LTE:

A feature based introduction

LTE Core Features

LTE Security

Irfan Ali

info@ikiteknoloji.com

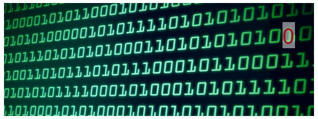
Focus

1. **User Authentication**

2. **Authorization**

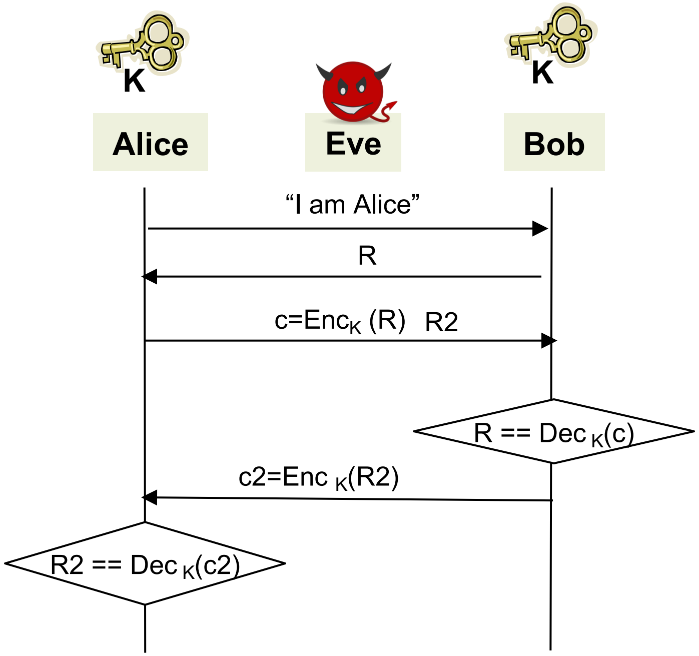
3. **Message Confidentiality**

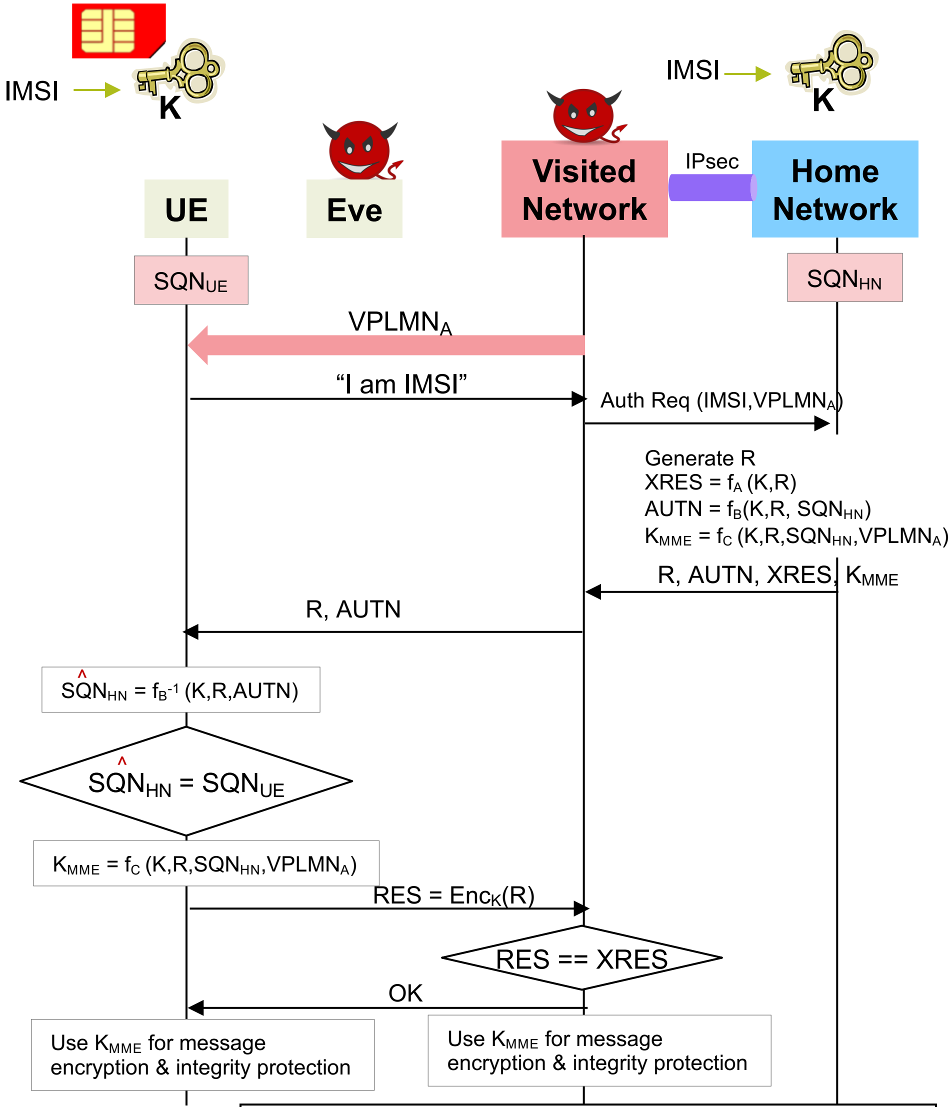
4. **Message Integrity Protection**



5. **User Identity Confidentiality**

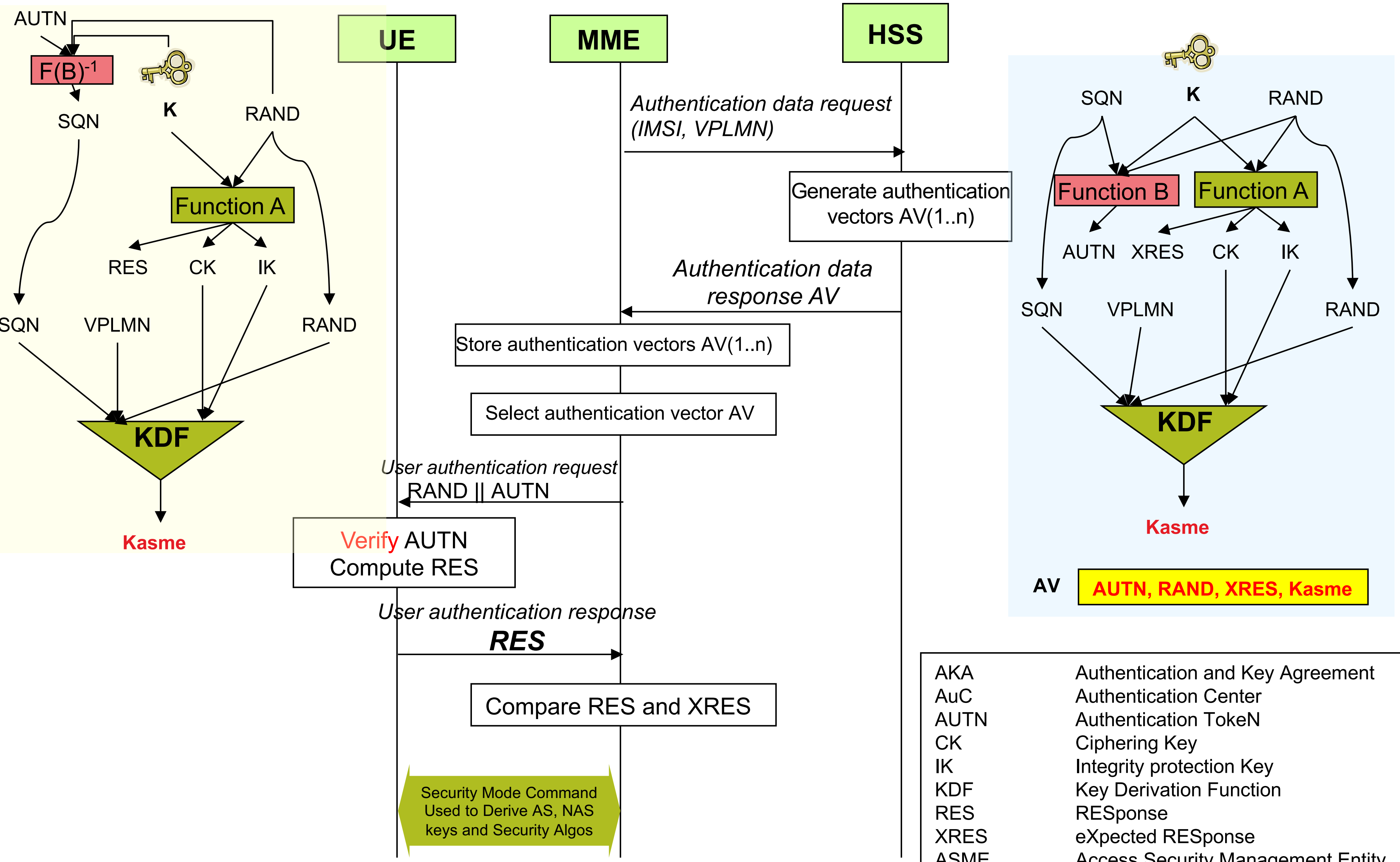
Mutual Authentication




IMSI
K
IMSI
K
UE
Eve
Visited Network
IPsec
Home Network
SQN_{UE}
SQN_{HN}
$VPLMN_A$
“I am IMSI”
Auth Req (IMSI,$VPLMN_A$)
Generate R
XRES = f_A (K,R)
AUTN = f_B(K,R, SQN_{HN})
K_{MME} = f_C (K,R,SQN_{HN},$VPLMN_A$)
R, AUTN, XRES, K_{MME}
R, AUTN
$\hat{SQN}_{HN}$ = f_B^{-1} (K,R,AUTN)
$\hat{SQN}_{HN}$ = SQN_{UE}
K_{MME} = f_C (K,R,SQN_{HN},$VPLMN_A$)
RES = Enc_K(R)
RES == XRES
OK
Use K_{MME} for message encryption & integrity protection
Use K_{MME} for message encryption & integrity protection

IMSI	International Mobile Subscriber Identity
SQN	Sequence number
AUTN	Authentication TokeN
RES	RESponse
XRES	eXpected RESponse

EPS AKA



UE

MME

HSS

Authentication data request (IMSI, VPLMN)

Generate authentication vectors AV(1..n)

Authentication data response AV

Store authentication vectors AV(1..n)

Select authentication vector AV

User authentication request
RAND || AUTN

Verify AUTN
Compute RES

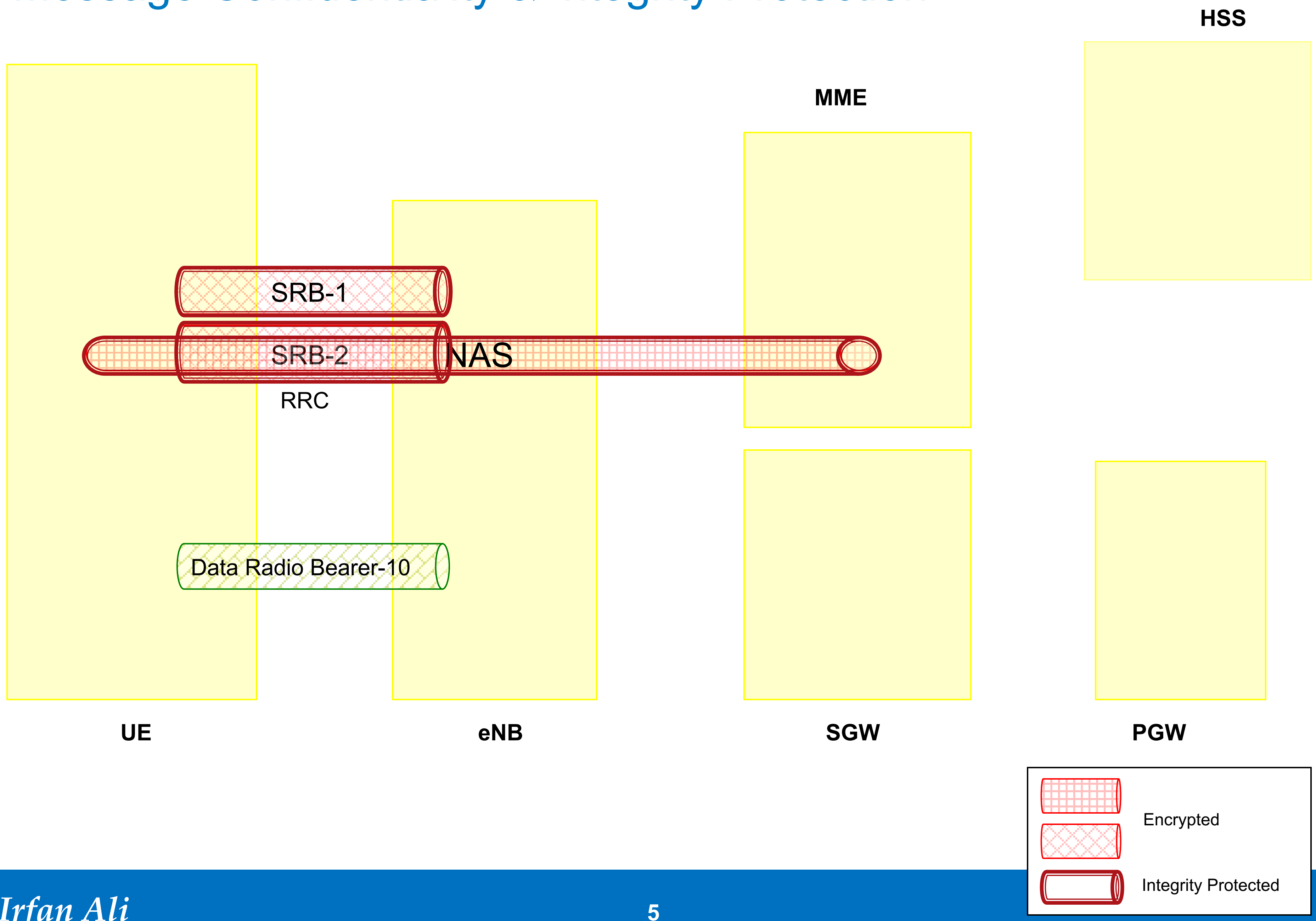
User authentication response
RES

Compare RES and XRES

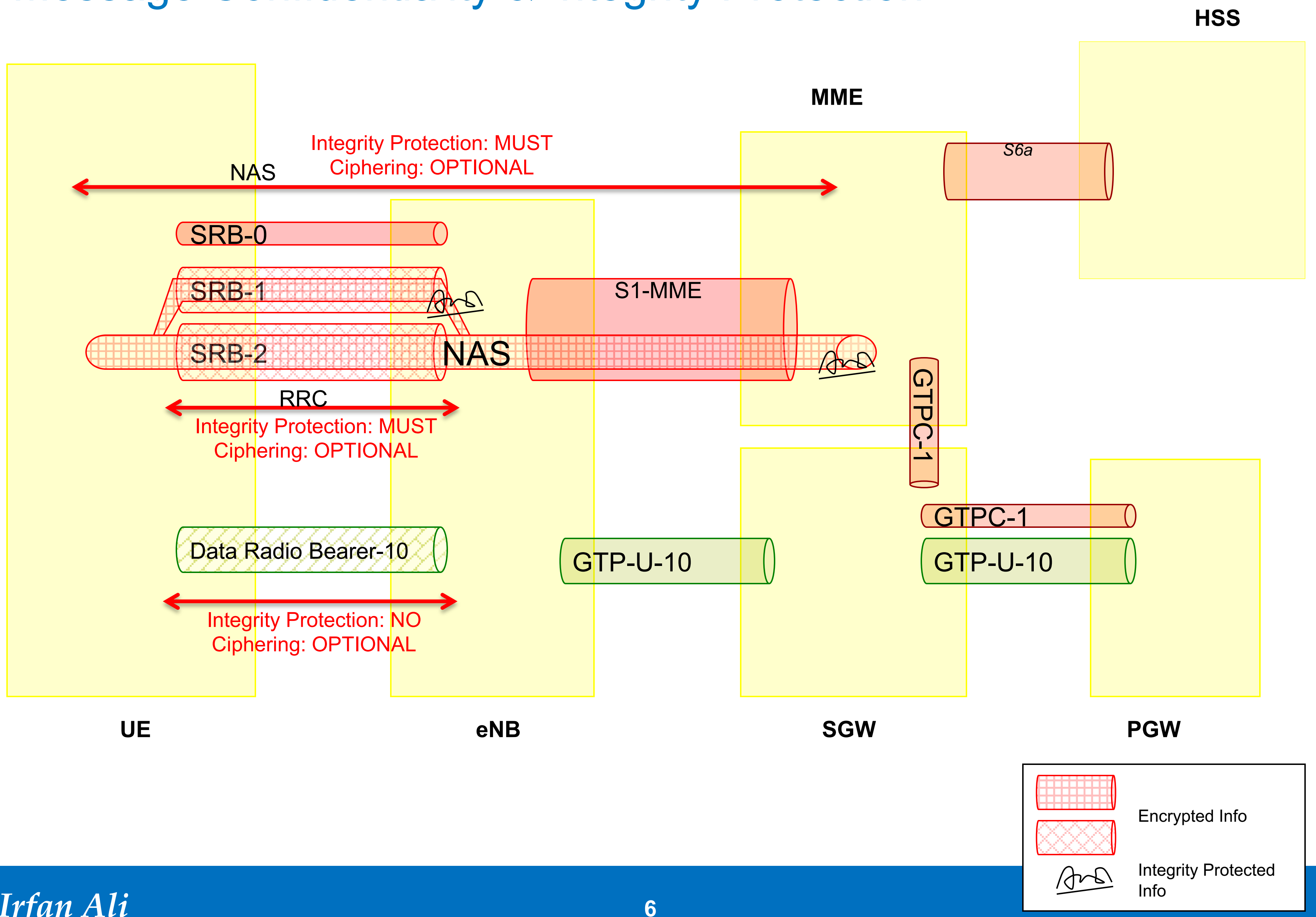
Security Mode Command Used to Derive AS, NAS keys and Security Algos

AKA	Authentication and Key Agreement
AuC	Authentication Center
AUTN	Authentication TokeN
CK	Ciphering Key
IK	Integrity protection Key
KDF	Key Derivation Function
RES	RESponse
XRES	eXpected RESponse
ASME	Access Security Management Entity

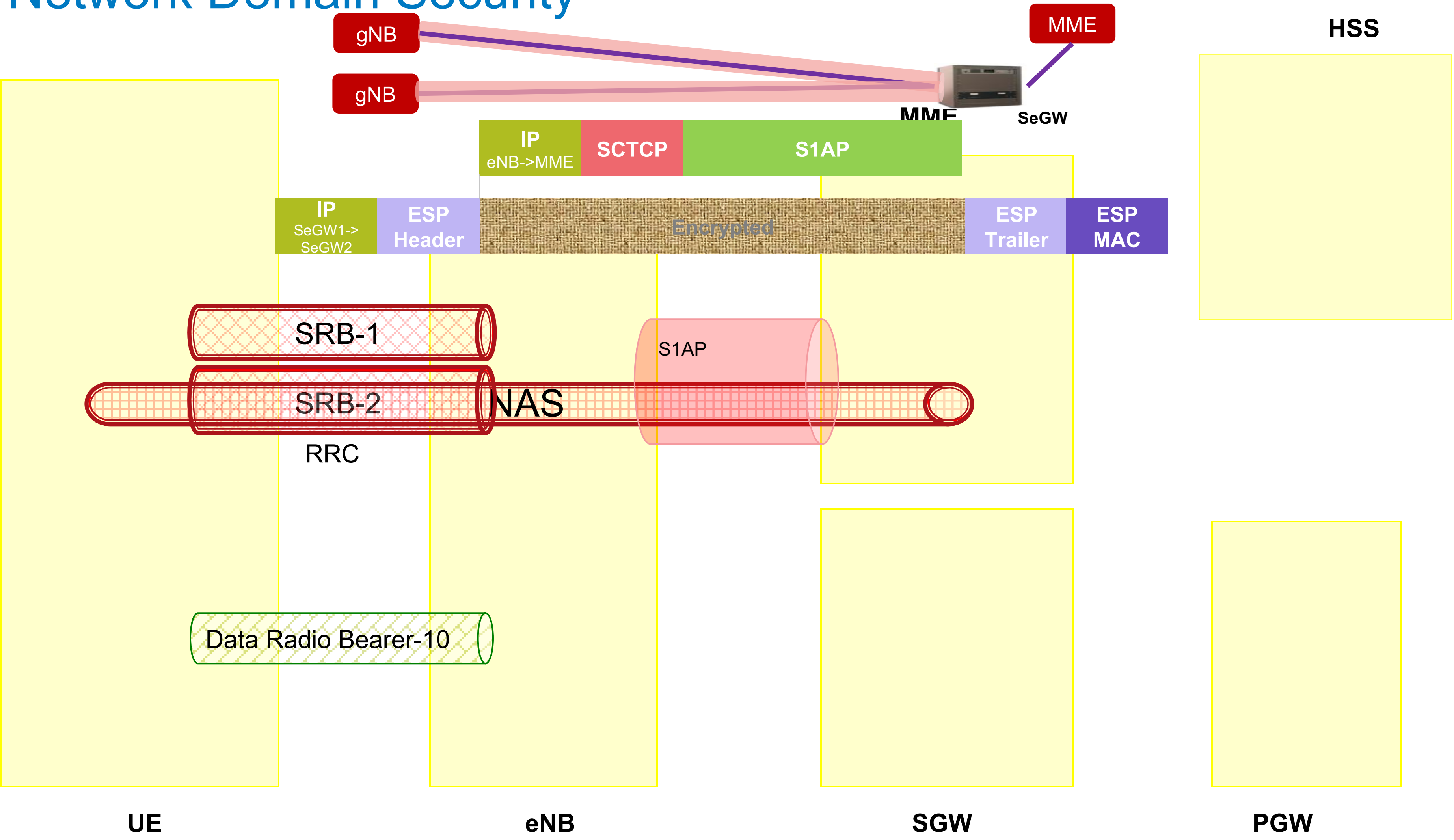
Message Confidentiality & Integrity Protection



Message Confidentiality & Integrity Protection



Network Domain Security

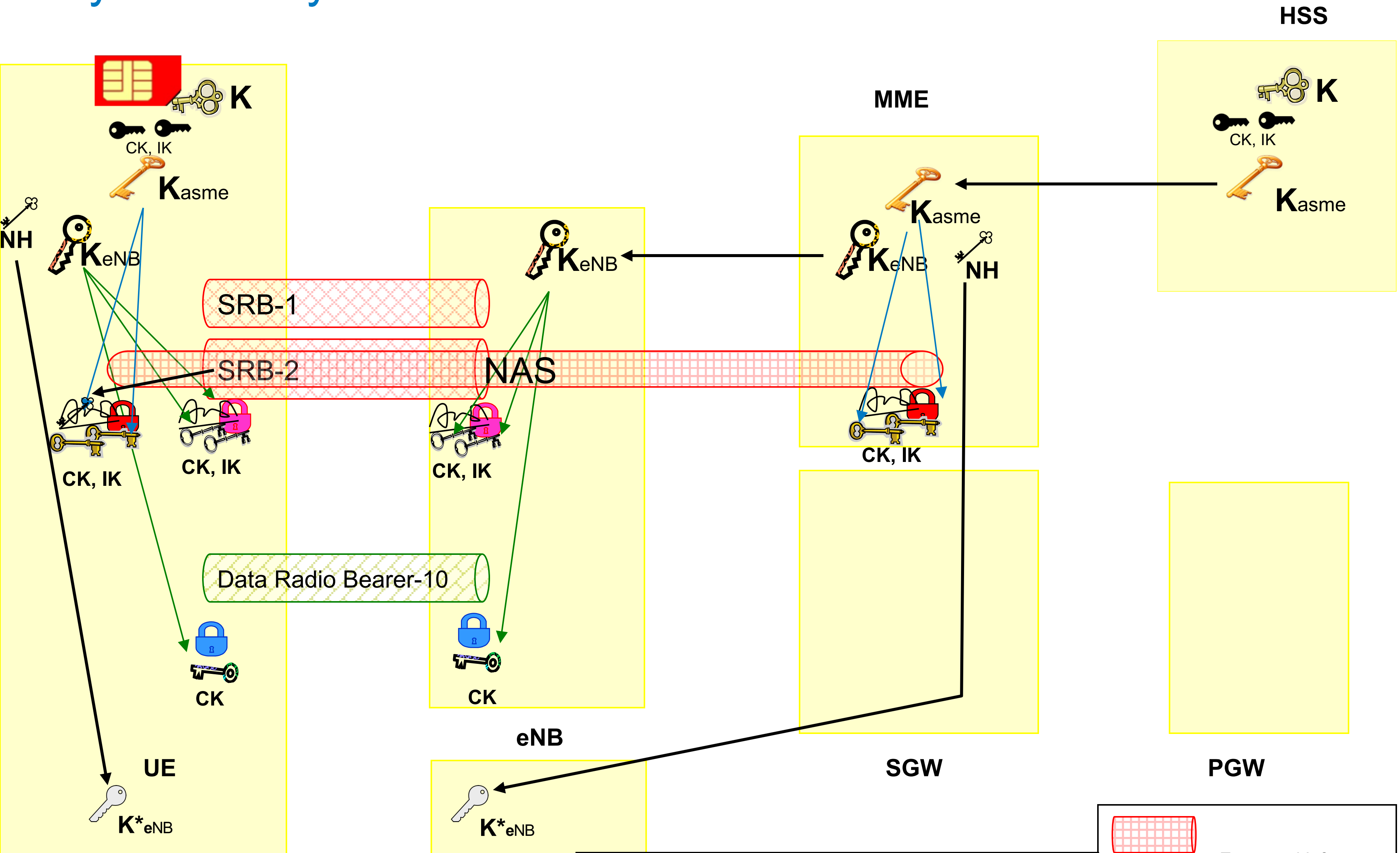


ESP	Encapsulating Security Payload
MAC	Message Authentication Code

▦ ▨ Encrypted

▭ Integrity Protected

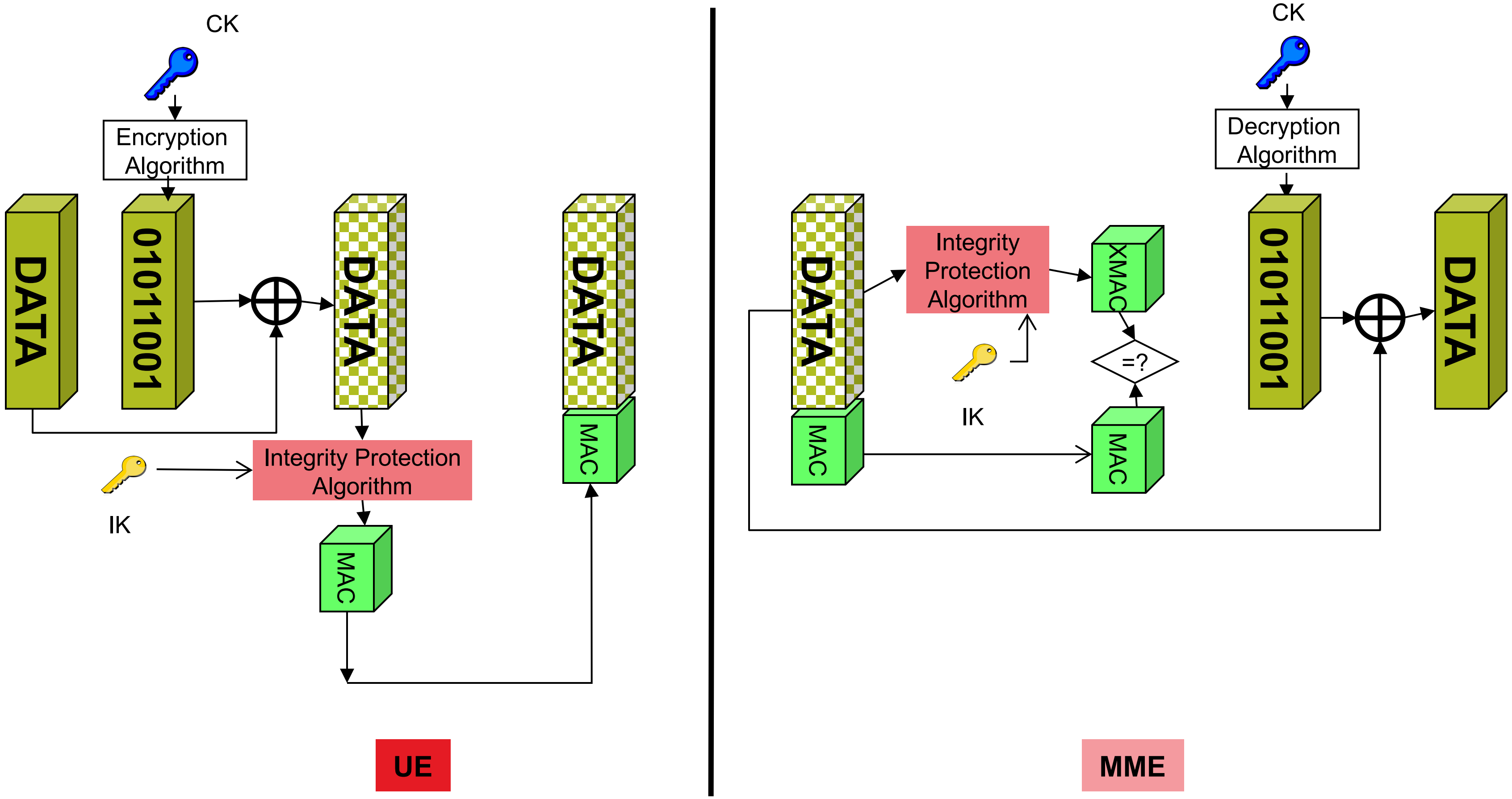
Key Heirarchy for LTE



ASME	Access Security Management Entity (MME)
CK, IK	Ciphering Key, Integrity Protection Key

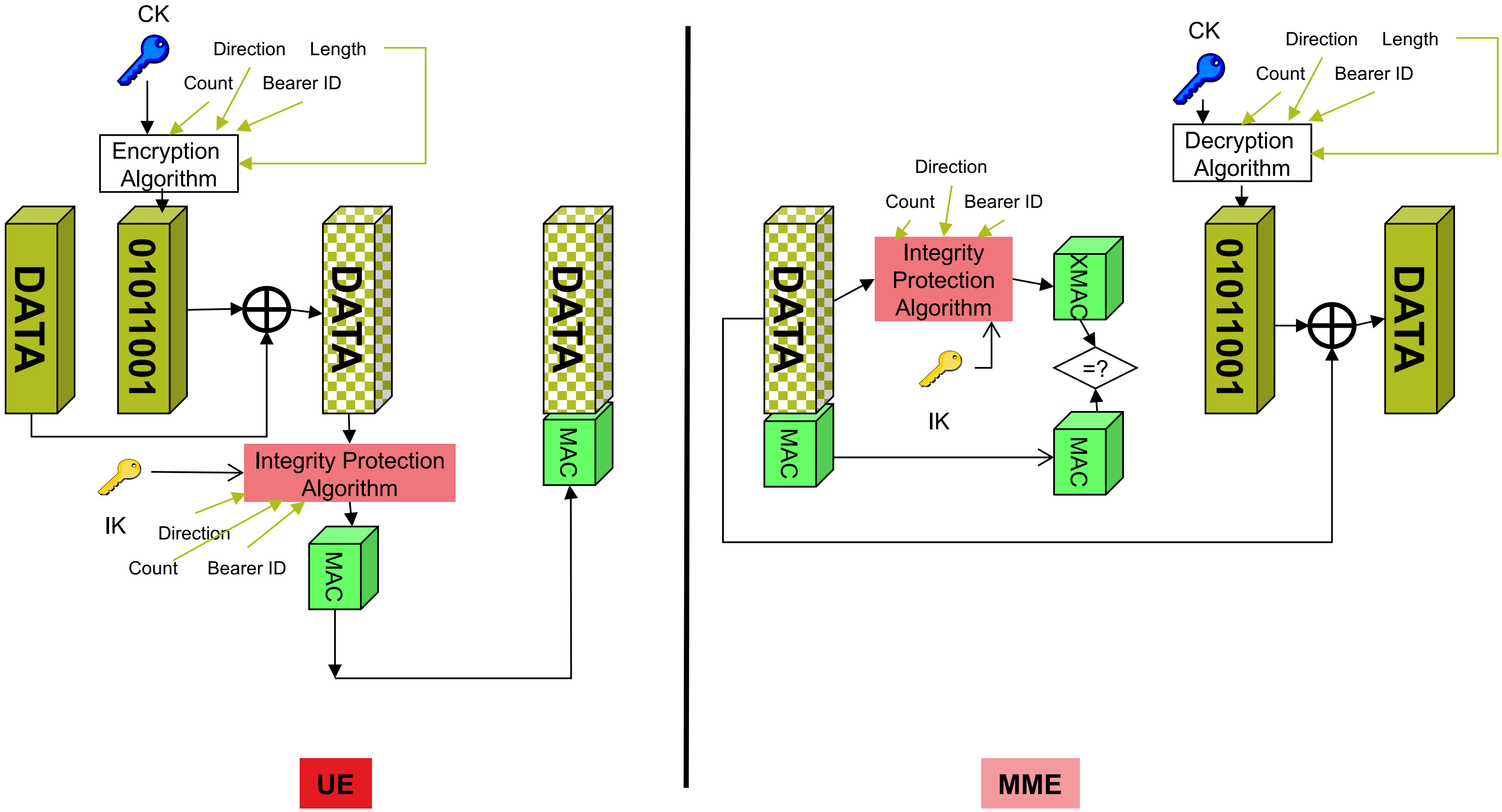
▦ Encrypted Info
▨
Integrity Protected Info

Encryption and Integrity Protection: NAS Layer



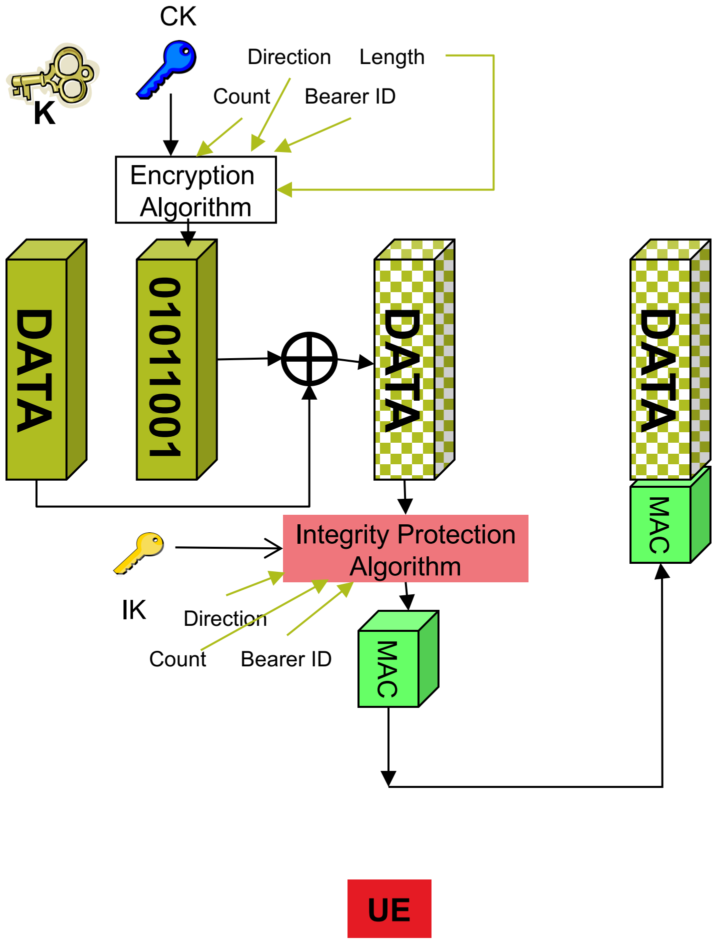
MAC	Message Authentication Code

Encryption and Integrity Protection: NAS Layer



MAC	Message Authentication Code

Encryption and Integrity Protection: NAS Layer



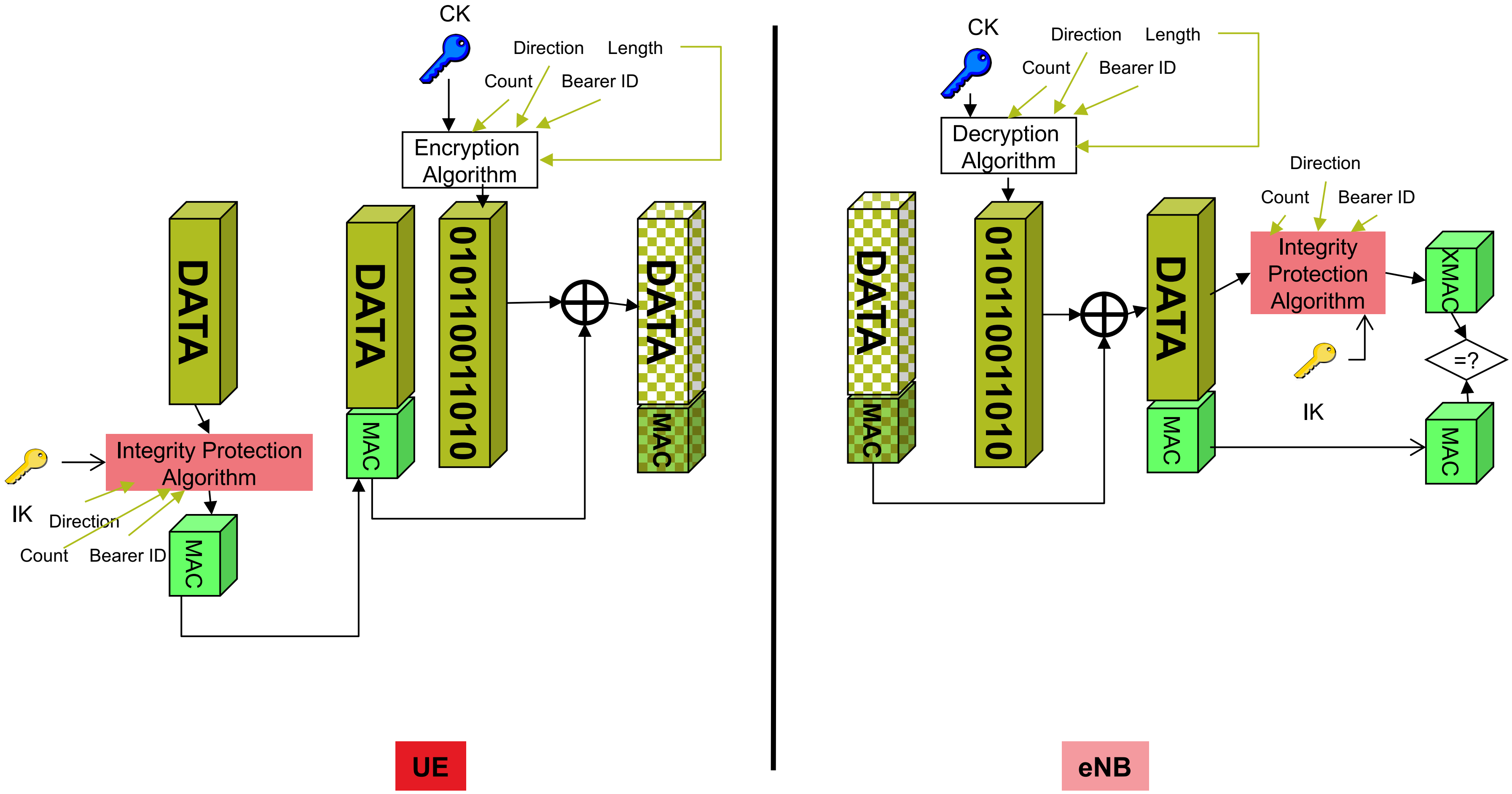
Octets	Bits							
	8	7	6	5	4	3	2	1
1	Security Type 0x0010				Protocol Discriminator 0x0111 (EMM)			
2	Message Authentication Code (MAC)							
3								
4								
5								
6	Sequence Number (SN)							
7	EMM or ESM NAS Message							

2 Integrity Protected

1 Encrypt

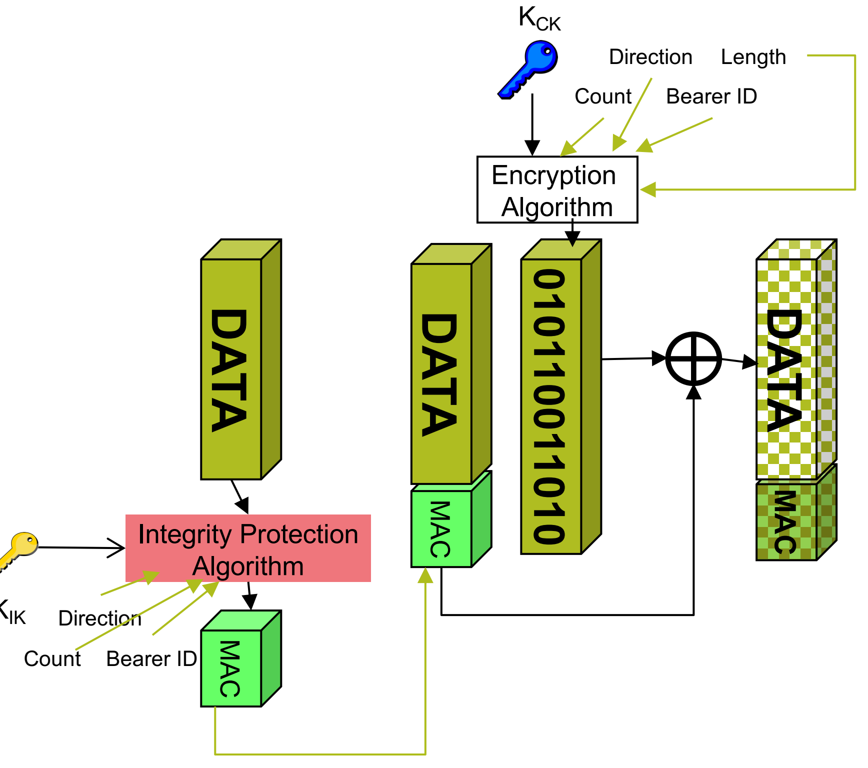
MAC	Message Authentication Code

Encryption and Integrity Protection: AS Layer

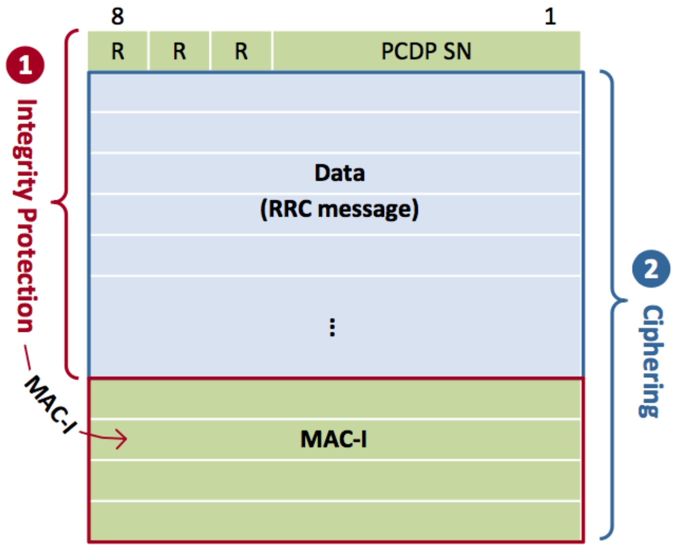


MAC	Message Authentication Code

Encryption and Integrity Protection: AS Layer



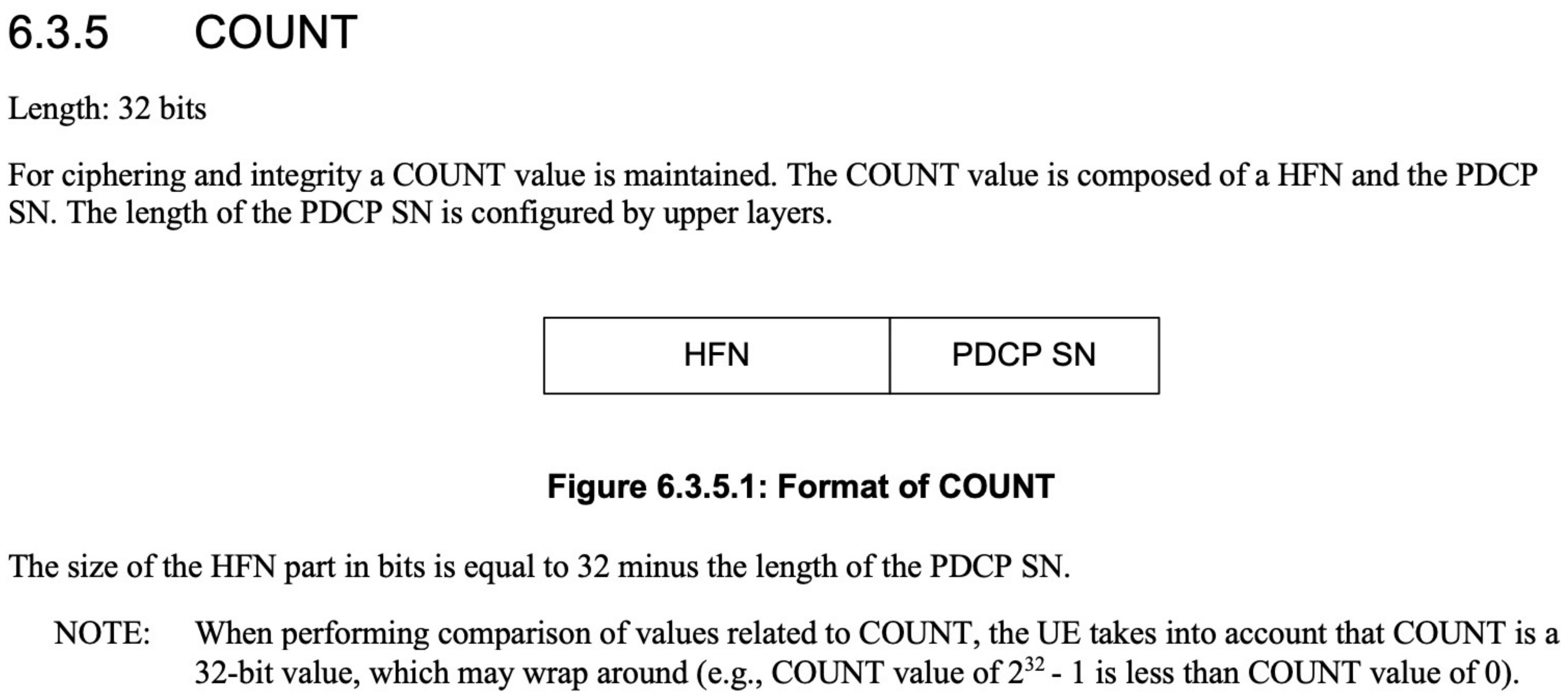
UE



Security protected RRC message (sender)

Source: Netmanias

MAC	Message Authentication Code



6.3.5 COUNT

Length: 32 bits

For ciphering and integrity a COUNT value is maintained. The COUNT value is composed of a HFN and the PDCP SN. The length of the PDCP SN is configured by upper layers.

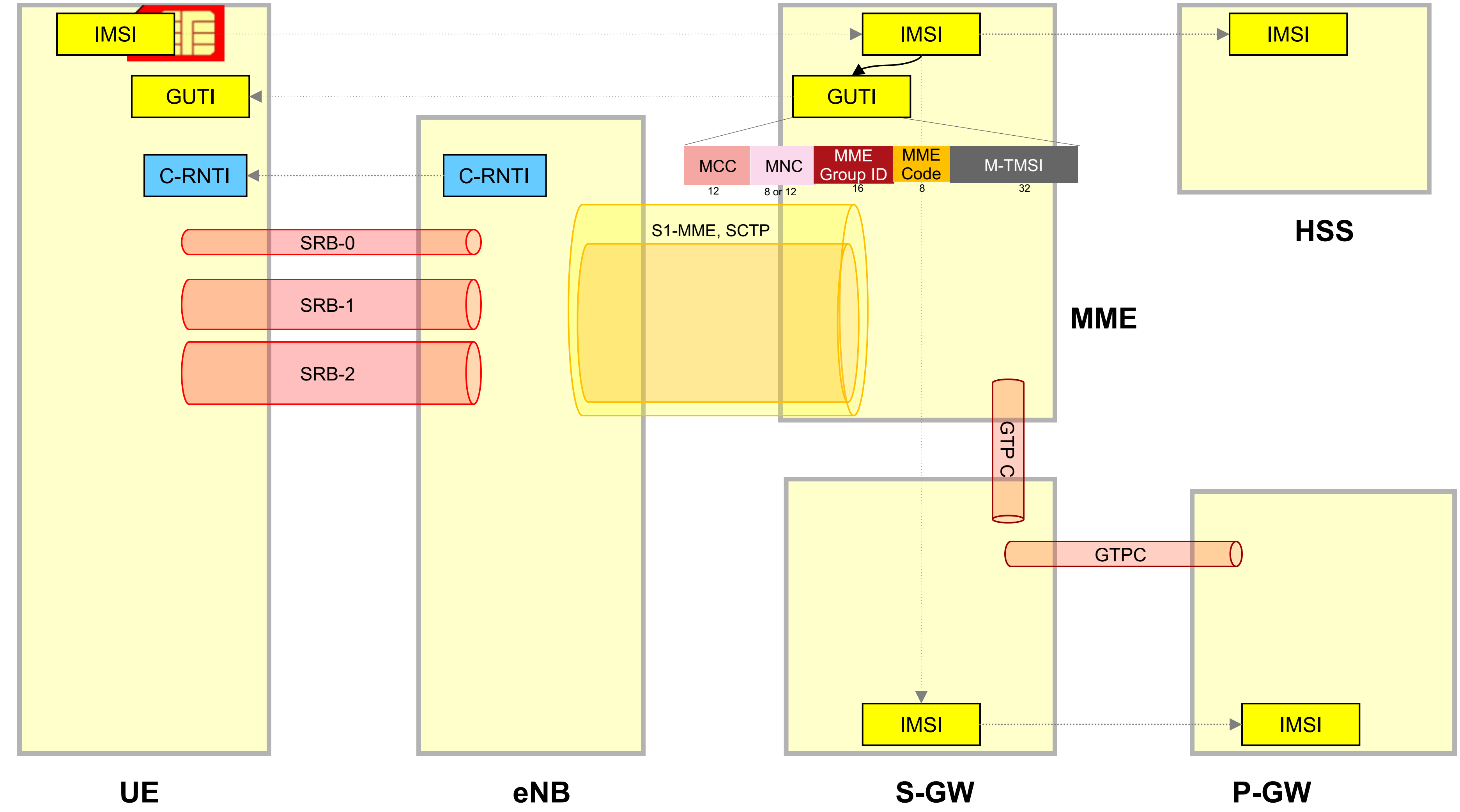
HFN	PDCP SN

Figure 6.3.5.1: Format of COUNT

The size of the HFN part in bits is equal to 32 minus the length of the PDCP SN.

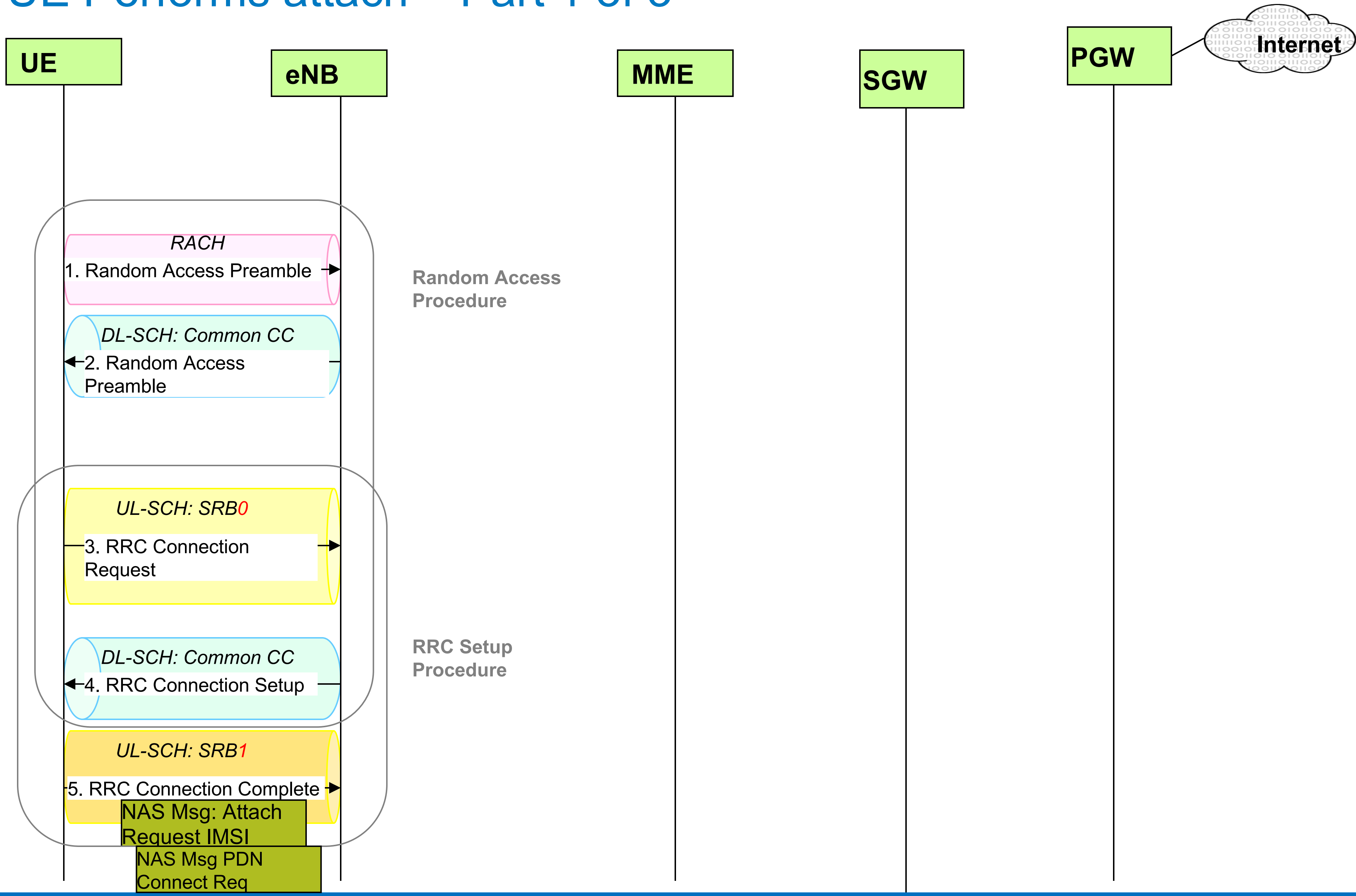
NOTE: When performing comparison of values related to COUNT, the UE takes into account that COUNT is a 32-bit value, which may wrap around (e.g., COUNT value of 2^{32} - 1 is less than COUNT value of 0).

Identity Confidentiality

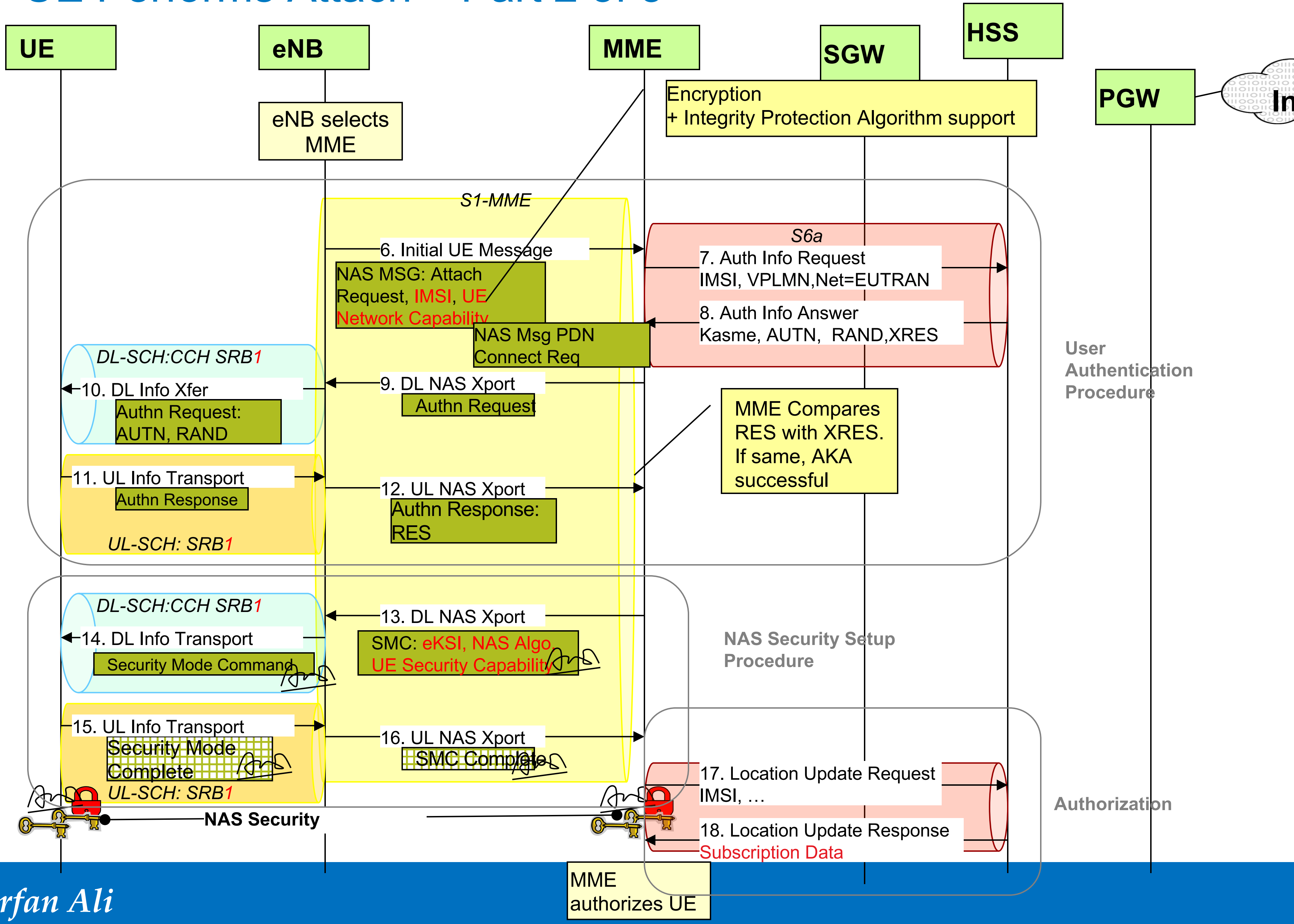


SRB	Signaling Radio Bearer
GTP	GPRS Tunneling Protocol
C-RNTI	Cell- Radio Network Temporary Identity
GUTI	Globally Unique Temporary Identity
IMSI	International Mobile Subscriber Identity
M-TMSI	M-Temporary Mobile Subscriber Identity
S-TMSI	S-Temporary Mobile Subscriber Identity

UE Performs attach – Part 1 of 3

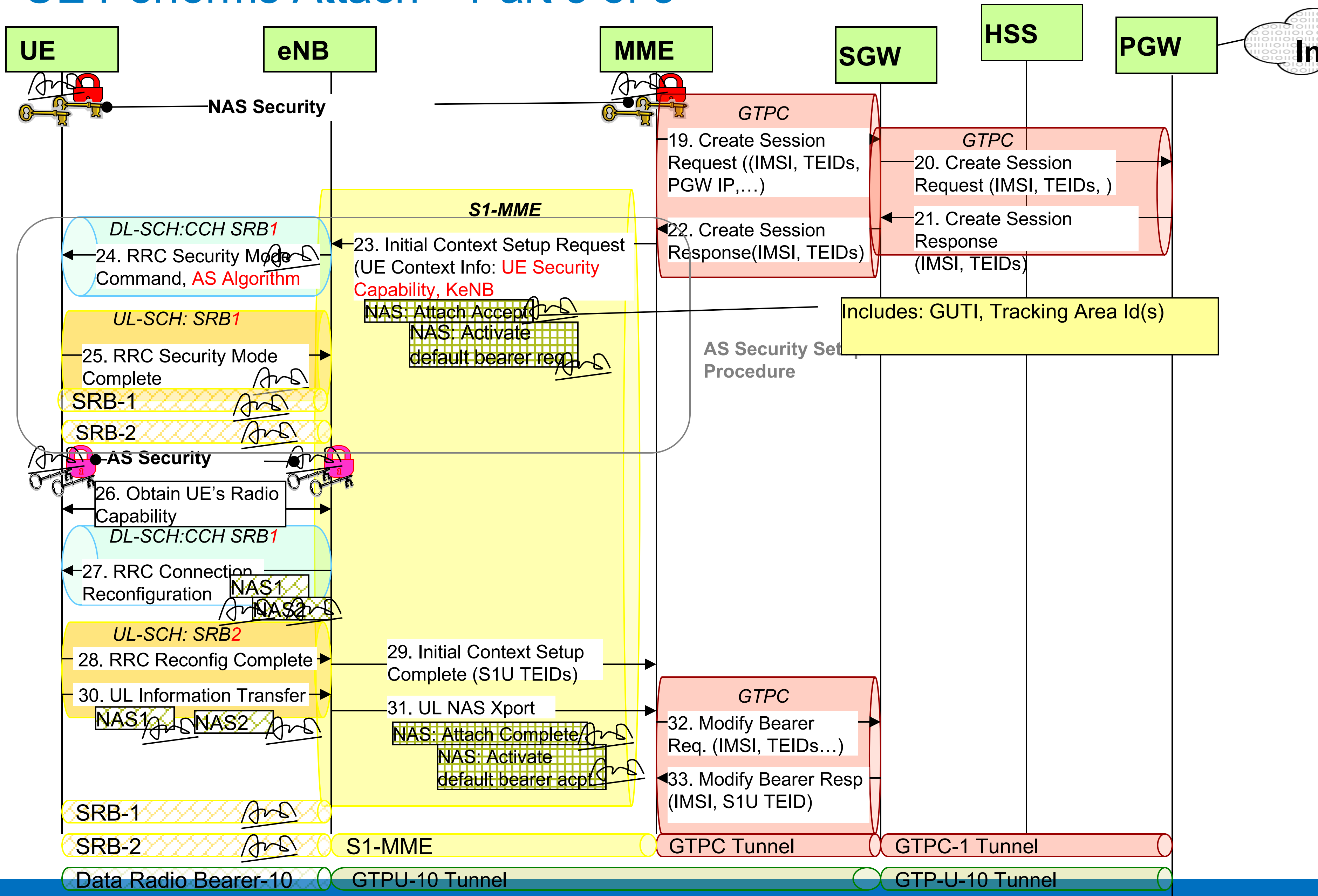


UE Performs Attach – Part 2 of 3



Irfan Ali

UE Performs Attach – Part 3 of 3



UE | eNB | MME | SGW | HSS | PGW

NAS Security

GTPC
19. Create Session Request ((IMSI, TEIDs, PGW IP,…)

GTPC
20. Create Session Request (IMSI, TEIDs,)

21. Create Session Response (IMSI, TEIDs)

22. Create Session Response(IMSI, TEIDs)

S1-MME

23. Initial Context Setup Request (UE Context Info: UE Security Capability, KeNB

NAS: Attach Accept

NAS: Activate default bearer req

Includes: GUTI, Tracking Area Id(s)

AS Security Setup Procedure

DL-SCH:CCH SRB1
24. RRC Security Mode Command, AS Algorithm

UL-SCH: SRB1
25. RRC Security Mode Complete

SRB-1

SRB-2

AS Security

26. Obtain UE's Radio Capability

DL-SCH:CCH SRB1
27. RRC Connection Reconfiguration

NAS1

NAS2

UL-SCH: SRB2
28. RRC Reconfig Complete

29. Initial Context Setup Complete (S1U TEIDs)

30. UL Information Transfer

NAS1

NAS2

31. UL NAS Xport

NAS: Attach Complete/

NAS: Activate default bearer acpt

GTPC
32. Modify Bearer Req. (IMSI, TEIDs…)

33. Modify Bearer Resp (IMSI, S1U TEID)

SRB-1

SRB-2

S1-MME

GTPC Tunnel

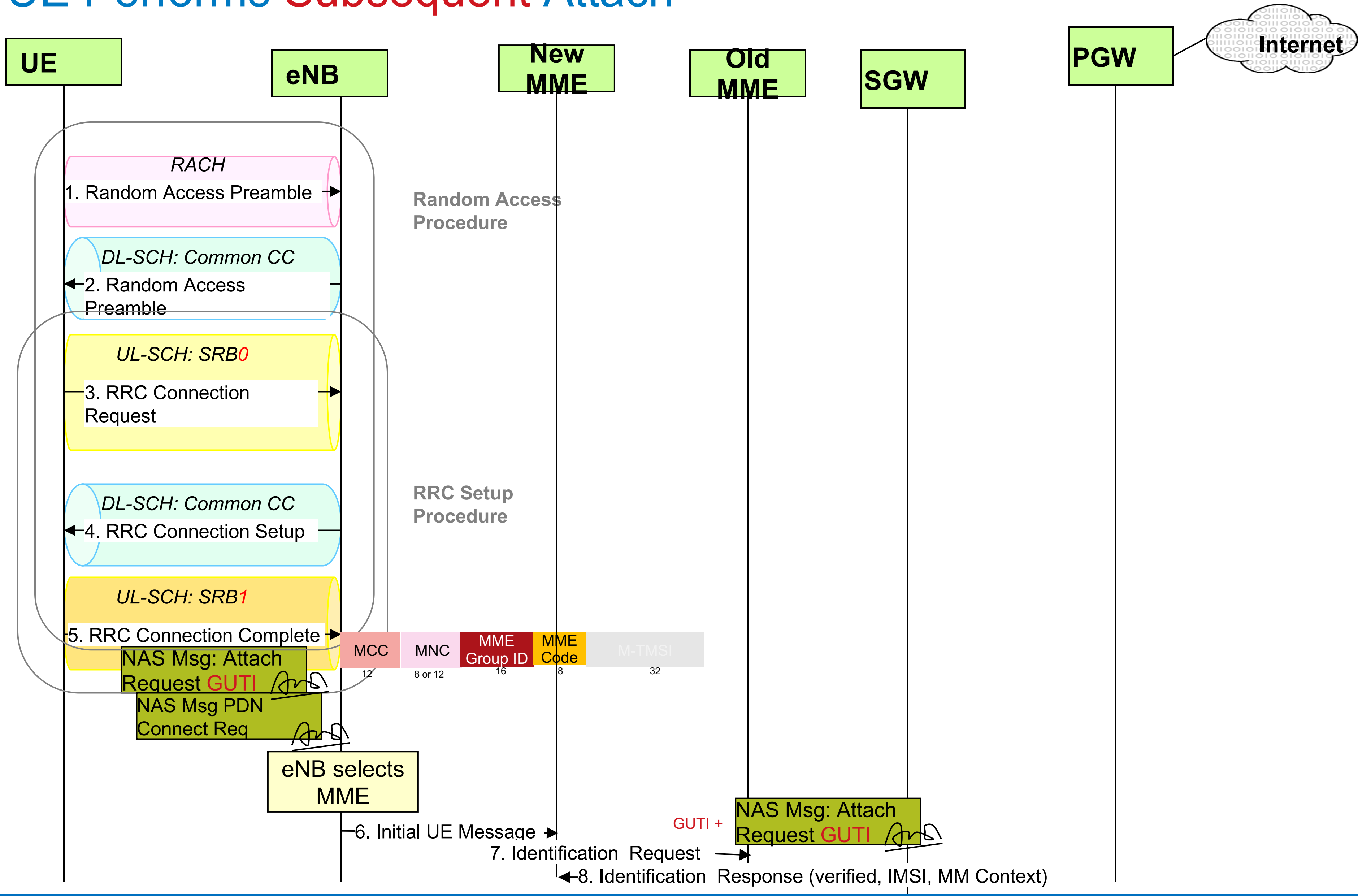
GTPC-1 Tunnel

Data Radio Bearer-10

GTPU-10 Tunnel

GTP-U-10 Tunnel

UE Performs Subsequent Attach



UE

eNB

New MME

Old MME

SGW

PGW

Internet

RACH

1. Random Access Preamble

DL-SCH: Common CC

2. Random Access Preamble

Random Access Procedure

UL-SCH: SRB0

3. RRC Connection Request

DL-SCH: Common CC

4. RRC Connection Setup

RRC Setup Procedure

UL-SCH: SRB1

5. RRC Connection Complete

MCC	MNC	MME Group ID	MME Code	M-TMSI
12	8 or 12	16	8	32

NAS Msg: Attach Request GUTI

NAS Msg PDN Connect Req

eNB selects MME

6. Initial UE Message

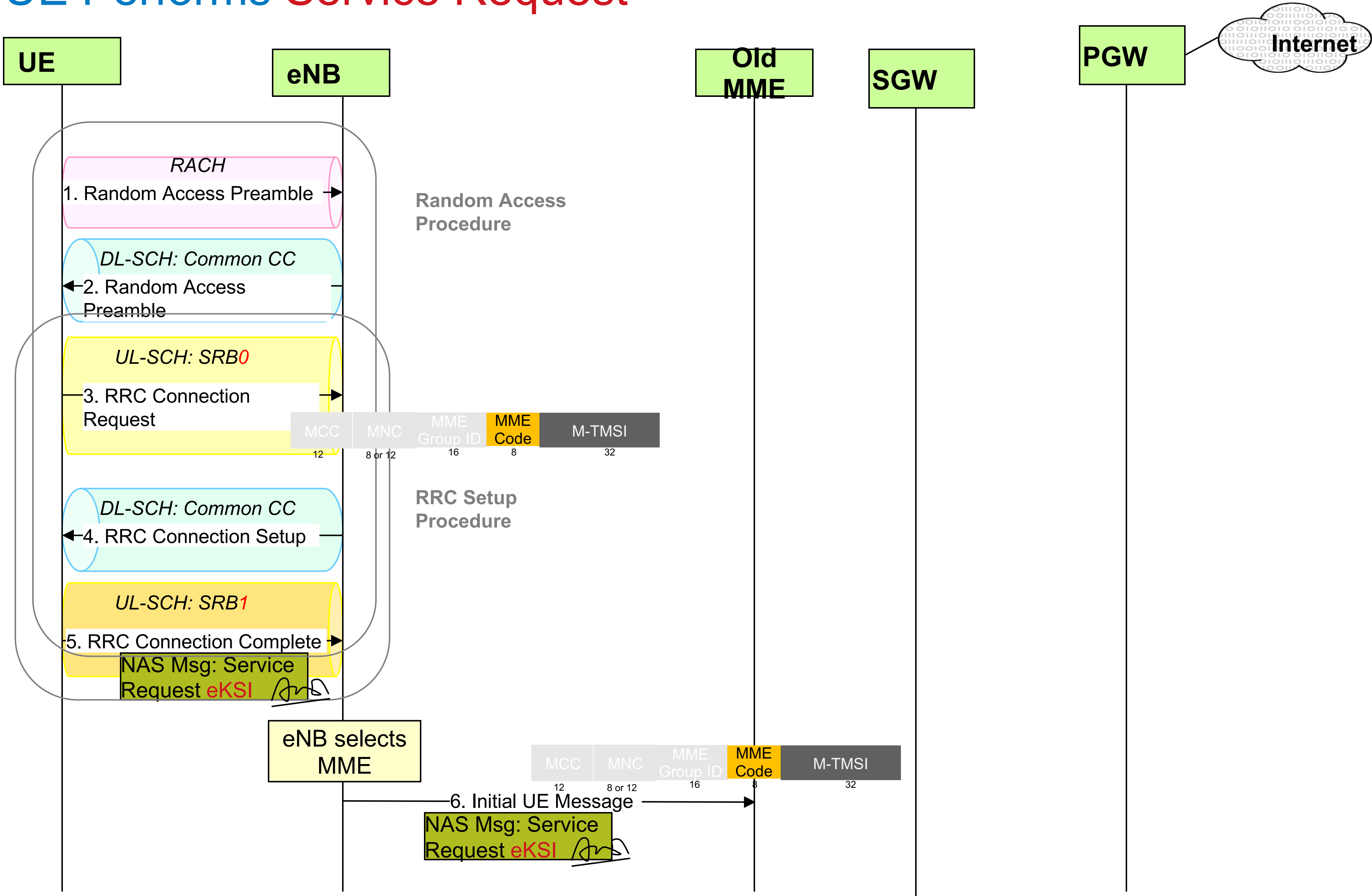
GUTI +

NAS Msg: Attach Request GUTI

7. Identification Request

8. Identification Response (verified, IMSI, MM Context)

UE Performs Service Request



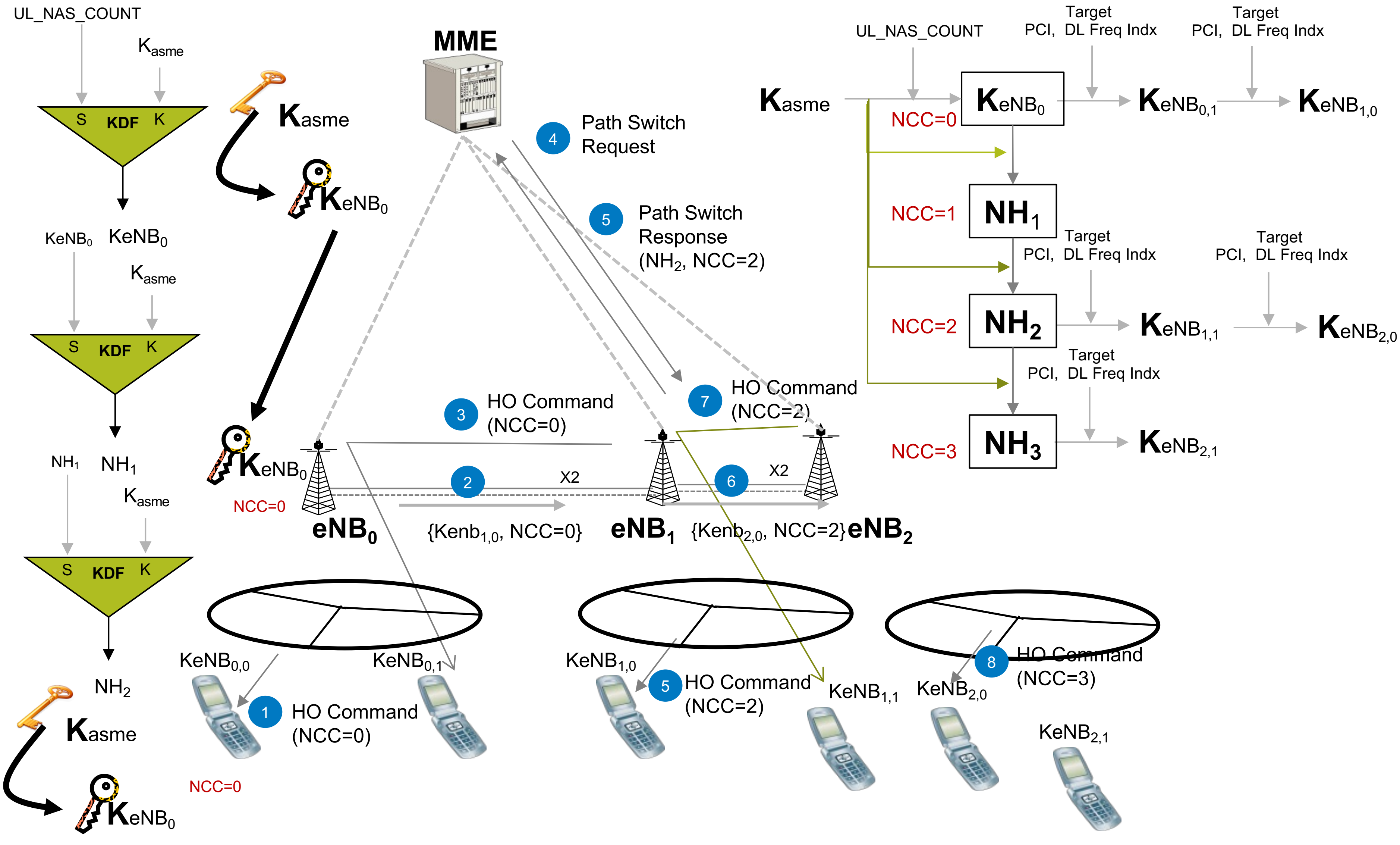
Specifications

- TS 33.401: LTE Security
- TS 33.210: Network Domain Security
- TS 33.220 Annex B: Key Derivation Function
- TS 33.102: 3G Security
- TS 35.206: 3GPP Authentication Algorithm (MILENAGE)

Security aspects of handovers

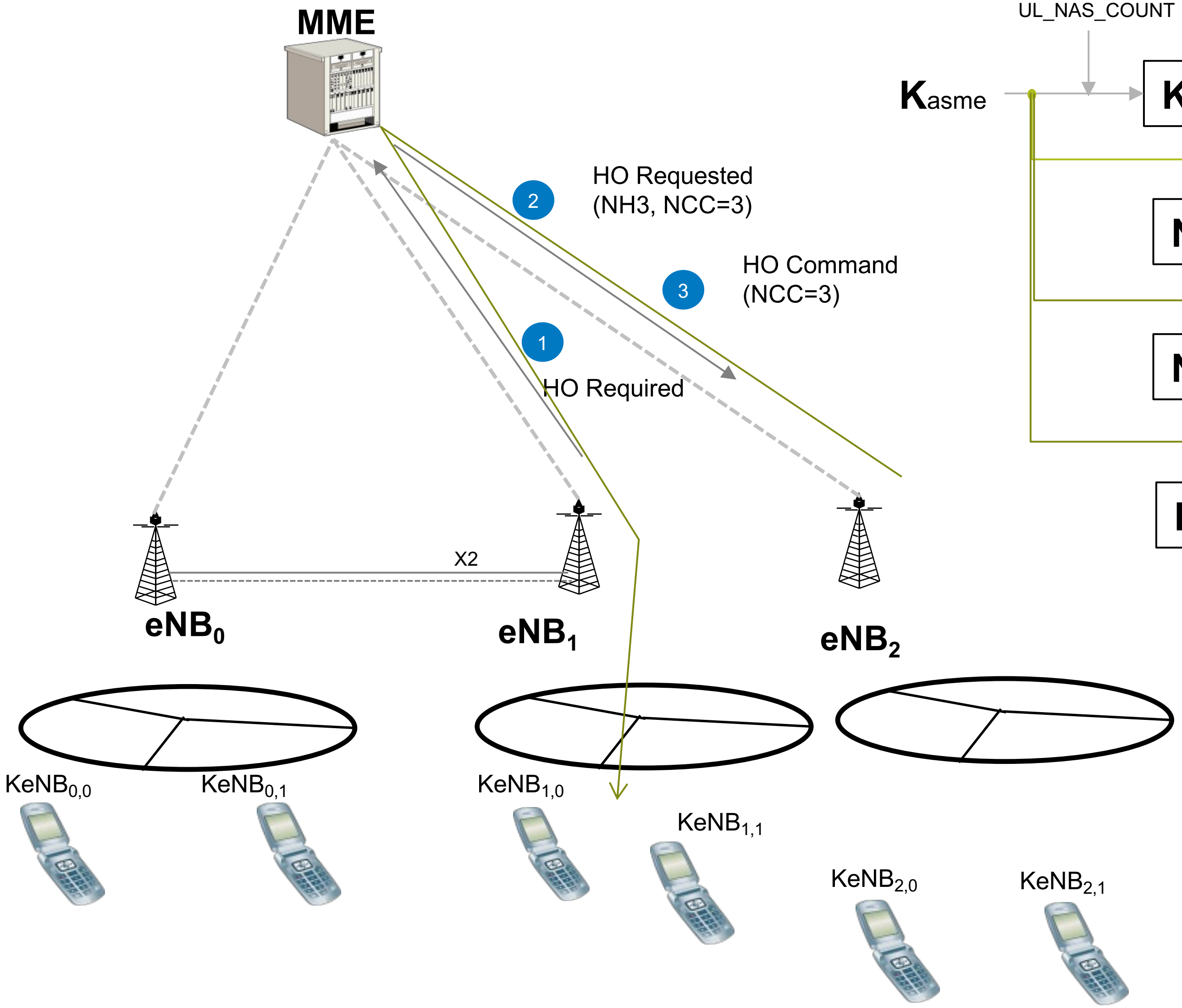
- Key Derivation
- PDCP count handling

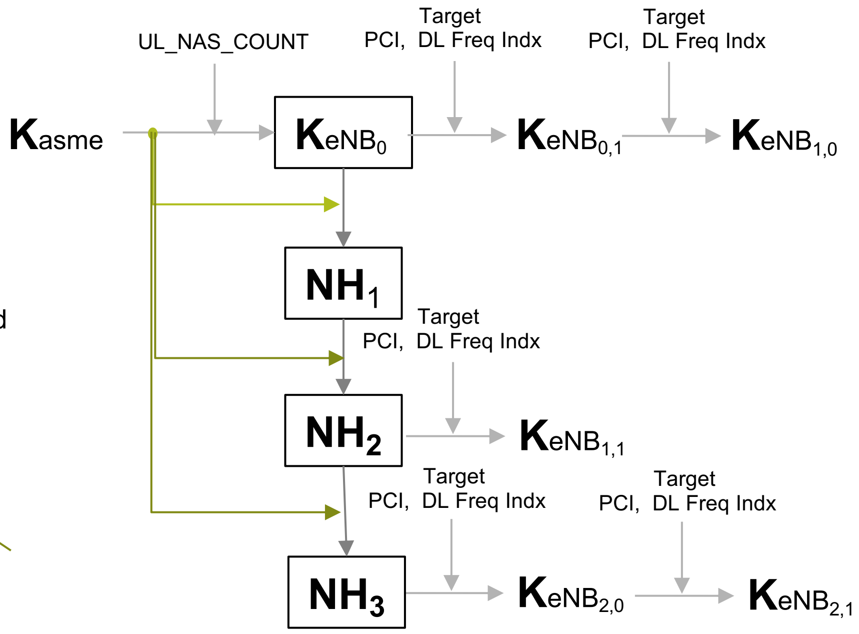
KeNB Key Derivation at Intra-eNB HO and X2 HO



PCI	Physical Cell Identity
EARFCN-DL	E-UTRAN Absolute Frequency Channel –DL
NH	Next Hop Parameter
NCC	NH Chaining Counter

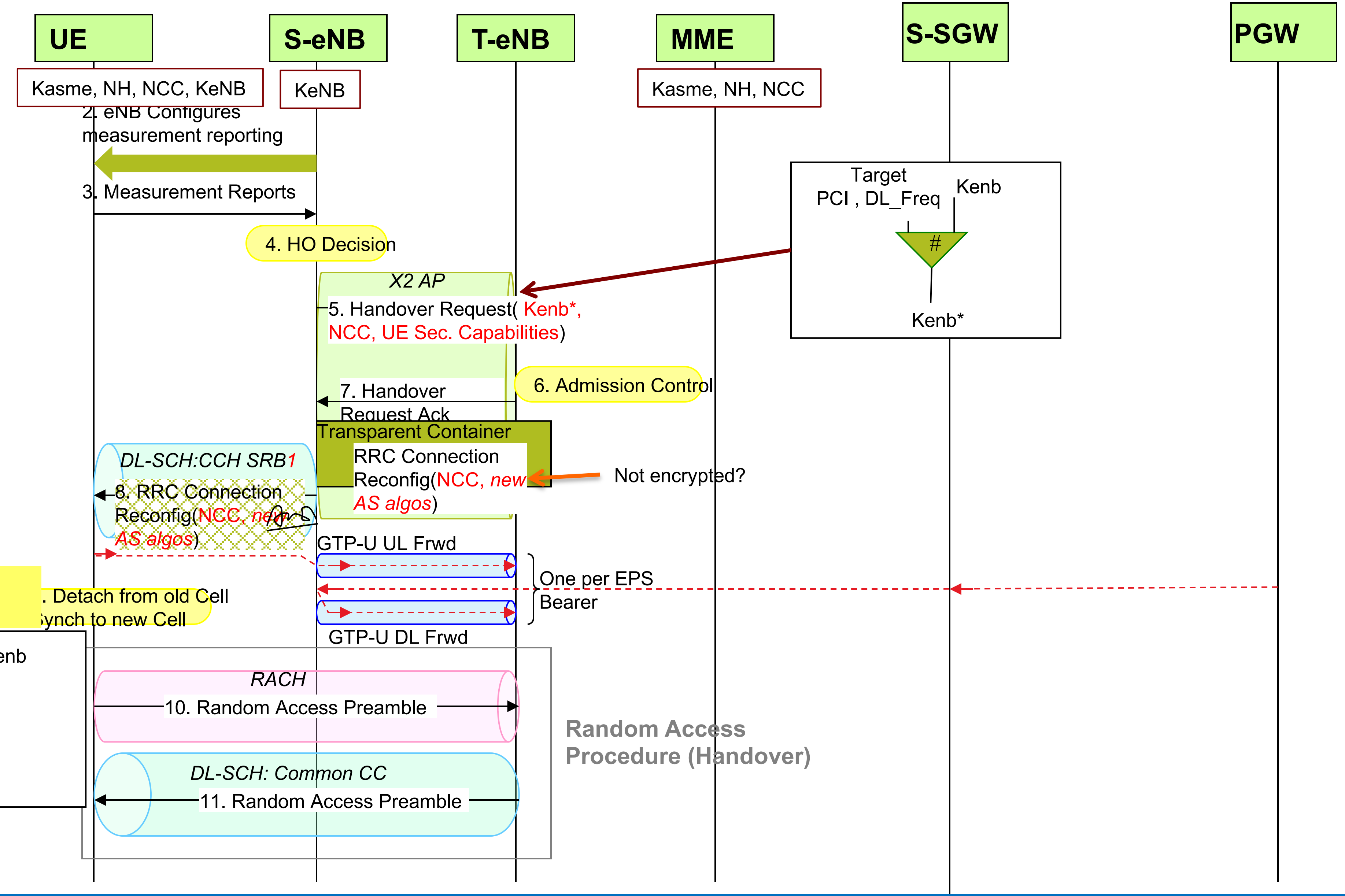
Kenb Key Derivation at S1 HO





PCI	Physical Cell Identity
EARFCN-DL	E-UTRAN Absolute Frequency Channel –DL
NH	Next Hop Parameter
NCC	NH Chaining Counter

1. Intra-eNB



UE

S-eNB

T-eNB

MME

S-SGW

PGW

Kasme, NH, NCC, KeNB

KeNB

Kasme, NH, NCC

2. eNB Configures measurement reporting

3. Measurement Reports

4. HO Decision

Target PCI , DL_Freq

Kenb

#

Kenb*

X2 AP

5. Handover Request(Kenb*, NCC, UE Sec. Capabilities)

6. Admission Control

7. Handover Request Ack

Transparent Container

RRC Connection Reconfig(NCC, *new AS algos*)

Not encrypted?

DL-SCH:CCH SRB1

8. RRC Connection Reconfig(NCC, *new AS algos*)

GTP-U UL Frwd

One per EPS Bearer

GTP-U DL Frwd

. Detach from old Cell

ynch to new Cell

enb

RACH

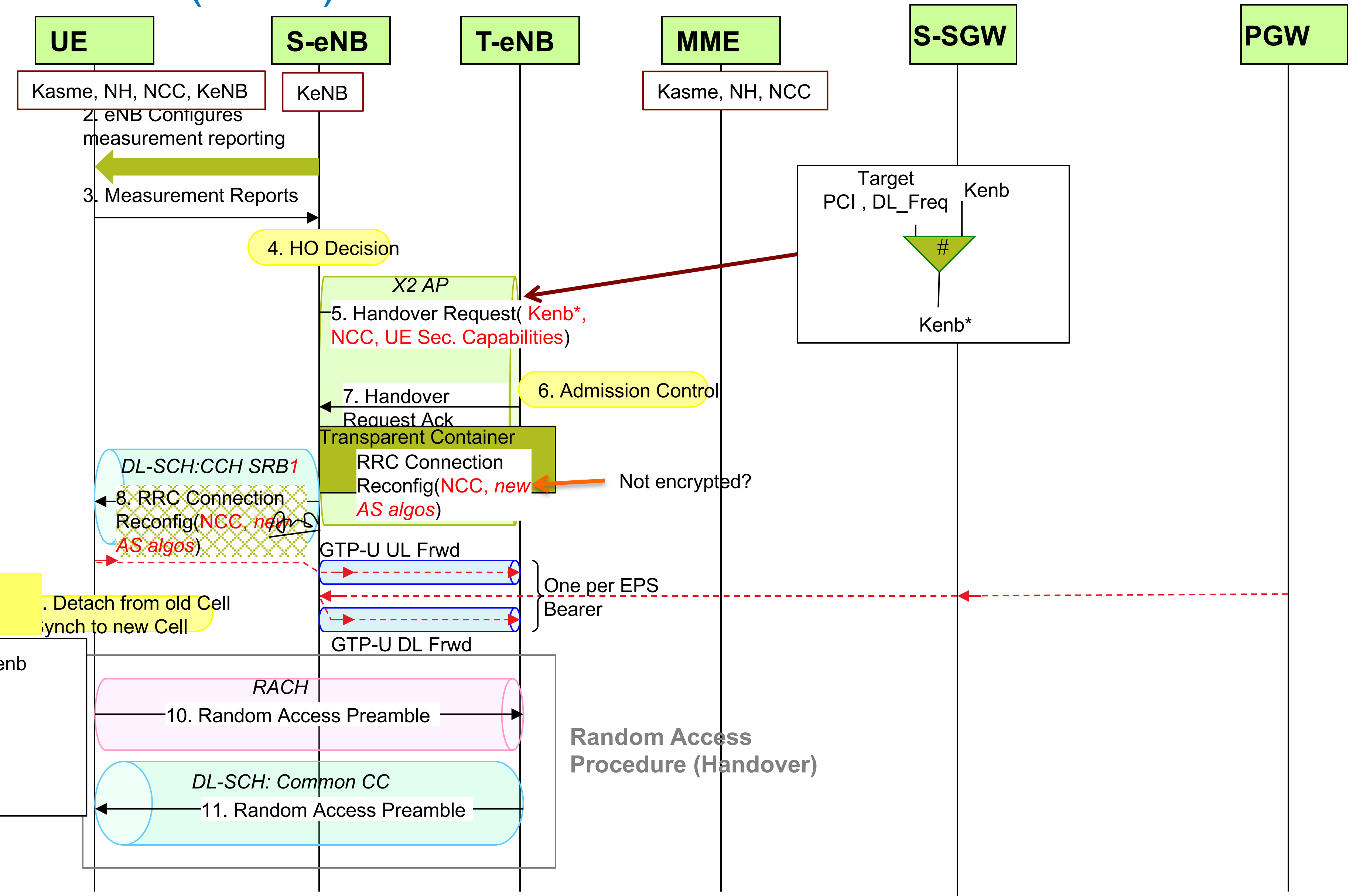
10. Random Access Preamble

DL-SCH: Common CC

11. Random Access Preamble

Random Access Procedure (Handover)

X2-HO (1 of 2)



UE

S-eNB

T-eNB

MME

S-SGW

PGW

Kasme, NH, NCC, KeNB

KeNB

Kasme, NH, NCC

2. eNB Configures measurement reporting

3. Measurement Reports

4. HO Decision

Target PCI , DL_Freq

Kenb

#

Kenb*

X2 AP

5. Handover Request(Kenb*, NCC, UE Sec. Capabilities)

6. Admission Control

7. Handover Request Ack

Transparent Container

RRC Connection Reconfig(NCC, *new AS algos*)

Not encrypted?

DL-SCH:CCH SRB1

8. RRC Connection Reconfig(NCC, *new AS algos*)

GTP-U UL Frwd

One per EPS Bearer

GTP-U DL Frwd

. Detach from old Cell

ynch to new Cell

enb

RACH

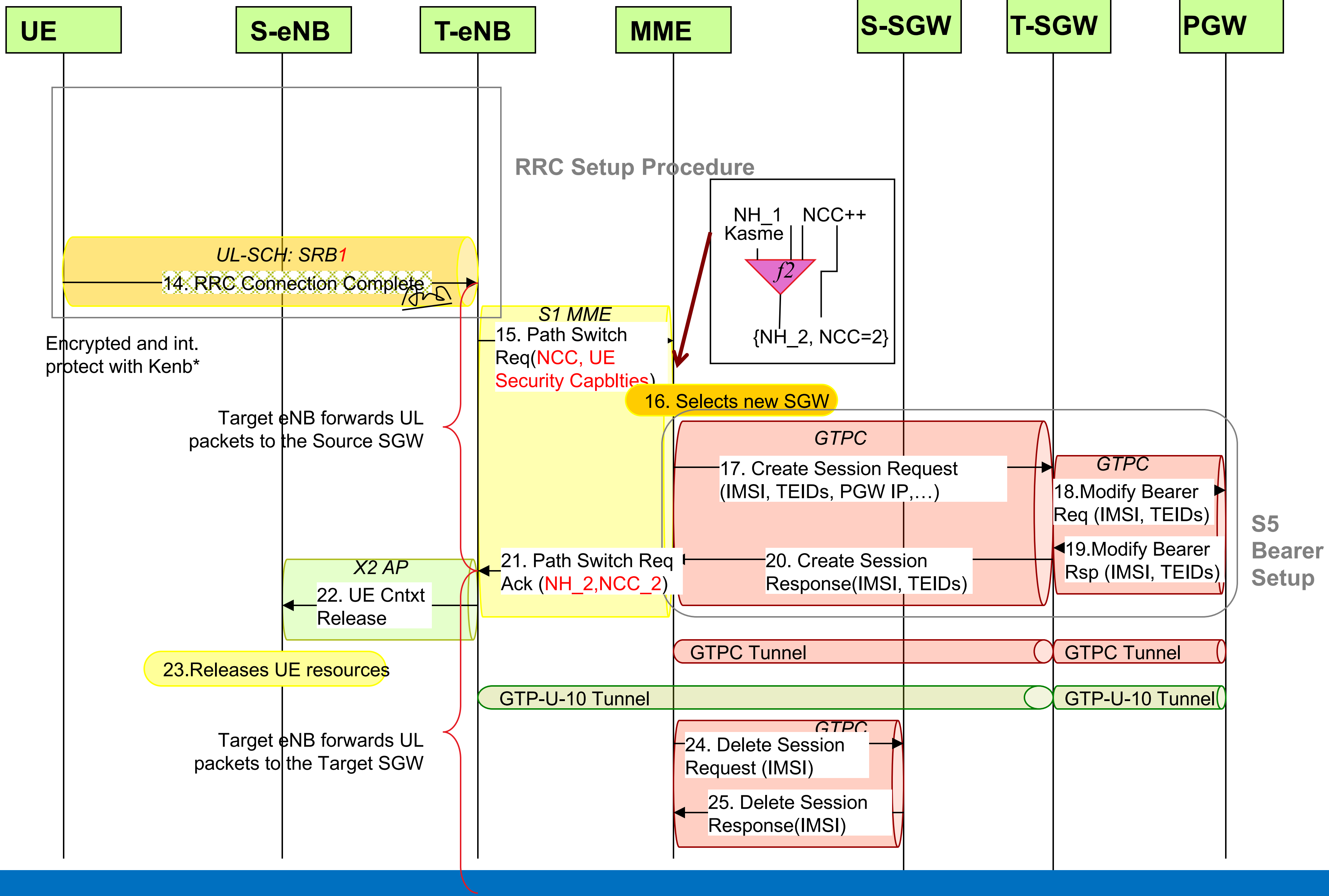
10. Random Access Preamble

DL-SCH: Common CC

11. Random Access Preamble

Random Access Procedure (Handover)

X2-HO (2 of 2)



UE

S-eNB

T-eNB

MME

S-SGW

T-SGW

PGW

RRC Setup Procedure

UL-SCH: SRB1

14. RRC Connection Complete

Encrypted and int. protect with Kenb*

S1 MME

15. Path Switch Req(NCC, UE Security Capblties)

NH_1 Kasme

NCC++

f2

{NH_2, NCC=2}

16. Selects new SGW

Target eNB forwards UL packets to the Source SGW

GTPC

17. Create Session Request (IMSI, TEIDs, PGW IP,…)

GTPC

18.Modify Bearer Req (IMSI, TEIDs)

19.Modify Bearer Rsp (IMSI, TEIDs)

20. Create Session Response(IMSI, TEIDs)

S5 Bearer Setup

X2 AP

21. Path Switch Req Ack (NH_2,NCC_2)

22. UE Cntxt Release

23.Releases UE resources

GTPC Tunnel

GTPC Tunnel

GTP-U-10 Tunnel

GTP-U-10 Tunnel

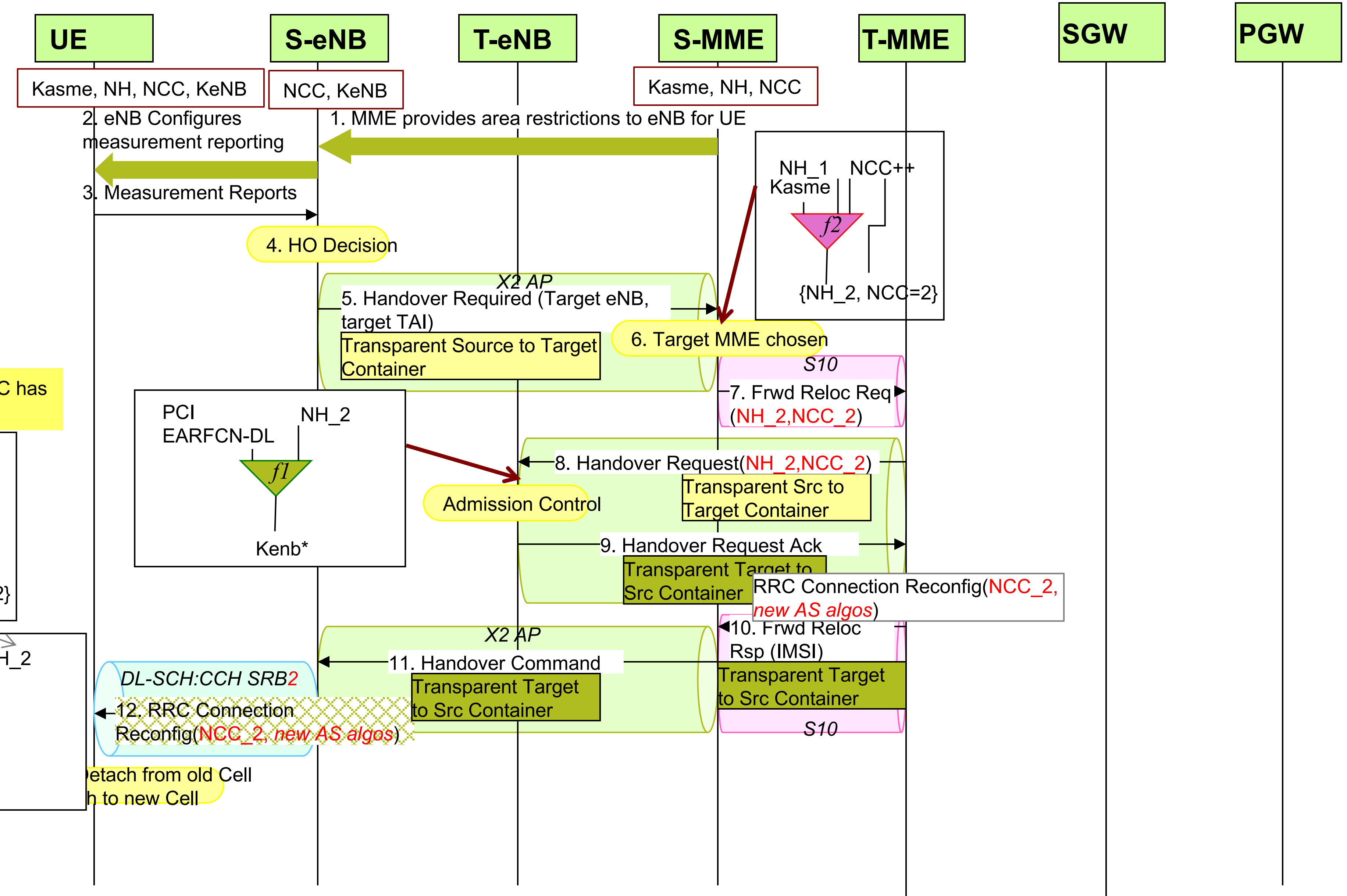
Target eNB forwards UL packets to the Target SGW

GTPC

24. Delete Session Request (IMSI)

25. Delete Session Response(IMSI)

S1-HO without Serving GW change (1 of 3)



UE

S-eNB

T-eNB

S-MME

T-MME

SGW

PGW

Kasme, NH, NCC, KeNB

NCC, KeNB

Kasme, NH, NCC

1. MME provides area restrictions to eNB for UE

2. eNB Configures measurement reporting

3. Measurement Reports

4. HO Decision

X2 AP

5. Handover Required (Target eNB, target TAI)

Transparent Source to Target Container

NH_1 NCC++

Kasme

f2

{NH_2, NCC=2}

6. Target MME chosen

S10

7. Frwd Reloc Req (NH_2,NCC_2)

C has

PCI

EARFCN-DL

NH_2

f1

Kenb*

2}

8. Handover Request(NH_2,NCC_2)

Transparent Src to Target Container

Admission Control

9. Handover Request Ack

Transparent Target to Src Container

RRC Connection Reconfig(NCC_2, *new AS algos*)

10. Frwd Reloc Rsp (IMSI)

Transparent Target to Src Container

S10

X2 AP

11. Handover Command

Transparent Target to Src Container

H_2

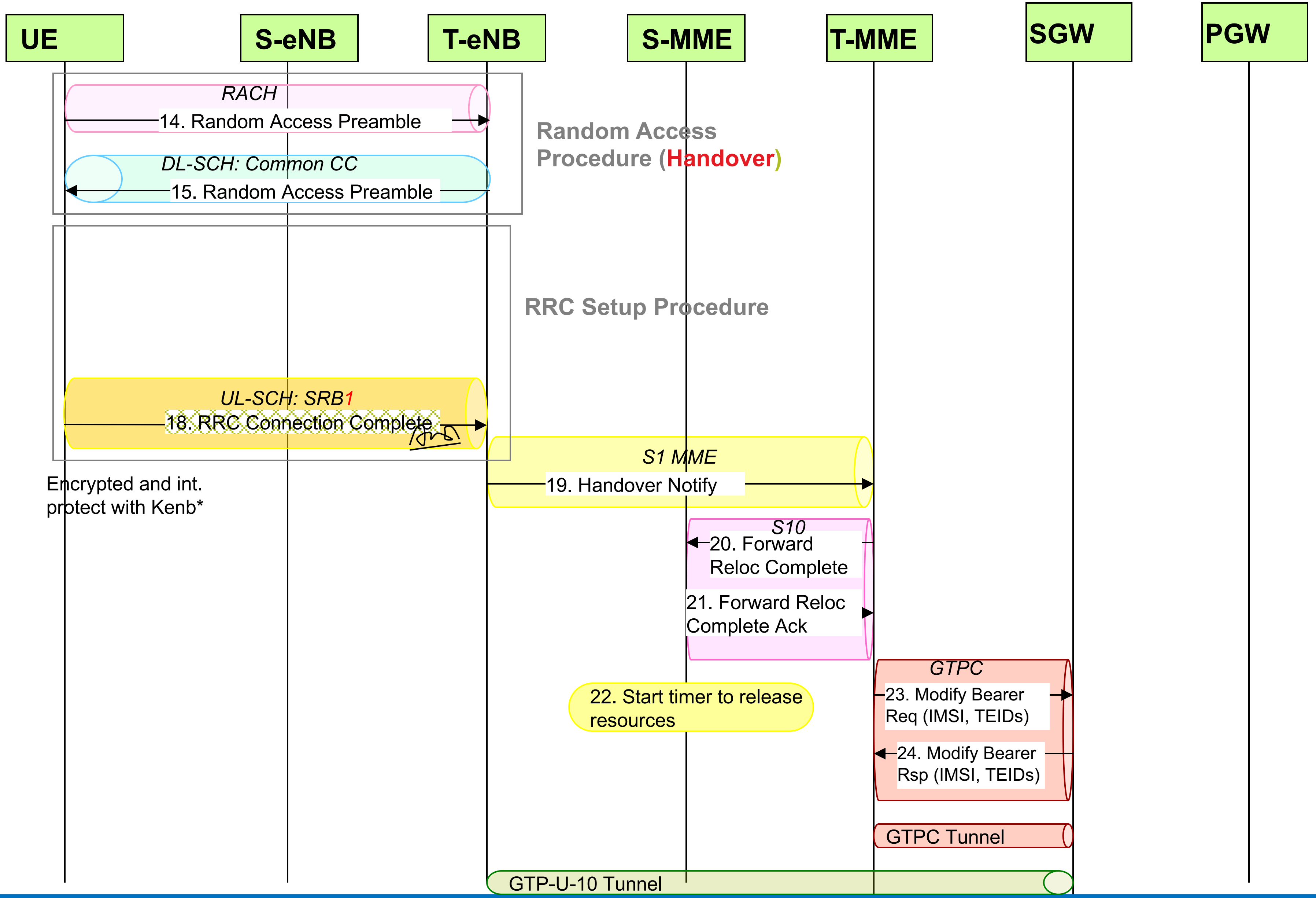
DL-SCH:CCH SRB2

12. RRC Connection Reconfig(NCC_2, *new AS algos*)

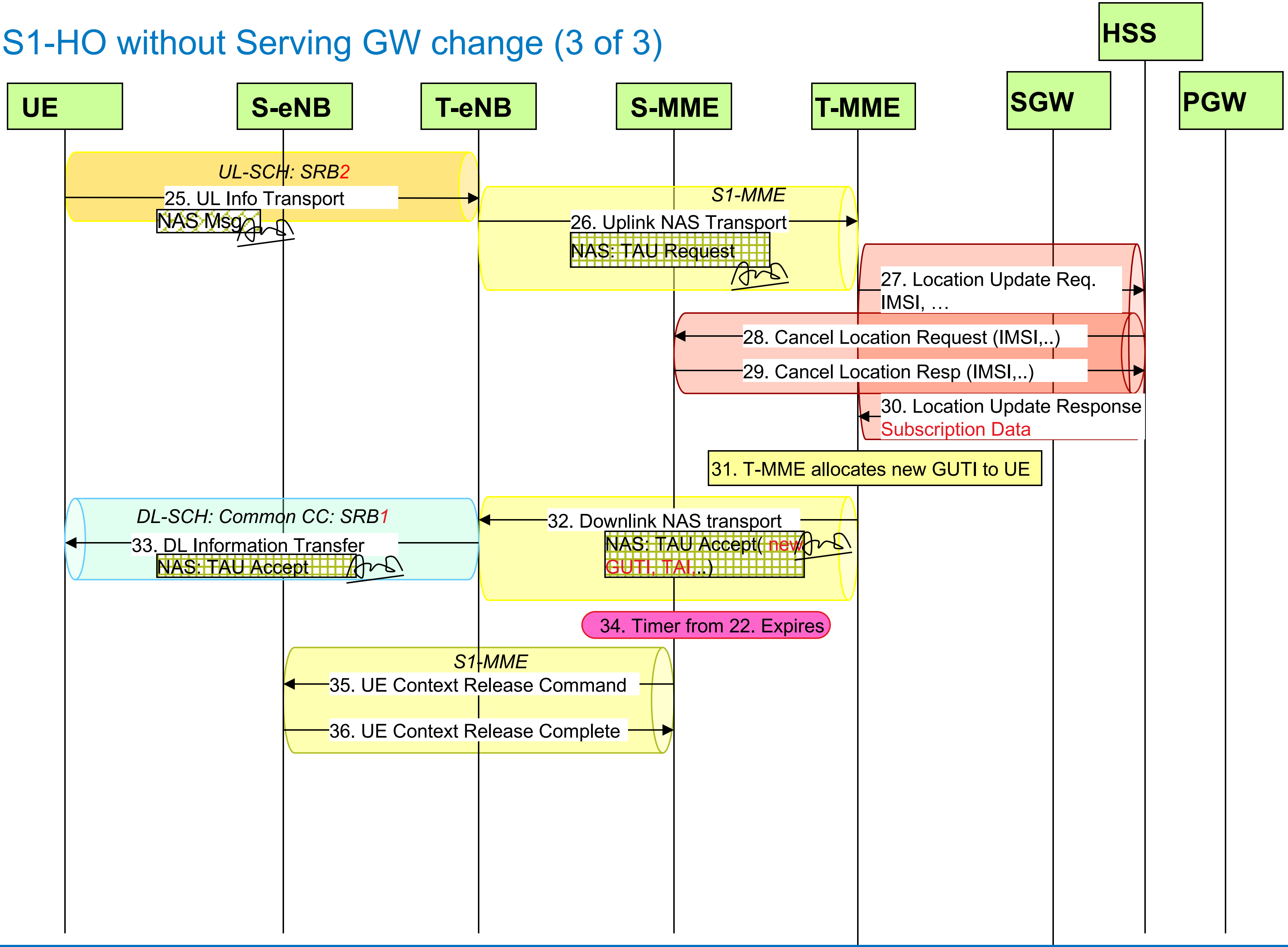
etach from old Cell

h to new Cell

S1-HO without Serving GW change (2 of 3)


UE
S-eNB
T-eNB
S-MME
T-MME
SGW
PGW
RACH
14. Random Access Preamble
DL-SCH: Common CC
15. Random Access Preamble
Random Access Procedure (Handover)
RRC Setup Procedure
UL-SCH: SRB1
18. RRC Connection Complete
S1 MME
19. Handover Notify
Encrypted and int. protect with Kenb*
S10
20. Forward Reloc Complete
21. Forward Reloc Complete Ack
22. Start timer to release resources
GTPC
23. Modify Bearer Req (IMSI, TEIDs)
24. Modify Bearer Rsp (IMSI, TEIDs)
GTPC Tunnel
GTP-U-10 Tunnel

S1-HO without Serving GW change (3 of 3)



HSS
UE
S-eNB
T-eNB
S-MME
T-MME
SGW
PGW
UL-SCH: SRB2
25. UL Info Transport
NAS Msg
S1-MME
26. Uplink NAS Transport
NAS: TAU Request
27. Location Update Req.
IMSI, …
28. Cancel Location Request (IMSI,..)
29. Cancel Location Resp (IMSI,..)
30. Location Update Response
Subscription Data
31. T-MME allocates new GUTI to UE
DL-SCH: Common CC: SRB1
33. DL Information Transfer
NAS: TAU Accept
32. Downlink NAS transport
NAS: TAU Accept(new GUTI, TAI,..)
34. Timer from 22. Expires
S1-MME
35. UE Context Release Command
36. UE Context Release Complete