

# Global System for mobile communications

## Architettura del sistema

a cura di Marcello Scatà

### INDICE GENERALE

[Mobile station Subsystem \(MS\)](#)

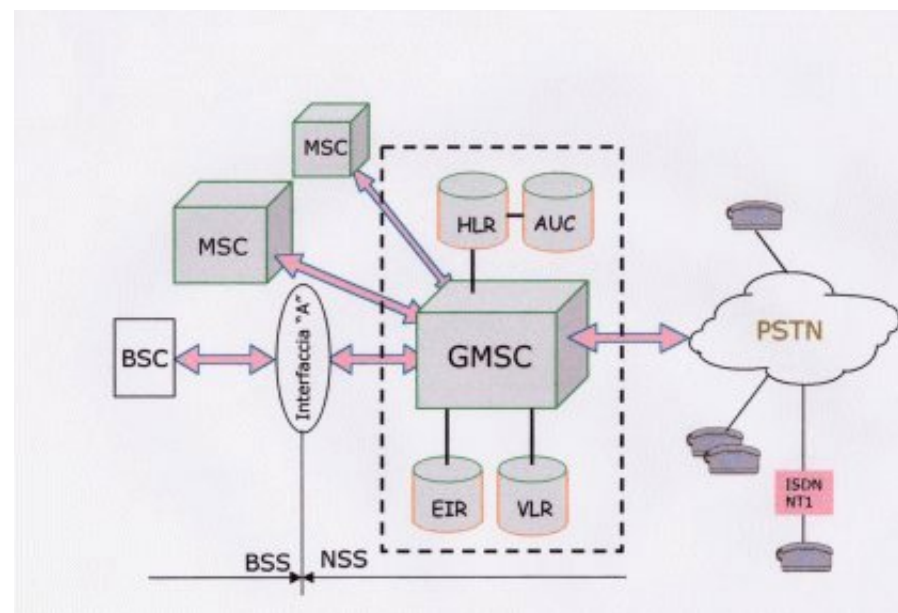
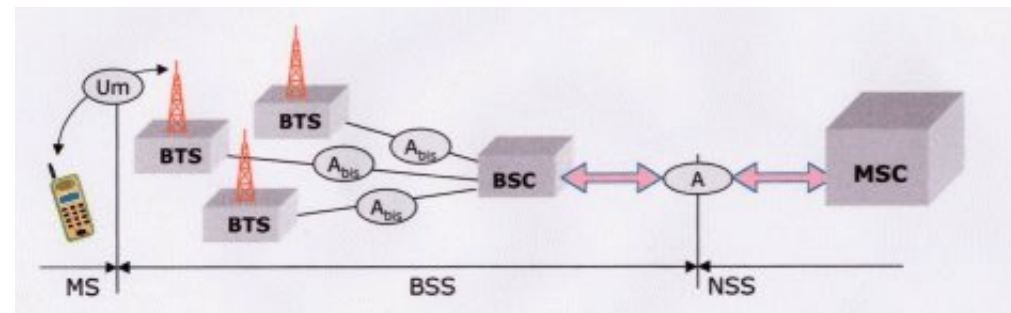
[Network Subsystem \(NS\)](#)

[Operation and Support Subsystem \(OSS\)](#)

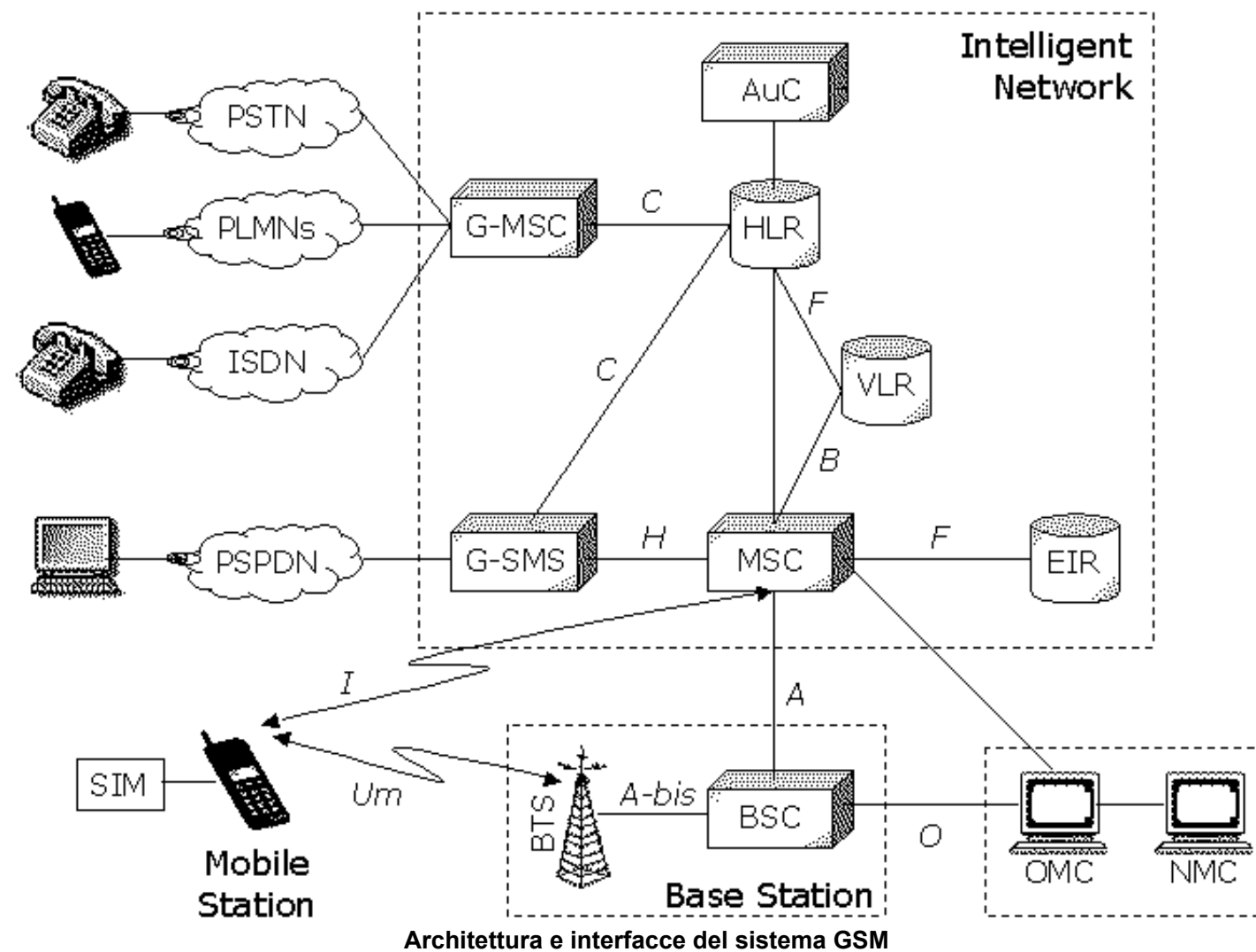
[Le interfacce GSM](#)

Una rete GSM é composta di numerose entità funzionali che possono essere raggruppate in quattro sottosistemi:

- La **Stazione Mobile** ([Mobile Station](#)) é il terminale mobile usato dall'abbonato.
- La **Stazione Base** ([Base Station Subsystem](#)) controlla la trasmissione radio con il terminale.
- Il **Sottosistema di rete** ([Network Subsystem](#)), la cui parte principale é il **Centro di Commutazione** ([Mobile services Switching Center](#)) realizza la connessione tra l'utente della rete mobile e gli utenti delle altre reti, fisse o mobili.
- Il **Sottosistema di esercizio e manutenzione** ([Operation and Support Subsystem](#)) sovrintende al corretto funzionamento e settaggio della rete.



La comunicazione tra le diverse entità del sistema GSM è assicurata da specifiche **interfacce**. La possibilità di effettuare il *roaming*, cioè di potersi spostare liberamente sul territorio servito dal proprio gestore, ed anche su quello servito dagli altri gestori delle nazioni che aderiscono al GSM, richiede di memorizzare in un database la posizione degli utenti ed aggiornarla man mano che questi si spostano. A tal scopo l'area geografica di servizio del sistema GSM è suddivisa gerarchicamente in diverse aree, dette **Network service areas**. Un operatore GSM è quindi sempre in grado di conoscere la posizione di ciascun suo abbonato.



### Mobile Station (MS)

La *mobile station* (**MS**) rappresenta la stazione mobile con la quale un utente può usufruire dei servizi offerti dal GSM. Consiste di un terminale mobile (*Mobile Equipment*, **ME**) e di una smart-card intelligente, detta **SIM** (*Subscriber Identity Module*), che permette ad un utente di caratterizzare come proprio un qualsiasi terminale mobile GSM. Vi è infatti una netta distinzione tra l'apparecchio mobile vero e proprio e la SIM che contiene tutti i dati dell'abbonato. Quest'ultima è distinta rispetto al terminale ed è, da esso, rimovibile.

### SIM Card

La SIM card contiene una memoria seriale, nella quale vengono memorizzate diverse informazioni, e un processore in grado di eseguire alcuni algoritmi di cifratura (*Encryption algorithms*). Le possibilità offerte da queste smart-card possono variare notevolmente da operatore a operatore, in dipendenza delle specifiche implementazioni.





SIM card ISO (ID-1).

Esempi di SIM card dei gestori Airtel (Spagna), Vodafone (Inghilterra) e Omnitel (Italia); tutte sono prodotte dalla casa tedesca Giesecke and Devrient GmbH.

La SIM card contiene le seguenti informazioni:

- International Mobile Subscriber Identity (**IMSI**)
- Temporary Mobile Subscriber Identity (**TMSI**)
- Individual subscribers authentication key (**Ki**)
- Ciphering key generating algorithm (**A8**)
- Authentication algorithm (**A3**)
- Personal Identity Number (**PIN** e **PIN2**)
- PIN Unblocking Key (**PUK** e **PUK2**)
- Rubrica telefonica dell'abbonato
- Messaggi SMS dell'abbonato
- Lista degli operatori GSM preferenziali scelti
- Campi informativi previsti dalle specifiche GSM Phase 2

LAI  
CODICE SERIALE SIM

E' la SIM card che fornisce l'abilitazione al servizio e viene attivata (per evitarne un uso non autorizzato) tramite un numero di identificazione personale di 4 o 8 cifre, denominato **PIN** (*Personal Identity Number*). Per garantire una sicurezza ancora maggiore, se il codice PIN viene digitato erroneamente per 3 volte consecutive la carta si blocca. In questo caso sarà necessario utilizzare il codice **PUK** di 8 cifre (*PIN Unblocking Key*) per sbloccarla. Se anche quest'ultimo venisse digitato erroneamente per 10 volte consecutive la carta andrebbe in blocco totale e sarebbe necessario sostituirla.

L'introduzione di alcuni nuovi servizi nella fase 2 di sviluppo del sistema GSM ha richiesto l'introduzione di un secondo PIN (**PIN2**) per proteggere il contenuto di alcuni nuovi campi e differenziare così l'accesso (ad esempio un abbonato può prestare la propria SIM card ad un amico fornendogli il solo PIN. Sarà così sicuro che questo, pur potendo telefonare, non potrà usufruire di tutti i servizi che richiedono invece il PIN2). Chiaramente, esiste anche un **PUK2** con le stesse funzionalità del PUK.

La SIM card contiene un codice per identificare l'utente, denominato **IMSI** (*International Mobile Subscriber Identity*), una chiave segreta di autenticazione **Ki** (*Individual subscribers authentication key*), un algoritmo di autenticazione (*Authentication algorithm*), detto **A3**, e uno di cifratura (*Encryption algorithm*), detto **A8** (questi ultimi possono riuniti in un solo algoritmo dello **A38**). Per maggiori dettagli si veda: [autenticazione](#) e [riservatezza dei dati e dei segnali di controllo](#).

Può memorizzare inoltre 100 numeri telefonici e per ognuno 12 caratteri alfanumerici descrittivi, 10 messaggi SMS (queste quantità possono variare secondo le specifiche implementazioni delle case produttrici) e una lista degli operatori GSM preferenziali dell'abbonato. ogniqualvolta non è più presente il segnale della rete su cui si è registrati, il sistema GSM provvede in modo automatico a chiedere l'accesso alla prima delle reti indicate in questa lista; se la registrazione ha esito negativo, provvede a rieseguire la stessa operazione con la successiva, e così via. La procedura continua ciclicamente fino alla avvenuta registrazione su una rete.

Il codice **IMSI** e la chiave di autenticazione **Ki** costituiscono le credenziali di identificazione dell'abbonato, equivalenti al numero seriale **ESN** (*Equipment Serial Number*) dei sistemi analogici (il codice ESN è un numero di 11 cifre: le prime tre identificano il costruttore, quindi due cifre sono di uso riservato (spesso sono poste a zero), le restanti sei cifre sono un numero seriale che identifica il terminale). Il codice IMSI è quindi associato all'utente che ha sottoscritto l'abbonamento al GSM, mentre è svincolato dall'apparato mobile (ME) utilizzato. Il codice IMSI, che ha una lunghezza massima di 15 cifre, ha la seguente struttura:

**IMSI = MCC / MNC / MSIN**

dove

**MCC** *Mobile Country Code* (3 cifre), identifica la nazione dell'operatore (Italia: 222).

**MNC** Mobile Network Code (2 cifre), identifica l'operatore all'interno della nazione (Tim: 01, Omnitel: 10).

**MSIN** Mobile Station Identification Number (max 13 cifre), numero seriale.

### La SIM card Phase II nel dettaglio (aspetti tecnici)

Tutti gli aspetti concernenti l'interfacciamento tra la SIM card e il ME, durante le operazioni di rete previste dal sistema GSM, e l'organizzazione interna di quella parte della SIM card stessa correlata con dette operazioni sono definiti da alcuni documenti ufficiali ETS (*European Telecommunication Standard*) approvati dall'ETSI. Questo è stato fatto proprio per assicurare la perfetta interoperabilità tra una SIM card ed un ME indipendentemente dai rispettivi produttori e operatori.

Per maggiori dettagli si rimanda alle raccomandazioni ETSI: GSM **11.11** (*Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface*), GSM **11.14** (*Specification of SIM-ME Interface for SIM Application Toolkit.*) e GSM **02.17** (*Subscriber identity modules, functional characteristics*). Quest'ultima tratta il concetto della divisione della *Mobile Station* in due elementi distinti (SIM e ME).

La SIM card può essere di due formati: carta di credito (formato ISO o ID-1) o francobollo di 25x15mm (formato *Plug-in*), introdotto da Nokia ed Ericsson. Entrambi i formati prevedono un marcatore che indichi il corretto verso di inserimento nel ME e devono rispettare le norme ISO **7816-1** e **7816-2** che ne specificano le caratteristiche fisiche e la dimensione e posizione dei contatti.

Il processore contenuto nella SIM card tipicamente è una CPU a 8 bit e di alcuni Kbytes di memoria (di tipo RAM, ROM ed EEPROM), in tecnologia CMOS. Il chip è progettato per lavorare tra le temperature di -25°C e +70°C con punte occasionali di +85°C, ed una umidità fino al 85%.

La *Read Only Memory* (ROM) contiene il sistema operativo, il sistema amministrativo (che gestisce i servizi GSM Phase II) e gli algoritmi di sicurezza A3 e A8. La *Random Access Memory* (RAM) è usata per l'esecuzione degli algoritmi e come buffer per la trasmissione dei dati. La *Electrically Erasable Programmable Read Only Memory* (EEPROM) contiene tutti i dati dell'abbonato (già elencati in precedenza).

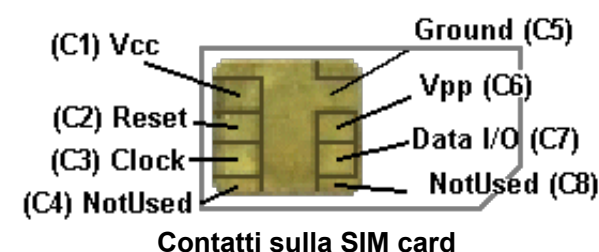
Ad oggi le smart card offrono le seguenti capacità: ROM 6-16 Kbytes, RAM 128-256 bytes, EEPROM 2-8-16 Kbytes. Le SIM di Phase I hanno 3 Kbytes di memoria EEPROM, mentre quelle di Phase II 8-16 Kbytes; queste ultime offrono quindi una capacità di memorizzazione superiore. 6 Kbytes di ROM sono sufficienti per la gestione di tutti i servizi Phase II. La quantità della memoria EEPROM determina direttamente la quantità di memoria offerta all'utente per i vari servizi. Per esempio, 1Kbyte di EEPROM può memorizzare circa 6 messaggi SMS oppure 40 numeri telefonici completi.

Un grosso problema per le tutte le smart-card è rappresentato dal degrado subito dalle EEPROM nei fasi di lettura/scrittura che ne consente un utilizzo limitato nel tempo (solitamente viene garantito il funzionamento corretto di una SIM card GSM per circa due anni). Le celle di memoria contenute nelle normali EEPROM attualmente in commercio possono infatti sopportare al massimo 10.000 cicli di lettura/scrittura. Per particolari applicazioni sono state sviluppate delle smart-card che riescono ad elevare questa soglia a 100.000 cicli.

### Interfacciamento elettrico e contatti

SIM card e ME si interfacciano mediante otto contatti, denominati da C1 a C8. La loro posizione sulla SIM e le loro dimensioni sono rigidamente fissate. I contatti C4 e C8 non sono utilizzati dallo standard GSM. Essendo la SIM una carta multi applicazione, potrebbero però essere utilizzati da altre applicazioni in futuro.

La tensione di alimentazione di una SIM Card di phase I è 5 volt. Per ridurre i consumi le SIM phase II necessitano invece di una alimentazione di soli 3 volt. La prima azienda produttrice di quest'ultimo tipo di SIM è stata la SOLAIC.



- **C1: Tensione di alimentazione (+Vcc)**

**SIM phase I:** la tensione di alimentazione Vcc può variare da 4,5v a 5,5v. L'assorbimento di corrente massimo è di 10mA; in *idle-mode* a 25°C a 1 MHz non supera i 200microA.

**SIM phase II:** la tensione di alimentazione Vcc può variare da 2,7v a 3,3v. L'assorbimento di corrente massimo è di 6mA; in *idle-mode* a 25°C a 1 MHz non supera i 200microA (con



clock-stop mode addirittura 100microA).

- **C2: Reset (RST)**
- **C3: Clock (CLK)**

La SIM ammette segnali di clock da 1 a 5 MHz, però non dispone di un "clock interno". Il segnale è fornito dal ME.

- **C6: Tensione di programmazione (+Vpp)**

La SIM card non necessita di una tensione di programmazione. Il contatto C6 può non essere presente nel ME, nel caso in cui lo sia la sua tensione è sempre posta a Vcc, mai a massa (C5).

- **C7: Data Input/Output**

## SIM locking

Il SIM locking è una funzione supportata da molti telefoni. Essa consente ad un operatore di inibire l'utilizzo del telefono con tutte le SIM che non siano le proprie. In questo modo un operatore si assicura che il nuovo l'utente rimanga suo abbonato per un dato periodo. Allo stesso tempo l'utente ha la possibilità di acquistare un telefono ad un prezzo spesso più conveniente. Alcuni operatori trascorso un certo lasso temporale, uno o due anni, forniscono un codice con cui sbloccare il telefono. Questo codice è diverso da telefono a telefono ed è calcolato in base all'IMEI.

Il SIM locking è proibito in molti paesi, ad esempio in Danimarca, ma viene utilizzato dagli operatori inglesi, svedesi (Comviq), e spagnoli (Airtel e Movistar).

## Mobile Equipment (ME)



Mobile Equipment Motorola 8700

**L'IMEI** (*International Mobile Equipment Identity*) identifica in modo univoco un *Mobile Equipment* (ME). E' quindi cablato nel ME, in modo sicuro, direttamente dal costruttore. I codici IMEI e IMSI sono completamente indipendenti l'uno dall'altro. L'IMEI, che ha una lunghezza di 15 cifre, è strutturato nel seguente modo:

**IMEI = TAC / FAC / SNR / sp**

dove

**TAC** *Type Approval Code*, fornito da una Autorità Centrale del GSM, identifica il corpo base del terminale, il modello (6 cifre).

**FAC** *Final Assembly Code*, identifica il luogo di costruzione o assemblaggio finale (2 cifre).

**SNR** *Serial Number*, numero seriale (6 cifre).

**sp** Cifra supplementare di riserva (1 cifra).

I terminali GSM sono suddivisi in cinque classi in base alla massima potenza con cui possono trasmettere sul canale radio. Possono inoltre variare la potenza di emissione in modo dinamico su 15 livelli (*Dynamic Power Control*) per mantenere una ottima qualità di trasmissione limitando al massimo le interferenze di cocanale e i consumi.

In base alla potenza di picco emessa i terminali sono stati suddivisi in 5 classi:

Classe 1: 20W; Classe 2: 8W; Classe 3: 5W; Classe 4: 2W; Classe 5: 0,8W.

La trasmissione e la ricezione radio avvengono in realtà in tempi diversi (3 timeslot di ritardo nominale). Ciò elimina la necessità del *filtro di duplice* (*duplexer*) indispensabile invece nei sistemi analogici per separare i segnali di trasmissione e ricezione che sono attivi in maniera continuativa e contemporanea.

Le principali funzioni che il terminale radiomobile deve svolgere sono le seguenti:

- trasmissione e ricezione radio
- selezione della cella migliore (cella servente), in termini di qualità di conversazione, sulla quale accamparsi
- registrazione nell'area di localizzazione
- misure trasmissive sul canale radio utilizzato e sui canali adiacenti
- controllo della potenza in trasmissione
- esecuzione dell'handover
- dichiarazione del proprio IMEI
- interfaccia uomo/macchina (display e tastiera)
- autenticazione e cifratura delle conversazioni

Base Station Subsystem (BSS)

Il sottosistema **BSS** (*Base Station Subsystem*) si occupa della parte radio del sistema e di conseguenza comprende le unità funzionali che consentono di fornire la copertura radio di un'area costituita da una o più celle.

La stazione base é composta di due unità: una *Base Transceiver Station* (**BTS**) e una *Base Station Controller* (**BSC**). L'interfaccia di comunicazione tra le due entità, detta *A-bis*, è standardizzata. In questo modo non si è vincolati a soluzioni proprietarie e si possono utilizzare componenti prodotti da fornitori diversi.

Base Transceiver Station (BTS)

Con il termine BTS si indica l'unità funzionale costituita dall'insieme dei transceiver (ricetrasmittitori) e degli apparati che consentono di fornire la copertura radio ad una cella. Solitamente ci si riferisce alle BTS anche con il termine *Stazioni Radio Base* (**SRB**).

Data la vastità dell'argomento **BTS**, vi abbiamo dedicato una sezione: [BTSmania](#).

Base Station Controller (BSC)

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 ci sono un gran numero di BTS controllate da una o poche BSC.

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).

La transcodifica può avvenire nel BSC (TRAU installato nel BSC) in modo da *infilare* multiplati quattro canali di traffico GSM in un canale PCM e quindi fruttare in modo migliore la connessione BTS-BSC (*transcodifica remota*); oppure direttamente nella BTS (TRAU installato nella BTS), conveniente solo nel caso di co-locazione BTS-BSC (*transcodifica locale*).

La trama PCM ha una durata pari a 0,125 ms. E' suddivisa mediante la tecnica TDM (*Time Division Multiplexing*) in 32 canali, ognuno da 64 kbps (TS pari a 0,125/8=3,9 microsec). La capacità complessiva del canale è quindi 64x32=2,048 Mbit/s. Il TS 0 è riservato al sincronismo, il TS 16 alle segnalazioni, i restanti 30 sono a disposizione dei canali di traffico. E' necessario un canale di segnalazione per ogni portante radio (**TRXC**), cioè 8 canali TCH. Analizziamo ora le prestazioni nei due casi. Transcodifica locale: il canale PCM trasporta fino a 3 portanti radio (TRXC), cioè 24 canali TCH, usando (8+1)x3=27 TS. Transcodifica remota: il canale PCM trasporta fino a 10 portanti radio (TRXC), cioè ben 80 canali TCH, usando (2+1)x10=30 TS (in questo caso per una portante TRXC occorrono 2 TS per i canali TCH e 1 per le segnalazioni).

Transcodifica LOCALE		TS	Transcodifica REMOTA	
	Sincronismo	0	Sincronismo	
	Segnalazione TRXC 1	1	Segnalazione TRXC 1	

TRXC 1	Canali di traffico 1-8 TRXC 1	2	Canali di traffico 1-8 TRXC 1	TRXC 1
		3		
		4	Segnalazione TRXC 2	TRXC 2
		5	Canali di traffico 1-8 TRXC 2	
		6		
		7	Segnalazione TRXC 3	TRXC 3
		8	Canali di traffico 1-8 TRXC 3	
		9		
TRXC 2	Segnalazione TRXC 2	10	Segnalazione TRXC 4	TRXC 4
	Canali di traffico 1-5 TRXC 2	11	Canali di traffico 1-8 TRXC 4	
		12		
		13	Segnalazione TRXC 5	TRXC 5
		14	Canali di traffico 1-8 TRXC 5	
		15		
	Segnalazione	16	Segnalazione	
	TRXC 2	Canali di traffico 6-8 TRXC 2	17	Segnalazione TRXC 6
18			Canali di traffico 1-8 TRXC 6	
19				
TRXC 3	Segnalazione TRXC 3	20	Segnalazione TRXC 7	TRXC 7
	Canali di traffico 1-8 TRXC 3	21	Canali di traffico 1-8 TRXC 7	
		22		
		23	Segnalazione TRXC 8	TRXC 8
		24	Canali di traffico 1-8 TRXC 8	
		25		
		26	Segnalazione TRXC 9	TRXC 9
	27	Canali di traffico 1-8 TRXC 9		
28				
	Non utilizzati	29	Segnalazione TRXC 10	TRXC 10
30		Canali di traffico 1-8 TRXC 10		

## Network Subsystem (NS)

Il sottosistema di rete, identificato a volte come *Intelligent Network* (IN), fornisce diversi servizi. Il sistema radiomobile GSM costituisce una rete pubblica di telecomunicazioni, esso deve quindi comprendere delle centrali di commutazioni che si occupino dell'instradamento delle chiamate. Il componente centrale è allora il centro di commutazione Mobile services Switching Center (MSC).

Un MSC ha in carico una certa area del territorio (controlla quindi tutte le BSC in quella zona) e deve servire tutte le MS che transitano in quell'area. Per gestire la mobilità degli utenti esso deve scambiare continuamente informazioni con un database, detto Visitor Location Register (VLR), che memorizza, temporaneamente, le informazioni relative alle MS che si trovano in quell'area (identità dell'utente IMEI, numero telefonico MSISDN, parametri di autenticazione, ecc.). Le MS in questione sono semplicemente "in visita" nell'area servita dal VLR. Esse, infatti, si possono spostare in qualsiasi momento entro l'area servita da un altro VLR. Nonostante quest'ultimo, 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. In questo caso entrambi servono la stessa area geografica, detta MSC/VLR area.

Ogni gestore possiede un database centrale, denominato Home Location Register (HLR), che memorizza permanentemente sia i dati di abbonamento degli utenti (noti come statici) sia i dati (detti dinamici) che possono variare a seguito di azioni degli utenti stessi (attivazione servizi supplementari, ecc.) che l'identità del VLR presso cui la MS dell'utente è registrata come "visitor".

L'HLR è semplicemente un database e quindi memorizza i parametri di sicurezza, ma non provvede alla loro generazione. Il compito di calcolare, tramite degli appositi algoritmi, questi parametri è demandato ad una unità funzionale denominata Authentication Center (AuC).

Per cercare di risolvere il problema del possibile utilizzo di apparati mobili ME rubati, difettosi o non omologati, esiste una unità funzionale, il Equipment Identity Register (EIR), che memorizza al suo interno tutti i codici IMEI segnalati come difettosi o rubati. La rete può così effettuare un controllo sull'IMEI richiedendolo alla MS e vietarne l'accesso nel caso questo non sia in regola.

## Mobile services Switching Center (MSC)

Il componente centrale del sottosistema di rete è il centro di commutazione **MSC** (*Mobile services Switching Center*). Esso svolge le funzionalità di un normale nodo di commutazione di una rete: per instaurare (call setup comprendente anche la procedura di autenticazione), controllare, tassare le chiamate da/verso le MS presenti nell'area geografica da esso servita. In più esegue tutti quei compiti essenziali per gestire un utente mobile come: la gestione della mobilità e l'instradamento delle chiamate. Funzioni queste che sono eseguite in collaborazione con le altre entità del network subsystem.

L'MSC fornisce la connessione con le reti fisse: *Public State Telephone Network* (PSTN), *Integrated Services Digital Network* (ISDN), rete dati a commutazione di pacchetto (PSPDN, *Packet Switched Public Data Network*) o di circuito (CSPDN, *Circuit Switched Public Data Network*).

## Gateway Mobile Switching Center (GMSC)

Tutte le chiamate originate presso le reti fisse o quelle mobili di altri gestori e dirette ad un network GSM sono dapprima inoltrate ad un particolare MSC, detto *Gateway MSC* (**GMSC**), che costituisce il punto di accesso alla PLMN GSM (*Public Land Mobile Network*) a cui appartiene l'utente mobile chiamato. Il GMSC interroga il registro HLR dell'abbonato, che a sua volta interroga il corretto registro VLR, e quindi instrada la chiamata verso il centro MSC che controlla la zona nella quale si trova l'abbonato.



## Home Location Register (HLR)

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 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 con la seguente struttura:

**MSISDN = CC / NDC / SN**

dove

**CC** *Country 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 (Tim: 335, 338, 339; Omnitel: 347, 348, 349).

**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.

I principali dati d'utente memorizzati nell'HLR:

*International Mobile Subscriber Identity (IMSI)*, che identifica univocamente l'abbonato all'interno di una qualunque rete GSM e che è contenuto anche all'interno della SIM card;

*Mobile Station ISDN Number (MSISDN)*, che identifica univocamente un abbonato nel piano di numerazione della rete telefonica commutata pubblica internazionale. Possono essere più d'uno in funzione dei servizi sottoscritti (ad esempio si possono avere numeri distinti per voce, dati e fax);

Tipo e stato dei servizi supplementari e dei servizi sottoscritti dall'abbonato a cui gli è consentito accedere (voce, servizio dati, SMS);

VLR number, per conoscere il VLR in cui è correntemente registrata la MS.

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).


## Visitor Location Register (VLR)

Il registro VLR contiene e mantiene aggiornate le informazioni relative alle MS che sono presenti, temporaneamente, nell'area da esso servita. Informazioni selezionate dal registro HLR e necessarie per il controllo delle chiamate e la gestione dei servizi supplementari.

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.

Principali dati d'utente memorizzati nel VLR:

- 
- **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.

### Authentication Center (AuC)

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.

### Equipment Identity Register (EIR)

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 con la rete, l'MSC mediante l'EIR verifica che il ME non sia contenuto nella *Black list* o *Grey list*, nel qual 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. In futuro é 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.

## Operation and Support Subsystem (OSS)

Una rete GSM è composta di molte entità funzionali di tipo diverso, le quali richiedono delle appropriate attività di Esercizio, Amministrazione e Manutenzione che devono essere opportunamente coordinate per evitare discrepanze tra i parametri di rete.

## Operation and Maintenance Center (OMC)

L'OMC è l'entità funzionale che permette all'operatore GSM di monitorare e controllare il corretto funzionamento di una parte della rete GSM costituita da uno o più MSC, con i BSC e BTS ad essi associati. L'OMC ha le seguenti funzioni:

- gestione delle configurazioni e delle prestazioni di tutti gli elementi che compongono il network GSM (BSC, BTS, MSC, VLR, HLR, EIR ed AUC);
- gestione dei guasti, degli allarmi e dello stato del sistema con possibilità di effettuare vari tipi di test per analizzare le prestazioni e per verificare il corretto funzionamento dello stesso;
- gestione della sicurezza;
- raccolta di tutti i dati relativi al traffico degli abbonati necessari per la fatturazione.

## Network Management Center (NMC)

Il NMC fornisce la visibilità globale di tutte le attività di controllo. Coordina e gestisce tutti gli OMC presenti nel network.

## Le interfacce GSM

Le raccomandazioni GSM hanno definito diverse interfacce per permettere la comunicazione tra le varie entità del sistema. Ad esse corrispondono protocolli diversi o porzioni specifiche di protocolli generali. Di seguito sono brevemente spiegate le loro principali caratteristiche.

**Um** L'interfaccia radio (*air-interface*) è utilizzata per trasportare la comunicazione tra MS e BTS.

**A-bis** E' l'interfaccia interna alla BSS che consente la comunicazione tra BTS e BSC. L'interfaccia Abis permette il controllo e l'allocazione delle frequenze radio nelle BST.

**A** L'interfaccia A è posta tra BSS e MSC; gestisce l'allocazione delle risorse radio alle MS e la loro mobilità.

**B** L'interfaccia B è posta tra MSC e VLR ed utilizza il protocollo MAP/B. Generalmente l'MSC contiene al suo interno il VLR, così questa diventa un'interfaccia "interna". Quando un MSC ha bisogno di informazioni sulla posizione di un MS, interroga il VLR usando il protocollo MAP/B sull'interfaccia B.

**C** L'interfaccia C è posta tra HLR e G-MSC o G-SMS. Ogni chiamata originata al di fuori della rete GSM e diretta ad un MS (ad esempio una chiamata dalla rete fissa PSTN) deve necessariamente passare dal Gateway per ottenere le informazioni sull'instradamento e completare la chiamata; il protocollo MAP/C sull'interfaccia C svolge proprio questa funzione. Inoltre, l'MSC può opzionalmente trasferire delle informazioni all'HLR sui costi delle chiamate effettuate.

**D** L'interfaccia D è posta tra VLR e HLR; utilizza il protocollo MAP/D per scambiare informazioni riguardanti la posizione o la gestione di un MS.

**E** L'interfaccia E interconnette due MSC; permette di scambiare i dati riguardanti gli handover tra l'*anchor* e il *relay* MSC usando il protocollo MAP/E.

**F** L'interfaccia F interconnette un MSC con l'EIR; utilizza il protocollo MAP/F per verificare lo stato dell'IMEI di un MS.

**G** L'interfaccia G interconnette due VLR di due MSC differenti e utilizza il protocollo MAP/G per trasferire le informazioni di un MS, ad esempio durante una procedura di location update.

**H** L'interfaccia H è posta tra un MSC e il G-SMS; usa il protocollo MAP/H per trasferire i brevi messaggi di testo (SMS).

- I** L'interfaccia I interconnette un MSC direttamente con un MS. I messaggi scambiati attraverso questa interfaccia sono trasparenti alle BSS.
- O** L'interfaccia O interconnette una BSC/BTS con l'OMC.

Copyright © Marcello Scatà 1997-2001 - Tutti i diritti riservati.  
Pubblicato su <http://www.gsmworld.it>