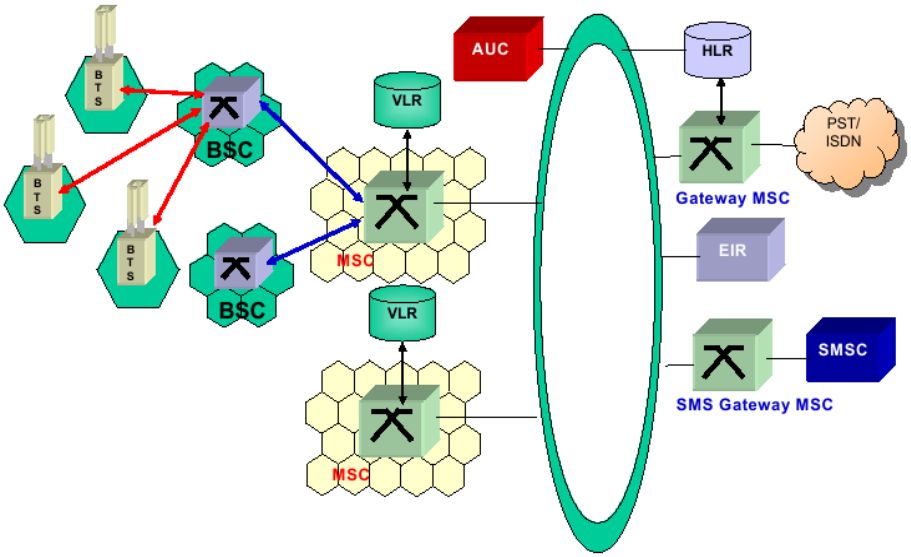
Architettura Sistema GSM



Mobile Station (MS)

Rappresenta la stazione mobile con la quale un utente puo' usufruire dei servizi offerti da GSM. Consiste di un terminale mobile (ME, Mobile Equipment), a sua volta composto da un MT (Mobile Termination) e un TE (Terminal Equipment), e di una smart card intelligente (SIM, Subscriber Identity Module).

SIM

La SIM permette ad un utente di caratterizzare come proprio un qualsiasi terminale mobile GSM. Essa contiene una memoria seriale, nella quale vengono memorizzate diverse informazioni, e un processore in grado di eseguire alcuni algoritmi di cifratura. La SIM contiene diverse informazioni obbligatorie, tra le quali di particolare interesse sono:

- IC Card Identification
- International Mobile Subscriber Identity (IMSI)
- Informazioni sulla localizzazione: Temporary Mobile Subscriber Identity (TMSI), Local Area Information (LAI), valore corrente del Periodic Location Updating Timer e del Location Update Status
- Individual Subscriber Authentication Key (Ki)
- Chiave di crittografia e chiper key sequence number
- Chipering key generating algorithm
- Authentication algorithm
- Informazioni BCCH: lista delle portanti che e' possibile utilizzare per il cell-reselection

Inoltre puo' contenere altri campi ed informazioni opzionali.
E' la SIM card che fornisce l'abilitazione al servizio e viene attivata tramite un numero di identificazione personale (PIN). Il codice IMSI e la chiave di autenticazione Ki costituiscono le credenziali di identificazione dell'abbonato. Il codice IMSI e' quindi associato all'utente che ha sottoscritto l'abbonamento al GSM, identifica l'abbonato all'interno di una qualunque rete GSM ed e' svincolato dall'apparato mobile utilizzato.

Il codice IMSI ha la seguente struttura: e' composto da una lunghezza massima di 15 cifre, suddivise in 3 campi:

- MCC – Mobile Country Code (3 cifre) identifica la nazione dell'operatore
- MNC – Mobile Network Code (2 o 3 cifre) identifica l'operatore all'interno della nazione
- MSIN – Mobile Subscriber Identification Number (max 10 cifre), numero seriale, identifica l'abbonato all'interno di una rete mobile terrestre.

ME – Mobile Equipment

I codici IMEI (International Mobile Equipment Identity e IMEISV (International Mobile Equipment Identity Software Version) identificano in modo univoco il terminale radiomobile.
L'IMEI e' composto da 15 cifre, suddivise in 4 campi:

- TAC – Type Approval Code (6 cifre)
- FAC – Final Assembly Code (2 cifre)
- SNR – Serial Number (6 cifre)

I terminali GSM sono suddivisi in 5 classi in base alla massima potenza con cui possono trasmettere sul canale radio. Possono inoltre variare la potenza di emissione su 15 livelli in modo dinamico, per mantenere un'ottima qualita' di trasmissione limitando al massimo le interferenze di cocanale e i consumi. Dal momento che la trasmissione e la ricezione avvengono in realta' in tempi diversi, viene eliminata la necessita' di utilizzare un filtro di duplice (duplexer), indispensabile per separare i segnali di trasmissione e ricezione che, ad esempio nei sistemi analogici, sono attivi in maniera continuativa e contemporanea.

Le principali funzioni svolte dal terminale radiomobile sono:

- trasmissione e ricezione del segnale radio
- selezione della cella migliore
- registrazione nell'area di localizzazione
- misure trasmissive sul canale radio utilizzato e sui canali adiacenti
- esecuzione dell'handover
- autenticazione e cifratura delle conversazioni

BSS – Base Station Subsystem

La stazione base e' l'entita responsabile delle comunicazioni con una stazione mobile (MS) all'interno di una data area. Essa si compone di due unita': una Base Transceiver Station (BTS) e una Base Station Controller (BSC). L'interfaccia di comunicazione tra le due entita', detta A-bis, e' standardizzata. In questo modo non si e' vincolati a soluzioni proprietarie e si possono utilizzare componenti prodotti da fornitori diversi. La connessione BTS-BSC, quando non sono co-locati, è assicurata da una linea dedicata PCM a 2,048 Mbit/s che mette a disposizione 32 canali a 64 kbps. Dato che la codifica vocale utilizzata dal GSM è diversa da quella PCM occorre un particolare dispositivo, detto TRAU (Transcoder Rate Adapter Unit), che realizzi un adattamento o transcodifica dalla codifica GSM (13 kbps netti; 16 kbps compresa la ridondanza per la codifica di linea) alla codifica PCM (64 kbps).

BTS – Base Transceiver Station

Si indica con questo termine l'unita' funzionale costituita dall'insieme dei tranceiver (ricetrasmettitori) e degli apparati che consentono di fornire la copertura radio ad una cella.

BSC - Base Station Controller

La stazione base di controllo (BSC) governa il funzionamento di uno o più BTS, gestisce il settaggio dei canali radio (instaurazione e rilascio delle connessioni), il frequency-hopping, gli handover interni e altro ancora. Fornisce la connessione tra una unità mobile (MS) e il centro di commutazione (MSC). In una grande area urbana generalmente ci sono un gran numero di BTS controllate da una o poche BSC.

MSC – Mobile-services Switching Center

E' il componente centrale del sottosistema di rete: e' un centro di commutazione che svolge le funzionalita' di un normale nodo di commutazione di una rete: per instaurare, controllare, tassare le chiamate da/verso le MS presenti nell'area geografica da esso servita. In piu' esegue tutti quei compiti essenziali per gestire un utente mobile:

- gestione della mobilita' (ad esempio gestione dell'handover)
- gestione delle risorse radio
- instradamento delle chiamate

VLR – Visitor Location Register

Il registro VLR contiene e mantiene aggiornate le informazioni relative alle MS che sono presenti, temporaneamente, nell'area MSC da esso servita. Complessivamente il territorio geografico coperto da una rete GSM risulta diviso in diverse aree di servizio, ciascuna controllata da un MSC e dotata di un registro VLR. Quando una MS entra nell'area coperta da un nuovo MSC, viene inserito nel registro dei visitatori (VLR) di quel MSC e contemporaneamente il registro generale degli utenti (HLR) viene aggiornato per tenere conto della nuova posizione geografica del terminale. I principali dati d'utente memorizzati nel VLR sono:

- IMSI, MSISDN, MSRN e parametri di sicurezza
- HLR number, per poter identificare il proprio HLR
- Temporary Mobile Subscriber Identity (TMSI), usato per garantire la sicurezza del IMSI, viene assegnato ogni volta che si cambia Location Area (LA)
- Stato della MS (spenta, non raggiungibile, ecc.), categoria (operatore, utente ordinario, chiamata di test) ed eventuale priorità
- Stato dei servizi supplementari (Call Waiting, Call Divert, Call Barring, etc.)
- Tipi e stato dei servizi sottoscritti dall'abbonato a cui gli é consentito accedere (voce, servizio dati, fax, SMS, ecc.), detti bearer e teleservices services
- Location Area Identity (LAI) in cui si trova la MS all'interno di quelle sotto il controllo del MSC/VLR. Viene adottata questa soluzione (e non la soluzione che prevede la registrazione della singola cella dove si trova la MS per evitare un overhead di trasmissione)

Nonostante il VLR, come entità funzionale, possa essere implementata in maniera indipendente dall'MSC, tutti i costruttori preferiscono integrarli assieme (l'interfaccia tra i due elementi può essere proprietaria) ed il tutto viene usualmente definito MSC/VLR.

HLR – Home Location Register

L'HLR costituisce il database su cui un gestore di rete GSM memorizza, in modo permanente, i dati relativi agli utenti che hanno sottoscritto un abbonamento presso di lui. Ogni azione di tipo amministrativo che il gestore di rete effettua sui dati di utente viene svolta attraverso l'HLR. Può essere unico, o stand-alone, per l'intero network oppure distribuito nel sistema; si possono quindi avere delle MSC prive di HLR, ma connesse a quello di altre MSC. E' possibile che ad un HLR sia associato un AuC con il compito di generare i parametri di sicurezza.

Ad ogni HLR viene associato un identificativo (HLR number), che viene fornito ai VLR interessati e permette loro di individuare l'HLR di appartenenza di ogni MS su di essi registrata. A sua volta ogni VLR è identificato da un VLR number, in modo tale che l'HLR sappia presso quale VLR è registrata correntemente ogni sua MS. Poiché una rete GSM è interconnessa con altre reti (PSTN, ISDN, altri PLMN), deve prevedere un piano di numerazione con esse compatibile. Ad ogni utenza sono associati due numerazioni, IMSI e MSISDN, che possono essere utilizzare come chiavi per accedere al record relativo ad una utenza.

Ad ogni MS è assegnato un numero di telefono (MSISDN), che identifica univocamente un abbonato nel piano di numerazione della rete telefonica commutata pubblica internazionale, in conformità con le specifiche E.164 sulla numerazione per reti ISDN (naturali sostituti delle tradizionali PSTN). L'MSISDN ha una lunghezza massima di 15 cifre, suddivise in 3 campi:

- CC – County Code, prefisso internazionale secondo le specifiche E.163 (Italia: 39)
- NDC – National Destination Code, identifica una PLMN GSM in un ambito nazionale. Ad una PLMN possono essere allocati più NDC.
- SN – Subscriber Number, numero che identifica l'abbonato nel PLMN del proprio operatore

I codici CC e NDC permettono di identificare l'operatore GSM, mentre le prime cifre di SN permettono di risalire all'HLR presso cui è registrata la MS chiamata.
Per ogni utente contiene due tipologie di informazioni:

- Dati relativi al contratto
- Dati sulla localizzazione del terminale ai fini della contabilizzazione e dell'instradamento delle chiamate verso l'MSC nella cui area si trova il mobile quindi:

- MS Roaming Number
- VLR Address
- MSC Address
- Local MS Identity

I principali compiti di un HLR possono essere riassunti come segue:

- sicurezza: dialogo con l'AuC e il VLR
- gestione della localizzazione: dialogo con il VLR
- informazioni sull'instradamento (MSRN): dialogo con il GSMC
- gestione dei dati di utente e dei costi delle chiamate
- gestione dei servizi supplementari (attivazione, disattivazione)

AuC – Authentication Center

L'AuC è l'unità funzionale del sistema GSM incaricata di generare i parametri necessari per l'autenticazione degli utenti. Si occupa di verificare se il servizio è stato richiesto da un abbonato legittimo, fornendo sia i codici per l'autenticazione che per la cifratura, per garantire tanto l'abbonato quanto l'operatore di rete da violazioni indesiderate del sistema da parte di terzi.

Il meccanismo di autenticazione verifica la legittimità della SIM senza trasmettere sul canale radio le informazioni personali dell'abbonato, quali IMSI e chiave di cifratura, al fine di verificare che l'abbonato che sta tentando l'accesso sia quello vero e non un clone; la cifratura invece genera alcuni codici segreti che verranno usati per criptare tutta la comunicazione scambiata sul canale radio.
L'AuC contiene: il codice IMSI, la chiave di autenticazione (Ki), il codice TMSI corrente e il codice LAI corrente, usati per autenticare e codificare i canali radio, oltre ad un generatore di numeri casuali (RAND), agli algoritmi A3 e A8.

L'autenticazione viene sempre effettuata ogni volta che la MS si collega al network: quando riceve o effettua una chiamata, alla scadenza dei location update periodici, alla richiesta di attivazione, disattivazione o interrogazione dei servizi supplementari.

Poiché i dati trattati dall'AuC sono di fondamentale importanza per la rete e per l'utente, vengono normalmente prese particolari misure di sicurezza e protezione per il loro mantenimento.

EIR – Equipment Identity Register

Nel GSM ogni apparato mobile (ME) è identificato univocamente dal codice IMEI. L'IMEI è distinto rispetto all'identità della persona che ha sottoscritto l'abbonamento (codice IMSI memorizzato nella SIM card). L'EIR é un database che memorizza gli IMEI. Un IMEI può essere invalido quando l'unità mobile risulta rubata oppure quando é di tipo non approvato.

Per consentire all'EIR di operare correttamente sono state definite diverse "liste", tra le quali citiamo le seguenti:

- White list - contiene gli IMEI di tutti i ME di tipo omologato, ed in condizioni operative, presenti nei paesi aderenti al GSM. Sono quindi autorizzati a connettersi alla rete.
- Black list - contiene tutti gli IMEI che sono considerati bloccati (per esempio quelli rubati oppure di tipo non autorizzato) che non sono quindi autorizzati a connettersi con la rete.
- Grey list - contiene tutti gli IMEI marcati come faulty oppure quelli relativi ad apparecchi non omologati (a discrezione del gestore). I terminali inseriti in questa lista vengono segnalati agli operatori di sistema mediante un allarme quando richiedono l'accesso, consentendo l'identificazione dell'abbonato che utilizza il terminale e l'area di chiamata in cui si trova.

Ad ogni tentativo di collegamento di un terminale, l'MSC mediante l'EIR verifica che il ME non sia contenuto nella Black list o Grey list, in tal caso gli viene sbarrato all'accesso alla rete.
L'EIR può essere unico per tutto il sistema oppure può essere implementato in una configurazione distribuita. In genere si preferisce mantenerlo fisicamente separato dalle altre entità (HLR, AuC, etc.) per ragioni di sicurezza. Esso é accessibile anche in modo remoto per consentire l'aggiornamento della varie liste in esso contenute da ogni punto della rete. E' prevista l'interconnessione di tutti gli EIR dei vari operatori GSM, per evitare l'utilizzo di apparati rubati, in nazioni diverse da quelle in cui é avvenuto il furto.

GSMC – Gateway MSC

Costituisce il punto d'accesso ad una rete GSM per chiamate da/a reti fisse o mobili di altri gestori. Nel caso di una chiamata entrante, il GMSC richiede al proprio HLR l'indirizzo dell'MSC che ha in carico il mobile. Quindi instrada la chiamata verso di esso.

SMS-GMSC – SMS Gateway MSC

L'SMS Gateway MSC agisce da interfaccia tra un centro per la gestione degli SMS ed una rete GSM per l'inoltro di SMS dal centro servizi alla stazione mobile.

SMS Interworking MSC

L'SMS Interworking MSC agisce da interfaccia tra un centro per la gestione degli SMS ed una rete GSM per la sottomissione di SMS dalla stazione mobile ad un centro servizi.

IWF – InterWorking Function

GCR – Group Call Register