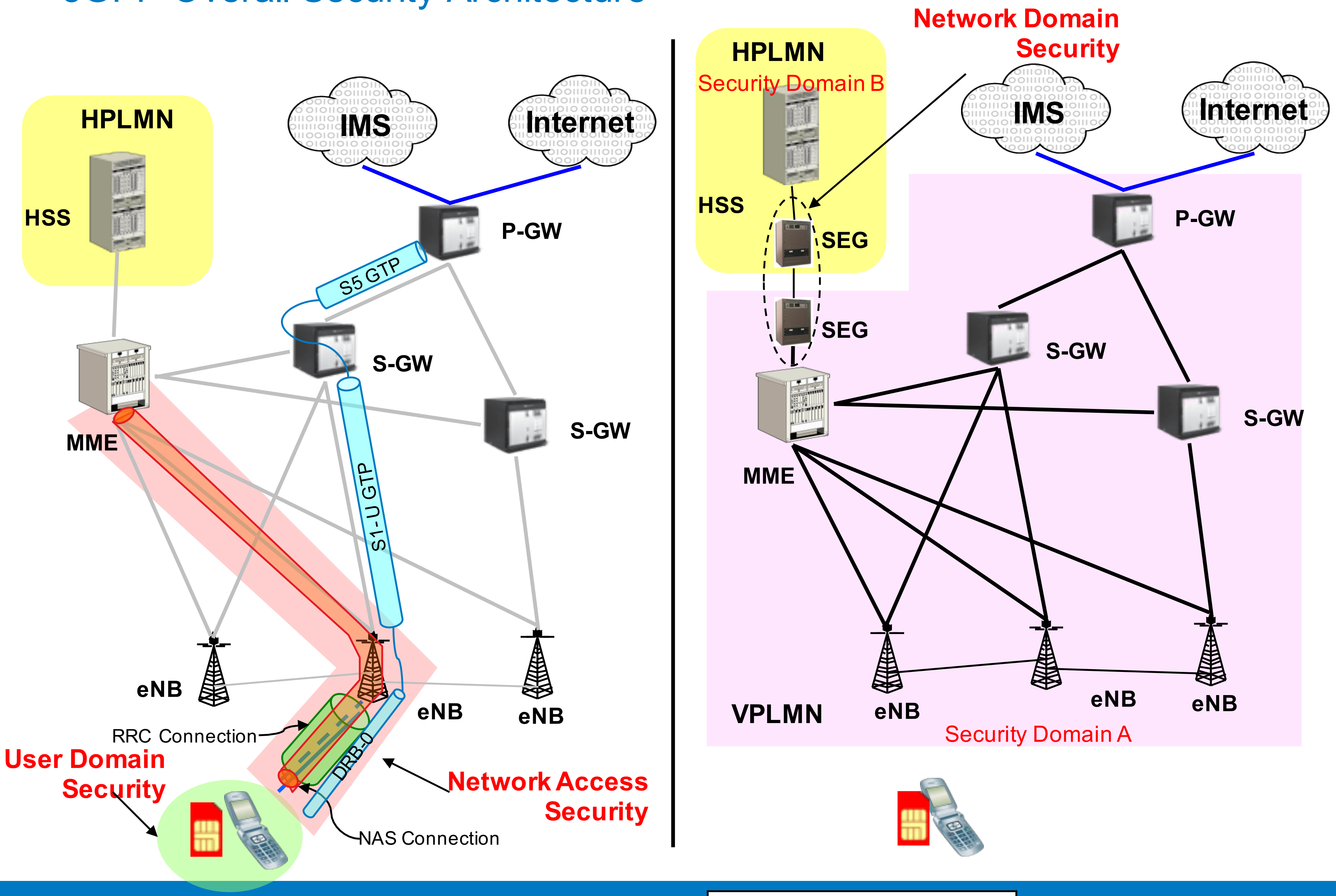
Security Framework for LTE

Irfan Ali

Overview

- ***Security in LTE***
  - Security Architecture for 3GPP
  - During Attach
    - Key Derivation
    - Mutual Authentication
    - NAS Security
    - AS Security
  - Handovers
    - Key derivation at target eNB

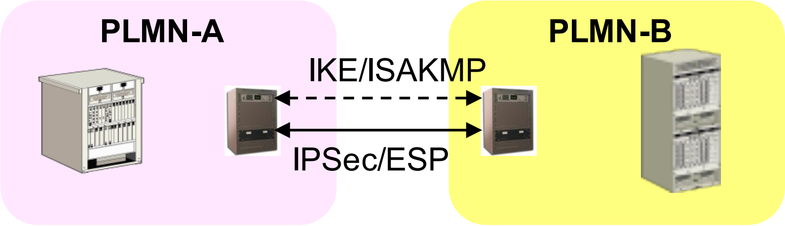
3GPP Overall Security Architecture



SEG	Security Gateway

3GPP Overall Security Architecture

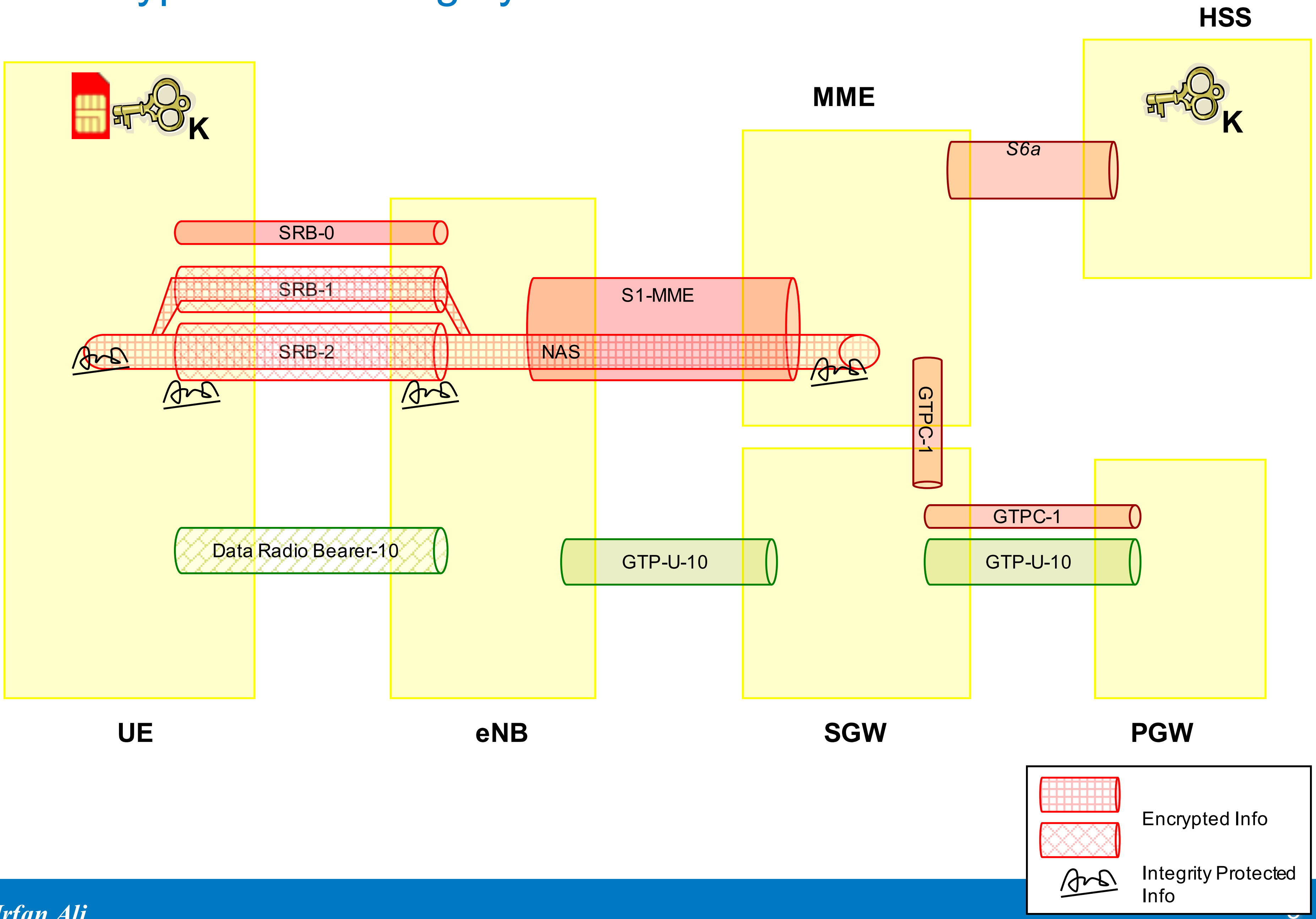
- ***Network Access Security***
  - Primarily radio link security
    - Encryption and Integrity protection of RRC
    - Encryption and Integrity protection of NAS
    - Encryption of Data Radio bearers (optional)
- ***Network Domain Security***
  - Security of the wireline network between PLMNs
    - Key negoation using IKE
    - Use of ISAKMP for setting up the security association between the SEG
    - Tunnel-mode ESP to be used
      - Encryption triple DES
      - Data Integrity and Authentication: MD5 and SHA-1
- ***User Domain Security***
  - User – USIM authentication:
    - Access to the USIM is restricted until the USIM has authenticated the user. Use of PIN. If user does not know PIN, user is not allowed to use SIM.
  - USIM – Terminal authentication
    - Used only for SIM-Locked Mobiles. When an ME is SIM-locked (SIM/USIM personalisation indicator in the ME to "on“), the ME stores the IMSI of the USIM. If the inserted USIN has a different IMSI, the ME goes into a emergency call only mode. Ref TS 22.022 Section 8.



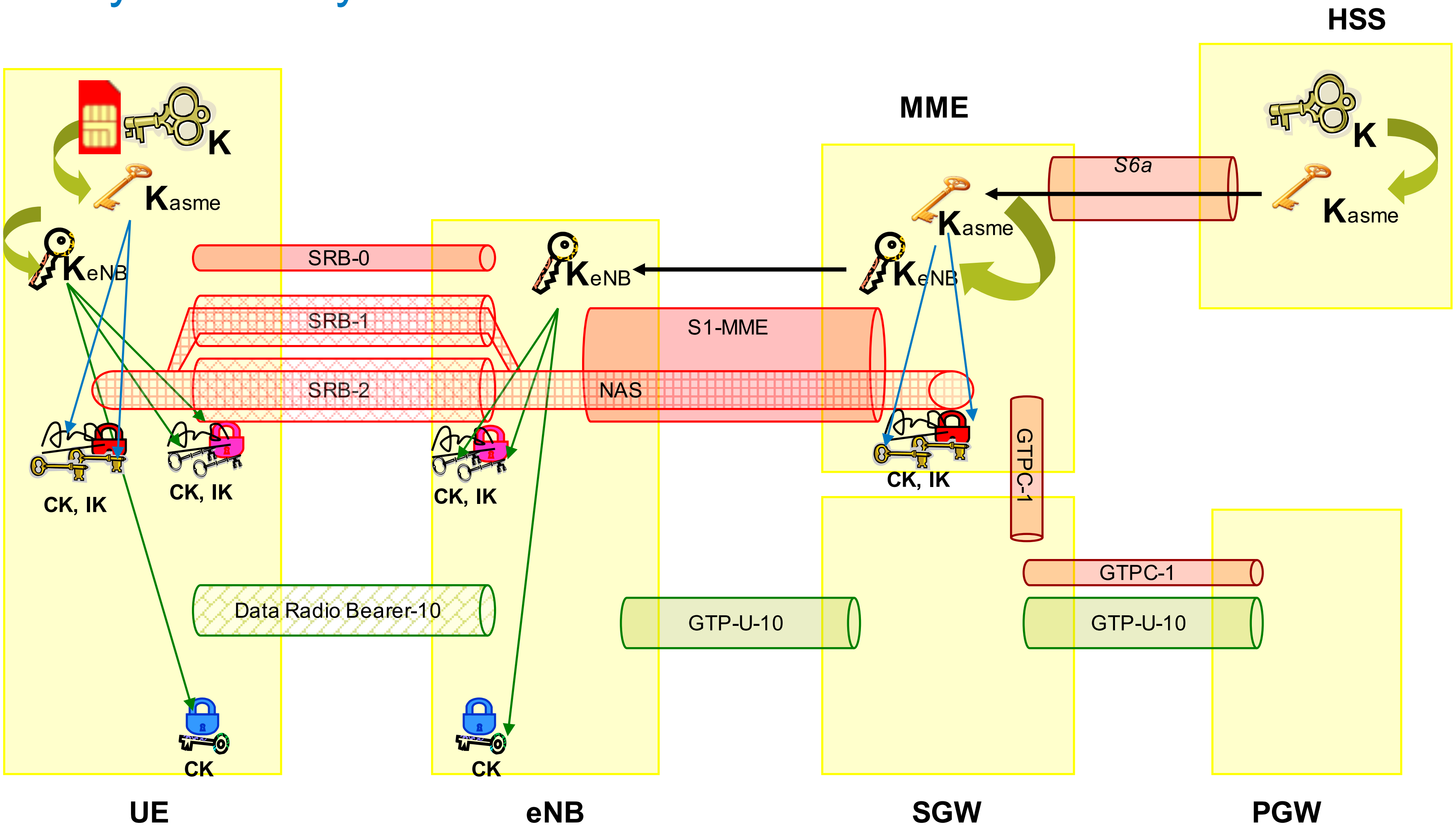
- <u>NOTE</u>: Maintaining Security on wired links within a security domain (i.e PLMN ,eg between eNB and MME) is responsibility of operator. Only recommendations in 3GPP Specifications.
  - In general, either links should be either physically secured or through IPSec (NDS/IP)

IKE	Internet Key Exchange
ISAKMP	Internet Security Association and Key Management Protocol
ESP	Encapsulation Security Protocol
IPSec	IP Security

Encryption and Integrity Protection used in LTE



Key Heirarchy for LTE

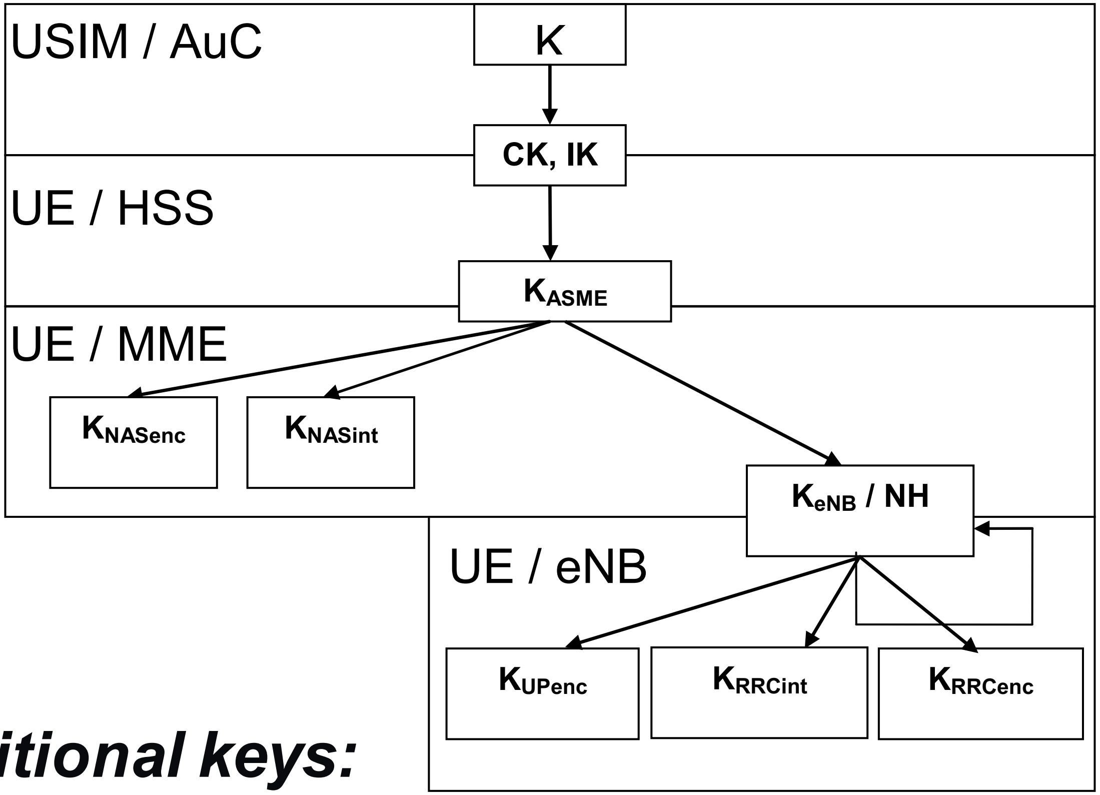


▦ ▨ Encrypted Info

Integrity Protected Info

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

LTE Key Hierarchy



- ***ASME** = **Access Security Management Entity, located at the MME***

- ***There are one additional keys:***
  - NH (Next Hop) is a key derived by ME and MME to provide forward security

Identity Protection

- ***The two permanent identities of UE are:***
  - IMSI (subscriber identity)
    - Seldom send over the air (only during attach, if no other valid temporary ID is present in the UE).
    - Temporary identities used instead (S-TMSI, GUTI)
  - IMEI (hardware identity)
    - Only sent to MME (in NAS), not to eNB.
    - Sent only after NAS security is setup (i.e encrypted and integrity protected).

S-TMSI	System architecture evolution Temporary Mobile Subscriber Identity
GUTI	Globally Unique Temporary Identity

General Security Characteristics

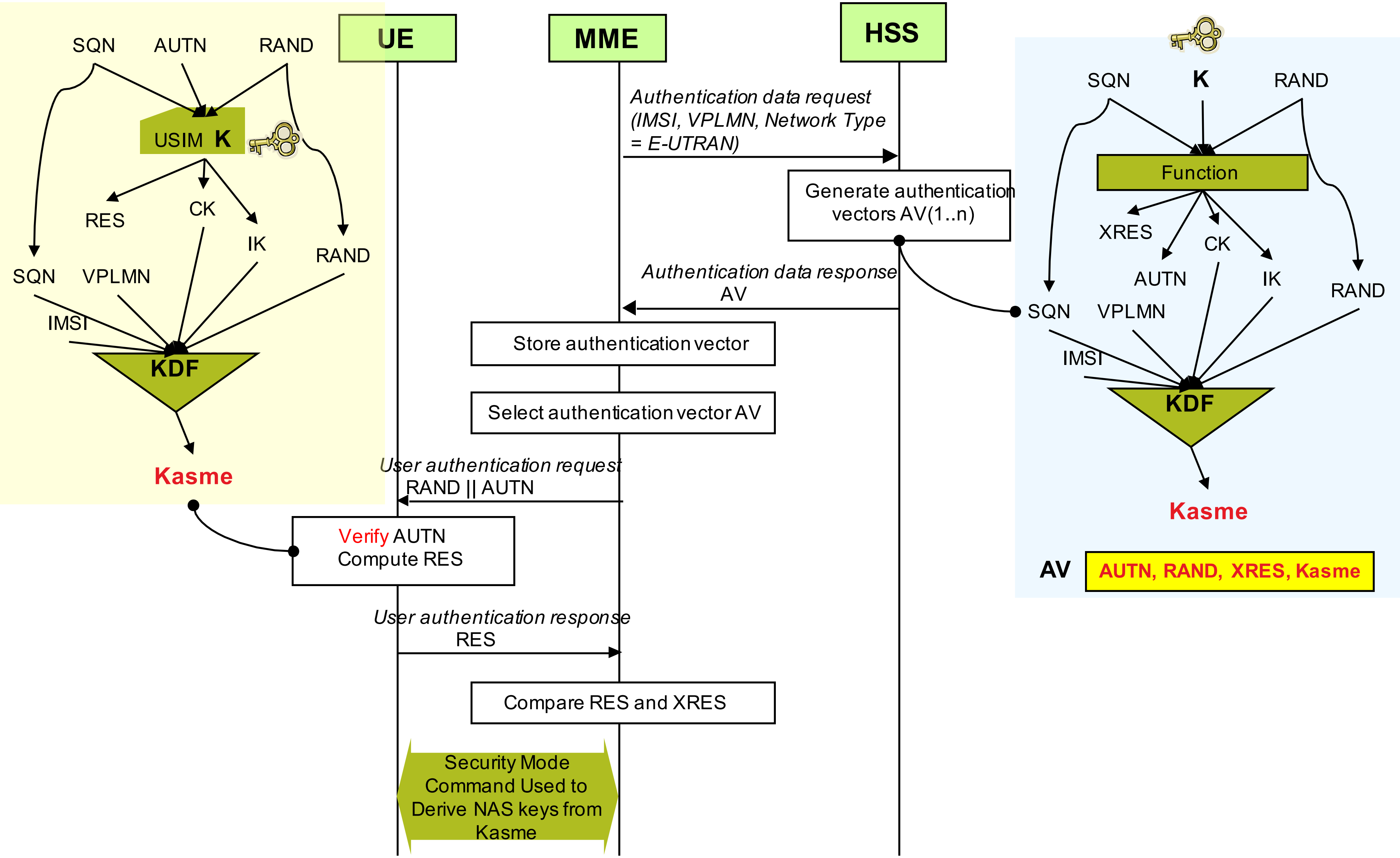
- ***Use of UMTS AKA (Authentication and Key Agreement) procedure***
- ***Use of 128-bit keys truncated from generated 256-bit keys***
- ***Ciphering Algorithms (AS and NAS):***
  - 0 = Null;
  - 1= SNOW 3G;
  - 2 = AES
- ***Integrity Algorithms (AS, NAS):***
  - 1= SNOW 3G;
  - 2 = AES

Rel-8 UE is required to support these algorithms

- ***Access Stratum (AS), between eNB and UE:***
  - Ciphering applicable to both user traffic and RRC-level signaling traffic.
  - Integrity protection applicable only to RRC-level signaling traffic. Integrity information is ciphered.
  - Located at the PDCP sublayer in both eNB and UE
- ***Non-Access Stratum (NAS), between MME and UE:***
  - Ciphering and Integrity of NAS messages, independent of the AS security
- ***Keys change at every intra-E-UTRAN handover, including intra-eNB handovers.***

AES	Advanced Encryption Standard

LTE AKA



SQN AUTN RAND

USIM K

RES CK IK RAND

SQN VPLMN IMSI

KDF

Kasme

UE

MME

HSS

Authentication data request (IMSI, VPLMN, Network Type = E-UTRAN)

Generate authentication vectors AV(1..n)

Authentication data response AV

Store authentication vector

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 NAS keys from Kasme

SQN K RAND

Function

XRES CK AUTN IK RAND

SQN VPLMN IMSI

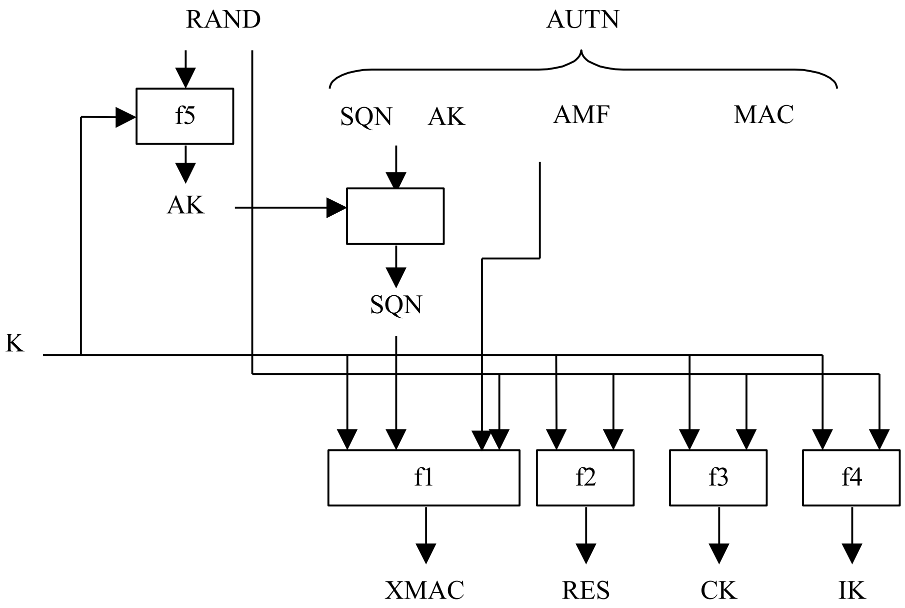
KDF

Kasme

AV **AUTN, RAND, XRES, Kasme**

AUTN	Authentication TokeN
GUTI	Globally Unique Temporary Identity
KSI	Key Set Identifier

User authentication function in the USIM



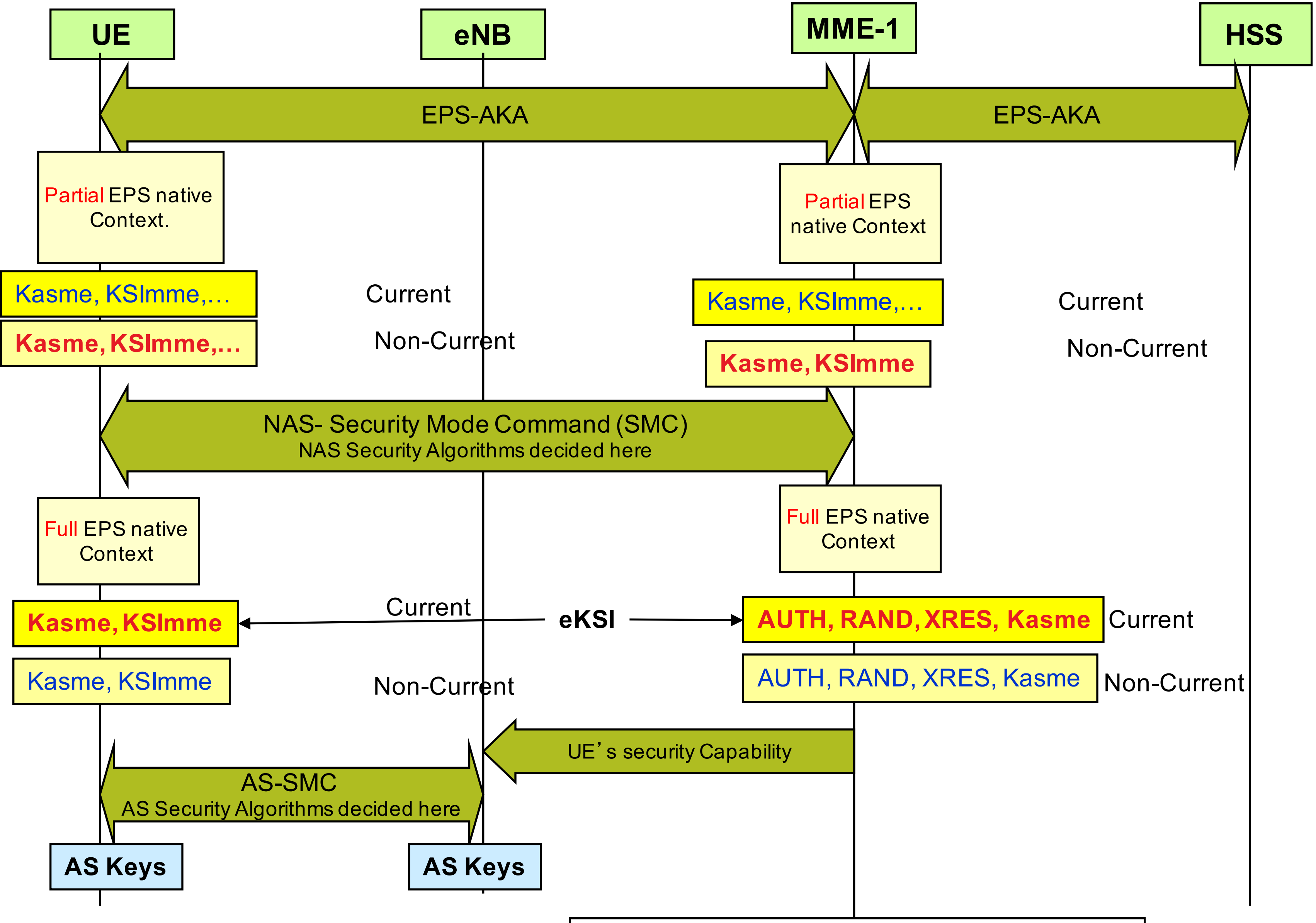
Verify MAC = XMAC

Verify that SQN is in the correct range

- USIM keeps track of last SQN received, SQNms
- USIM only accepts a sequence number from HSS if |SQN – SQNms | < Δ

AUTN	Authentication TokeN
AMF	Authentication management field
SQN	Sequence Number
AK	Anonymity Key
MAC	Message Authentication Code

Overview of NAS and AS Security negotiations

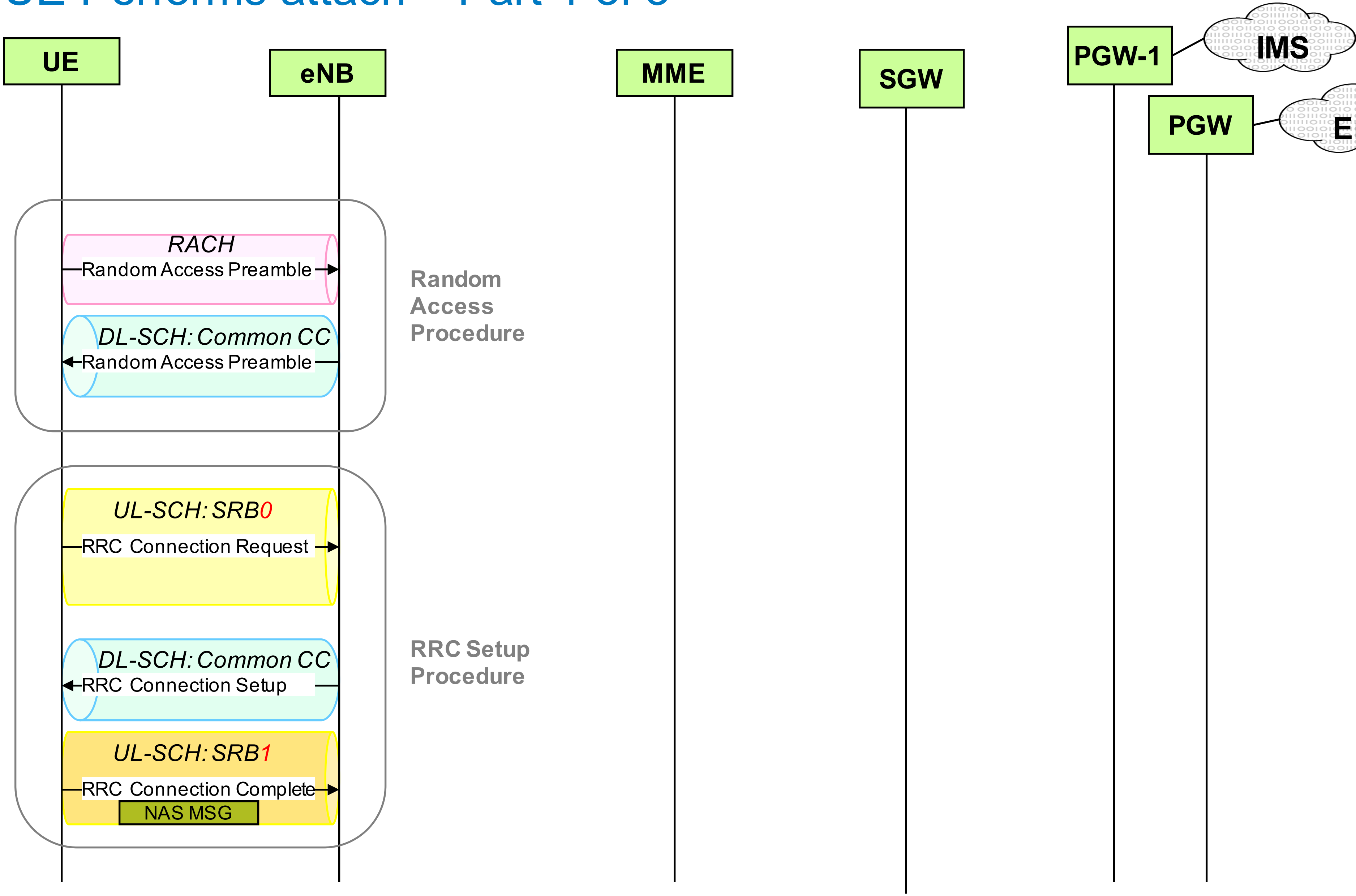


ASME Access Security Management Entity (MME)
KSI Key Set Identifier

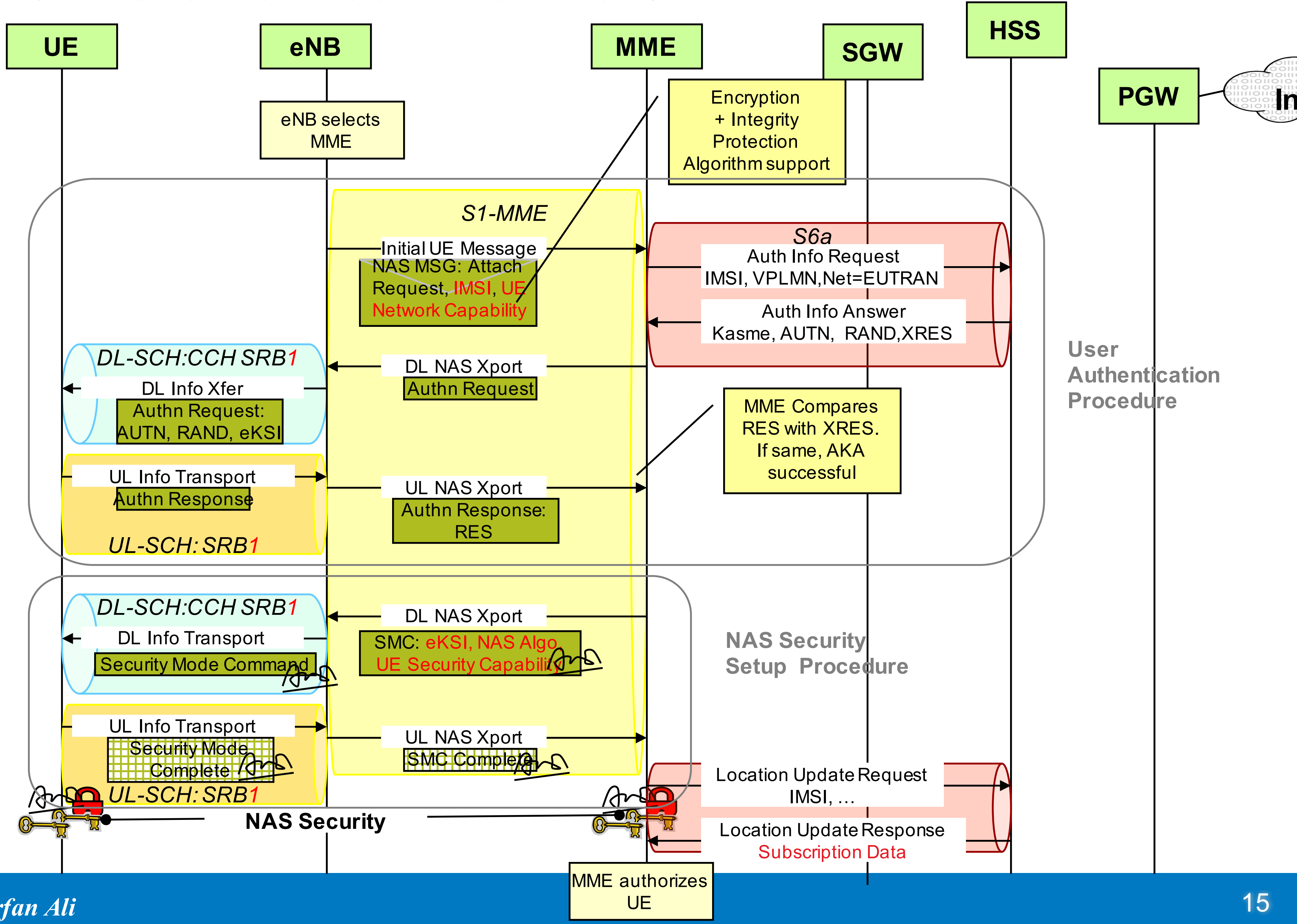
Negotiation of NAS/AS Enc & Inc Algorithm

- ***ME provides support of different EPS encryption (EEA) and integrity protection (EIA) algorithm support as part of "UE Network Capability" IE.***
  - ➡ The same set of ciphering and integrity algorithms shall be supported by the UE both for AS and NAS level
- ***The eNB and MME are configured with a prioritized list of EEA and EIA algorithms to use. Eg***
  - ➡ Priority-0 EIA2
  - ➡ Priority-1: EIA1
- ***eNB/MME selects first intersection of configured algorithm with UE's capability.***
- ***NAS and AS security algorithms can be different.***

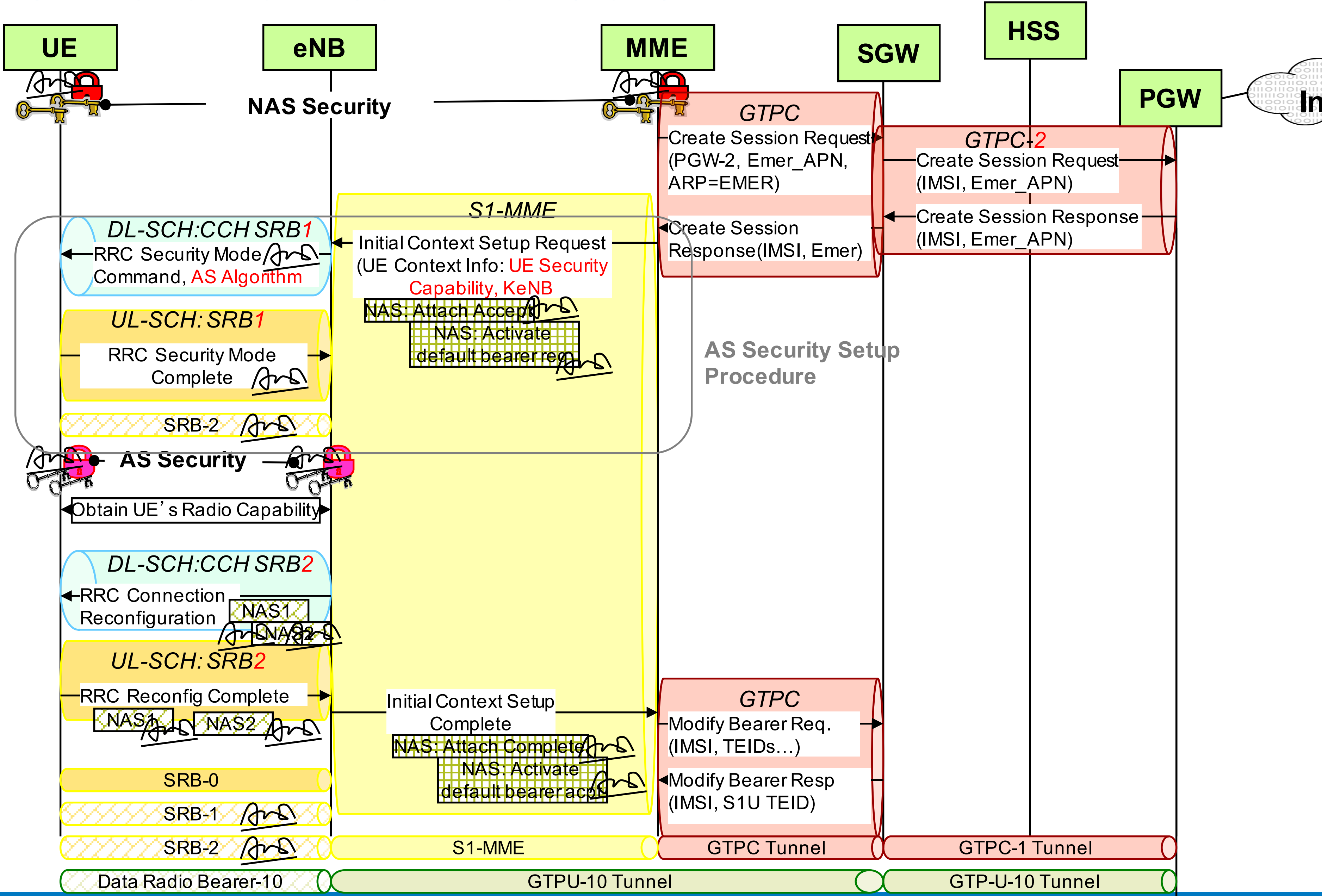
UE Performs attach – Part 1 of 3



UE Performs Attach – Part 2 of 3



UE Performs Attach – Part 3 of 3



UE

eNB

MME

SGW

HSS

PGW

In

NAS Security

GTPC

Create Session Request

(PGW-2, Emer_APN, ARP=EMER)

GTPC-2

Create Session Request

(IMSI, Emer_APN)

Create Session Response

(IMSI, Emer_APN)

Create Session Response(IMSI, Emer)

S1-MME

Initial Context Setup Request

(UE Context Info: UE Security Capability, KeNB

NAS: Attach Accept

NAS: Activate default bearer req

DL-SCH:CCH SRB1

RRC Security Mode Command, AS Algorithm

UL-SCH: SRB1

RRC Security Mode Complete

SRB-2

AS Security Setup Procedure

AS Security

Obtain UE's Radio Capability

DL-SCH:CCH SRB2

RRC Connection Reconfiguration

NAS1

NAS2

UL-SCH: SRB2

RRC Reconfig Complete

NAS1

NAS2

Initial Context Setup Complete

NAS: Attach Complete

NAS: Activate default bearer acpt

GTPC

Modify Bearer Req. (IMSI, TEIDs…)

Modify Bearer Resp (IMSI, S1U TEID)

SRB-0

SRB-1

SRB-2

S1-MME

GTPC Tunnel

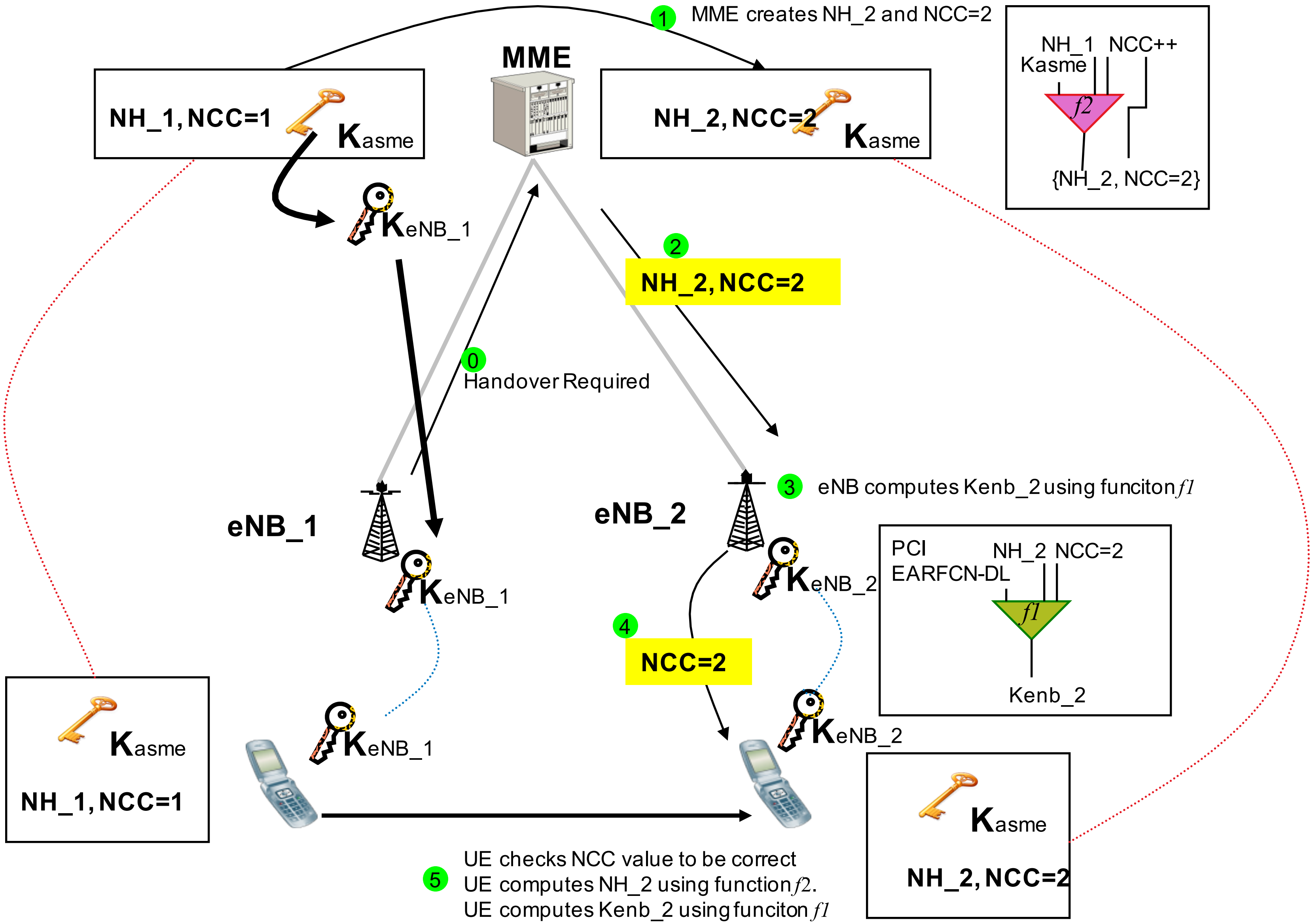
GTPC-1 Tunnel

Data Radio Bearer-10

GTPU-10 Tunnel

GTP-U-10 Tunnel

Kenb Key Derivation at S1 Handover



1 MME creates NH_2 and NCC=2

3 eNB computes Kenb_2 using funciton *f1*

5 UE checks NCC value to be correct
UE computes NH_2 using function *f2*.
UE computes Kenb_2 using funciton *f1*

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

Power-off/Power-on issue

Power-off

- The objective is to store a fully valid native EPS security context, preferably in USIM otherwise in non-volatile memory of the ME.

Power-on

- Retrieve a “valid” EPS security context either from (a) USIM, or (b) if-not from ME non-volatile memory. This becomes the current EPS security context.
- If no valid EPS security context can be retrieved, UE signals to MME in attach that it has “no valid keys”.

Specifications

- ***TS 33.401 – LTE Security***
- ***TS 33.102 – 3G Security***