GSM - Parte I

- Breve storia
- Elementi e componenti
- Architettura
- Interfacce

Breve Storia - 1

1982: la CEPT (Conférence Européenne des Administrations des Postes et des Télécommunications) istituisce un gruppo speciale per lo studio di un insieme uniforme di regole per lo sviluppo di una futura rete cellulare pan-europea: il Groupe Spécial Mobile da cui **GSM**

1984: istituzione di 3 Working Parties (WP1-3) per la definizione di servizi da offrire in GSM: l'interfaccia radio, i formati di trasmissione e i protocolli di segnalazione, le interfacce e l'architettura di rete

Breve Storia - 2

1985: definizione della lista di raccomandazioni che il GSM deve produrre (finiranno per essere circa 130: 1500 pagine in 12 volumi! ... piu` tutti quelli relativi all'evoluzione, cioe` le fasi 2+ e 3 di GSM, rilasciati in anni successivi)

1986: viene istituito il cosiddetto *nucleo permanente* con lo scopo di coordinare il lavoro del GSM, soprattutto visto il forte interesse da parte dell'industria

1987: viene firmato un primo Memorandum of Understanding (MoU) tra operatori Telecom in rappresentanza di 12 Nazioni (europee) con i seguenti obiettivi:

- coordinare lo sviluppo temporale delle reti GSM europee e verificarne lo standard
- pianificare l'introduzione dei servizi
- concordare politiche di instradamento e la tariffazione (modalità e prezzi)

Breve Storia - 4

1988: con l'istituzione di ETSI (European Telecommunication Standards Institute) il lavoro su GSM viene "spostato" in questo foro

1990: viene deciso di applicare le specifiche GSM anche al sistema DCS1800 (Digital Cellular System on 1800 MHz), un sistema di tipo PCN (Personal Communication Networks) inizialmente sviluppato in U.K.

1991: (luglio) il lancio commerciale del GSM, pianificato per questa data, viene rimandato al 1992 per la mancanza di terminali mobili conformi allo standard (?!?)

1992: viene rilasciato lo standard definitivo relativo a GSM, che a questo punto diventa l'acronimo di
Global System for Mobile-communications

1992: introduzione ufficiale dei sistemi GSM commerciali

1993: il MoU raccoglie 62 membri di 39 paesi; inoltre altre 32 organizzazioni in rappresentanza di 19 paesi partecipano come osservatori in attesa di firmare il MoU

1994-95: introduzione degli SMS

1995-97: introduzione dei servizi a 1800MHz

1996: standardizzazione dei codificatori enhanced sia full che half-rate

1997: terminali dual-band con codificatore enhanced

1999: standard GPRS (lo tratteremo a parte) per la trasmissione a pacchetto;
primi terminali WAP (Wireless Access Protocol) su circuito commutato

2000/01: introduzione dei servizi GPRS

1993-2001: GSM diventa la rete cellulare piu` diffusa al mondo, con quasi 80M utenti in Europa e 200M a livello mondiale (quasi 40M solo in Cina), una penetrazione non marginale anche in USA con quasi 10 operatori, che hanno una quota di mercato seconda solo a AMPS/D-AMPS.
Di fatto e` diventato una standard mondiale, influenzando in modo significativo l'evoluzione verso le reti di 3ª generazione e contribuendo a determinare il fallimento commerciale delle reti satellitari

Servizi attualmente offerti dal GSM

Servizi di trasporto:

- trasmissione dati (non strutturata) sincrona e asincrona tra 300 bit/s e 9.6 kbit/s
- accesso PAD (Packet Assembly/Disassembly) asincrono tra 300 bit/s e 9.6 kbit/s
- trasmissione dati a pacchetto sincrona con velocità compresa tra 2.4 e 9.6 kbit/s
- trasmissione dati con affasciamento di canali (HSCSD) fino a 76.8 kbit/s

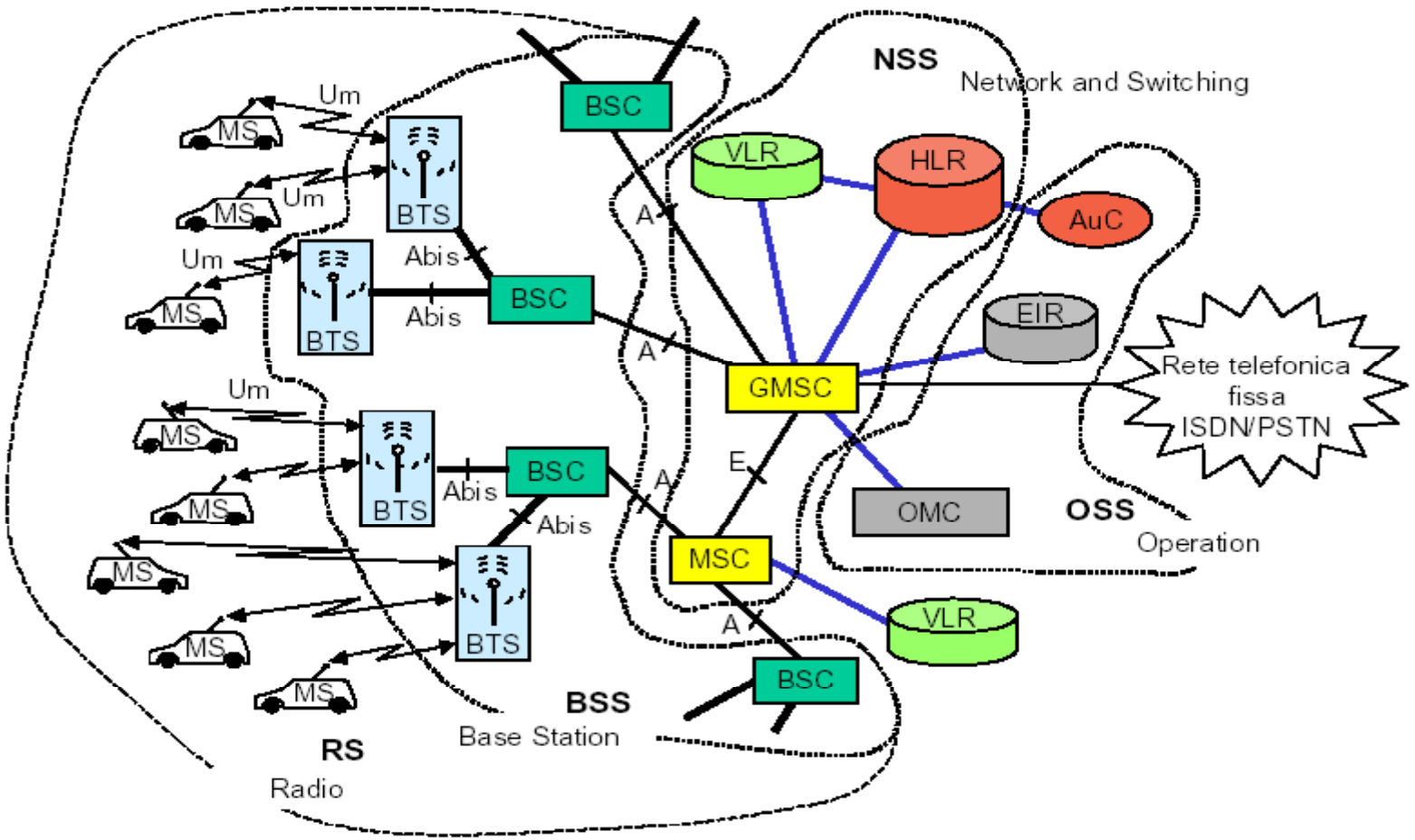
Servizi attualmente offerti dal GSM

Teleservizi:

- telefonia sia full rate (13 kbit/s, 12.6 Enhanced coder), sia half rate (6.5 kbit/s)
- telefax di Gruppo 3
- messaggeria sia unicast che multicast
- Messaggi brevi (SMS)

Servizi supplementari: praticamente tutti quelli della rete PSTN (inoltro di chiamata, richiamata su occupato, gruppi di utenti chiusi, ...)

Architettura del GSM



BSS	**Sistema stazione base**
BSC	**Controllore stazione base**
BTS	**Stazione base ricetrasmittente**
BS	**Stazione base**
MS	**Stazione mobile**
OSS	**Centro di gestione della rete**
OMC	**Centro operativo e di manutenzione**

NSS	**Sottosistema di rete**
MSC	**Centro di commutazione servizi mobili**
HLR	**Registro utenti locali**
VLR	**Registro utenti ospiti**
AuC	**Centro di autenticazione**
EIR	**Registro identità apparato**

Terminale Mobile (Mobile Station - MS)

- È il terminale di proprietà dell'utente
- Ne esistono molti tipi diversi, a seconda delle applicazioni e dei luoghi di installazione
- Tre categorie a seconda della potenza nominale:
  - veicolari: possono emettere fino a 20 W all'antenna
  - portatili: fino a 8 W all'antenna, sono trasportabili, ma hanno bisogno di una notevole fonte di alimentazione per il funzionamento (es. PC portatili, fax, etc.)
  - personali (hand-terminal): fino a 2 W all'antenna, è il "telefonino"

Terminale Mobile (MS)

- "Dual-Band" se funziona sia a 900 MHz che a 1800 MHz
- MS è solamente "hardware", per poter funzionare e collegarsi alla rete ha bisogno di una scheda di abilitazione: la **SIM**
- Nei paesi dove i numeri di emergenza (Ambulanza, Polizia, Pompieri, etc.) sono considerati un bene primario (USA, Scandinavia, etc.) MS è abilitato a chiamare questi numeri anche senza la SIM.

  In Italia dovrebbe funzionare il 113

Modulo di Identificazione Utente (Subscriber Identity Module - SIM)

- È una scheda intelligente (con processore e memoria) di tipo *smart card* che rende "operativo" un qualunque terminale MS
- Deve essere inserita nell'apposito *lettore* di MS
- Sono ammessi 2 possibili formati: tipo carta di credito e un formato ridotto (*plug-in* SIM, attualmente la più diffusa)

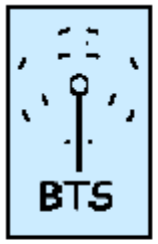
Modulo di Identificazione Utente (Subscriber Identity Module - SIM)

- Le caratteristiche dell'utente (# telefonico, servizi accessibili, etc.) sono memorizzate in modo permanente e crittografato nella SIM, che rappresenta quindi il vero e proprio "servizio" offerto dai gestori; ad esempio è possibile acquistare SIM da gestori diversi e usarle dallo stesso MS a seconda delle esigenze, oppure è possibile recarsi all'estero portando solo la SIM, affittare un MS localmente e connettersi

Modulo di Identificazione Utente (Subscriber Identity Module - SIM)

- Memorizza messaggi brevi inviati dalla rete (più evolve la tecnologia maggiori capacità potranno essere associate alla SIM) tra cui gli SMS
- La SIM viene abilitata attraverso un codice di 4 cifre (**PIN** - Personal Identification Number)
- Se il PIN viene sbagliato 3 volte consecutive, la SIM si autoblocca e può essere sbloccata solo con un codice di sblocco a 8 cifre (**PUK** - Personal Unblocking Key)

L'insieme MS+SIM fa un **terminale mobile (TM)**



Stazione Radio Base (Base Tranceiver Station - BTS)

- È il punto di accesso alla rete di TLC, o se si vuole, la "controparte" di MS
- È collocata in un punto opportuno della cella (es. al centro per celle circolari, nel vertice delle celle settorizzate, ad un estremo delle celle oblunghe per la copertura stradale...)
- Dalla potenza del BTS dipende l'effettiva dimensione fisica della cella: grazie a questa caratteristica è possibile "aggiustare" in modo dinamico le dimensioni delle celle

Stazione Radio Base (Base Tranceiver Station - BTS)

- Ciascuna BTS può avere da 1 a 16 interfacce radio, corrispondenti a diversi canali in FDM
- Ciascuna interfaccia radio corrispondende a 8 canali TDM
- La BTS è un apparato di livello fisico e non ha praticamente alcuna "intelligenza": nel GSM anche la valutazione e la decisione sugli handover da effettuare è demandata ad altre entità (MS, BSC e MSC)

BSC

Controllore della Stazione Radio Base (Baser Station Controller- BSC)

- Un BSC controlla un numero elevato di BTS: da alcune *decine* ad alcune *centinaia*
- I compiti principali del BSC sono:
  - la gestione delle frequenze, che possono essere assegnate in modo dinamico alle varie BTS
  - la concentrazione del traffico verso un MSC e lo smistamento del traffico verso le BTS
  - la gestione degli handover tra BTS adiacenti

BSC

Controllore della Stazione Radio Base (Baser Station Controller- BSC)

- I BSC possono essere collocate nel sito di un MSC o essere autonome, o ancora essere posizionate vicino (o insieme) ad alcune BTS. Normalmente vengono colocate con MSC per questioni di controllo e manutenzione
- **Presso i BSC avviene la transcodifica della voce GSM ⇔ PCM e viceversa ed anche la crittografia per il canale radio**

(G)MSC

(Mobile Switching Center - MSC)
Centro di Commutazione dei Servizi Mobili

- Sono "normali" commutatori PCM (commutatori a circuito) cui sono state aggiunte funzionalita` di segnalazione per la gestione della mobilita`
- Consentono l'instradamento delle chiamate da un MS ad un altro o verso telefoni fissi
- Un caso particolare di MSC è il **GMSC** (*Gateway-MSC*), che è l'interfaccia tra la rete GSM e le reti fisse (PSTN)
- GMSC e` anche il "punto di partenza" per la ricerca degli MS nella rete cellulare

(G)MSC

(Mobile Switching Center - MSC)
Centro di Commutazione dei Servizi Mobili

- **Le funzioni legate alla sicurezza e all'autenticazione sono effettuate solo presso i GMSC**
- A seconda delle dimensioni della rete e del numero di utenti un operatore può avere uno o più GMSC a cui sono associati in modo fisso i terminali mobili (TM)
- Una chiamata entrante verso un TM passa sempre attraverso il "suo" GMSC

Registro di Localizzazione Principale (Home Location Register)

- È una base dati ***permanente*** associata in modo univoco a un *GMSC*
- Memorizza le informazioni relative a tutti gli MS la cui localizzazione **di *default*** è presso il *GMSC* considerato
- HLR memorizza informazioni permanenti come l'IMSI (International Mobile Subscriber Identity), il numero di telefono della SIM associata (che **NON** sono la stessa cosa) e la sua chiave di autenticazione, i servizi supplementari a cui l'utente è abilitato, . . .

Registro di Localizzazione Principale (Home Location Register)

- HLR memorizza anche informazioni volatili; es.
  - l'indirizzo del VLR presso cui può essere reperito l'utente
  - parametri transitori per identificazione e crittografia
  - un eventuale numero di telefono per l'inoltro delle chiamate
  - stato dell'MS (acceso, spento, ...)
  - ...
- HLR gioca un ruolo fondamentale nella gestione delle chiamate che provengono dalla rete fissa e sono inoltrate verso un TM

Registro di Localizzazione dei Visitatori (Visitor Location Register - VLR)

- È una base dati ***temporanea*** associata a tutti gli MSC, anche ai GMSC
- contiene i dati essenziali per il servizio dei TM attualmente sotto la giurisdizione del (G)MSC cui VLR è associato
- Si noti che per questione di uniformità viene usato il VLR anche per gli MS che si trovano presso il proprio GMSC: l'informazione in HLR viene "duplicata" localmente

Registro di Localizzazione dei Visitatori (Visitor Location Register - VLR)

- In VLR vengono duplicati tutti i dati permanenti di un utente
- L'IMSI viene "mappato" su un TMSI (Temporary Mobile Subscriber Identity) per non trasmettere regolarmente l'IMSI via radio (protezione da intrusioni)
- Il TMSI viene modificato frequentemente ed è legato anche alla posizione del mobile
- VLR gioca un ruolo fondamentale nella gestione delle chiamate che provengono dagli MS

IMSI

- Numero di identificazione di uso interno alla rete
- Composto da 3 campi:
  - **MCC**: Mobile Country Code (3 cifre)
  - **MNC**: Mobile Network Code, che identifica l'operatore che fornisce il servizio (2 cifre)
  - **MSIC**: Mobile Subscriber Identification Number, che identifica la SIM (fino a 10 cifre)
- Es: 222 01 4572228769, identifica una SIM italiana (222) del gestore TIM (01)
- Il numero di telefono dell'apparato in questione è completamente scorrelato dall'IMSI

TMSI

- Numero assegnato temporaneamente dalla rete (VLR) a MT per questioni di privacy e protezione
- Strutturalmente uguale a IMSI
- E` legato a VLR (in effetti alla Location Area)
- Cambiato ad ogni uso, e ad ogni location update
- Trasmesso in chiaro dal MT per autenticarsi, viene ri-assegnato dalla rete dopo aver instaurato un canale sicuro (criptografato) --> una eventuale intercettazione e` inutile

MSISDN & MSRN

- MSISDN: Mobile Station International ISDN Number ... il numero di telefono

- MSRN: Mobile Station Roaming Number
  - ✓ numero usato dalla rete per l'instradamento delle chiamate
  - ✓ memorizzato presso HLR, identifica il VLR dove si trova il mobile, quindi anche l'eventuale operatore di roaming

IMEI e IMEISV

- International Mobile station Equipment Identity
- Numeri di identificazione dell'apparato
- IMEI (60 bit) identifica l'hardware
- IMEISV (64 bit) identifica anche eventuali diverse versioni di software/firmware
  - 24 bit: TAC (Type Approval Code)
  - 8 bit: FAC (Final Assembly Code) - il produttore
  - 24 bit: SN (Serial Number)
  - 4 bit non usati in IMEI
  - 8 bit: SVN (Software Version Number) in IMEISV

(Equipment Identity Register)
Registro di Identificazione degli apparati

- È una base dati il cui uso è a discrezione dell'operatore
- Contiene l'identificativo e le caratteristiche di tutti gli apparati GSM (MS - l'hardware!!!) prodotti, insieme al produttore, al paese di fabbricazione, etc.
- Può essere usato per proteggere la rete dall'uso di apparecchiature non a norma, rubate, esportate illegalmente, ...

Centro di Autenticazione (Authentication Center - AuC)

- È associato a ciascun HLR
- È il "motore" per l'autenticazione delle SIM
- È in grado di effettuare correttamente le operazioni di codifica che sono associate a ciascuna SIM
- Gestisce alcune importanti operazioni per abilitare la cifratura della trasmissione sull'interfaccia radio

OMC

Centro Gestione e Controllo (Operation and Maintenance Center)

- È la sede di tutte le operazioni di gestione (tecnica e non) della rete
- Effettua la tariffazione, controlla il traffico in rete, gestisce i messaggi di errore provenienti dalla rete, controlla e memorizza il carico delle singole BTS e BSC per operazioni di pianificazione (eventualmente dinamica)
- Consente di configurare le singole BTS tramite le BSC e di controllare il funzionamento (corretto o meno) di tutte le apparecchiature periferiche della rete (cioè in pratica di tutti gli elementi descritti fino ad ora)