Risorse radio e mobilità in GSM

Procedure di assegnazione iniziale

Mobile-Originated Call

Analizzaziamo il caso di una chiamata originata da un terminale radiomobile verso un numero di telefono di rete fissa.

1. L'utente digita il numero dell'apparato da chiamare
2. Il terminale mobile accede al *Random Access Channel* (tramite protocollo S-ALOHA), ed invia un messaggio di *call request* alla BS che lo sta servendo
3. La BS inoltra la richiesta (numero MSISDN dell'utente che sta effettuando la chiamata, parametri di qualità richiesti...) all'MSC competente
4. Per evadere la richiesta, l'MSC effettua una query al VLR, per ottenere le necessarie autorizzazioni alle operazioni.
5. Inoltre, controlla le risorse disponibili per effettuare il collegamento verso il numero di telefono chiamato
6. Se le autorizzazioni hanno avuto riscontro positivo, l'MSC alloca le risorse per la connessione, seleziona la necessaria funzione di transcodifica (interworking function IWF).
7. Se la connessione è stata stabilita con successo verso il numero di telefono destinazione, allora notifica la BS dell'utente
8. La BS notifica l'avvenuta allocazione delle risorse all'utente tramite l'*Access Grant Channel*
9. La chiamata è stabilita.

Handover

Una delle caratteristica peculiari dei sistemi cellulari è la possibilità di mantenere attiva una comunicazione pur continuando a spostarsi liberamente nel territorio. Questa mobilità può causare la necessità di cambiare frequentemente cella di servizio oppure canale di trasmissione per continuare a garantire all'utente una buona qualità del segnale. Questa commutazione automatica senza interruzione nel collegamento è chiamato *handover*.

Esistono quattro tipi differenti di handover nel sistema GSM, che coinvolgono il trasferimento di una comunicazione tra:

- canali (o TDMA timeslot) diversi di una stessa cella, cioè di una stessa BTS;
- celle diverse ma controllate da una stessa BSC;
- celle di diverse BSC, ma controllate da uno stesso MSC;
- celle controllate da diversi MSC.

I primi due tipi, chiamati **handover interni**, coinvolgono solo una stazione base (BSC). Sono gestiti direttamente dalla BSC senza coinvolgere l'MSC, eccetto che per notificargli il completamento del handover, così da non sovraccaricare inutilmente la rete.

Gli ultimi due tipi, chiamati **handover esterni**, sono invece trattati dagli MSC direttamente coinvolti. Nell'ultimo caso, l'MSC originale, detto *anchor* MSC, continua a rimanere responsabile della maggior parte delle funzioni relative alla chiamata in corso mentre gli handover interni (inter-BSC) che dovessero eventualmente verificarsi saranno gestiti dal nuovo MSC, detto *relay* MSC.

Gli handover possono venire richiesti sia da un terminale che da un MSC (per bilanciare il carico del traffico). Durante i timeslot di inattività, la stazione mobile sonda i canali di broadcast (Broadcast Control Channel) delle celle geograficamente adiacenti che riesce a ricevere (al massimo di 16 celle). Queste informazioni sono passate, almeno una volta al secondo, al BSC che prepara una lista delle 6 migliori candidate per un handover in base alla potenza del segnale ricevuto.

Esistono due algoritmi di base utilizzati per decidere quando effettuare un handover, entrambi sono

strettamente vincolati al controllo della potenza. Spesso la stazione base non sa quando una bassa qualità del segnale sia imputabile alle eccessive riflessioni raccolte lungo il percorso oppure al terminale mobile che si è avvicinato ai confini di copertura della cella. Questo è vero soprattutto quando le celle sono molte e geograficamente vicine, ad esempio nelle zone urbane.

L'algoritmo **Minimum Acceptable Performance** dà la precedenza al controllo della potenza sugli handover, così quando la qualità del segnale degrada oltre un certo valore, il livello di potenza del terminale viene aumentato. Se questo aumento non produce nessun beneficio, allora si prende in considerazione la possibilità di effettuare per forza un handover. Questo metodo è il più semplice e il più comunemente adottato, però, continuare ad incrementare la potenza, può portare ad avere un terminale che trasmette con elevata potenza, producendo una elevata interferenza di co-canale, fuori dai naturali confini della cella a cui è agganciato (e quindi dentro ad una cella adiacente).

Inoltre riduce l'autonomia del terminale e, se non adeguatamente progettato, può portare al fenomeno che Walke chiama “*pingpong handover*”. Avviene quando viene effettuato continuamente un handover tra due base station a seguito di variazioni della qualità del segnale che avvengono al limite della soglia minima. Si pensi al caso di un terminale mobile che si trovi nella zona di frontiera di due BS (chiamate A e B), in cui la potenza dei loro segnali è praticamente la stessa. Si supponga che il MS venga servito da A. Per evitare l'effetto “pingpong”, non viene effettuato l'handover non appena il segnale di B diventa più forte rispetto a quello di A, ma si aggiunge una isteresi al sistema, cioè un ulteriore livello di guardia. E' da tenere comunque presente che la MS può solo proporre un handover. L'effettiva decisione spetta alla BSC (per gli handover interni) o all'MSC (handover esterni).

Oltre al controllo di potenza, ma sempre correlato ad esso, il MS periodicamente invia alla BSC un report contenente una stima della probabilità d'errore, calcolata grazie ai training sequence di 104 trame. Questa elaborazione viene effettuata durante i 4 timeslot tra trasmissione e ricezione. Se la probabilità viene ritenuta sufficientemente bassa (minore della massima probabilità consentita), la BS abbassa la potenza di trasmissione. In tal modo viene ridotta l'interferenza di co-canale anche da parte della BS. Il sistema propone un handover quando:

- la BS non può trasmettere più forte (a causa dei limiti imposti dalle normative)
- c'è traffico su una cella, e minore traffico su un'altra
- la MS è al massimo della potenza

L'algoritmo **Power Budget** invece usa gli handover per mantenere o migliorare la qualità del segnale senza aumentare, o addirittura cercando di diminuire, il livello di potenza. Così facendo non si hanno problemi di `sconfinamenti' e viene anche ridotta l'interferenza tra canali. Purtroppo è un metodo molto più complicato da implementare.

L'handover effettuato da GSM prende il nome di *Hard Handover* (a causa della impossibilità del terminale di colloquiare con due BTS contemporaneamente). In UMTS sono disponbili anche *Soft* e *Softer Handover*.

Paging

Mobile-Terminated Call

Analizziamo in dettaglio la procedura di instradamento per una chiamata originata da rete fissa (PSTN o ISDN) e diretta ad un utente mobile.

1. Il chiamante, dalla rete fissa (PSTN o ISDN), compone il numero MSISDN dell'utente mobile che vuole contattare.
2. Le centrali di commutazione della rete fissa, analizzando i prefissi **CC** e **NDC** del numero MSISDN, instradano la chiamata verso il GMSC della rete GSM a cui appartiene la MS chiamata.
3. Il GMSC riceve il messaggio di segnalazione SS7 IAM (*Initial Address Message*) contenente il numero MSISDN di destinazione. Dalle prime cifre del numero **SN**, ricava il HLR su cui è registrata la MS e gli invia un messaggio di *Send routing information*.
4. L'HLR, in base al numero MSISDN, rintraccia tutte le informazioni dell'abbonato, compreso il codice IMSI e l'indirizzo SS7 del VLR su cui è temporaneamente registrata la MS (*VLR number*). Non conosce, però, il *roaming number* correntemente assegnato alla MS e così invia un messaggio di *Provide roaming number* al VLR indicando il codice IMSI della MS di cui richiede il numero MSRN.

5. Il VLR di destinazione fornisce al HLR dell'abbonato chiamato il numero MSRN.
6. HLR ritorna al GMSC lo stesso numero MSRN.
7. Ora il GMSC, analizzato il numero MSRN ricevuto, può instradare la chiamata fino al MSC/VLR che serve (temporaneamente) la MS, attraversando anche eventuali reti di transito.
8. Adesso è necessario localizzare la MS. Il MSC/VLR, in base al codice IMSI, individua la *location area* corrente di registrazione. Invia quindi un messaggio di *page* ai BSC, che servono quell'area, perché trasmettano il paging.
9. I BSC comandano a tutte le loro BTS di irradiare il messaggio di paging, sul canale PCH, indirizzato alla MS chiamata.
10. La MS risponde al messaggio di paging attraverso una richiesta di accesso alla rete, sul canale RACH.
11. La rete assegna un canale dedicato (SDCCH) alla MS e, attraverso un messaggio sul canale logico AGCH, gli ordina di spostarsi immediatamente su esso per effettuare le procedure di autenticazione.
12. Conclusasi positivamente la fase di autenticazione, il MSC/VLR assegna alla MS un canale di traffico (TCH) e le ordina di spostarsi su di esso.
13. La connessione è instaurata e gli utenti possono comunicare.

Location update

Il sistema GSM differisce dalle telecomunicazioni via cavo principalmente per la necessità di gestire la mobilità dell'utente. In un sistema cellulare l'utente mobile deve quindi essere localizzato prima che il sistema possa instradare una chiamata in arrivo al suo terminale.

Un procedura legata all'aggiornamento di posizione è la connessione / sconnessione (*IMSI attach / detach*) dalla rete di una MS. La sconnessione informa la rete (MSC) che una MS è spenta o non più raggiungibile, così da evitare allocazione dei canali di controllo ad essa necessari e inoltro dei messaggi di paging. La connessione, invece, informa la rete (MSC) che la MS, già marcata come detached, è nuovamente raggiungibile. Si verifica quando una MS viene spenta e successivamente riaccesa, oppure quando rientra nell'area di copertura della rete.

L'arrivo di una chiamata è notificato al terminale mobile (MS) attraverso un messaggio inviato sul canale di paging (PCH). Sarebbe inutilmente dispendioso, in termini di occupazione di banda, inviare questo messaggio da tutte le celle della rete per ogni chiamata. All'opposto sarebbe troppo complicato inviarlo solo dalla BTS corrente cui è "agganciato" il terminale. Così si è preferito adottare una soluzione di compromesso consistente nel raggruppare le celle in area più estese, dette aree di localizzazione (*Location Areas*) e identificate in modo univoco dal *Local Area Identity* (LAI). Il messaggio di paging (PCH) verso un MS, per notificargli una chiamata in arrivo, è allora inviato solamente alle celle dell'area di localizzazione dove la MS è attualmente registrato (localizzato).

Ogni BTS irradia, su un apposito canale di broadcast (BCCH), un messaggio di sistema che contiene proprio il codice LAI dell'area a cui appartiene la cella. Quando una MS attraversa il confine tra due aree di localizzazione, riceve un codice LAI diverso dal precedente. Di conseguenza essa deve informare la rete della sua nuova posizione.

La procedura di *location updating* consiste nell'aggiornare la localizzazione della MS, in termini di codice LAI, nel registro VLR di competenza. Se la nuova e la vecchia location area appartengono ad MSC/VLR diversi, è cambiato anche il VLR. In questo caso è necessario informare anche il registro HLR. Quest'ultimo, infatti, memorizza la posizione della MS in termini di indirizzo del VLR (*VLR number*) in cui essa è correntemente registrata.

Per ottimizzare lo sfruttamento del canale radio, è necessario evitare trasmissioni inutili. Ad esempio irradiare i messaggi di paging verso MS che non sono raggiungibili, e quindi che non sono in grado di ricevere chiamate.

Una MS non è più raggiungibile quando viene spenta (in questo caso effettua un *IMSI detach*) oppure quando esce dall'area di copertura senza poterlo comunicare alla rete che così continua ad allocare i canali di controllo anche per essa.

La rete si accorge delle non raggiungibilità di una MS nel momento in cui tenta di inoltrargli una chiamata (non riceve risposta al messaggio di paging). Ora può marcare la MS come sconnessa (*implicit IMSI detach*).

Se però non vi sono chiamate dirette ad una MS non raggiungibile, questa continuerebbe ad essere considerata connessa per un tempo indefinito. Per evitarlo è stata introdotta la procedura di registrazione periodica (*periodic registration*). Una MS che si sposti all'interno di una stessa LA senza accedere alla rete per ricevere o effettuare chiamate, deve comunque, ad intervalli di tempo regolari (*location update timer*), confermare la propria localizzazione al VLR. Il valore del timer, scelto a discrezione dell'operatore di rete è trasmesso sul canale BCCH. Se una MS non effettua accessi alla rete per un tempo superiore al limite prefissato (e quindi non effettua la registrazione periodica), viene automaticamente marcata come sconnessa dalla rete stessa (*implicit IMSI detach*).

Tale valore deve essere un gusto compromesso: infatti un LU ad intervalli brevi eviterebbe di inviare messaggi di paging inutili per la LAC, ma in compenso saturerebbe subito i canali SDCCH. Viceversa un LU "lungo" gioverebbe al tempo di stanby del terminale, risparmiando batteria, e saturerebbe meno i canali di SDCCH, ma se la MS uscisse di copertura verrebbe inutilmente "cercata" per un periodo oggettivamente troppo lungo.

Gestione della sicurezza

All'aspetto sicurezza nel sistema GSM sono dedicate specifiche raccomandazioni ETSI (02.09, 02.17, 03.20, 03.21) che prendono in esame aspetti quali: l'autenticazione e la riservatezza dell'identità dell'utente, la riservatezza delle conversazioni (o dati trasmessi dall'utente) e delle segnalazioni di controllo. L'abb**onato è** identificato univocamente dal codice IMSI (*International Mobile Subscriber Identity*), questo codice unitamente alla personale chiave di autenticazione Ki costituiscono le credenziali di id**e**ntificazione analogamente al codice ESN (*Equipment Serial Number*) dei sistemi analogici.
Le procedure di autenticazione e crittografia prevedono che queste informazioni non vengano mai trasmesse sul canale radio. Per l'autenticazione è utilizzato un meccanismo di tipo *challenge-response*; mentre per la crittografia dei dati trasmessi viene usata una chiave temporanea Kc ed anch'essa non viene mai trasmessa sul canale radio.

Possiamo guardare alle procedure che si occupano della sicurezza come a un sistema distribuito. È la distribuzione che fornisce una ulteriore misura di sicurezza. Gli elementi del sistema GSM che intervengono attivamente nella realizzazione delle procedure e dove quindi sono distribuite le informazioni e le risorse relative alla sicurezza, sono: la SIM (*Subscriber Identity Module*), il ME (*Mobile Equipment*) e la rete GSM.

La SIM contiene il codice IMSI, la chiave personale di autenticazione Ki, l'algoritmo A8 che genera la chiave temporanea di crittografia Kc, l'algoritmo A3 di autenticazione e il *Personal Identification Number* (PIN) assieme a molti altri dati. Il terminale mobile ME contiene l'algoritmo A5 di crittografia.

Nella rete GSM le informazioni sono ulteriormente distribuite. Nella Base Transceiver Station (BTS) sono contenuti l'algoritmo A5 e in fase di crittografia la chiave Kc. Alla base dei processi di crittografia e autenticazione è l'unità funzionale Authentication Center ha a disposizione i codici TMSI/IMSI, il codice LAI, la chiave Ki e gli algoritmi A3 e A8 oltre ad un algoritmo per la generazione di numeri pseudocasuali. L'AuC memorizza nei database VLR e HLR i parametri di sicurezza.

Tutti questi elementi (SIM,ME e GSM Network) sono necessari per il corretto funzionamento dei meccanismi di autenticazione e sicurezza. Ma è da sottolineare l'incredibile apporto al sistema complessivo dovuto all'introduzione della SIM.

La SIM e il sistema di sicurezza
Il sistema GSM è il primo sistema internazionale che ha impiegato una smart card (Subscriber Identity Module SIM) come dispositivo di sicurezza per l'autenticazione dell'abbonamento e dell'abbonato. L'idea di utilizzare un microprocessore per l'autenticazione in una rete radiomobile nasce in Germania nei primi anni ottanta, dove smart cards vengono utilizzate nella rete radiomobile analogica "Netz-C". Queste idee coincisero temporalmente con le prime discussioni sulla realizzazione di un sistema radiomobile multinazionale, il *Global System for Mobile Communications*.

Diversi comitati tecnici dal 1988 al 1994 si sono occupati di studiare, definire e sviluppare quali dovessero essere le caratteristiche della SIM. Opinione comune era che la carta dovesse avere l'aspetto di una carta di credito (formato ID-1). Per un certo tempo si considerarono altre due possibili implementazioni: un modulo plug-in, formato francobollo (25mm x 15mm) per terminali troppo piccoli per consentire l'uso di una ID-1 card e un modulo integrato che fosse parte integrante del terminale (ME). Il modulo integrato presentava il vantaggio di non richiedere alcuna interfaccia ma non venne ritenuto idoneo ai requisiti del sistema GSM. In modo particolare i problemi riguardavano la gestione dei dati correlati alla sicurezza. Sarebbe stato difficile per gli operatori del servizio usare propri specifici algoritmi di sicurezza e mantenere uno stretto controllo delle chiavi segrete e degli altri dati personali senza un modulo dedicato alla sicurezza. Infatti ciò avrebbe

reso necessario lo sviluppo e la produzione da parte di ogni singolo operatore dei propri specifici terminali: si pensò che terminali non proprietari avrebbero garantito l'allargamento del mercato a tutti i produttori e ridotto le barriere commerciali in quanto ogni terminale poteva essere utilizzato su ogni rete. ID-1 card e plug in sono invece ancora utilizzate entrambe malgrado la scarsa maneggiabilità della plug-in.

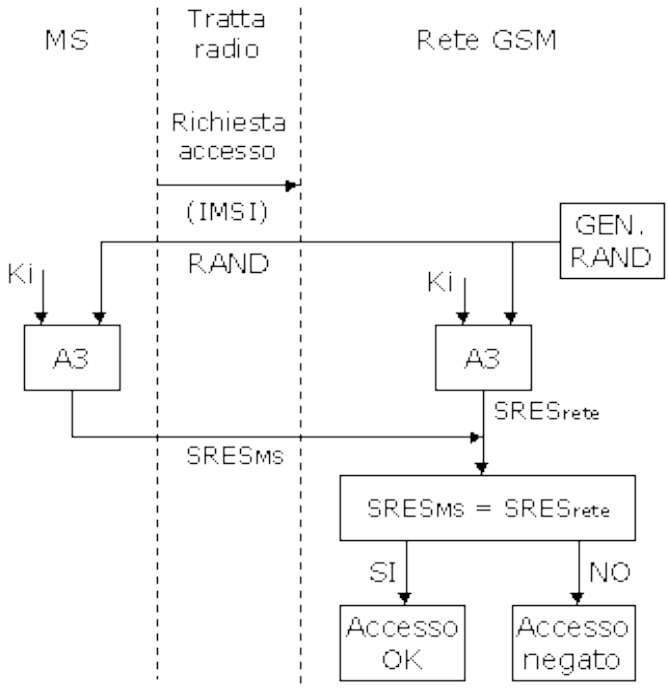
La divisione della Mobile Station in Mobile Equipment (ME), sostanzialmente un sistema radio che non contiene alcuna informazione correlata all'abbonamento e SIM, dà all'operatore che si cura della programmazione e distribuzione di quest'ultima, un completo controllo su tutti i dati legati alla sicurezza. La SIM rimovibile dà inoltre una nuova dimensione alla mobilità dell'utente, ed è perciò, parte integrante del complessivo sistema di sicurezza, e "gettone" per la mobilità dell'abbonato.

Autenticazione
La procedura di autenticazione viene avviata ogniqualvolta la Mobile Station (MS) si collega alla rete, e più precisamente nei seguenti casi:

- ogniqualvolta la MS riceve o effettua una chiamata,
- ogniqualvolta venga effettuato l'aggiornamento della posizione della Mobile Station (Location Updating),
- ogniqualvolta venga effettuata l'attivazione, disattivazione o interrogazione dei servizi supplementari.

Le unità funzionali in gioco nel processo di autenticazione sono: la SIM nel terminale e l'AuC (*Authentication Center*) nella home network. L'autenticazione avviene adottando un meccanismo di tipo challenge-response. Nel momento in cui l'AuC riceve una richiesta di autenticazione, riconosce (vedremo in seguito come) la probabile identità dell'utente, genera e trasmette al Mobile Equipment (ME) un numero casuale di 128 bit (RAND) come sfida (*challenge*). Il ME riceve e trasmette alla SIM la sfida. La SIM calcola la risposta (*response*) SRES di 32 bit alla sfida dando in input all'algoritmo di autenticazione A3 (*key-dependent one-way hash function*) il numero casuale (RAND) e la chiave di autenticazione dell'utente Ki, che ha una lunghezza di 128 bit ed è memorizzata nella stessa SIM. La risposta "firmata" SRES viene trasmessa alla visited network dove viene confrontata con il valore che la home network ha calcolato applicando lo stesso algoritmo A3 al numero casuale RAND e alla chiave Ki corrispondente alla identità dichiarata dall'utente (di cui conserva copia).

L'utente è autenticato e può accedere alla rete se e solo se i due valori, quello ricevuto SRES e quello calcolato coincidono (la SIM è in possesso dell'esatta chiave di identificazione), altrimenti la connessione viene rifiutata e un messaggio di *authentication failure* viene notificato alla Mobile Station.



Procedura di autenticazione

Possiamo notare come la chiave personale di autenticazione Ki non venga mai trasmessa sul canale radio. Essa è presente nella SIM come pure nell'AuC come descritto precedentemente. Inoltre il calcolo della response viene effettuato all'interno della SIM e le informazioni riservate dell'utente, come il codice IMSI e la chiave Ki, non vengono mai rilasciate dalla SIM durante la fase di autenticazione. Questo fornisce una sicurezza ulteriore.

Riservatezza dell'identità dell'abbonato
Abbiamo visto che le procedure di sicurezza si propongono di non trasmettere mai sul canale radio le credenziali di identificazione: codice IMSI e chiave Ki. Per evitare ad esempio che possa essere monitorata la posizione dell'utente intercettandone sul canale radio l'identità etc, etc..

D'altro canto la rete può autenticare la SIM solo se conosce l'identità della SIM. E questa identità deve essere trasmessa dalla MS sul canale radio. Vengono allora utilizzate delle identità temporanee. Chiaramente il codice IMSI che identifica univocamente l'abbonato nel mondo deve essere usato per aprire la sessione se non vi sono altri modi di identificare l'abbonato. Ciò accade ad esempio quando l'utente utilizza per la prima volta la SIM. Non appena si conclude con successo una autenticazione, la rete (specificatamente il VRL) assegna alla SIM un *Temporary Mobile Subscriber Identity* (TMSI), e lo trasmette, dopo che è stato attivato il processo di crittografia, in forma cifrata alla MS dove viene decifrato. La MS risponde confermando l'avvenuta ricezione e memorizza il TMSI nella SIM. Il codice TMSI viene da quel momento in poi utilizzato al posto del codice IMSI, dove ciò sia possibile, fino a che un nuovo TMSI non venga assegnato alla SIM.

Le riallocazioni avvengono in istanti prefissati specifici di ogni operatore (ad esempio ad ogni accesso alla rete). Il codice TMSI è valido nella Location Area in cui è stato rilasciato, per comunicazioni al di fuori della Location Area è necessario utilizzare il *Location Area Identity* (LAI) in aggiunta al TMSI. Ogni volta che si esegue una Location Updating cioè l'utente passa da una Location Area ad un'altra, il VLR assegna una nuova TMSI alla MS e la invia assieme al messaggio che comunica l'aggiornamento della localizzazione (Location Updating Accept). Alla ricezione di questo messaggio, la MS risponde con un messaggio di conferma (*TMSI Reallocation Complete*).

Il codice TMSI può essere riallocato anche in occasione di altri accessi alla rete quando il processo di crittografia è stato attivato: la rete trasmette una esplicita TMSI *Reallocation Request* cifrata assieme al codice, la MS risponde con una TMSI *Reallocation Confirmation* cifrata. Se per qualche motivo il codice TMSI inviato da una MS non viene riconosciuto dalla rete, ad esempio fallisce la fase di autenticazione, viene attivata la procedura di *Identity Request* tramite la quale viene richiesto alla MS l'invio del codice IMSI.

Autenticazione del Mobile Equipment
Un altro livello di sicurezza è implementato nel Mobile Equipment (ME). Ogni terminale GSM è identificato univocamente dall'*International Mobile Equipment Identity* (IMEI). Tale codice è completamente indipendente dal codice IMSI, dalla identità della persona che ha sottoscritto l'abbonamento. La SIM può essere utilizzata con una qualsiasi ME (prestata, noleggiata etc) personalizzandola, e ciò fa nascere la necessità di proteggere la rete e gli utenti, da ME non autorizzate, rubate o difettose. Come abbiamo visto è perciò previsto un particolare registro *Equipment Identity Register* (EIR) che consente di memorizzare i codici IMEI e verificare quelli corrispondenti a ME cui non è consentito l'accesso alla rete (black list). Il controllo dell'IMEI può essere effettuato in vari momenti : la rete (MSC) richiede l'IMEI al ME, la MS invia l'informazione alla rete che effettua una richiesta all'EIR, in base alla risposta il MSC concede l'accesso (ME autorizzato) o intraprende le azioni del caso (ME non autorizzato).