
2.1.3.3 – Registro de localização do visitante (VLR)
Pode acontecer de um assinante passar para outra PLMN que não a sua de origem, o que é óbvio em se tratando de sistemas de comunicação móveis. Para se realizar a comunicação com esse usuário "de fora", ou seja, visitante, existe o VLR. Ele guarda uma cópia dos principais dados do assinante, contidos no seu HLR de origem. Essas informações são :
- Estado da estação móvel (livre / ocupado/ não responde);
- Identidade de área de localização (*Location Area Identity* - LAI);
- Identidade temporária do assinante móvel (*Temporary Mobile Subscriber Identity* – TMSI);
- Número da estação móvel visitante (*Mobile Station Roaming Number* – MSRN).
A cópia desses dados é mantida no VLR por um tempo determinado pelo operador de rede (especificado em minutos ou horas).
A seguir discutiremos os papéis dessas identidades associadas ao assinante e à estação móvel.

2.1.3.4 – Identidades de um usuário em um sistema GSM
Para identificar um usuário em um sistema GSM usa-se algumas identidades, cujas estruturas e funções serão apresentadas agora:

2.1.3.4.1 – Identidade internacional do assinante móvel
A identidade internacional do assinante móvel (*International Mobile Subscriber Identity*) identifica a MS internamente à rede GSM. É transmitido apenas na fase inicial da chamada. Não consiste no número que discamos para realizar uma chamada, e sim um número que identifica o assinante dentro da rede GSM. Para que a implementação seja mais fácil, esse número é parecido com o número que discamos (MSISDN, mencionado mais à frente).
O IMSI é formado por três campos :
- Código móvel do país (*Mobile Country Code* – MCC) : três dígitos (12 bits) que identificam a operadora de telefonia móvel em um certo país.
- Código da rede móvel (*Mobile Network Code* – MNC) : dois (8 bits) dígitos que identificam a rede PLMN local do assinante móvel (por exemplo, Rio de Janeiro = 21);
- Número de identificação do assinante móvel (*Mobile Subscriber Identification Number* – MSIN) : com até dez dígitos (40 bits), esse número identifica o assinante dentro de uma PLMN (por exemplo, 98876550). Veja que pode haver o mesmo MSIN em outra PLMN, associado a outro assinante.

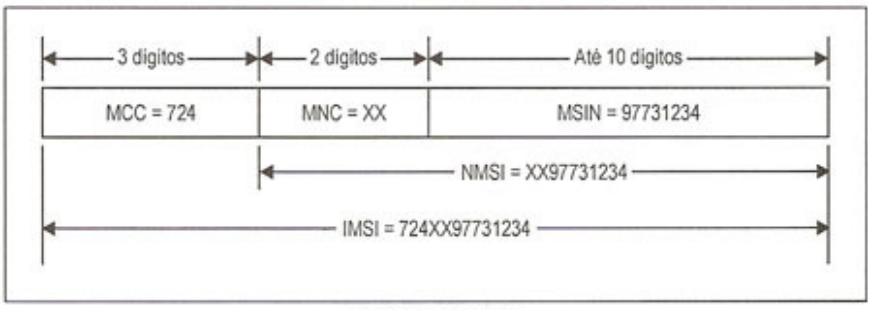
2.1.3.4.2 – Identidade de área de localização (LAI)
A LAI (*Location Area Identity*) é o nome dado a um conjunto de células da PLMN. Tipicamente, uma LAI

contém 30 células. Quando o assinante passa de sua LAI para outra, o VLR identifica sua presença e percebe que não há dados do perfil desse assinante. Utilizando a rede de sinalização, solicita esses dados do HLR (1, na figura abaixo).
O HLR então retorna esses dados para o VLR, que os armazena em uma memória RAM/flash, por um período determinado pelo operador da rede. Enquanto guarda essa cópia, o VLR não consulta o HLR (2, na figura abaixo).



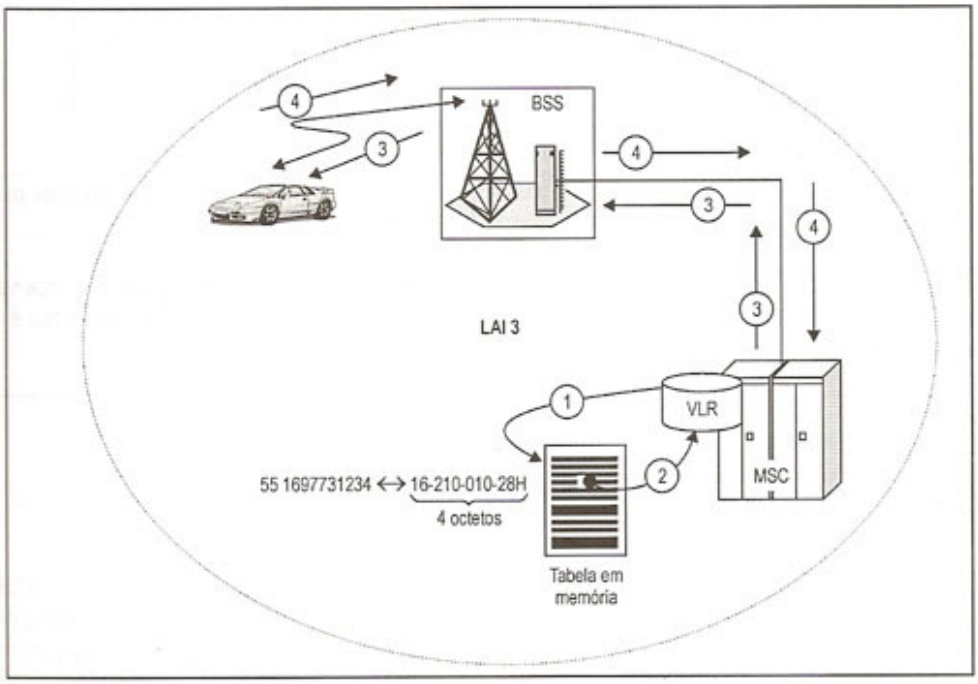
Relacão entre HLR. VLR e LAI.

2.1.3.4.3 – Identidade temporária do assinante móvel (TMSI)
A identidade temporária do assinante é usada para prover confidencialidade ao usuário. Quando o assinante passa de uma LAI para outra, um número é alocado para ele, aleatoriamente. A VLR então associa esse número a seu IMSI, mas como a alocação é aleatória, apenas a VLR sabe qual é o TMSI.



Estrutura da IMSI.

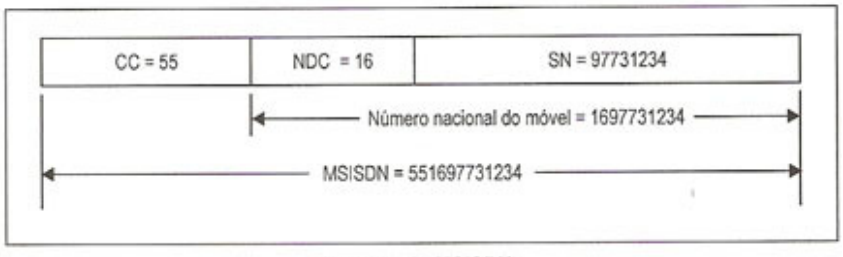
O usuário pode ou não exigir esse serviço. Caso ele exija, a implementação é feita da seguinte forma :



Utilização da TMSI na rede GSM.

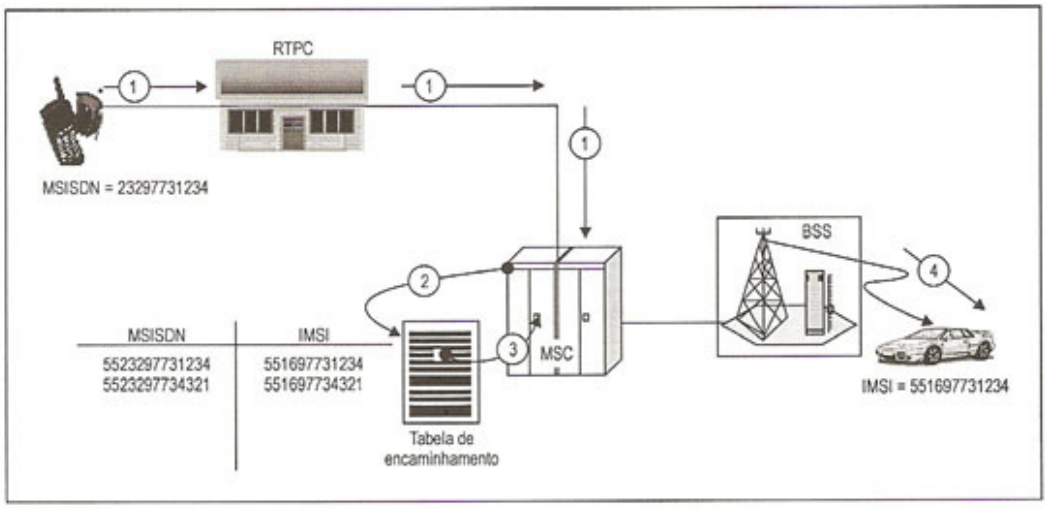
1) Após o VLR adquirir os dados do HLR, começa a troca de informações entre a BSS e a MS. Caso a confidencialidade esteja prevista, o VLR aloca o TMSI, de quatro octetos;
2) Após alocar um TMSI, o VLR associa-o ao respectivo IMSI e guarda em uma tabela, em memória RAM ou flash;
3) As informações transmitidas pela BSS passam a ser direcionadas a esse número TMSI em vez do IMSI, o que evita o monitoramento pela interface aérea;
4) A MS passa a usar o TMSI também. O número TMSI com 32 bits iguais a 1 é usado como inválido pelo cartão SIM.
O número TMSI é registrado no cartão SIM da MS.

2.1.3.4.4 – Número Internacional ISDN da estação móvel (MSISDN)
O MSISDN (*Mobile Station International Integrated Service Digital Network*) é usado para integrar a rede GSM à rede pública.
Formado por três campos, é o número que os usuários mais conhecem. Um campo informa o país de origem, outro a PLMN e outro o número do móvel. O MSISDN 552199988887, por exemplo, é do Brasil (código 55), da PLMN do Rio de Janeiro (21), com o número 99988887. Em diferentes PLMNs pode-se usar o mesmo número. É por isso que quando estamos viajando (ou seja, em outra PLMN) e discamos um número esquecendo de fazer uma ligação DDD – na qual informamos o código da PLMN - , a ligação cai em um número existente, mas dentro da PLMN em que somos visitantes.



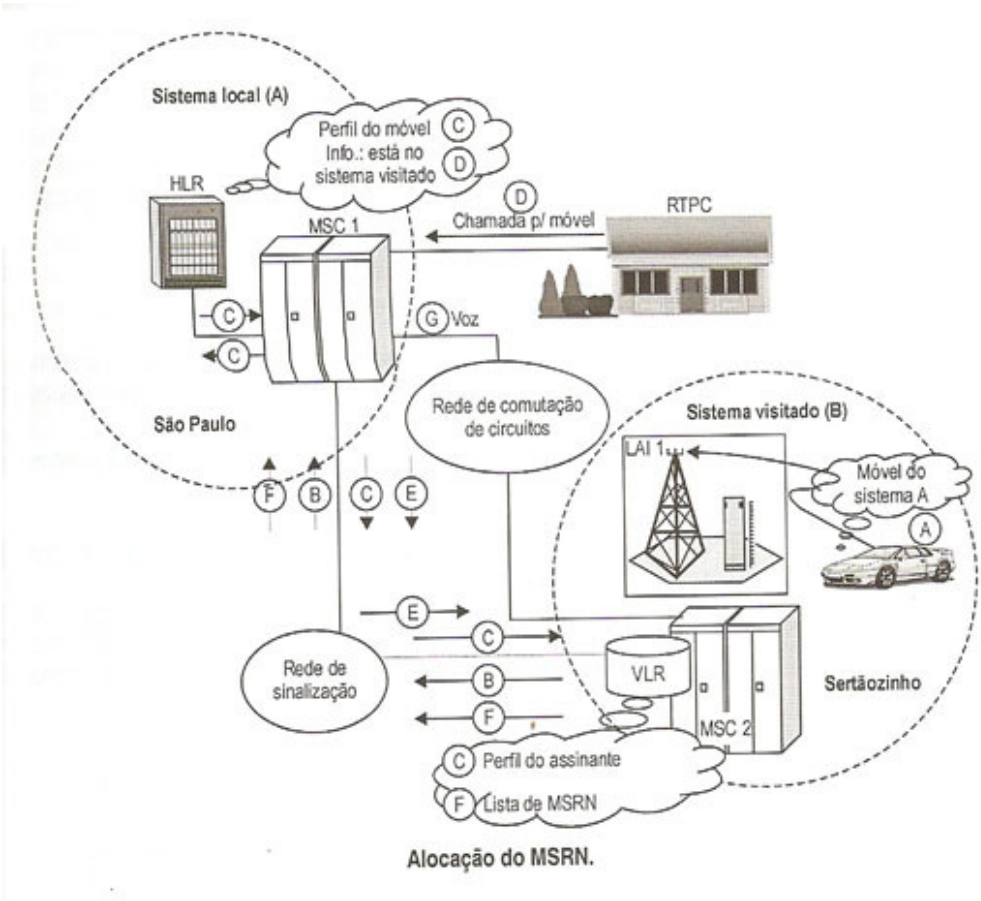
Estrutura do MSISDN.

Enquanto a ligação DDD (Discagem Direta à Distância) exige que informemos o código da PLMN (NDC – *National Destination Code*), a DDI (Discagem Direta Internacional) exige o NDC e o código do país (CC – *Country Code*).
Quando um usuário da RTCP chama um usuário móvel, disca seu MSISDN, dentro do formato da ligação. A MSC converte o MSISDN para um IMSI, pois a rede GSM usa o IMSI internamente. Para isso, usa uma tabela de encaminhamento. O móvel é acessado, então, pelo seu IMSI.



Conversão dos números MSISDN e IMSI.

2.1.3.4.5 – Número da estação móvel do visitante (MSRN)
O número de estação móvel do visitante é usado para estabelecer o canal de voz entre o assinante e a rede quando esse passa a outra PLMN, que não a sua de origem. Essa nova PLMN é comandada por outra MSC. Quando o assinante entra em outra PLMN, o VLR da MSC dessa PLMN aloca um número de uma lista feita para prover esse serviço, chamado *roaming* automático. O usuário não precisa, portanto, avisar manualmente que mudou de PLMN.
Esse serviço necessita da troca de várias informações entre o MSC de origem e o novo MSC. Para tanto foi criado um protocolo chamado *Mobile Application Part* (MAP).

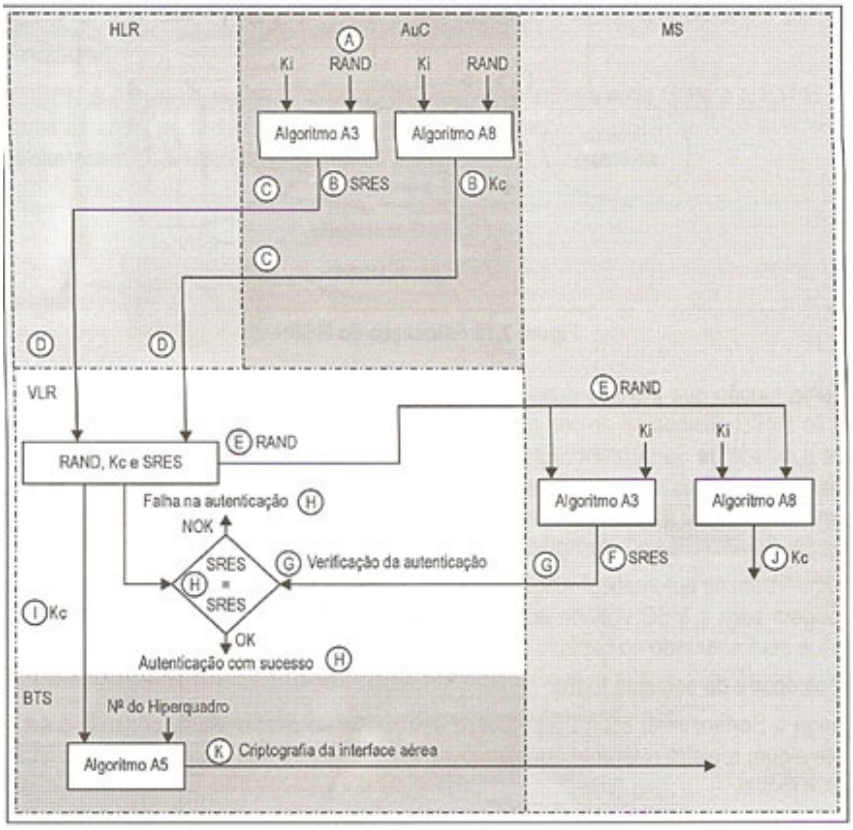


Alocação do MSRN.

Os passos a seguir mostram como o serviço é feito :
A) Ao chegar em outra PLMN, devido à sinalização da MS o MSC identifica um novo usuário e verifica se há um registro para esse aparelho no VLR. O VLR, então, consulta sua base de dados e não acha.
B) O VLR envia uma mensagem de sinalização para o MSC de origem. Ao perceber a nova MS na sua

PLMN, o MSC sabe qual é o MSC de origem através das informações contidas no cartão SIM do aparelho.
C) A MSC de origem envia os dados, e atualiza seu próprio banco de dados informando a localidade na qual o móvel se encontra.
D) Um assinante da RTCP (rede pública) origina uma chamada para o móvel. Quando a chamada chega na MSC do local de origem, esse consulta seu HLR, que diz onde está o móvel.
E) A MSC de origem solicita ao VLR do local visitado um número MSRN, para que a chamada possa ser estabelecida.
F) O VLR do local visitado consulta a lista de MSRNs e aloca um disponível e envia para a MSC de origem.
G) Com o MSRN, a MSC de origem estabelece uma conexão de voz com a MSC do local visitado.

2.1.3.5 – Centro de Autenticação (AuC)
Normalmente instalado no mesmo hardware do HLR, o *Authentication Center* (AuC) tem as funções de autenticar e criptografar as mensagens, para impedir ataques à rede, como MSs clonadas, por exemplo. Esses processos são executados simultaneamente no AuC e na MS.
Ao tentar acessar o sistema, a MS é obrigada a apresentar uma chave de autenticação (Ki), que fica registrada no cartão SIM e no AuC. Os processos de autenticação e de criptografia dependem dessa chave, e estão descritos a seguir:

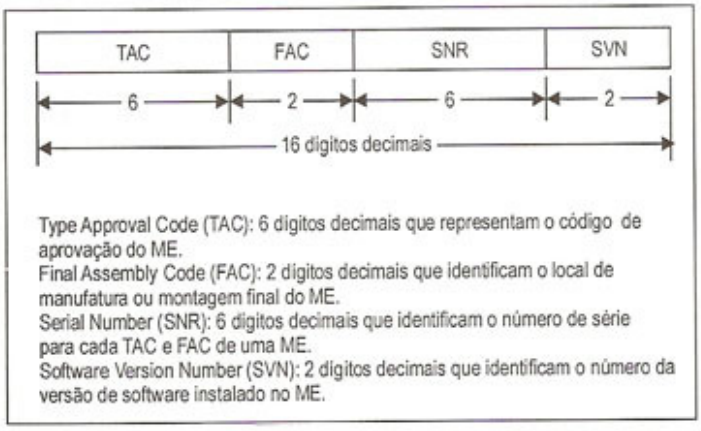


Processo de autenticação e criptografia.

A) Ao receber informações sobre a MS, no início de uma chamada ou na atualização de um registro, o AuC gera um número aleatório chamado RAND.
B) Através do algoritmo A3, de autenticação, e usando o número RAND e a chave secreta Ki, o AuC gera a resposta cifrada SRES (*Signed RESponse*).
Através do algoritmo A8, de criptografia, gera a chave de criptografia Kc, usando RAND e Ki.
C) O AuC envia SRES, Kc e RAND para o HLR.
D) O HLR envia esses 3 dados para o VLR, que os guarda temporariamente.
E) O VLR envia RAND para a MS, através da MSS e da BSS.
F) A MS calcula o SRES, separadamente, usando o algoritmo A3 e a chave Ki, contidos no cartão SIM.
G) A MS envia o SRES para o VLR.
H) A VLR compara os SRES enviados pela MS e pelo AuC. Se forem diferentes, o processo termina com falha; se forem iguais, a autenticação é terminada com sucesso.
I) Se a criptografia estiver sendo executada, o VLR envia a seqüência Kc para a BTS.
J) A MS calcula Kc e armazena no cartão SIM, usando A8, Ki e RAND. A partir de então, todas as

informações transmitidas pela MS serão criptografadas pela chave Kc.
K) Usando o algoritmo de criptografia A5 e o número do hiperquadro GSM, a BTS passa também a só enviar mensagens criptografadas.
J e K consistem nos passos de criptografia.

2.1.3.6 – Registro de identidade do equipamento (EIR)
O EIR (*Equipment Identity Register*) possui a base de dados centralizada dos números de identidade internacional do equipamento móvel (IMEI), os quais são únicos por EIR.
O formato do IMEI está representado na figura abaixo.



Formato do IMEI.

A base de dados do EIR é organizada em listas de IMEIs, de acordo com os critérios abaixo :
- Lista Branca : todos os IMEIs de MSs habilitadas a usar a rede GSM;
- Lista negra : IMEIs de MSs não habilitadas, como MSs roubadas ou clonadas;
- Lista Cinza : IMEIs de MSs com algum problema temporário, como defeito do hardware ou em manutenção na rede autorizada, mas que, enfim, não justificam a presença na lista negra.

2.1.3.7 – Função de Interfuncionamento (IWF)
O IWF (*InternetWorking Function*) é responsável por interfacear a rede GSM com outras redes de dados, como a internet, por exemplo. É sua função adaptar a taxa de dados e converter os protocolos quando necessário.

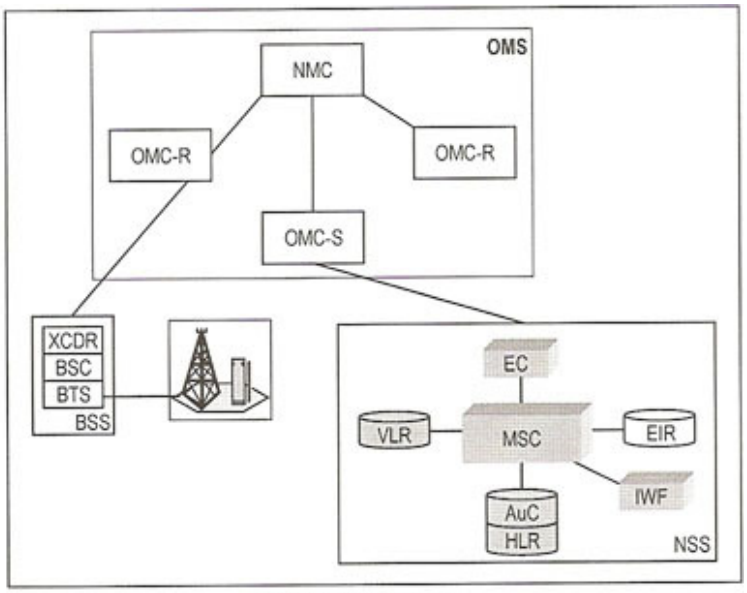
2.1.3.8 – Supressor de Eco (EC)
O EC (*Echo Canceler*) é responsável por eliminar o efeito de eco presente nas conexões entre a MSC e a RTPC. Esse efeito acontece quando um sinal de voz chega em um tempo errado, superposto a outro sinal no tempo certo. Atrasos de propagação na interface aérea, ou provocado pelo processo de transcodificação podem gerar esse problema.

2.1.3.9 – Sistema de Operação e Manutenção (OMS)
O OMS (*Operations and Maintence System*) administra, opera, mantém e supervisiona os elementos da rede GSM. Faz isso ora de forma centralizada, ora de forma remota.
É subdividido em dois subsistemas, como mostra a figura abaixo.

2.1.3.9.1 – Centro de gerenciamento de rede (NMC)
O NMC (*Network Management Center*) é o de mais alta hierarquia em uma rede GSM, pois é o de mais alto nível no OMS, que controla a rede. Só existe um NMC por rede.
Suas principais funções são de monitoramento:
- Dos nós da rede;
- Dos dados estatísticos da rede GSM;
- Dos OMCs.

2.1.3.9.2 – Centro de Operação e Manutenção (OMC)
O OMC (*Operation and Maintence Center*) é o elemento que controla os outros elementos da rede GSM (BTS, MSC, HLR, EIR, etc.)

Um OMC controla uma determinada região, e uma rede GSM é composta por vários OMCs.
Existem dois tipos de OMCs :



OMC (R) e OMC (S).

- OMC (R): controla o Subsistema de estação base (BSS)
- OMC (S) : controla o subsistema de comutação de rede (NSS).

A função do OMC é gerenciar as seguintes funções :
- Eventos e alarmes;
- Performance do sistema;
- Configuração do sistema.

Em suma, o OMC define os principais parâmetros, para atuar em protocolos já implementados.

<< Anterior - Próxima >>

Índice

Redes de Computadores II - 2008.2

Professor Luis Henrique Costa

Professor Otto Carlos Muniz Bandeira Duarte