for MIDTERM

3GPP Process

Stage-1 — defines service requirements

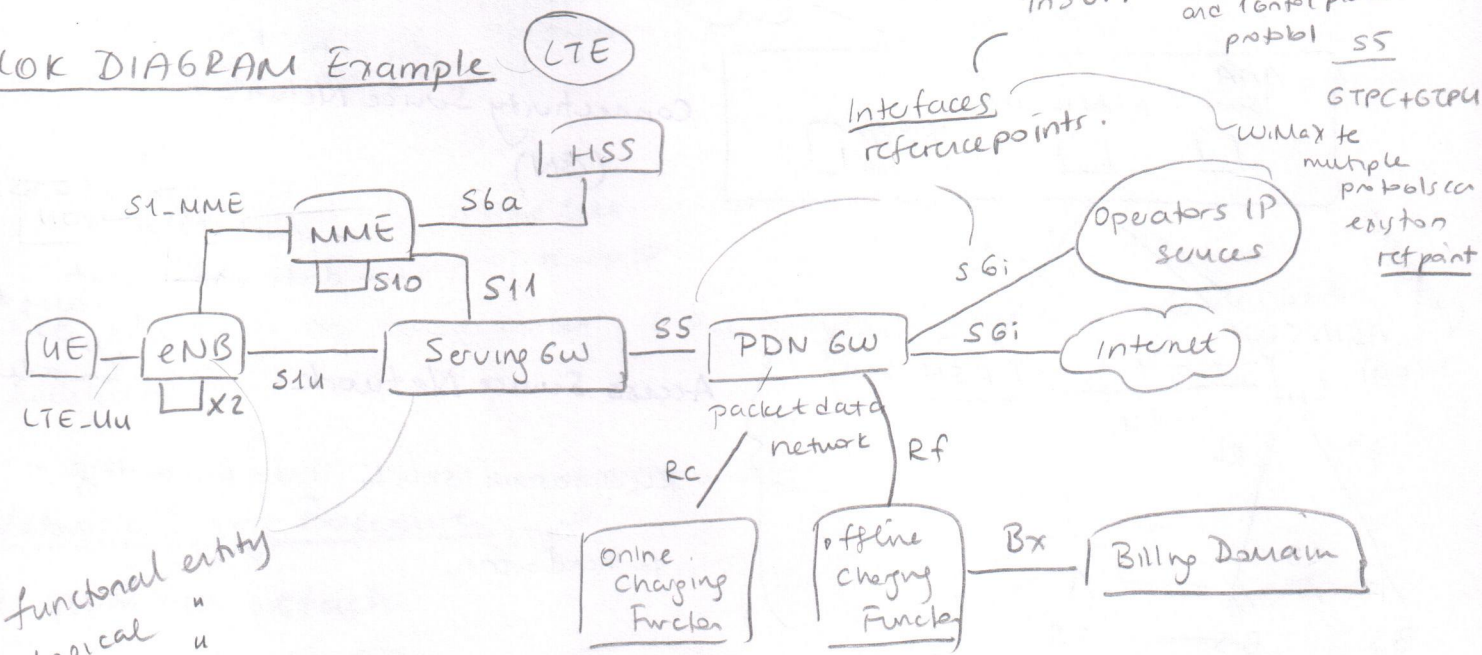
Stage 2 — Defines architecture, network elements & high level flows (network architecture, flow diagrams); network reference model + functional decomposition

Stage-3 — defines protocols (state mlc, messages..) → Conformance Testing Specification

Low level of detail → High

timeline →

BLOK DIAGRAM Example (LTE)



in 3GPP max 1 user plane and 1 control plane protocol S5

Interfaces reference points.

GTPC+GTPU

WiMAX te multiple protocols can exist on ref point

IEEE 802.16 include PHY+MAC (Terminal ↔ BS)

WiMAX standard = E -- end to end

Lab Research → Industry interest → SDO standard defined org. → technology spec → product spec → product → develop → Market use

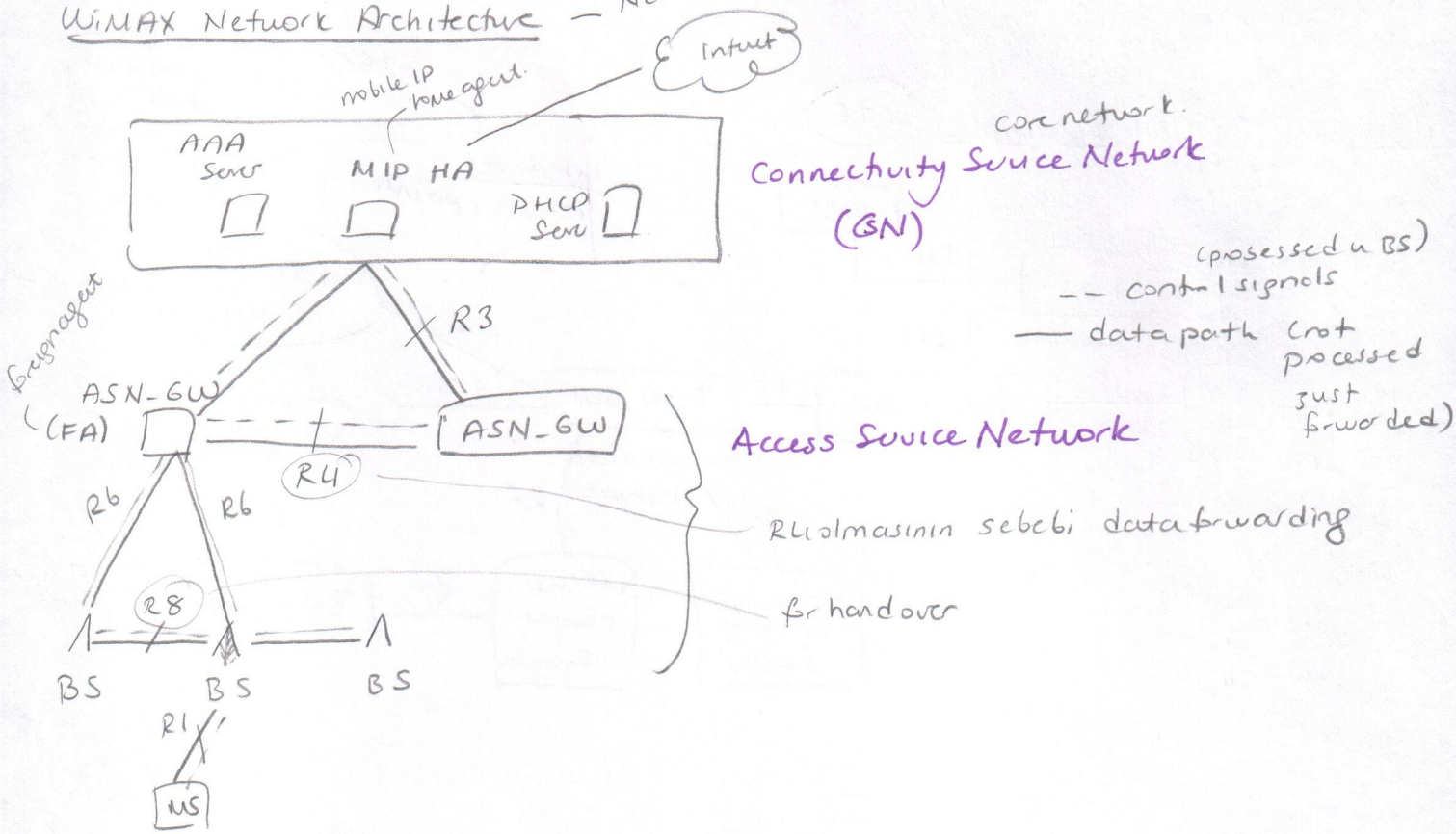
ex 5/6

WiMAX is a IEEE 802.16 d/e/m (not mobile / real 4G!) standard based technology enabling the delivery of last mile mobile wireless access at broadband speeds.

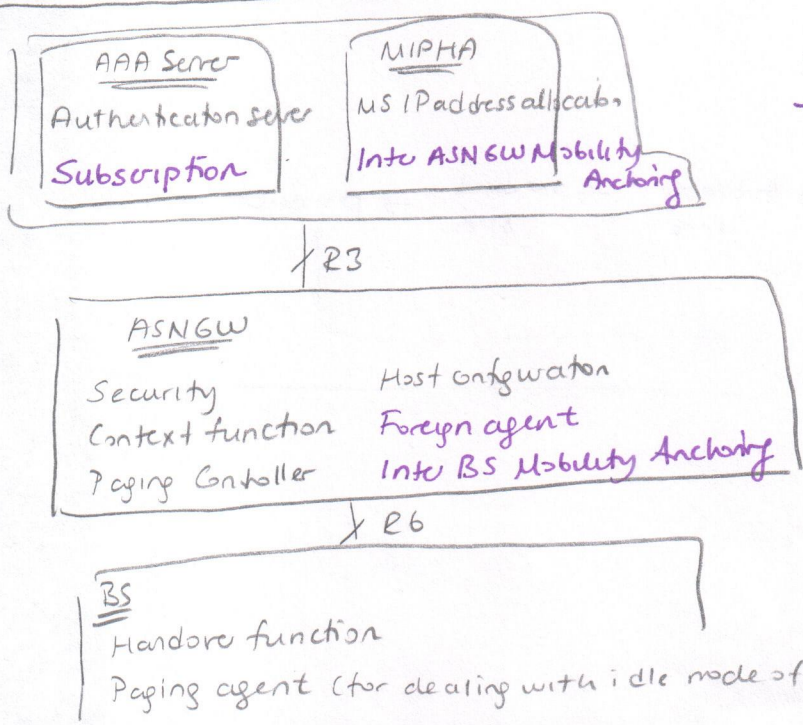
WiMAX Forum certification
Network specifications
Air interface profile specs
MAC/PHY standards in IEEE

Profile : narrowing down features.
profiles are defined by WiMAX Forum.

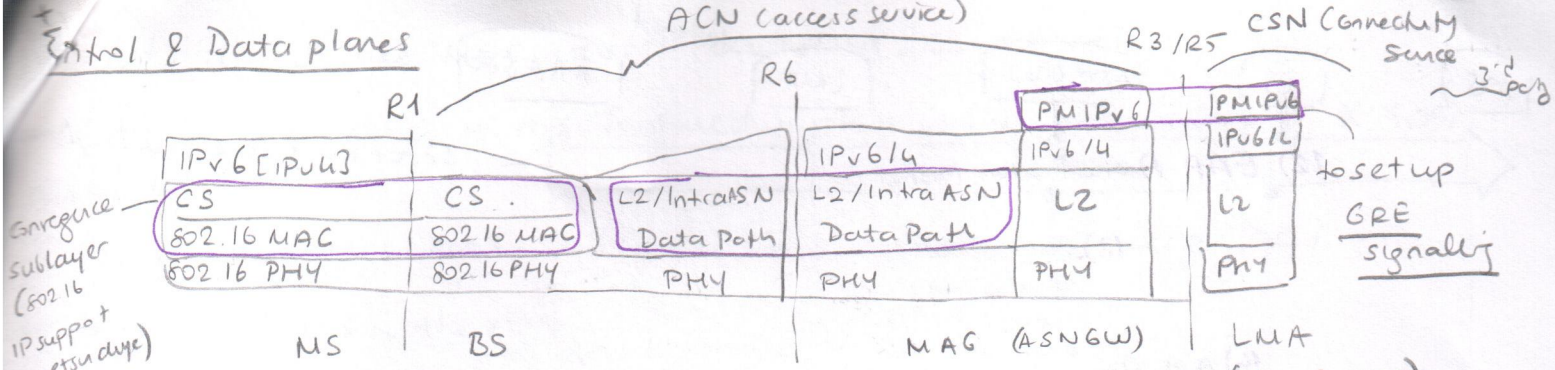
WiMAX Network Architecture — Network Reference Model

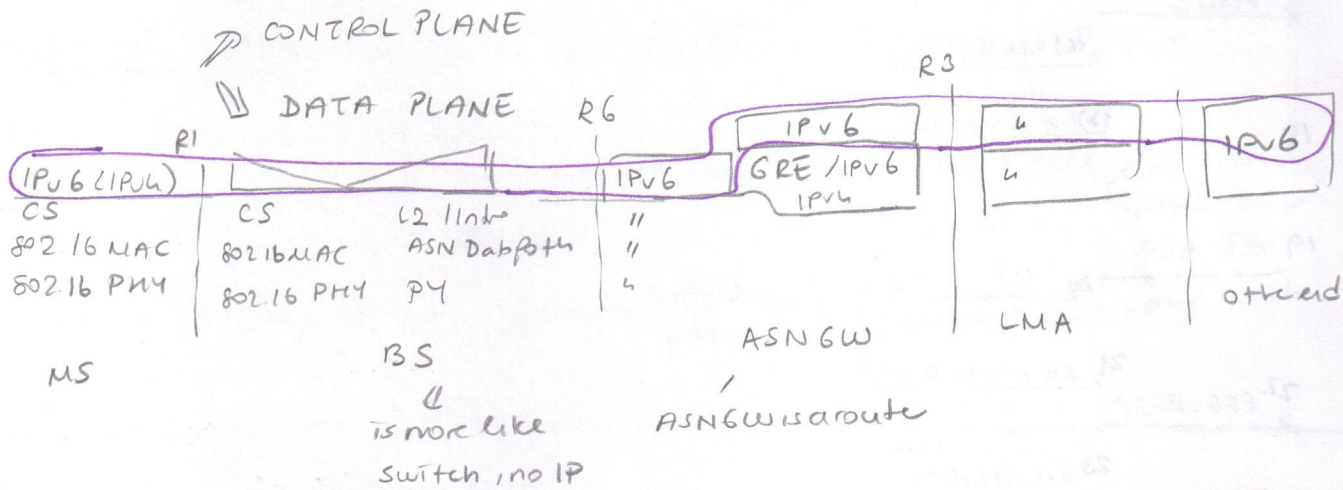


Functional Decomposition



Control & Data planes



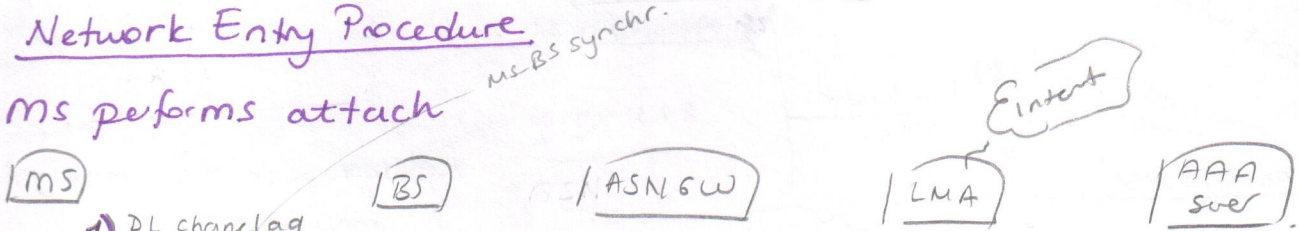


GRE: General Routing Encapsulation (IPv4'te aynı IP adresli host olabilir, GRE bunu halleder!)

Network Entry Procedure

MS-BS synchr.

MS performs attach



1) DL channel q
(MS listens BS's anchors)

2) Ranging and
PHY adj

3) SBC-REQ
Subscriber station basic capability exch

4) MS Pre attachment
Req. (MSID)
kaydı tekrar mi mesela

5) MS Pre attachment
Resp.

6) SBC-RESP

7) MS Pre attachment
ACK

8) Auth Relay EAP
Transfer

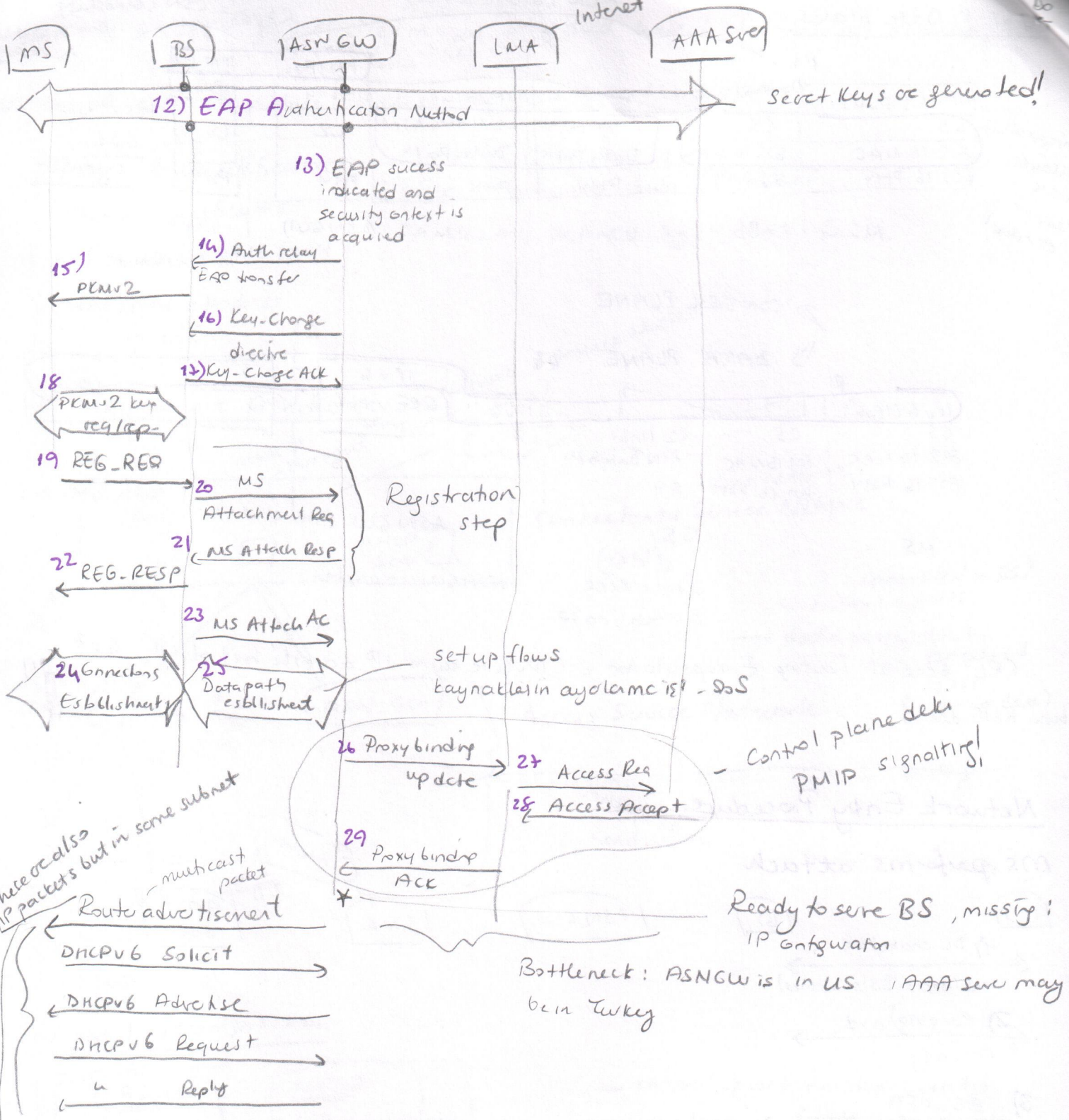
9) PKMv2-RSP/EAP
Transfer

10) PKMv2 REQ/EAP
Transfer

11) Auth-Relay EAP
Transfer

authentication initialization

authentication process.



—o— network entry bitti lifetime-i var

(lifetime > 690 a gelince tekor authorized olat, suclece authorizeten mesaj alıyeteli)

IPv6 da
link local IP address ile (DHCP olmadan alınan adres)
IPv6'te 0.0.0.0 gibi kullanılmayan bir adresle haberleşir.

WiMAX Identifiers

Device Identifier: (3GPP de = IMEI fakat IMEI kopyalanabilir, WiMAX te MAC + sertifika var)

- 6bit, Ethernet like MAC address 00_1A_C5_C2_FE_9D

- Every WiMAX device is manifactured with a unique MA Caddress + X.509 cathfcate.

  - MAC addresses can be cryptographically authenticated using PKI

= Identifier of MS in the ASN = access service

Subscriber Identifier

- NAI (RFC 4282) (network address identifier) Bob@myISP.com

- identifier of the subscriber in CSN
  core network: connectivity service

∝ a subscriber can use multiple devices.

Exception device identifier can also substitute for subscriber. 1↦1 mapping with Bob and 00_1A--

---

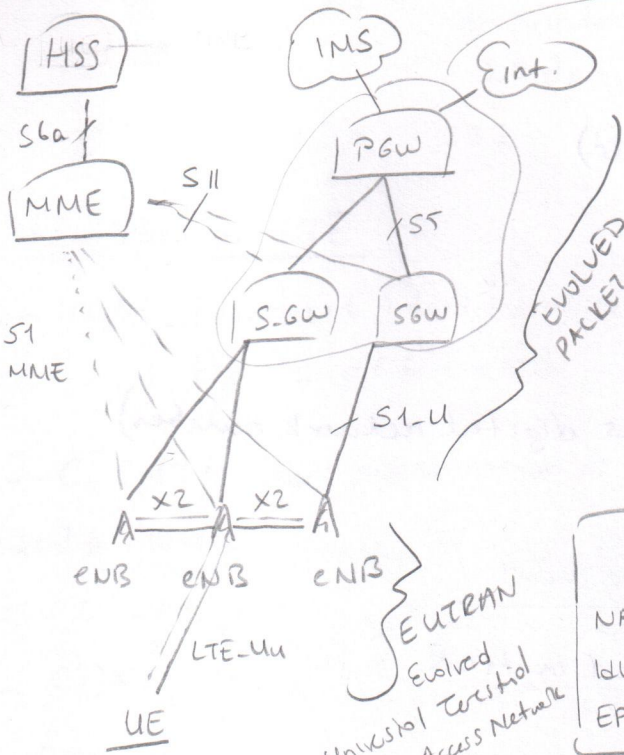
Why standards - compatibility
  - multiple vendors for equipment (cost ↓)
  - sharing system engineering

How → organization specifies standards.

WHAT → systems engineering process

LTE Architecture Block Diagram (dana once ciz dik)

LTE Network Architecture



neden boyle yapmis olabilir? butun eNB ler bir SGW de degil. low latency handoff (anchor point BS e yakin) olursa low latency hand

HSS
Authentication
Location Man.
Subscription

PGW
UE, IP address alloc.
Inter SGW Mobility Anchoring

S6a

S5

MME
NAS security
Idle state mobility hand.
EPS Bearer Cntrl

S-GW
Inter eNB mobility Anchoring

S1 MME

S1-U

eNB
RB control
Radio Admission Cntrl
Schedular
Intel Cell RRM
Connection Mobility Mgmt
eNB Measurement OAM
Radio Bearer Transmission
L1/L2/L3

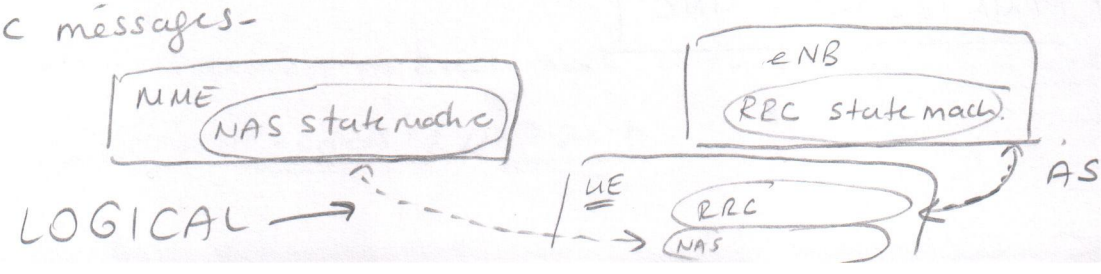
— Control plane functional entity
— User plane " "

⇒ All radio related functions are pushed down to the eNB
no centralized radio resource management entity like RNC

⇒ In core network, control plane & user plane separated.

MME: control plane entity
SGW, PGW: user plane "
} allow independent scaling of cntrl & user plane

AS → UE performs cntrl signalling with eNB via Radio Resource Control RRC protocol
NAS → " " " " " " MME via NAS (NAS messages are carried inside RRC messages-



Home PLMN — roaming require – from VPLMN, identify HPLMN of subscr

Visited PLMN — – authenticate subscribe from VPLMN

– sharing of revenue between H/V PLMN

2 Important Identifiers

1) IMSI (International mobile subscriber identifier)

Embedded in SIM card

Stored in subscriber data of HLR (HSS)

used to index UE's info in most network nodes

2) MSISDN (mobile station integrated services digital network number)

your phone number

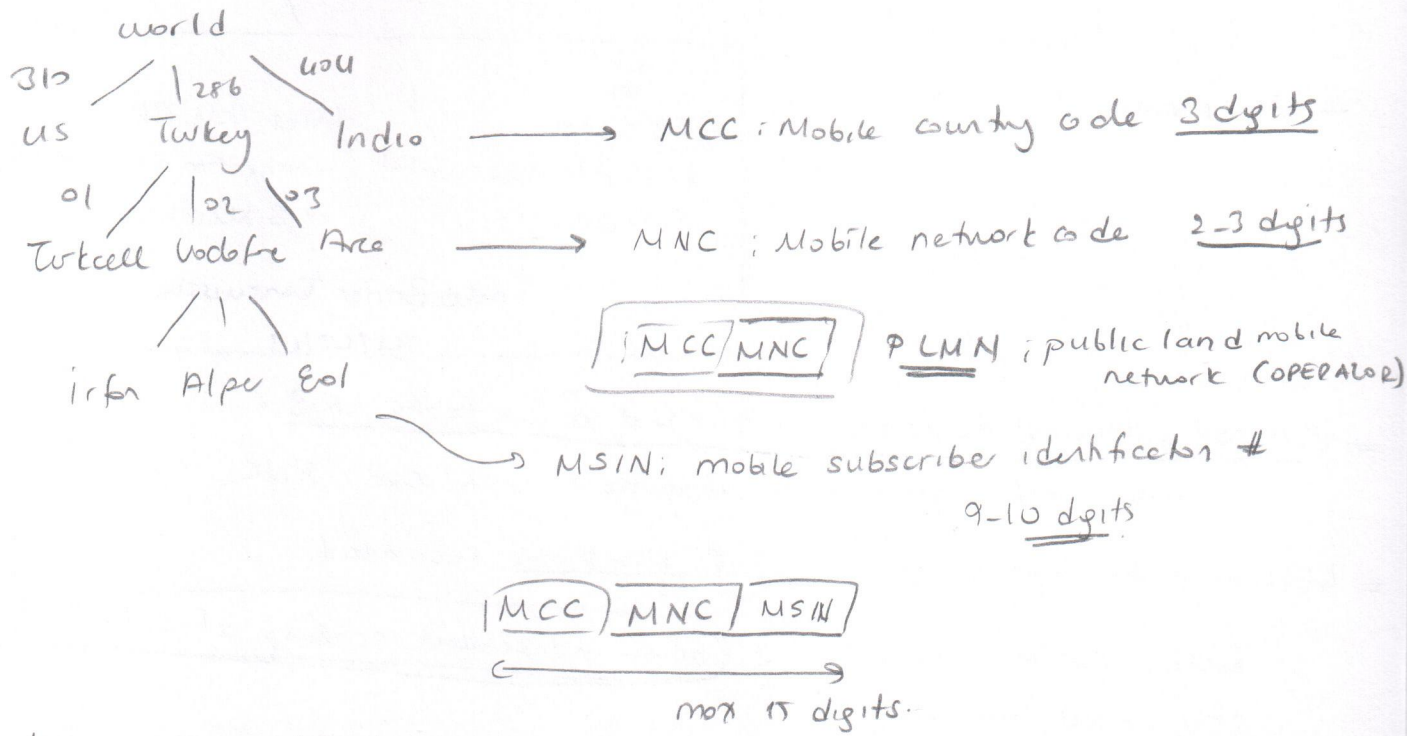
used to identify a subscriber when making a call / SMS -.

mapping between IMSI & MSISDN is stored in HCR

(MSISDN not required to be stored in SIM)

IMSI is core identifier entry w.r.

IMSI structure



– an operator may be identified by more than one PLMN ID.

PLMN ID = MCC + MNC

MSISDN

| CC | NDC | SN |

country code 1-3 digits | national destination code (identify operator) 2-3 digits | subscribe number 9-10 digits

+90 533 123 4567

Identities in LTE

- IMSI : permanent identity of UE in SIM (MCC + MNC + MSIN) home PLMN, max 15 digit
  kept secret from eNB

- C-RNTI (cell radio network temporary identity) 16 bit
  is created by eNB and only used to identify UE with the scope of eNB, provided to UE during random access process and setup of RRC connection.

- GUTI (globally unique temporary identity)
  - created by MME for UE used between MME & UE, instead of IMSI
  - GUTI may be seen by eNB if NAS message is sent un-encrypted (eg when UE has moved to new area and needs to be served by new MME)
  - 56 bits + MCC + MNC

Objective of network attach (network entry) procedure

Goal: obtain IP address!

during attach process
- UE is authenticated & authorized to send/rec data
- Data path created : UE ↔ ENB ↔ S-GW ↔ PGW
- UE context created in the network
- UE provides IP address.

GTP-C tunnel
GTP-U tunnel - encapsulate & send user plane traffic between them.

2 protocols for S5 S-GW ↔ P-GW : GTP
PMIP

GTP tunnels are identified in each node with unique Tunnel End Point Identifier TEID, IP address & UDP port

→

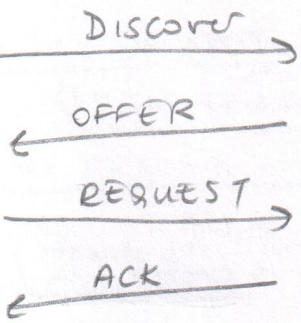
In LTE, there are 2 protocols for S5 (SGW ↔ PGW)

GTP & PMIP

In wimax several protocols in ASN and ASN → CSN

Homework 2

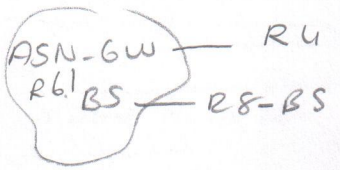
- DHCP



can come from multiple DHCP servers

goes to 1 DHCP server.

-



R6 goes away
R8 also disappears!

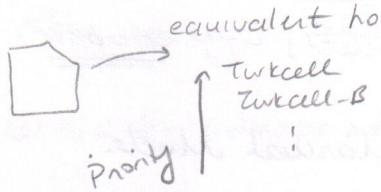
colocated ie

3GPP Network Selection and RAT

- network selection = choose operator select PLMN
- RAT selection = choose radio access (GSM, UMTS, LTE...)
- in all 3GPP techs, network advertises in broadcast channel, the PLMN of operator (if, network is not shared, only 1 PLMN identity)
- in LTE: PLMN identity(ies) are contained in SIB-1 blok

Concept of Equivalent PLMNs

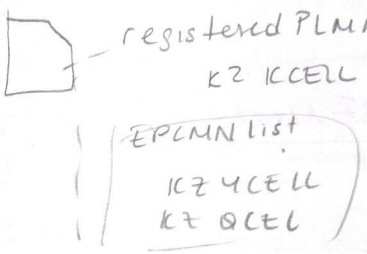
HPLMN, eHPLMN



Registred PLMN : RPLMN (user is connected to)

RPLMN, ePLMN

= EPLMN list is always provided by VPLMN when UE is registered.

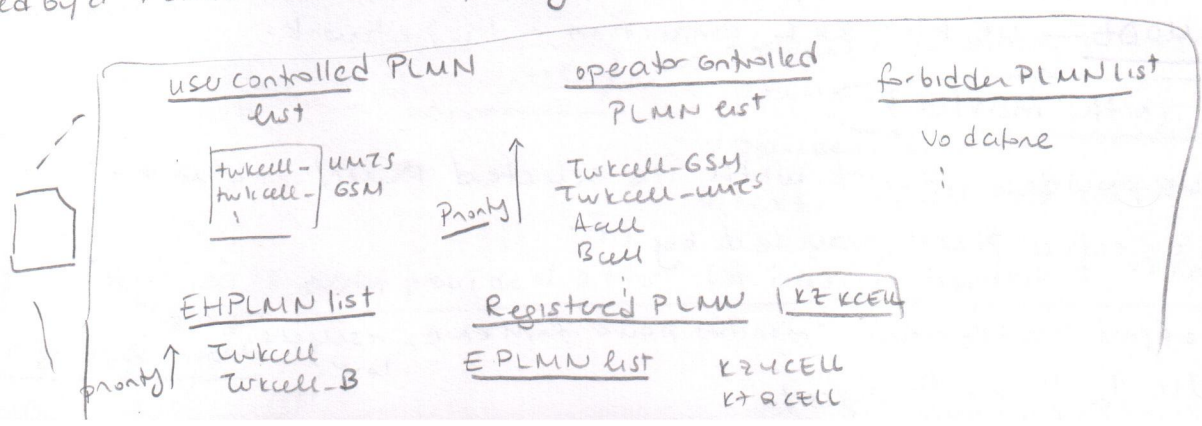


2 modes of PLMN selection: manual / automatic

user can set preference of which selection mode to be used on power on.

for PLMN selection 2 prioritized lists → user controlled PLMN
↘ operator " "

each element in list: PLMN + optional Access tech identifier. (all access techs provided by a PLMN has equal priority)



PLMN Selection Power On, Automatic Mode

- network advetises list of PLMNs in bcast message in each frequency band.
- UE scans all access tech and all freq bands and selects a network corresponding to the last registered PLMN
  UE is allowed to instead register in HPLMN or EHPLMN if one is available.
- if no success
  UE selects EPLMN
  if no EPLMN, UE selects highest priority EHPLMN (and corresponding RAT)
  if no EHPLMN, UE selects PLMN from user list in priority order
  if no user PLMN then selects a n operator

PLMN Selection at Power On, Manual Mode

again last registered PLMN

exception! if neither RPLMN or EPLMN are available, but EHPLMN are available, UE may register highest priority EHPLMN

If no success: user is offered a list of PLMNs in the same order as previous.

EPLMN, EHPLMN, user PLMN, operator PLMN, other techs with sufficient SS.

UE selects in IDLE mode

PLMN Selection, cell selection, cell reselection in IDLE Mode

UE is not actively communicating with network no DRB, SRB

Periodic PLMN selection in VPLMN

automatic mode: UE shall look for higher priority PLMN & check also other RATs (AT regularly depending on SIM)

* UE can change PLMN only within same country (same MCC) & new RPLMN's MCC = RPLMN's MCC

- periodicity of reselection 6 min. to 8 hours! (may be stored in SIM)

Cell selection & PLMN selection -- ?

In ACTIVE MODE — UE has RRC connection to the network.

The network is the master!

At attach, UE provides network with its selected PLMN, network shall register UE to selected PLMN provided by UE.

UE performs cell selection (monitors power from eNB, reselects if low) periodically listens for pages!

handover network can only change UE's PLMN to one of EPLMNS

PLMN is only changed if UE's RPLMN is not available in target cell in the RAT that network wants to handover UE to

cell selection network tells UE to measure cells in frequencies and RATs for candidate target cell, based on measurements, eNB decides.

PLMN selection in Network Sharing Scenario

multiple operators share radio access network.

mobile operator core network — MOCN

gateway core network — GWCN sharing ability.

- PLMN ids of both broadcasted for both operators
- eNB needs to figure out which MME to direct UE's initial message (attach request) (MME provides UE the GUTI)

UE can provide selected PLMN ID info to eNB.

Selection of non 3GPP technologies

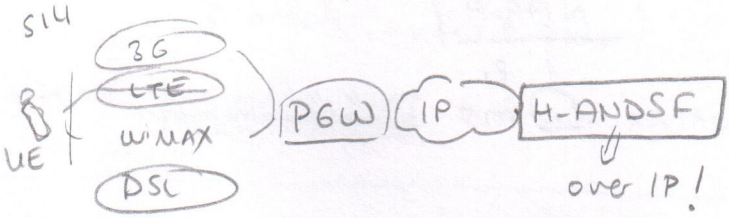
3GPP does not provide info about other techs like WiMAX

UE can do "blind periodic search"

Access Network Discovery & Selection Function provides UE info about

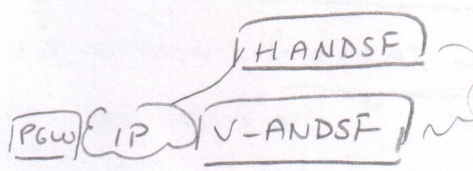
ANDSF

- different access techs in vicinity
- policies about which traffic UE can place on.



over IP! (like a server telling you can connect to WiFi, WiMax, etc.

in roaming

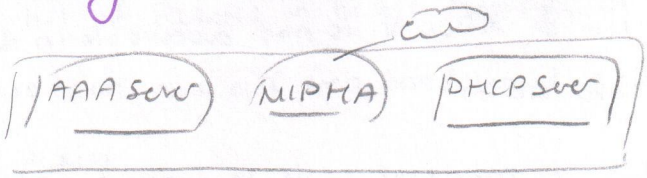


- provides info about access networks in VPLMN only
- provides info about access nws of all PLMNs, HPLMN has associations with.

* the information is only provided after UE has IP address & is in connected mode.

Network Discovery / selection / reselection in WiMAX

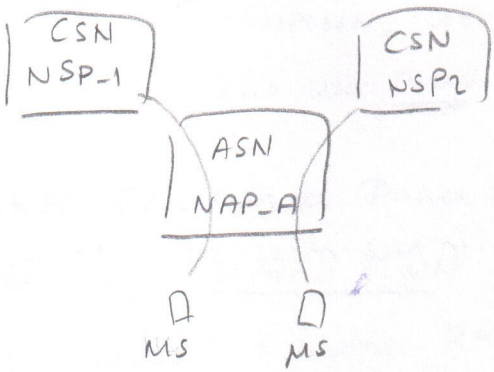
non roaming



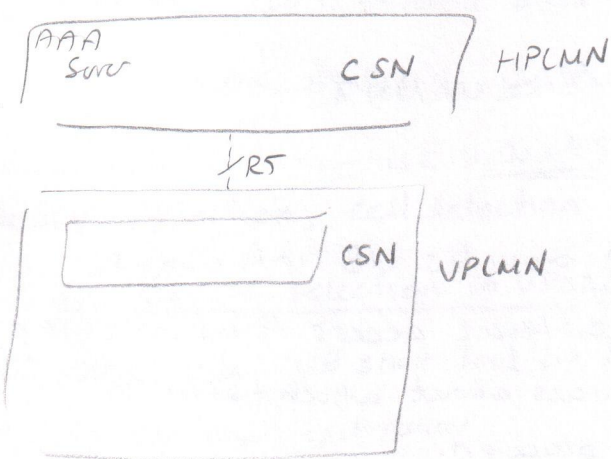
Network Service Provider — NSP

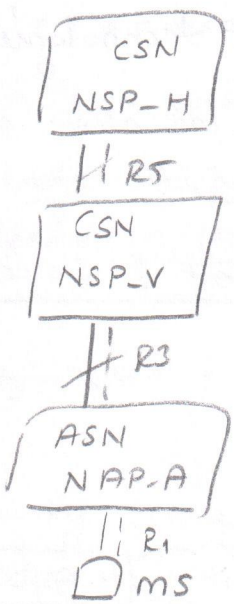
ASN — Network Access Provider — NAP

non-roaming, shared ASN

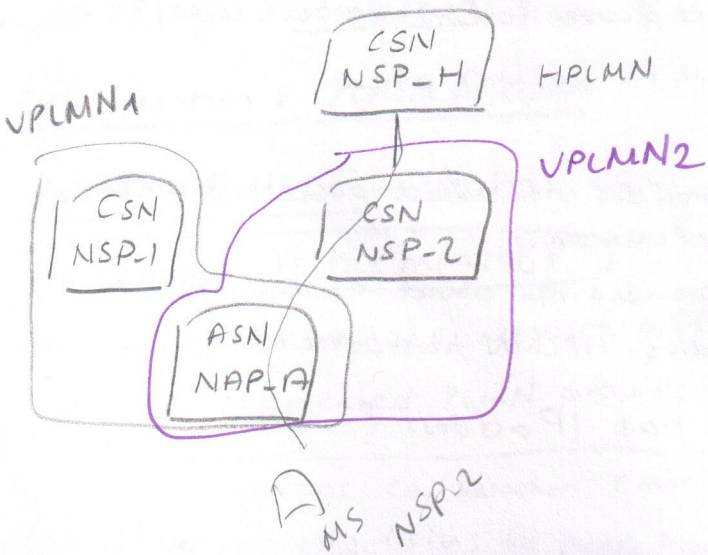


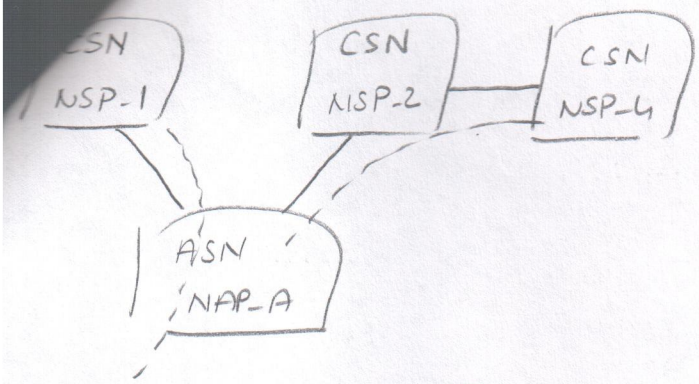
roaming, local breakout traffic





roaming shared ASN





MS MS : met@ns-4.com

osman@NSP-1.com

Summary

- How to advertise supported operators of network?

  Link Layer – 3GPP: using PLMN IDs in System Broadcast Info.
  – WiMAX: NAP in DL MAP info in bcast channel (NSP_IDs are also bcasted)

- What is home domain (or realm) of user

  Part of UE's provided entity

  – 3GPP: IMSI has MCC, MNC (123, 89) home realm: mnc089.mcc123.pub.3gppnetwork.org

  – WiMAX: UE's provided normal/root NAI user_name@nsp-1.com

- How to route UE's authentication request to home AAA / HSS?

  – 3GPP/WiMAX: based on realm part of NAI

  RADIUS: static IP mapping of realms to IP addresses held in RADIUS proxies

  Diameter: use of DNS & Service loc. protocol.

  – use of decorated NAI to force a particular path home ! user@ visited-realm

---

How does UE determine which RATs and frequencies to scan for?

3GPP: SIM card contains freq/RATs atleast for HPLMN and EHPLMN

in VPLMN, UE scans all " based on its capabilities.

How does UE select particular access network and RAT

3GPP: based on prioritized, user/operator defined PLMN lists stored in SIM

WiMAX: " " " " " " NSP lists stored in device

overall procedure

- In wimax network, a full network discovery & selection has 4 steps

1) wimax NAP Discovery
2) NSP Access "
3) NSP Enumeration & Selection
4) ASN Attachment based on NSP selection

- 2 modes : automatic / manual.

1) NAP Discovery

- MS (SS) detects available NAPs by scanning & decoding DL-MAP of ASN on detected channel

NAP identifier = Operator ID + BSID
(24bit)

2) NSP Access Discovery

- MS should associate with each NAP for discovering supported NSPs.
- ASN transmits the NSP ID list message every T sec.
- MS has configuration info mapping NAP + NSP military mapping.

3) NAS Enumeration & Selection

manual / automatic

a) home NSP
b) NSPs in user controlled NSP identifier list in MS
c) NSPs " operator " " " " "
d) any other NSP in random order

signal quality shall not be used as parameter for NSP selection.

4) ASN attachment based on A NSP selection

MS indicates his NSP selection by attaching to a ASN associated with selected NSP providing his identity and home NSP domain info of NAI

- ASN uses NAI to determine the next AAA hop to where MS's AAA packets should be routed!

NAI example _ user_name@NSP-1.com

decorated = NSP-1 ! user_name@NSP-2.com
(home realm) (visited realm)

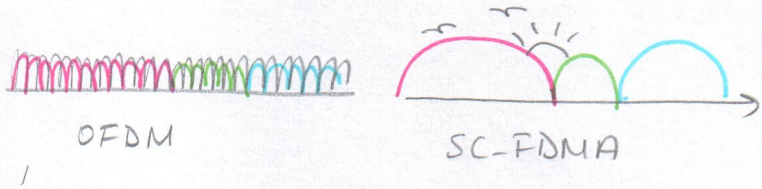
Uplink Direction (Single carrier FDMA) SCFDMA

OFDM in LTE

harmonic series, $f_0, 2f, 3f, \ldots$

base frequency in LTE ⇒ 15 kHz

(66.67 μsec)



has good performance for broadband communication due to inherent robustness to radio-channel time dispersion but also suffers from

- high peak to peak average power ratio → power amplifier inefficiency
- sensitivity to frequency errors
- robustness to time dispersion can also be achieved with single carrier transmission together with receive side frequency-domain equalization

downlink

- power amplifier inefficiency less critic at base station side } OFDM
- avoid excessive user-terminal receive complexity

uplink

- high power amplifier complexity is critical in terms of terminal cost, power consumption and uplink coverage } single carrier
- receiver complexity less critical at BS side

36 LTE Uplink radio access

Single carrier ⇒ improved power amplifier efficiency (reduced terminal power cons. and cost and improved coverage)

FDMA → Intracell orthogonality in time AND frequency domain

(improved uplink coverage & capacity)

Downlink Frame Structure

| #0 | #1 | ---- | #18 | #19 |

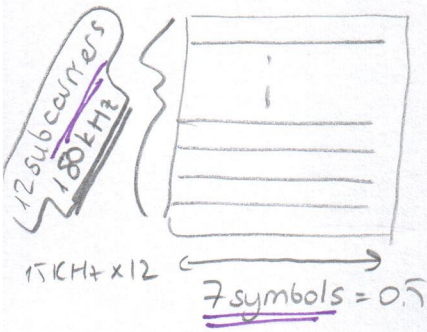
⟵ One radio frame (10ms) ⟶

⟷ 1ms subframe (minimum scheduling unit)

⟷ Slot: 0.5ms

10 subframes = radio frame.

in freq domain, downlink subcarriers are grouped into resource block:



How Does UE Figure out the DL frame-timings & read broadcast info of a cell?

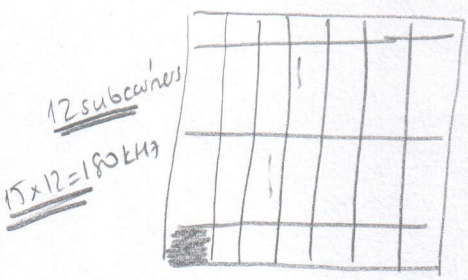
Primary Synch. Signal — PSS
Seonday Synch Signal — SSS
} well-known signal patterns in well known loc of DL channel.

2 PSSs in 10ms radio frame
2 SSSs " " "

What does a UE measure to determine if, t can camp on a cell?

RSRP: reference signal receive power.

4 resource elements per resource block that are dedicated to Reference Signal



resource blk (6, 1)
(12, 1)
(3, 5)
(9, 5)

Power Management & Location Management

- high power mode (active mode)
  "connected"

  network controls UE's movement through handoff

  Location of UE is known to the network at granularity of a cell.

  Radio is ON state

  UE is constantly communicating with the network.

- low power mode (idle mode) – no NAS signaling (UE ↔ MME)

  – network does not control UE's movement, UE autonomously selects new cell as it moves.

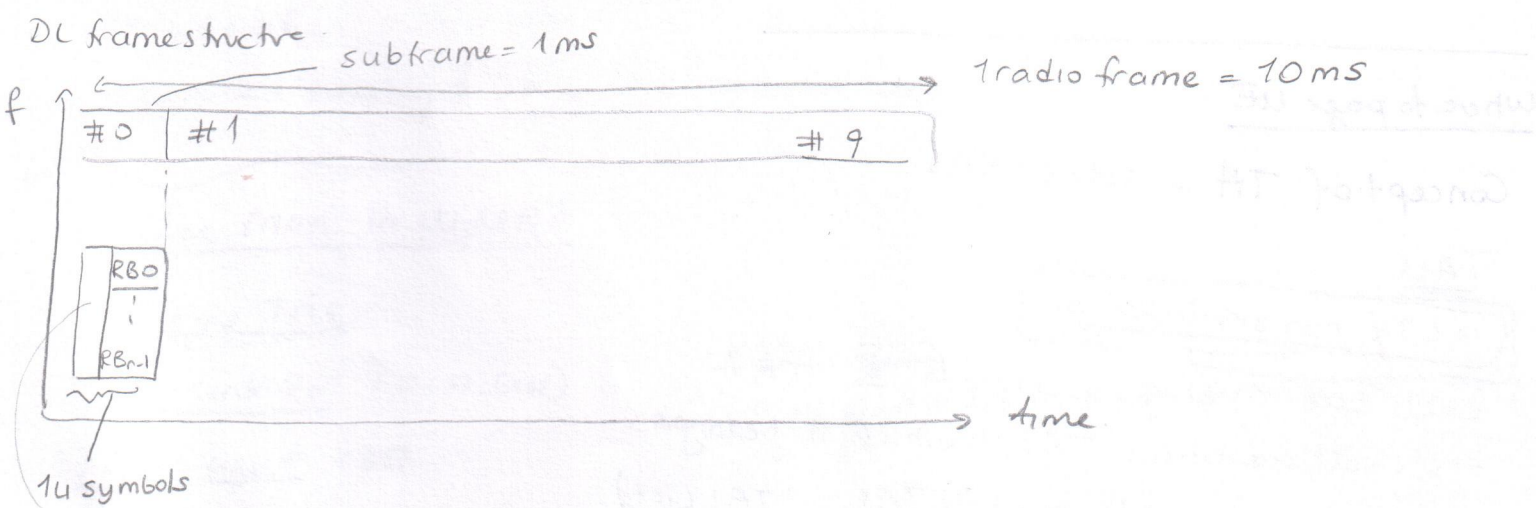
  - network knows loc. of UE at granularity of a location area (3GPP, WiMAX'te TA)
  - UE's radio is in low power state
  - UE's transmitter is OFF
  - UE listens periodically to control channel, if UE enters new LA, based on heasing info from BS, UE informs network of new LA it entes.

Location Management : set of procedures used by network and UE to determine UE's loc.
at granularity of a cell when a new call / packet arrives at network for UE.

Loc. Man. in LTE

After UE stops transmitting / receiving data/signal for a period of time called inactivity period, network moves UE's state to idle

When does UE switch on its receiver?



DL control signalling is first 1-3 symbols others (11-13) are used for data

dedicated control channels.

Page message for UE will be contained in Common Control Channel

may only be present in the subframe 0, 4, 5, 9

UE's paging DRX cycle period Tue is one of following (SIB den yada dedicated sunuldu)

{32, 64, 128, 256} frames (each frame is 10ms)

0.32, 0.64, 1.28, 2.56 sec.

paging occasion PO : subframe that contains paging message {0, 4, 5, 9}

paging frame PF : radio frame that 4 1 or more PO

SFN (system frame number)

which frame and which subframe?

$$SFN_T = \frac{T}{N} \cdot (UE\,id \bmod N)$$

T: min (Tc, Tue)

N: # of paging frames within paging cycle of UE = min (T, # of paging subframes per frame × T)

$$i\_s = \left\lfloor \frac{UE\,id}{N} \right\rfloor \bmod Ns$$

Ns: max (1, Nf) — # of 4 per frame. 4, 2, 1, 1/2, 1/4, 1/16, 1/32

Ns	PO is=0	is=1	is=2	is=3
1	9	—	—	—
2	4	9	—	—
4	0	4	5	9

Where to page UE

Concept of TA - set of eNBs

TAU

in LTE non overlapping

each cell in eNB can belong to 1 TAI

each cell advertises TAI to which it belongs.

UE can be admitted to multiple TAs. (TAI List)

UE is idle and MME needs to locate UE, MME pages UE in the sets of eNB which belong to the TAI that the UE is registered into.

Large TA — less frequent UE need to signal to network however larger # of eNBs that UE will need to be paged in

TAI = MCC + MNC + TAC
(tracking area code 16bit)

finding context of UE in idle mode

MME Service Area {TA-1, TA-2, ...}

UE, in idle mode informs MME about its current loc. by Tracking Area Update

Routing to get to the old MME : identity used for this routing is GUTI

cell selection reselection in idle mode

Network does not control UE's movement, UE autonomously selects new cells as it moves. network knows loc of UE to the granularity of LA

--

what does UE measure to determine it can camp on cell?

Reference Signal Receive Power. RSRP

" " " Quality RSRQ = $\frac{RSRP}{(\frac{RSSI}{N})}$

which frequencies & RAT to scan

up to 8 priorities can be provided by

- broadcast in system info
- signalled directly to UE in RRC connection release.

Loc. man. in WiMAX

Overlapping TAs

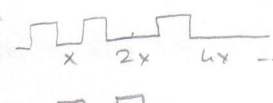
Paging controller (ASN-GW)

Paging agent (BS)

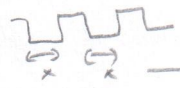
Paging group TA

Location register (ASN GW)

a distributed DB with each instance corresponding to PC

3 power saving classes Power Save Class 1 

min to max exponentially increase

Power Save Class 2  — fixed length sleep window

Power Save Class 3 1 time sleep!

(HW-4 again)

overlapping TAs → increases paging cost
→ decreases loc update cost
↳ increases # of TAs to cover a specific area

Powe Management

- connect to network when necessary
- interval for listenning network should be large.
- 2 states → idle
  → active

Loc. Management

- schemes: what should be the shape of TAs?

  overlapping / non overlapping

  static / dynamic

---

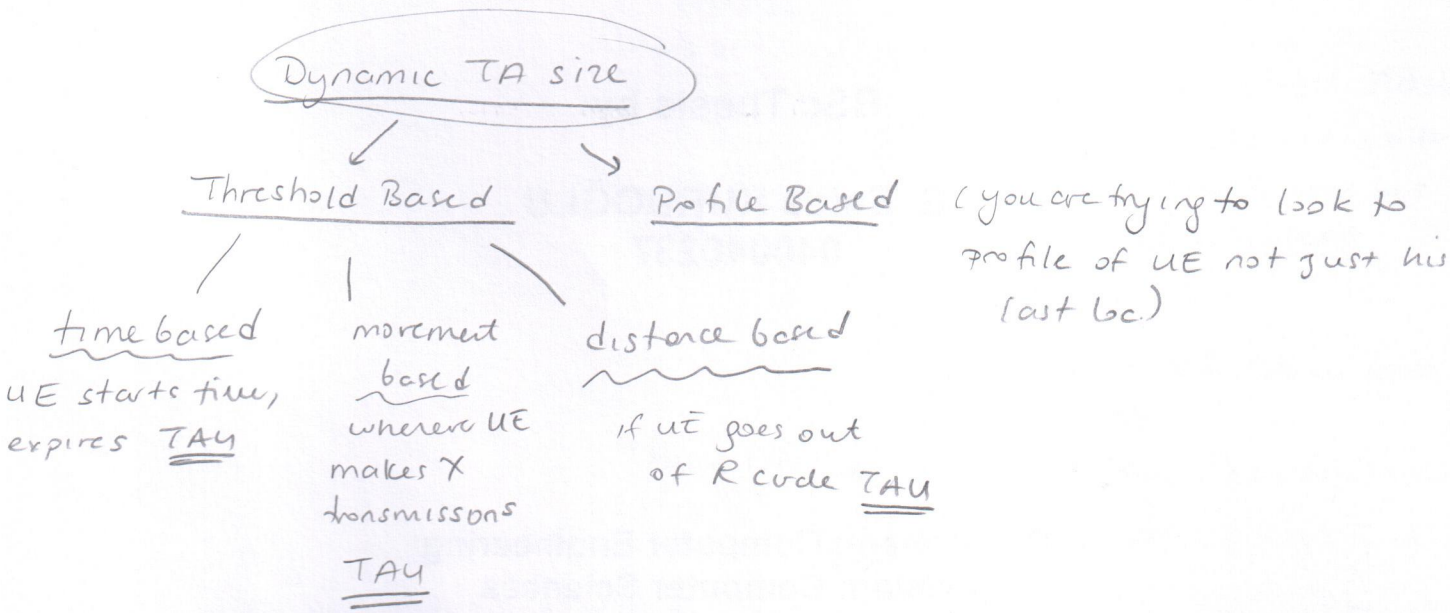
paging cost : cost from network side, # of cells where UE needs to be peged

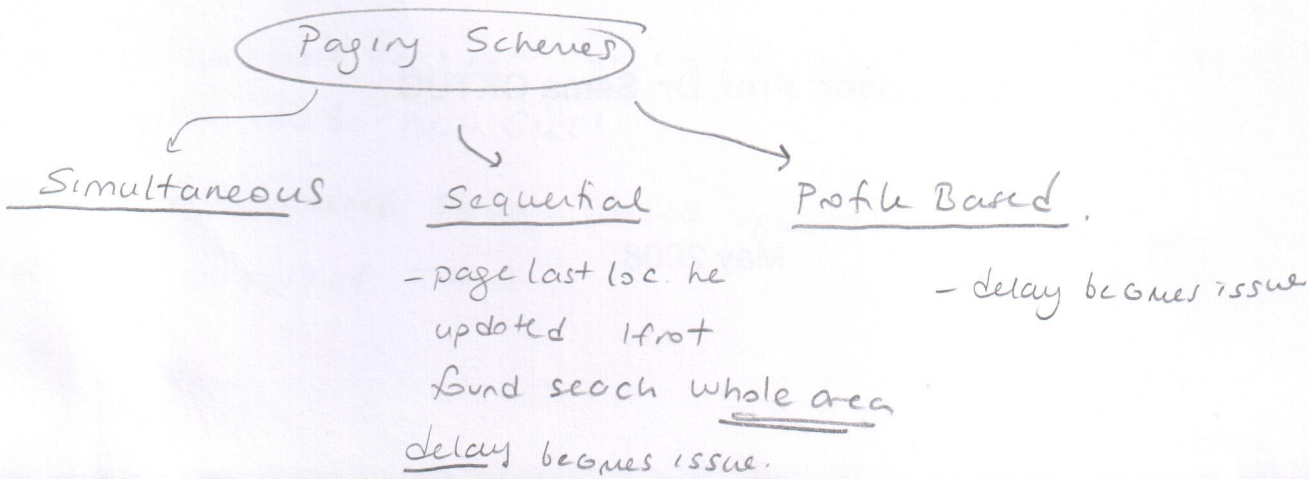
- paging channel capacity is also important

eNB searches for UE

update cost

- transmission powe cost on UE for sending TA updates
- signalling cost on network.



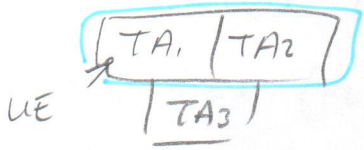


LTE

STATIC TAs

nonoverlapping TAs

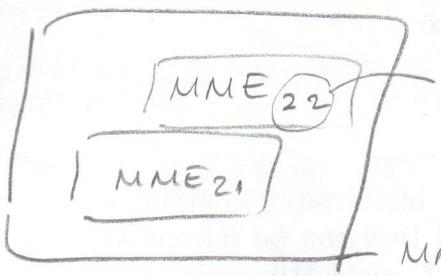
UE can admit to multiple TAs.

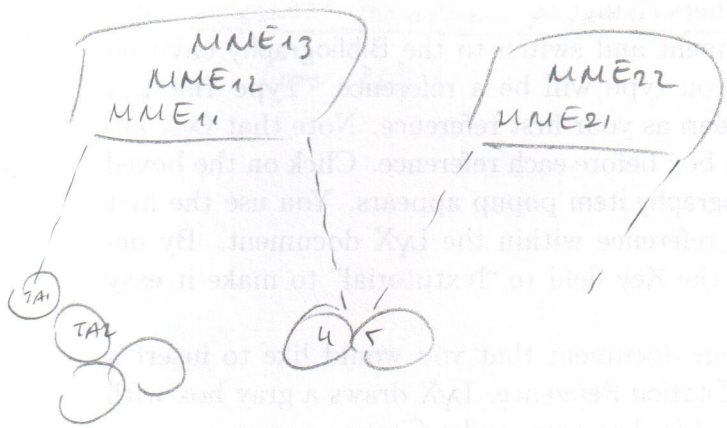


when UE comes to •, network can say you belong to TA1 & TA2 then when he passes to TA2 → no need to update!

BUT UE needs to be paged in both TAs.

MME Group is load sharing particular set of TAs.





TA1 → TA2 ; UE's TAU should go to MME who has his Context

how solved?

→ UE tells eNB which MME has its Context

TAU → TAS → when UE does TAU, MME povides GUTI which has MME group id + color

GUTI will say I'm connected to MME11. when eNB in TAS receives that update, he knows he is not connected to MME11 & peforms Context transfer MME21 will provide new GUTI.

⇒ moving to new MME Group! MME updates GUTI to point new MME (all done as part of TAU)

Idle mode procedures

- check for pages
- select different cell (bs) ⇒ (cell re-selection) ← if power of neighbor cells is bigger then current
- bcast message has (PLMN, cellid, TAI) ← then UE decides whether a TAU is needed.

LTE (sleep mode): short DRX, long DRX

Differences in WiMAX

paging group ≡ TA

can have overlapping PG

UE can belong to 1 PG

ASNGW can request another ASNGW to also page UE? (over R4)

(in LTE, only 1 MME is responsible for paging UE)

Security

mobile / wireless challange

- physical security limited
- mobility means involved parties are changing frequently
- mobile devices are constrained
- performance important. (real-time!)

network security

- **authentication** entity authentication, data origin authentication (device auth. / this packet is transmitted by my same phone so I'm authenticated with.)
- **authorization** determine if user should be allowed to access particular net / service
- **integrity protection** (make sure data is not modified)
- **replay protection** (reproduced packets!)
- **privacy** (prevent info known by unauthorized entities)
- **non-repudiation** benden mi geldi, kesin mi (inkar edememe)

* symmetric key kullanıyorsan, non-repudiation sağlanamaz! ortak anahtarla şifrelenmiş metin, benden mi, senden mi belli değil!

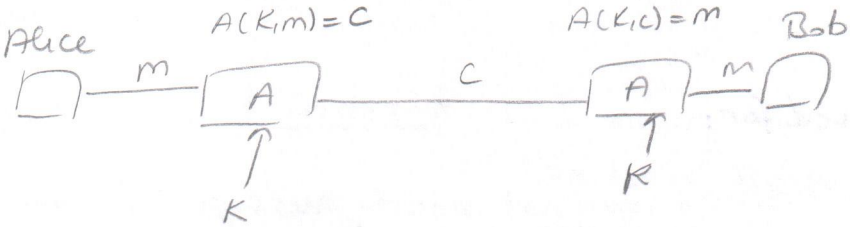
Symmetric key uses same key at both ends! (shared keys)

DES, 3DES, IDEA (encryption algorithms)

Asymmetric key uses private-public key pairs

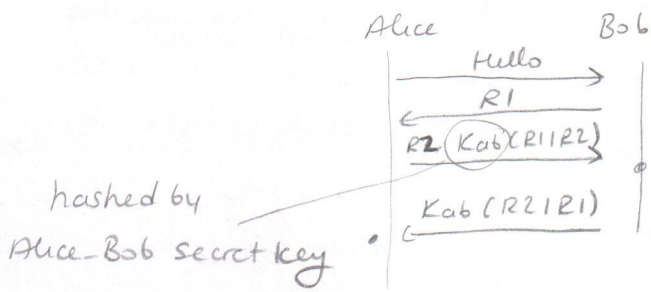
hash function one way transformation; used for digital signature generation

Symmetric Key Cryptography: Encryption & Message Authentication



no non-repudiation

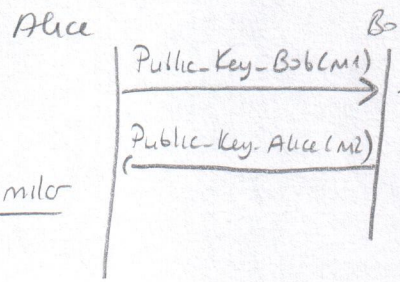
for replay attack use random #



mutual authentication with Secret Key

Symmetric key limitation
- sharing of the keys need to be done out of band
- does not scale
- can not provide non-repudiation.

Public Key Cryptography



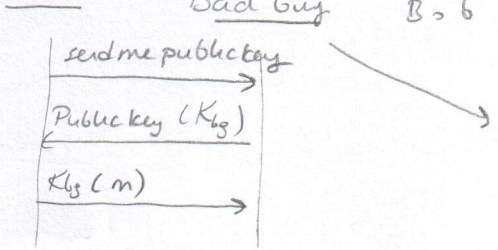
- only Bob can decipher message using his private key

similar ~~~ encryption with public key

Confidentiality

uses 2 keys
- public key
- private " (only known by 1 entity)

obtaining public key



Bad Guy is impersonating Bob

- impersonation attack can be avoided using public key certificates

certificate is signed by (CA)'s private key — certificate authority.

certificate binds identifier to public key.

X509 is a widely used standard of ITU.

One-way hash function is used for:

- message integrity checking — "3rd party can not modify message & still have same hashed value."

- authentication — user on host — computer hashes password & stores result (not password) on re login compares new hash with stored.

algorithms — MD5, SHA-1 ⇒ untyped hash functions

(HMAC)-SHA-1 ⇒ hash based message authentication code

takes input message and a key and generates hash

$K_{AB}(R1 | R2)$

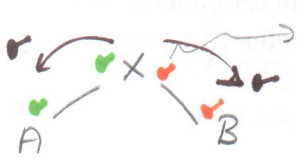
hashed using K_{eyab}.

Trusted Third Party & Key Delivery → should also be performed securely

- A and X trust each other sharing 🔑 key

(there is a <u>security association</u> between the two; they can identify and authenticate each other.

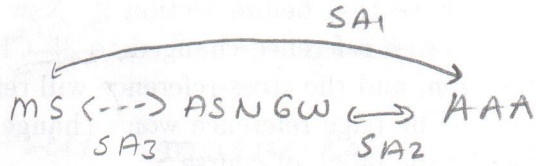
- B and X trust each other using 🔑 key



→ trusted third party

— X delivers shared secret key to A & B for their mutual use.

aynı şekilde;



SA1 ile SA2 den SA3 kurulmuş oldu!

Rekeying

- each key shall have a <u>finite lifetime</u> and replaced with a new one before expiration.

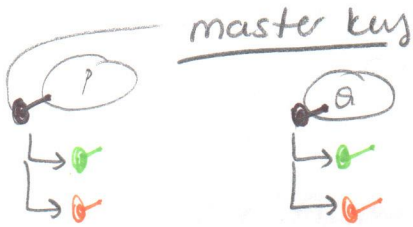
- key <u>naming</u> & <u>indexing</u> (I'm using K_{100} now!)
  packet is signed by K_{100}
  eski key ile şifrelenmiş paketler sonra ulaşmamış olabilir, onları da eski şifre ile çöz. Bu gibi durumlar için eskisini bi'nn sakla

- Başka keyler de var; encryption, integrity protection .. için değişik keyler kullan.

SPI: security parameter index CMIP6-SPI

Key Derivation

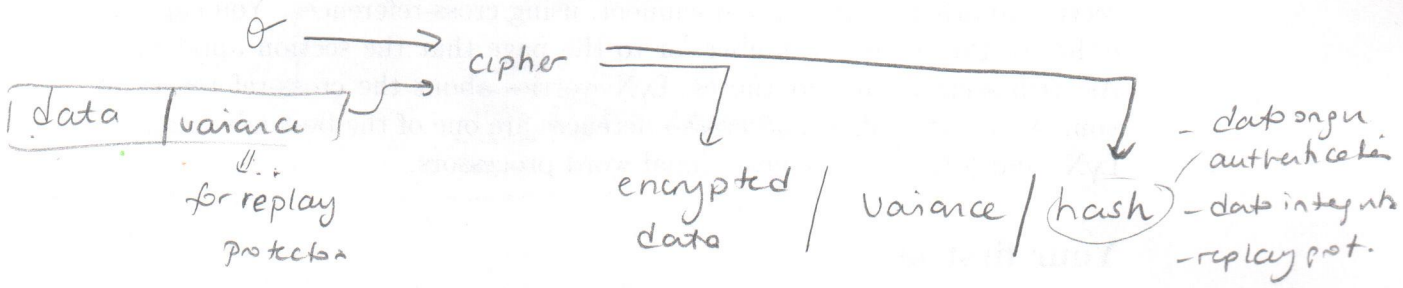
- subordinate keys are computed for purpose-specific use



HMAC-SHA1 (, "data key")

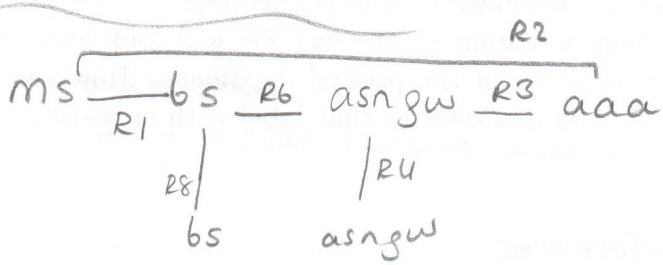
HMAC-SHA1 (, "signalling key")

* Anahtar dagitim islevi maliyetli, 30 tane yeni key dagitmak yerine, master key'den türetiyorlar.



Trusted 3rd party (is AAA) sends generated key to ASNGW but not terminal, MS generates itself (master key = secret key terminalde ve AAA'de var sadece)

WiMAX



R1 → Dynamically established trust

R6-R4-R8-R3-R2 → pre-established trust

WiMax identifiers

- Device Identifiers

48bit MAC & X.509 certificate

Device Authentication!

(MACs can be authenticated using PKI)

primary identifier of MS in the RAN

Subscriber Identifier NAI Bob@MyISP.com

- primary identifier of MS in CN

Extensible Authentication Protocol

EAP (IETF RFC 3748) used in WiFi, WiMAX, ZigBee, DSL, ...

enable 50+ authentication methods on any access technology

TLS uses certificate
AKA " SIM
MD5 " hash
} different methods.

Network
MAC — security layers
PHY

RADIUS / Diameter → 2 methods for authorization.

EAP messages (LinkLayer Frames)

Roaming

Subscriber NAI = alper@kt.com

decorated NAI = kt.com ! alper@clearwire.com

visited

bunu oluşturuyorsa cihazım KT ile clearwire arasında roaming aggreement olduğunu biliyor.

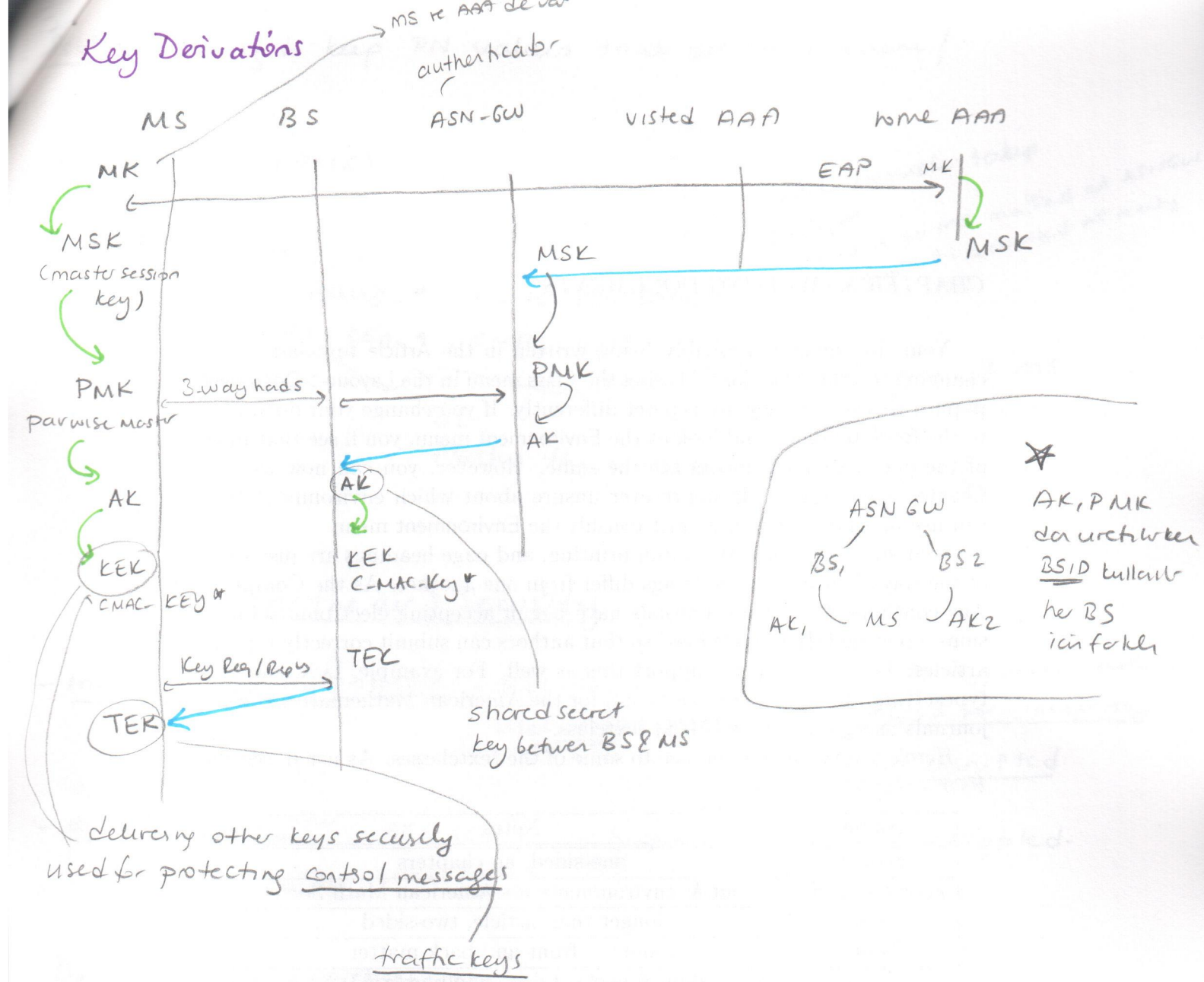
network access authentication

flow .. ⇒ session key comes to AGW from AAA

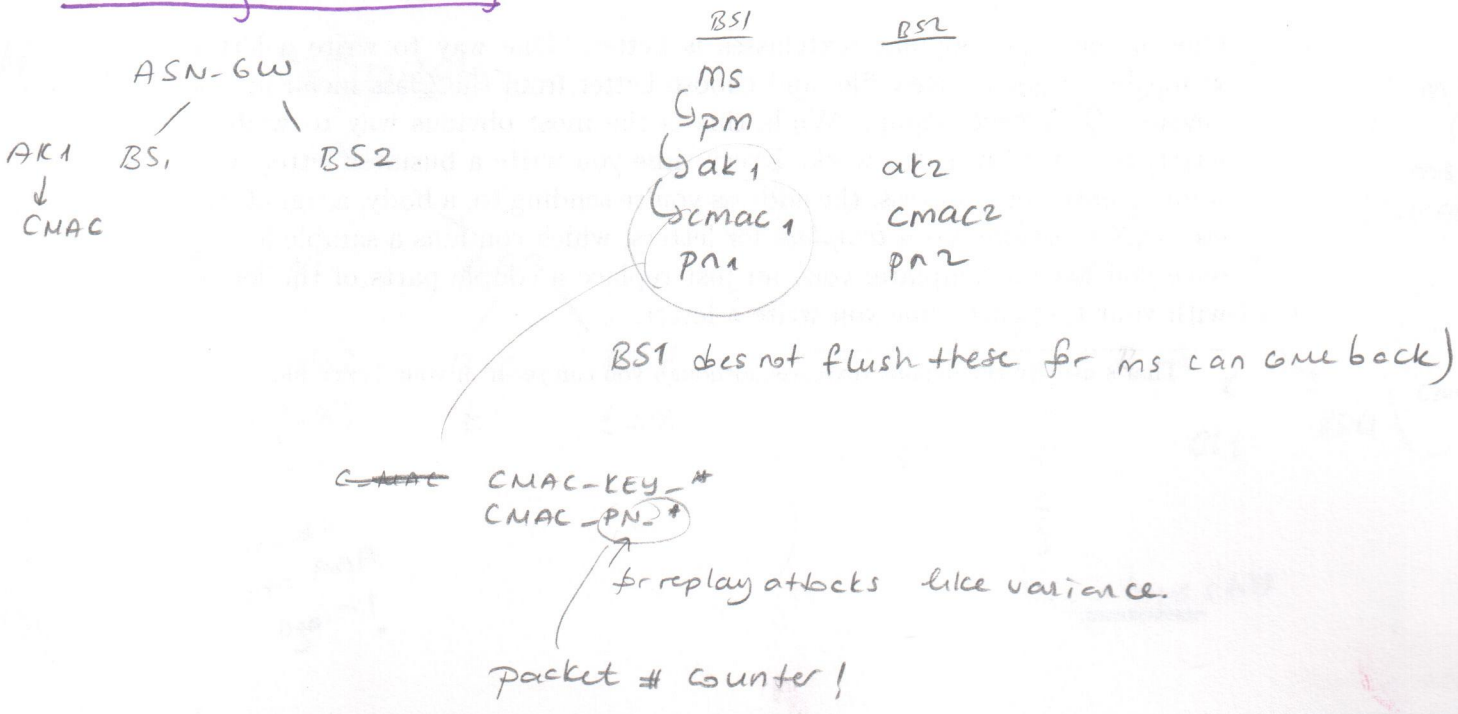
- multicast re broadcast'te bir sıkıntı kişide olmadı gerekli key ! generated olmaz o yüzden BS " " " için key üretip dağıtır

PKM RSP

Key Derivations



Reducing BS Caching



blem: having to keep PN values that pressures cache!

ASN-GW (PMK)
/
BS (AK,
CMAC-PREKEY-*, CMAC-KEY-COUNT,
CMAC-KEY-*, CMAC-PN*

network user under take up edily on.
one value per MS maintained at ASNGW
starts from 1 & incremented at events or LAU.

starts from 0 when MS comes back!

BS flushes these values when MS departs.

R1 (over the air) Security

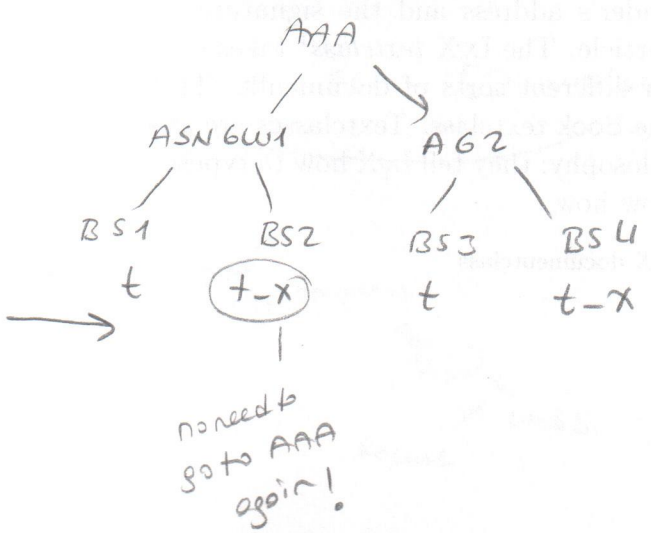
- message integrity protection : AES-CMAC
  uses CMAC-KEY-* } CONTROL packets are protected for integrity but not encrypted

- encryption algorithm AES CCM
  uses TEKs } DATA packets are encrypted.

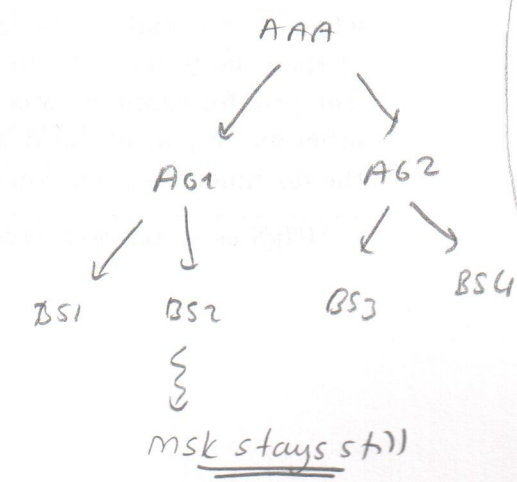
Device + Subscriber Authentication EAP-TTLS

Accounting starts after IP service has started.

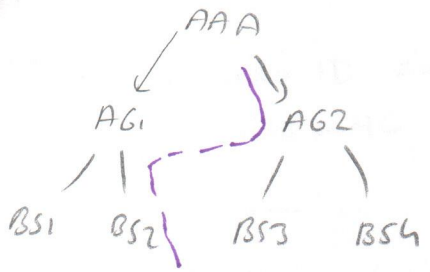
Hierarchical optimization



Key Hierarchy



Pre authentication



L3 or L2 pre-authentication

BS3 e geçeceğini anlayınca AG1-AG2-AAA pathi üzerinden authentication yapar - (bu authentication has lifetime!)

ASN'lerde security context saklanıyor, ms geldiğinde bakar, context varsa hemen authorize eder.

Context Transfer

AG1 ⟶ AG2 — key sharing — vulnerability ↑

MSK, ---

domino effect!

→ proactive : bs knows ms will most probably pass to AG2

→ reactive : when ms starts network entry procedure, AG2 connects to AG1.

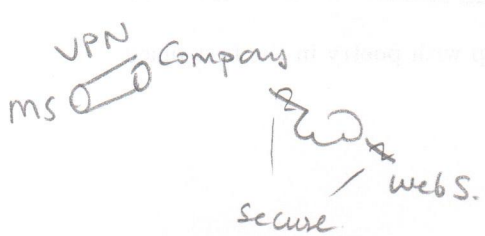
End2End Security — IP sec

Last Mile → Secure L2 — EAP — AP-laptop arası secure DSL e geçince not secure

ms - BS
ms - ASNGW) last mile

ms - bs - asn - PGW - ☺ - webserver

end to end.



Application Layer Security

- HTTPS

privacy pseudo ID during access authentication
pseudo MAC

HW 6

mutual authentication between MS-BS

authenticate MS → operator needs to know who MS really is
authenticate BS → user needs " " BS is " his operator's BS!

⇒ TEK are not generated but delivered from BS to MS
because they can be used for bcast or multicast

Security for LTE

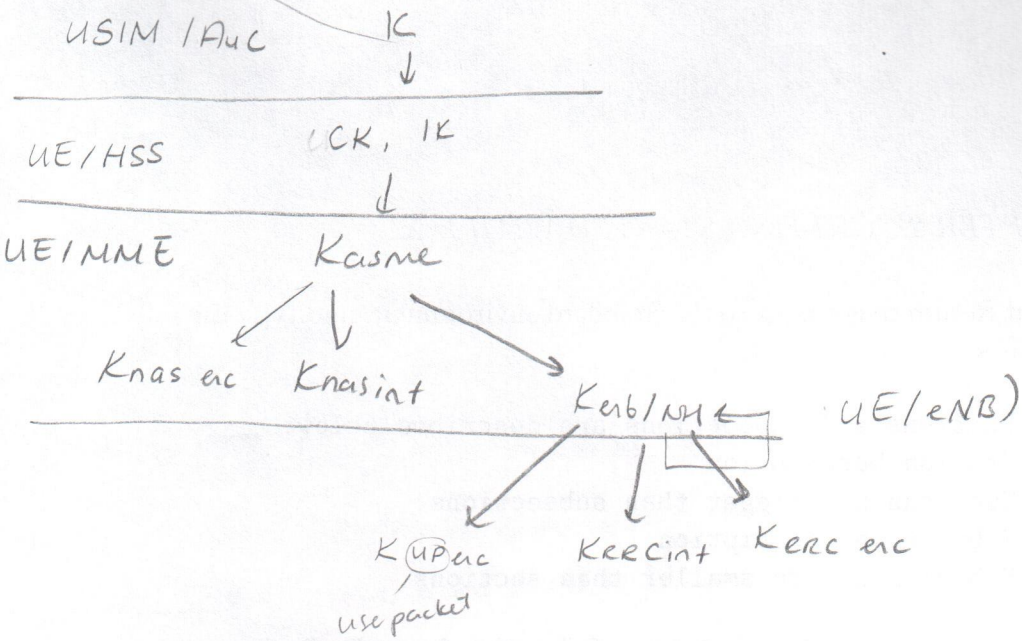
network access security primarily radio link security

encry + integrity for RRC (radio resource control)
encry + " for NAS
encry for DATA (not integrity!)

network domain security of wireline network between PLMNs.
IKEv2
tunnel-mode EAP.

user domain - user SIM ⇒ USIM
- user Terminal authentication → if phone is SIM-locked

LTE Key Hierarchy



NH: next hop is a key derived by ME & MME for providing forward security.

IMSI (subscribe identity) S-TMSI or GUTI

IMEI (hardware)

only sent to MME ! in NAS (not eNB!)

sent after NAS security is setup!

HW 7

"mesaj içeriğini bilmeden manipule edersen zaten error response" kabulu ile integrity yok

HW #1

- Key functons of MME → - NAS signalling, security
  - Inter CN node signalling for mobility between 3GPP AN's.
  - handover management
  - roaming
  - authentication / authorization

- UE's IP address allocation is performed by P-GW

⇒ IP address & subnet mask ≙ prefix

255.255.255.0

for --/24

HW-4

Determine radioframe number SFN (SFN mod T) & subframe within frame UE monitors for page messages.

$T = \min\{T_c, T_{UE}\} = 128$

T_c: cell specific paging cycle, T_{UE}: UE specific paging cycle

N : number of paging frames within paging cycle of UE

$= \min(T, \underbrace{\text{number of paging subframes per frame} * T}_{Nf})$

$= \min\{128, \frac{1}{4} \cdot 128\}$

$= 32$

$SFN_{\bmod T} = \frac{T}{N}(UE_{id} \bmod N) = \frac{128}{32} \underbrace{172}_{IMSI} \bmod 32$

$= 48$

SFN subframe 0, 4, 5 raya 9 olurda

$Ns = \max\{1, Nf\}$

$\max\{1, 0.25\} = 1$

$is = \left\lfloor \frac{UE_{id}}{N} \right\rfloor \bmod Ns$

$= \left\{ \frac{172}{32} \right\}_{\bmod 1} = 0$

Subframe # = 9

Ns	is=0	is=1	is=2	is=3
1	9	NA	NA	NA
2	4	9	NA	NA
4	0	4	5	9

- pingpong effect