http://alpha.tmit.bme.hu/meresek/ttmer103/

1. Melyek a vizsgált LTE maghálózat főbb komponensei? Röviden jellemezze a hálózatban betöltött szerepüket.

MME - Mobility Management Entity - vezérli az SGW-k működését, a HSSből érkező adatok segítségével.
S-GW - Serving Gateway - A maghálózatban általában több SGW gyűjti össze az eNB-k felhasználói forgalmát, és továbbítja az (általában egy) PGW felé.
P-GW - Packet Data Gateway - A felhasználói adatforgalom ezen keresztül jut ki a nyilvános csomagkapcsolt adathálózatra.

2. Mi a ENB szerepe az LTE rádiós hozzáférési hálózatban?

Evolved Node-B az LTE bázisállomásaként működik, a rádiós hozzáférési hálózat (RAN) része.

3. Mi a mobil hálózatban használt SIM/USIM kártyák szerepe?

Integrált áramkör, amely hardver formában valósítja meg az azonosítási, titkosítási és adattárolási funkciókat.

4. Mi a főbb különbség a SIM és USIM kártyák között?

Az Universal Subscriber Identity Module (USIM) abban különbözik a SIM-től, hogy nagyobb tárhely van a telefonkönyv számára, hosszabb titkos kulcsot tud használni, és segítségével a végberendezés is képes a hálózat viszont-autentikációjára, ami a készüléket védetté teszi a hálózat nevében fellépő adathalászattal szemben.

5. Hol tárolódik a végberendezés és a mobilhálózat közötti jelzés- és adatforgalom integritás-ellenőrzéséhez és titkosításához szükséges K titkos kulcs?

Az USIM kártyán, valamint a HSS-ben.

6. Milyen üzeneteken keresztül zajlik a végberendezés autentikációja? Mely üzenetben mi a releváns autentikációs paraméter?

Az autentikációt a hálózat kezdeményezi.
Ennek során a hálózat generál egy véletlen számot (RAND), és azt az előfizet USIM kártyájához tartozó K kulcs felhasználásával titkosítja. Ezt követően a RAND értékét és a titkosított véletlen bitsorozat egy részét (az AUTN mezőben) elküldi a végberendezésben az Authentication request üzenet részeként.

A végberendezés a kapott RAND számot szintén titkosítja az USIM kártyán található K kulcs felhasználásával. Ezt követően ellenőrzi, hogy az AUTN paraméterben kapott érték megegyezik-e az általa kapott titkosított bitsorozat megfelelő részével. Ha az AUTN értéke különbözik, akkor az UE megszakítja az Attach procedúrát.
Ha a két érték megegyezik, akkor az UE meggyőződött róla, hogy a hálózat valóban ismeri azt a K kulcsot, amely az USIM kártyán is szerepel. Ekkor az Authentication response üzenet RES mezőjében visszaküldi a titkosított bitsorozat egy másik szakaszát. A hálózat a kapott RES értéket összeveti az általa titkosított érték megfelelő szakaszával. Ha az érték különbözik, akkor a hálózat megszakítja az Attach eljárást. Ha megegyezik, akkor a hálózat folytatja az Authentication and key agreement (AKA) műveletet a Security Mode procedúrával.

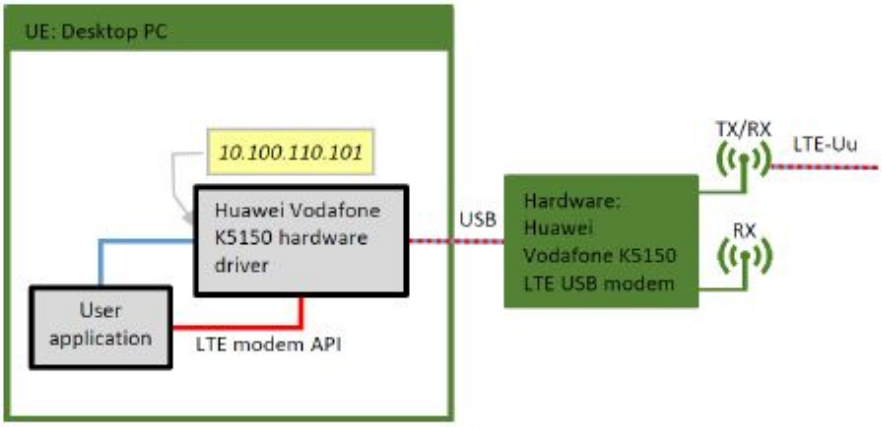
7. Mi az IMSI, IMEISV és MSISDN rövidítések feloldása? Mire valók ezek az azonosítók?

IMSI - International Mobile Subscriber Identity - Egyedi előfizetői azonosító, meghatározza az országot és a hálózatot, ahová az előfizető tartozik.
IMEISV - International Mobile Equipment Identity software version - 16 jegyű egyedi UE azonosító, szoftver verzió információval kiegészítve
MSISDN - Mobile Station International Subscriber Directory Number - a hívószám

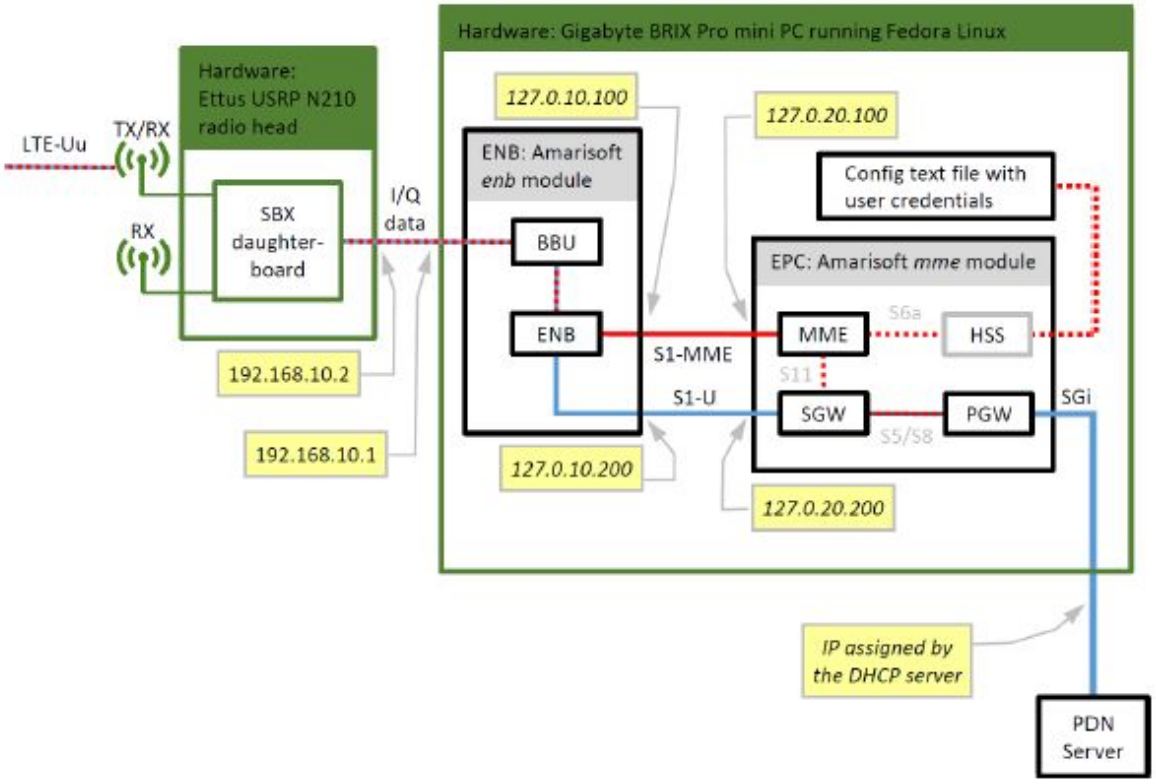
8. Mi a GTP-U protokoll szerepe?

A felhasználói adatforgalmat a GPRS Tunneling Protocol (GTP-U) szállítja.

9. Rajzolja fel a mérési elrendezés blokkvázlatát.



1.4. ábra. A mérési elrendezés a végberendezés oldalán



1.5. ábra. A mérési elrendezés az LTE maghálózat oldalán