# Varne komunikacije

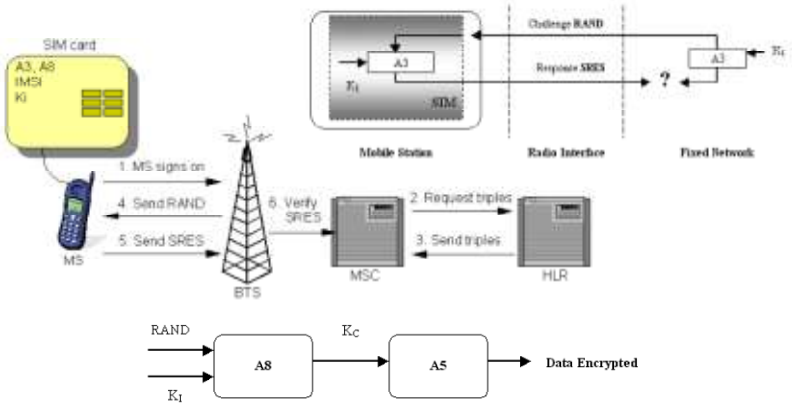
Varnost v mobilnih komunikacijah

## Varnost v mobilnih komunikacijah

- Varnost komunikacij v komercialnih mobilnih omrežjih
  - GSM
- Varnost v profesionalnih mobilnih omrežjih
  - TETRA

# Varnostni mehanizmi v GSM

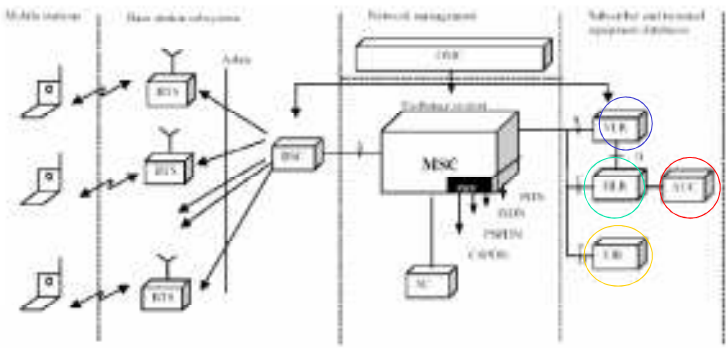
- tajni ključ *Ki* je shranjen na SIM kartici in varovan z dostopovnimi kodami (PIN, PUK) in se ne prenaša po radijskem kanalu
- identiteta uporabnika je v komunikaciji prikrita: TMSI - IMSI
- avtentikacija mobilne postaje s strani omrežja
- komunikacija na radijskem delu zveze je šifrirana





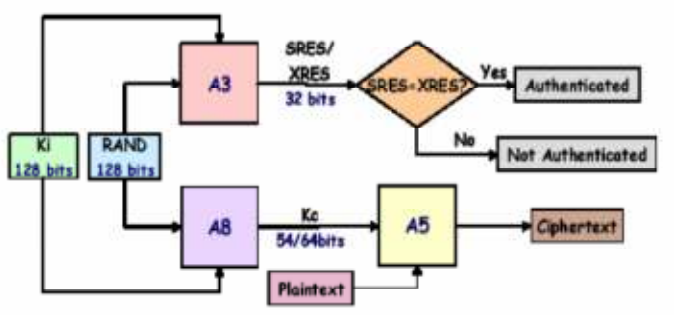

# Podatkovne baze v arhitekturi GSM

- HLR : vsi admin. podatki reg. naročnikov vključno s trenutno lokacijo
- VLR : podatki uporabnikov ki so zunaj domačega omrežja
- EIR : seznami vseh IMEI, ki imajo dovoljen, opazovan ali prepovedan dostop do omrežja
- AUC : baza identifikacijskih podatkov hrani IMSI, TMSI, LMI in tajni šifrirni ključ ***Ki***



## Algoritmi v GSM

- Varnostni mehanizmi so bili razviti v tajnosti in algoritmi A3, A5 in A8 niso bili javno objavljeni (security by obscurity ?)
- Ob vsakem klicu se generira nov šifrirni ključ Kc.
- A5-1 je pretočna šifra, ki uporablja tri LFSR z dolžinami 19,22 in 23 bitov ☺





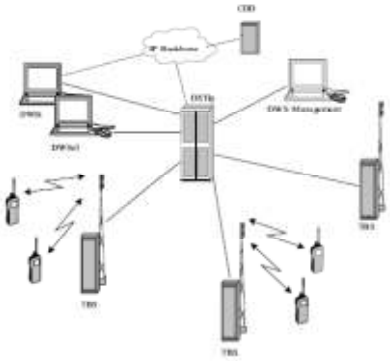

## Možni napadi v GSM

- Kraja ključa ? kloniranje SIM je sicer težavno vendar mogoče s "specialno" opremo.
- Tajnost algoritmov poraja upravičene dvome o varnosti ...
- Napad na pretočni šifrirni algoritem A5, ki se uporablja za šifriranje komunikacij na radijskem linku je dokazano uspešen! Ključ je dolg samo 54 bitov ...
- Ni vzajemne avtentikacije: omrežje preverja identiteto uporabnika, uporabnik pa ne preverja identitete omrežja ! Mogoč je napad na sredini z lažno BS: (TE <-> LBS <-> BS)
- Varovana je le komunikacija po radijskem linku med terminalom in bazno postajo ! Signalizacijsko omrežje operaterja ni zavarovano (SS7). Najbolj nevaren je napad z dostopom do omrežja operaterja (npr. uspeli nepooblaščeni dostop do administrativne baze uporabnikov = HLR ☹ )
- *Za povprečnega uporabnika je GSM dovolj varen, saj naštete pomankljivosti zaenkrat še ne pomenijo resnih možnosti prisluškovanja s strani radovednih sosedov !!*

## Profesionalno radijsko omrežje TETRA

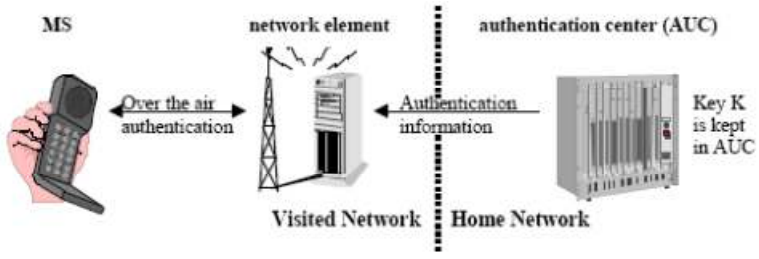
Varnostni mehanizmi:

- zagotavljanje avtentičnosti : vzajemna avtentikacija
  - avtentikacija terminala (uporabnika)
  - avtentikacija omrežja
- zagotavljanje tajnosti : šifriranje komunikacij
  - na radijskem kanalu
  - šifriranje med koncema zveze





## Vzajemna avtentikacija uporabnika in omrežja

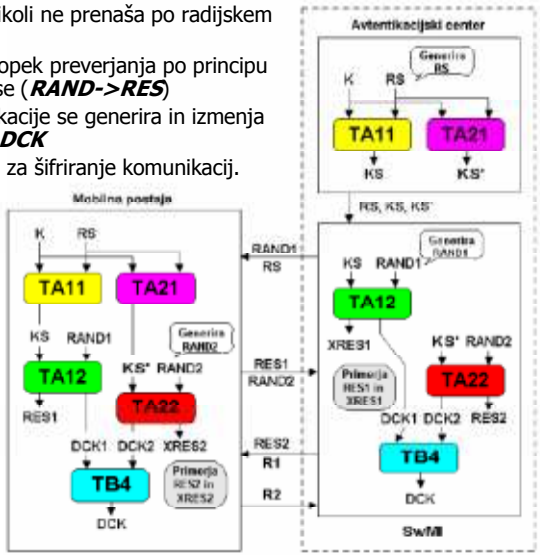



Ali je pravo omrežje ?

Ali je pravi uporabnik ?

## Algoritmi za avtentikacijo

- Tajni ključ ***K*** se nikoli ne prenaša po radijskem kanalu!
- Uporablja se postopek preverjanja po principu challenge-response (***RAND->RES***)
- V procesu avtentikacije se generira in izmenja skupni tajni ključ ***DCK***
- ***DCK*** se uporablja za šifriranje komunikacij.

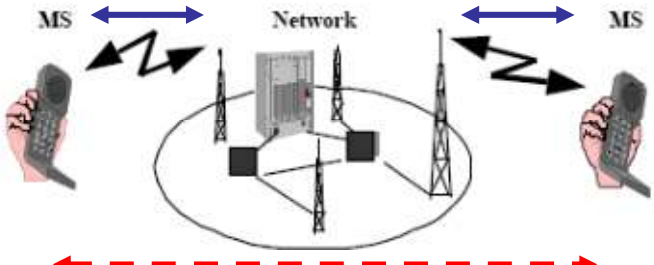





## Varovanje tajnosti komunikacij v TETRA

- Šifriranje radijskega vmesnika AIE je zaščita pred zunanjim napadalcem. Uporablja se pretočne šifrirne algoritme TEA.
- Omrežje TETRA podpira tudi šifriranje med koncema zveze E2E. Za šifriranje med koncema se uporablja blokovne šifrirne algoritme (npr. IDEA, AES ..)
- Razpoložljivost, zanesljivost in varnost so glavne odlike profesionalnih celičnih omrežij !

šifriranje na radijskem kanalu:




šifriranje med koncema