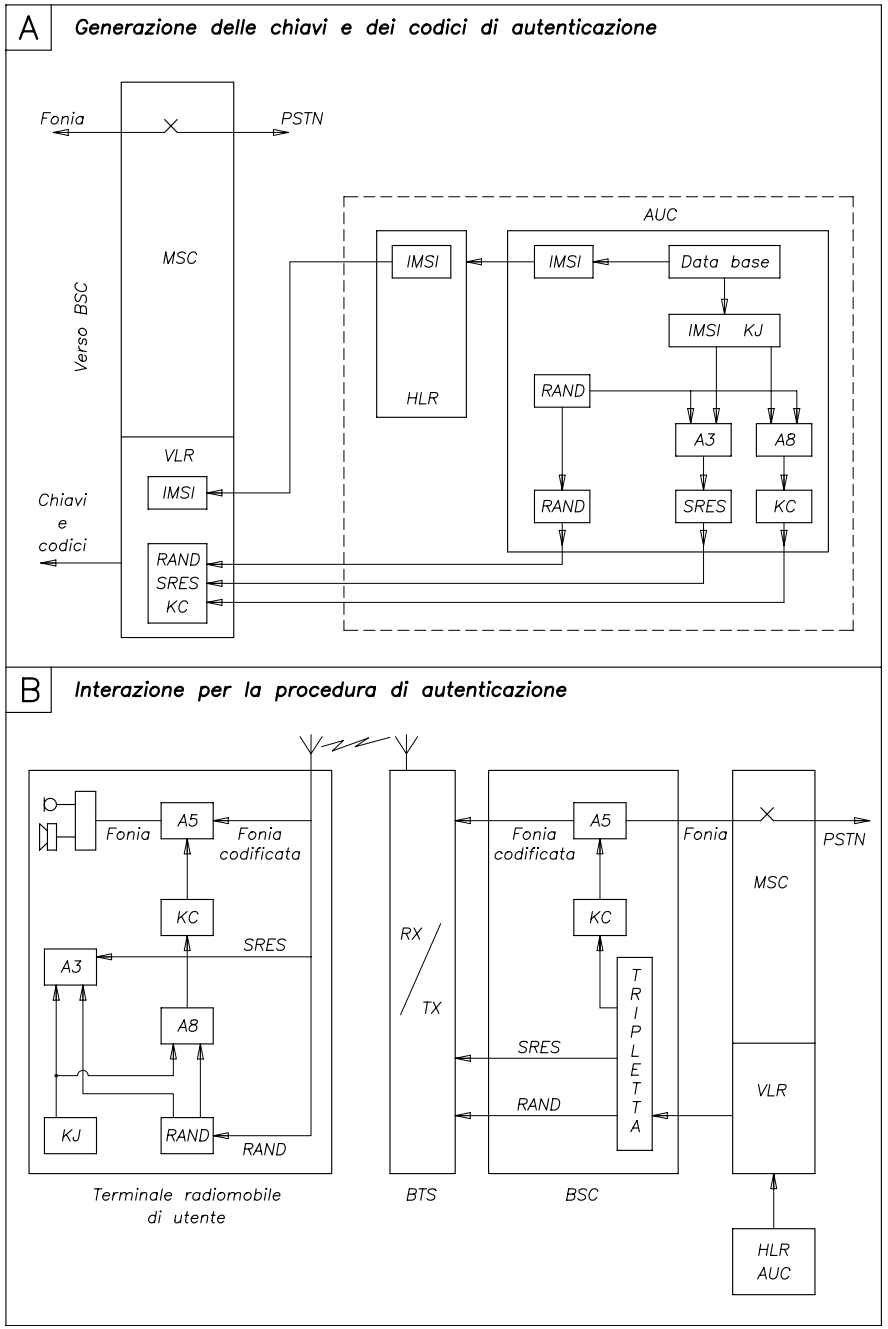
ACCESSO ALLA RETE

Introduzione. Ogni utente, per poter accedere a una rete cellulare, dev'essere registrato nel corrispondente *database* HLR con tre specifici e univoci numeri: MISDN, IMSI, MSRN. • MISDN (*Mobile International Subscriber Directory Number*): è il numero che identifica in elenco l'utente mobile e che viene utilizzato dalla rete fissa quando un abbonato chiama un utente radiomobile. • IMSI (*International Mobile Subscriber Identity*): è utilizzato dal terminale mobile ogni qualvolta impegna la rete per la prima volta. Viene poi sostituito dal TMSI che gli viene assegnato temporaneamente dalla rete. • MSRN (*Mobile Station Roaming Number*): viene assegnato temporaneamente dal VLR all'utente ed è usato dalla PSTN per instradare le chiamate. Anche altri dati temporanei vengono attribuiti all'utente e gestiti dall'HLR per identificarlo e localizzarlo in ogni momento.

Meccanismi di protezione. Servono per impedire connessioni improprie o intercettazioni. Con la procedura di *autenticate* il canale di traffico viene codificato con una chiave di cifratura multipla, modificata a ogni connessione. La chiave è composta da tre parti: RAND, SRES e KC, che costituiscono la cosiddetta tripletta di cifratura. Ogni terminale radiomobile possiede una propria chiave di sicurezza KJ e una sua copia è memorizzata nel centro di autenticazione AUC (Autentication Center) presso l'HLR. Quando un VLR prende in carico un terminale radiomobile, riceve da questo il proprio identificativo IMSI. Da questo il VLR stabilisce in quale HLR è depositato l'identificativo dell'utente e si connette inviandogli l'IMSI dell'utente, il proprio identificativo e quello del suo MSC. In tal modo la rete potrà localizzare l'utente in ogni momento. Di conseguenza l'AUC associato al registro HLR, con la chiave KJ calcola diverse triplette e le invia al VLR specifico per essere in esso memorizzate e successivamente utilizzate a ogni impegno della rete da parte del terminale mobile. Quando tutte le triplette saranno utilizzate, AUC ne genererà delle altre e le invierà al VLR. Al momento della connessione il terminale mobile e la BSC con il relativo VLR disponendo di RAND, SRES e KJ ne verificano la coincidenza e tramite opportuni algoritmi generano la chiave KC di criptatura da utilizzare per la comunicazione. Essa è presente sul terminale e nella BSC ma non viene trasmessa. Appena il terminale mobile viene abilitato, il VLR gli assegna un identificativo temporaneo TMSI (Temporary Mobile Subscriber Identification) e glielo invia. A ritroso il VLR riceverà la conferma della regolare ricezione. Il TMSI potrà essere riutilizzato dall'utente finché rimane nell'area di competenza del VLR che glielo ha comunicato.

La sicurezza è quindi data dal fatto che le chiavi KC e KJ non vengono mai trasmesse, mentre i codici TMSI, SRES e RAND vengono trasmessi solo a codifica in atto. Senza la corretta autenticazione non è possibile l'accesso alla rete e senza la conoscenza delle chiavi di codifica non è possibile decifrare i messaggi e le conversazioni tramite l'ascolto del canale radio. Nella figura A è rappresentata la generazione delle varie chiavi e codici presso l'AUC a partire dai dati di utente (KJ e IMSI) presenti nel database HLR. La tripletta costituita da RAND, SRES e KC viene comunicata all'MSC e, di seguito, alla stazione BSC che è in contatto con l'utente (fig. B). Vengono usati tre algoritmi (A3, A5 e A8) per la cifratura sia della fonia sia della trasmissione dati.

Un'ulteriore protezione, che può essere abilitata su decisione del gestore, è costituita dalla variazione continua, durante la conversazione, della frequenza del canale in uso all'utente (frequency hopping).



Alfio Spoldi