LTE Security Tutorial

TKK 2009-12-09

T-110.5120

Dan Forsberg

dan@forsberg.fi

http://forsberg.fi/

Topics

1. General: Mobile Network Security
2. LTE Security Architecture
3. Authentication and Security Setup
4. Intra-LTE Mobility Security
5. Intersystem Mobility Security

1. General: Mobile Network Security

Terminology

- **Non-repudiation**
  - kiistattomuus (finnish)
  - Something that can not be denied

- **Service Theft**
  - Stealing service from others or from the service provider

Why Mobile Network Security?

- Main goal is to secure the business and services
  - Protect business models and services
  - Sufficient non-repudiation of charging
  - Privacy: user identity and data confidentiality
  - Sufficiently future proof as a design goal
  - Regulatory requirements (Legal Interception)
  - Perceived security
  - …

How to Apply Security?

- Goal is to minimize risks and reduce the number of security threats
- Need to be interoperable with legacy systems (e.g. UMTS and GSM)
- Need to be cost efficient and with high performance
- Practical design issues
  - Network architecture decisions influence design/complexity of security but also other way around in the early phase…
  - Standardization challenges, schedule (especially with security)
  - Link layer or application layer security or both?
  - End-to-end or hop-by-hop security?
  - What is good enough?

→ LTE Main Security Objectives

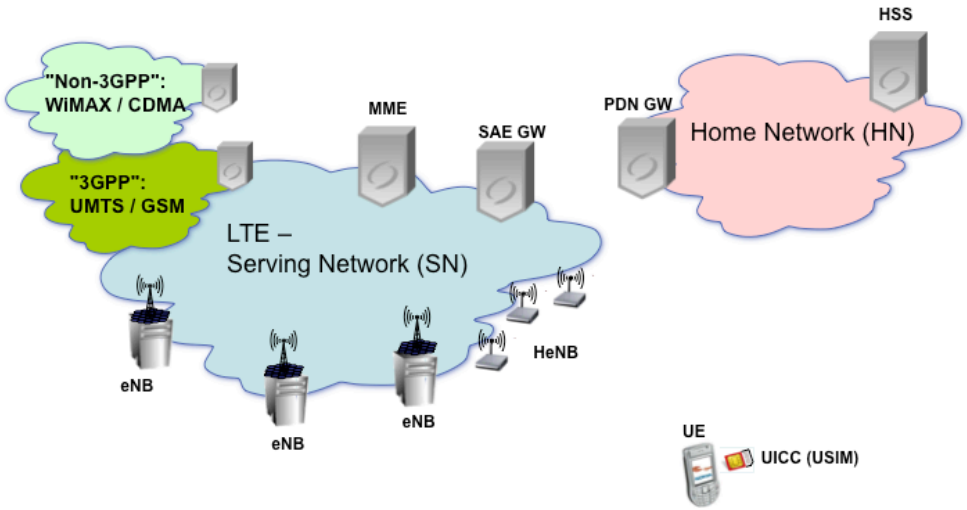
1. User and network authentication
2. Signaling data integrity
3. User data and signaling data confidentiality
4. User and device identity confidentiality
5. User location confidentiality
6. User untraceability
7. Ciphering and integrity requirements - algorithms
8. At least two strong security algorithms and algorithm extensibility for future proofness
9. UMTS Evolution

□

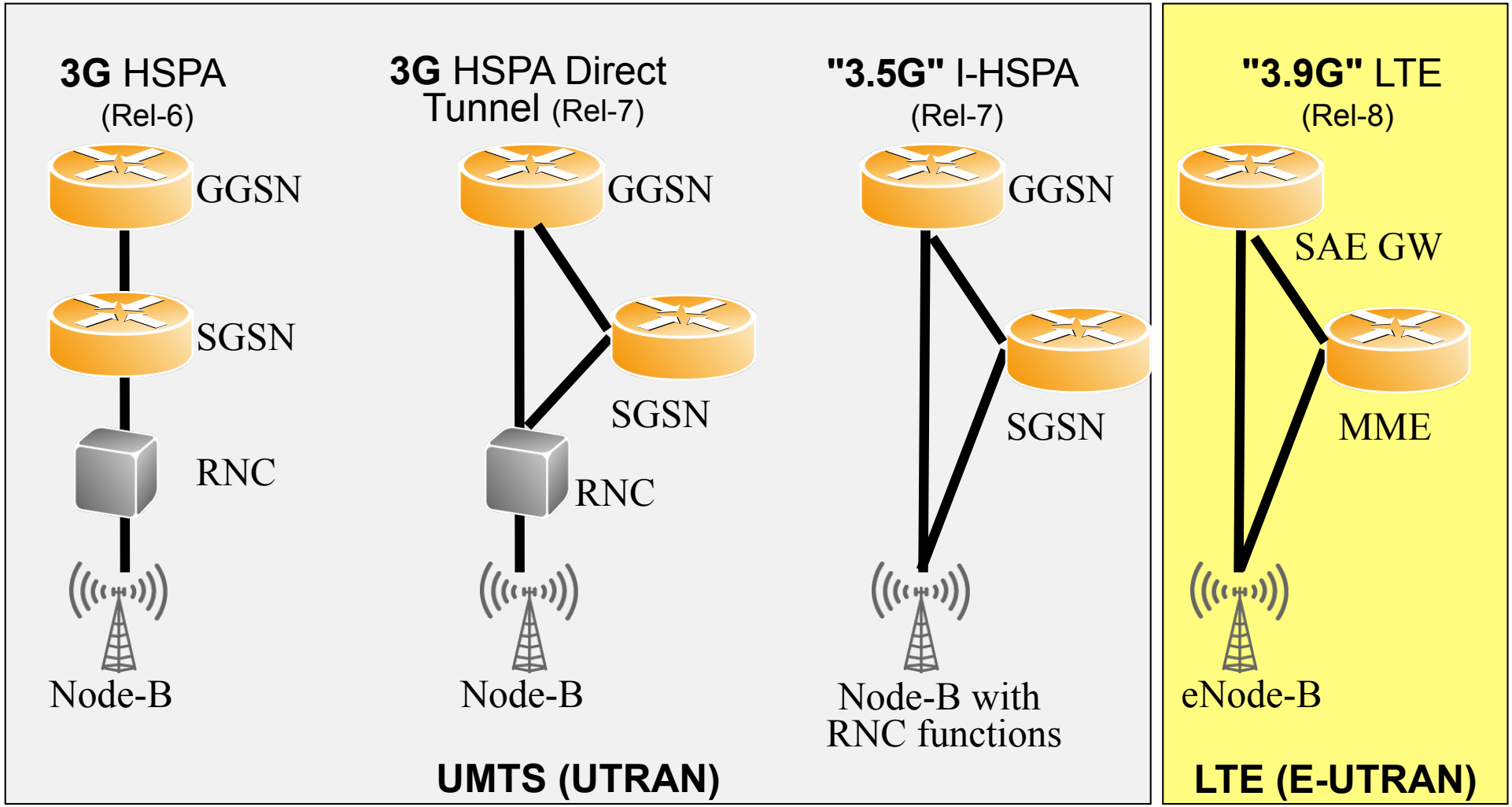
2. LTE Security Architecture

Terminology

- **MME** – Mobile Management Entity
  - Similar to SGSN and takes care of the Control Plane
- **SAE GW** – System Architecture Evolution Gateway
  - Similar to GGSN, user plane gateway
- **PDN GW** – Packet Data Network Gateway
  - Home network gateway
- **eNB** – Evolved Node B
  - LTE Base station
- **HeNB** – Home eNB
  - LTE Base station in home environment
- **HSS** – Home Subscriber Server
  - User credential storage, like home AAA server
- **EPS** – Evolved Packet System
  - ~ EPC + E-UTRAN
- **LTE** - Long Term Evolution
  - Short name for Evolved UTRAN (E-UTRAN) network
- **UE** – User Equipment



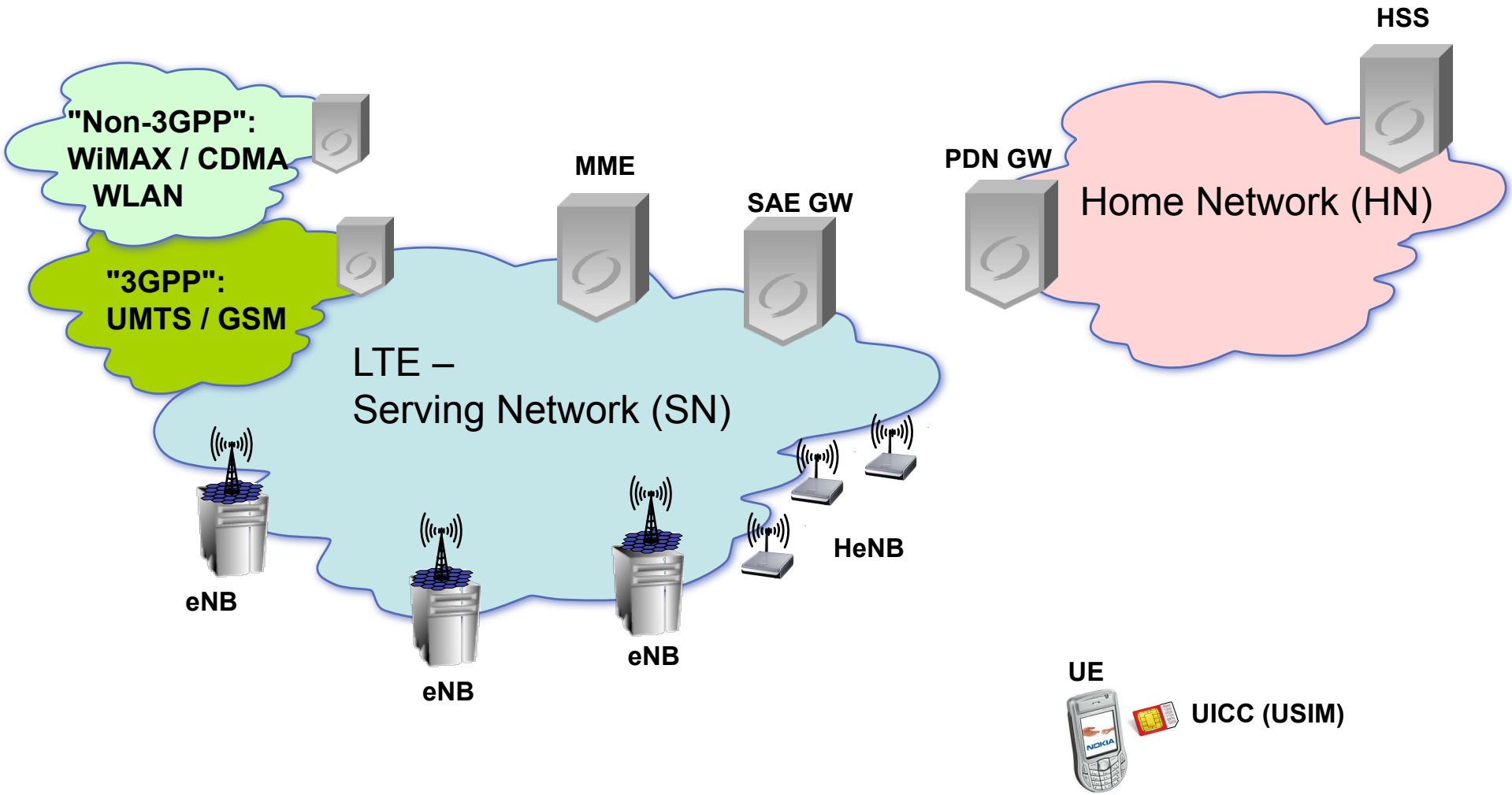
Architecture Evolution



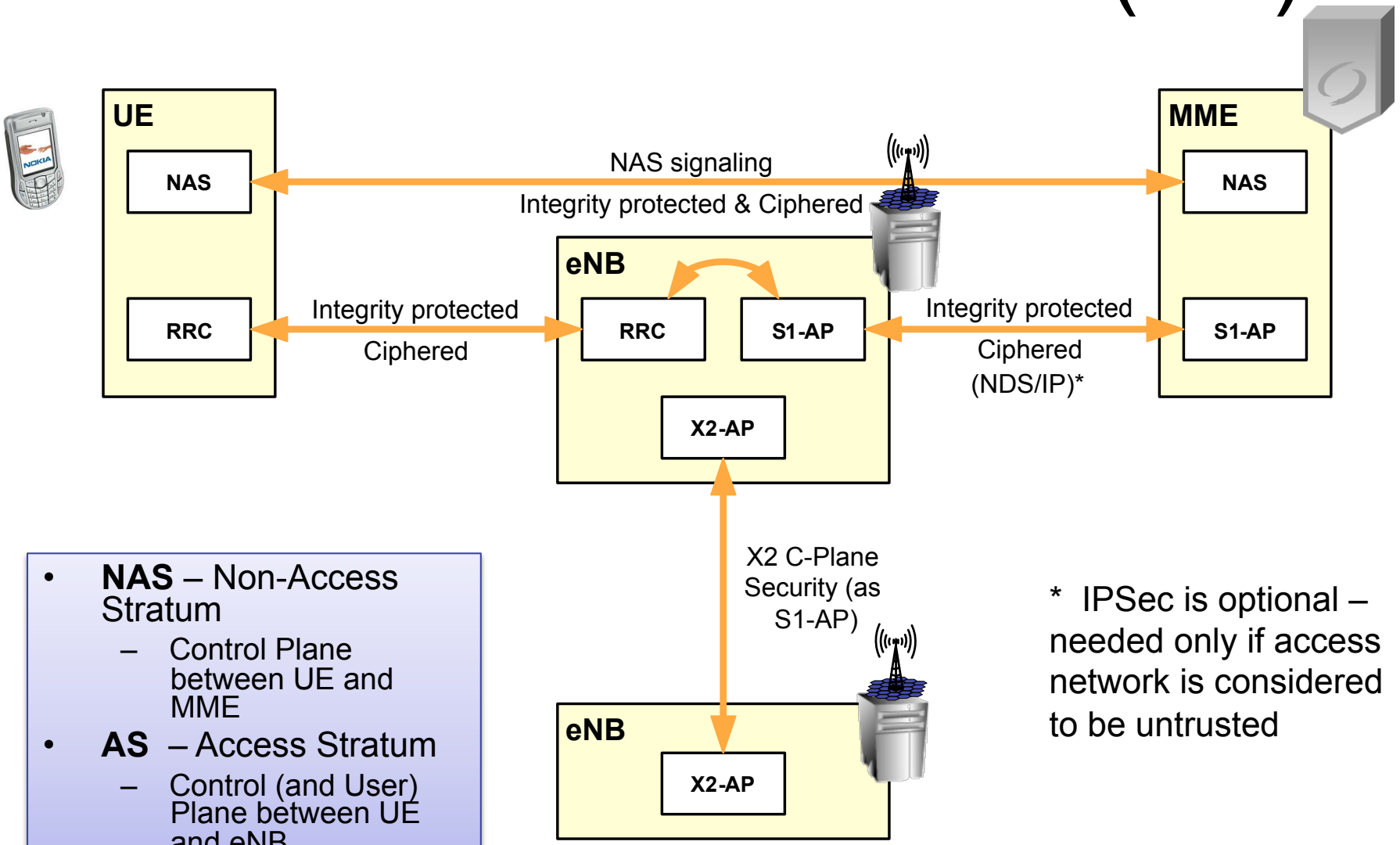
Peek: Changes compared to UMTS

- Security at different protocol layers
- Termination point for air interface security
- Key hierarchy
- Cryptographic network separation, key binding – serving network authentication
- Key separation in intra-LTE handovers
- Use of trusted base station platforms (implementation)
- Two strong security algorithms and algorithm extensibility for future proofness from day one
- Key separation in intersystem mobility
- Homogeneous security concept for connecting heterogeneous access networks (not handled in this presentation)

EPS Architecture



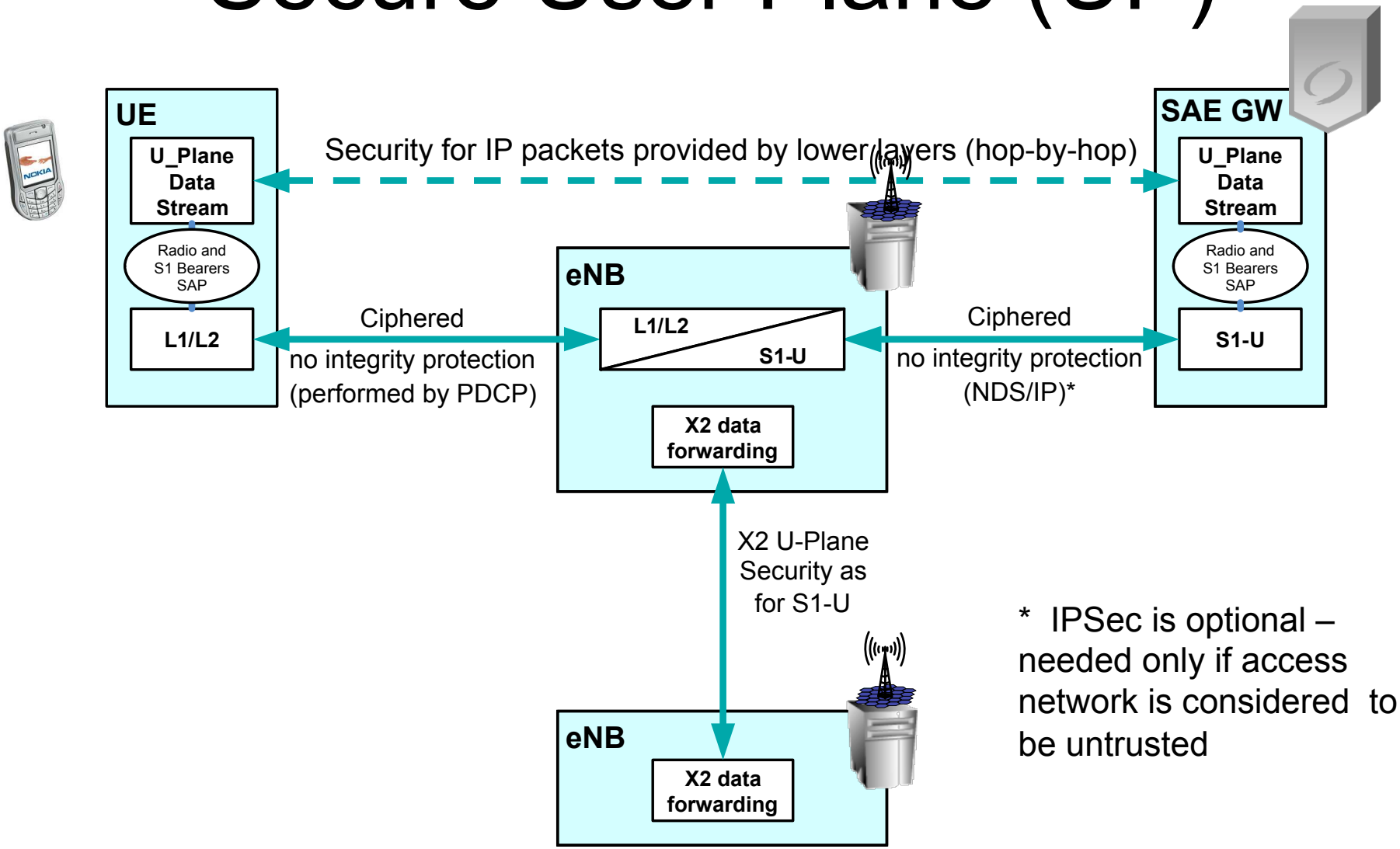
Secure Control Plane (CP)



- **NAS** – Non-Access Stratum
  - Control Plane between UE and MME
- **AS** – Access Stratum
  - Control (and User) Plane between UE and eNB

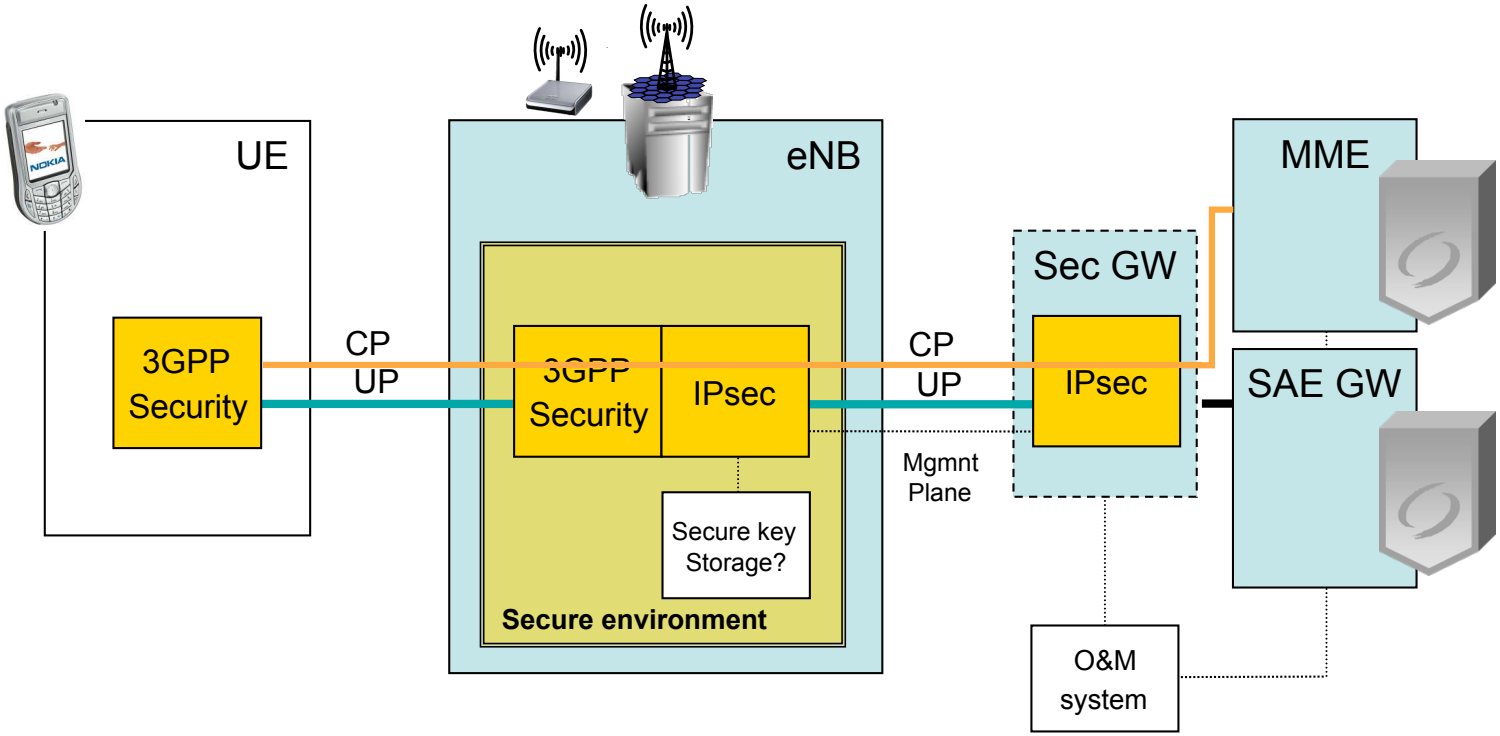
* IPSec is optional – needed only if access network is considered to be untrusted

Secure User Plane (UP)



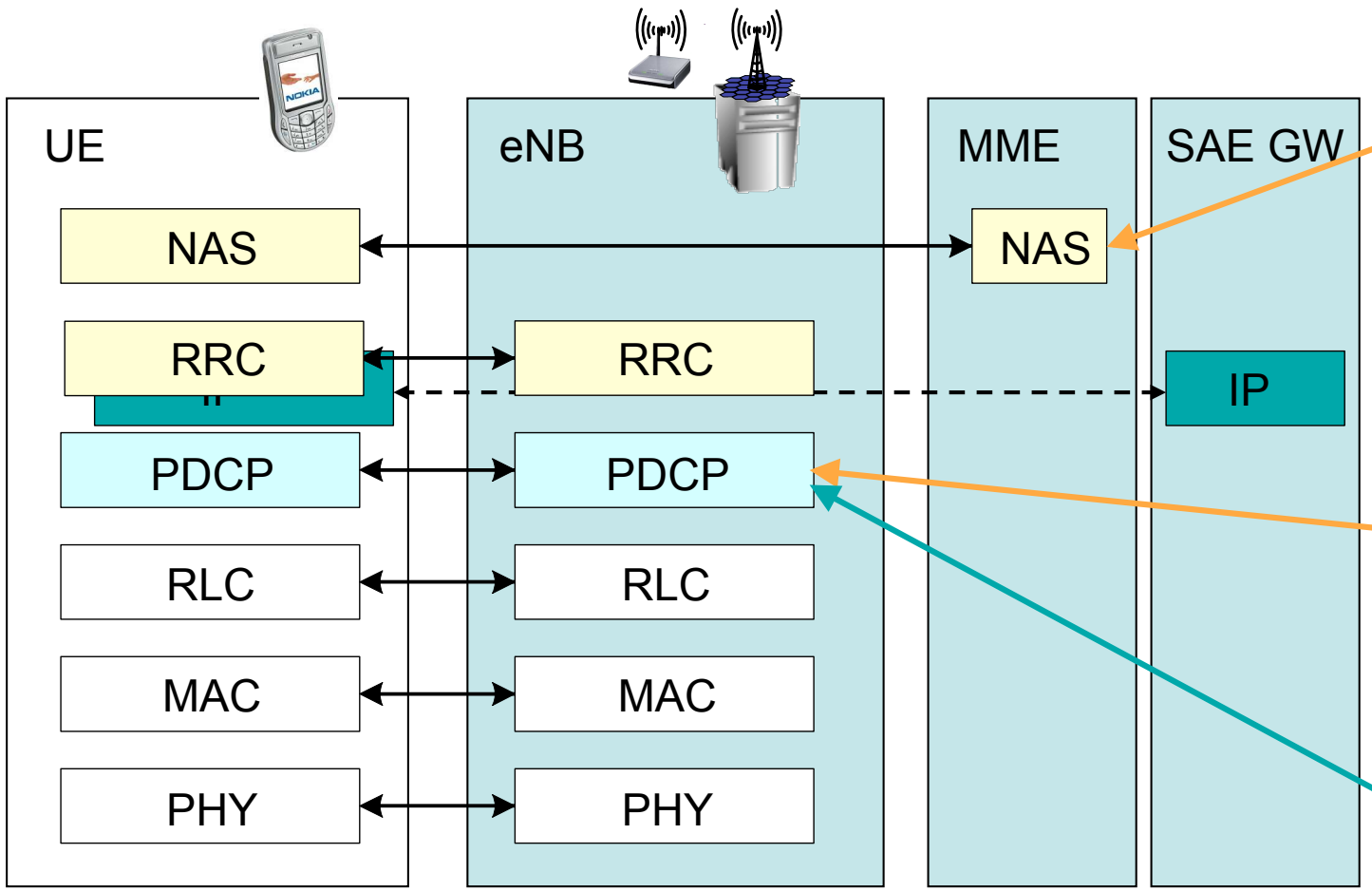
* IPSec is optional – needed only if access network is considered to be untrusted

Secure Path - example



- eNB implements termination of encryption of UP and CP
- eNB's backhaul traffic is encrypted
  - optional, used if network is untrusted
- Encryption / decryption takes place in a secure environment in eNB
- Secure storage solution for long term keys in eNB

Protocol Stack



NAS Control Plane (CP) signaling is e2e encrypted and integrity protected between UE and MME

AS Control Plane (CP) (RRC) is encrypted and integrity protected over the air on PDCP

User Plane (UP) (TCP/IP) is encrypted over the air on PDCP

3. Authentication and Security Setup

Terminology

ARCHITECTURE

- **HSS** – Home Subscriber Server
  - Contains the User credentials and profile settings
- **ME** – Mobile Equipment
  - UE without UICC / USIM
- **UICC** – Universal Integrated Circuit Card
  - Smart Card used in UMTS and GSM
- **(U)SIM** – (UMTS) Subscriber Identity Module
  - Application in the UICC for (3G) 2G

FUNCTION

- **KDF** – Key Derivation Function
  - One way hash function like SHA256

EPS AKA

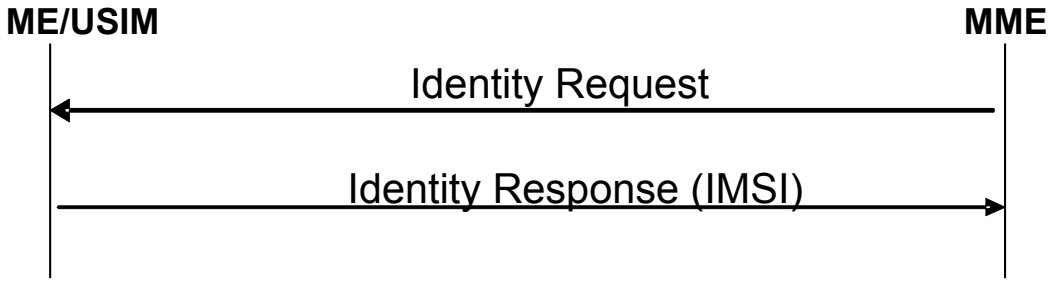
- **AKA** – Authentication and Key Agreement
- **RAND** – AKA: Random challenge
- **AUTN** – AKA: Authentication Token
- **XRES** – AKA: Expected Response
- **E-AV** – EPS Authentication Vector
  - Contains: AUTN, XRES, K_{ASME}, RAND
- **K_{ASME}** – EPS AKA: 256bit root key
  - Created in HSS from CK, IK, and SN identity

IDENTITY

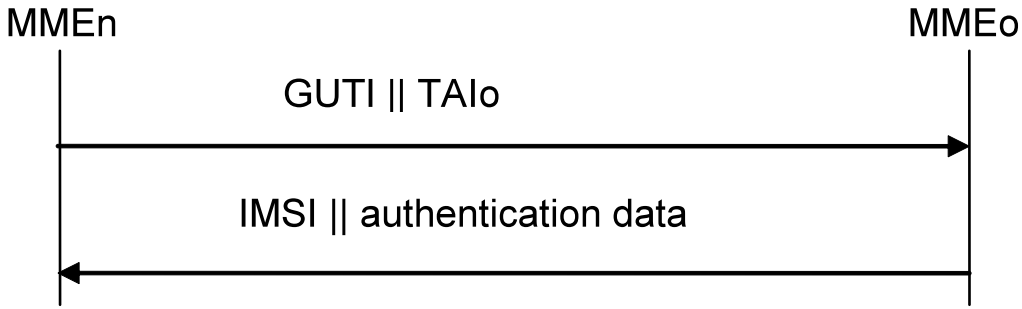
- **IMSI** – International Mobile Subscriber Identity (user id)
- **IMEI** – International Mobile Equipment Identity (device id)
- **GUTI** – Globally Unique Temporary Identity
  - Similar to P-TMSI in UMTS but longer

First: Identity Request

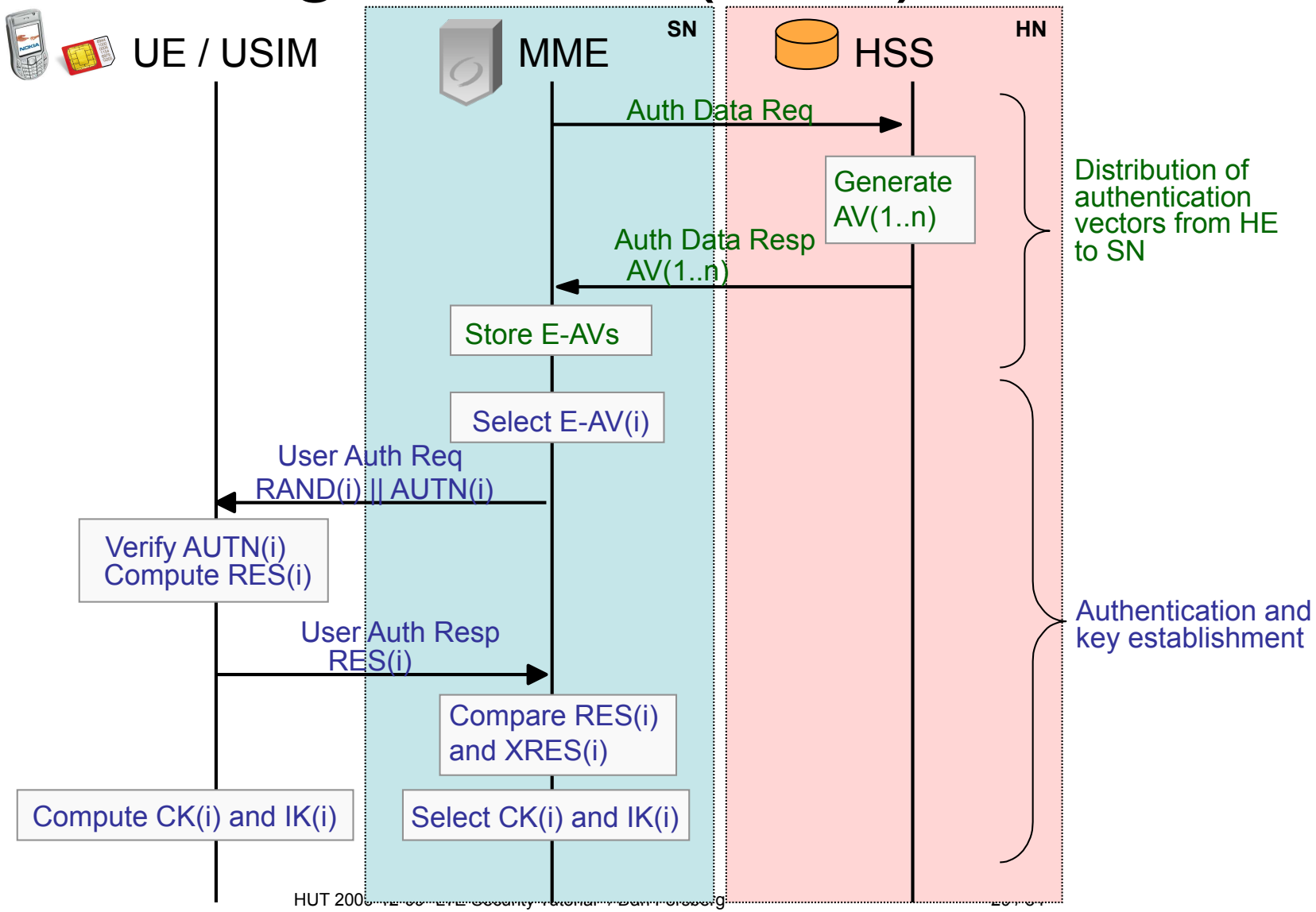
- Network requests the user identity if UE did not provide
- User gives (temporary) GUTI if it has it, otherwise (permanent) IMSI



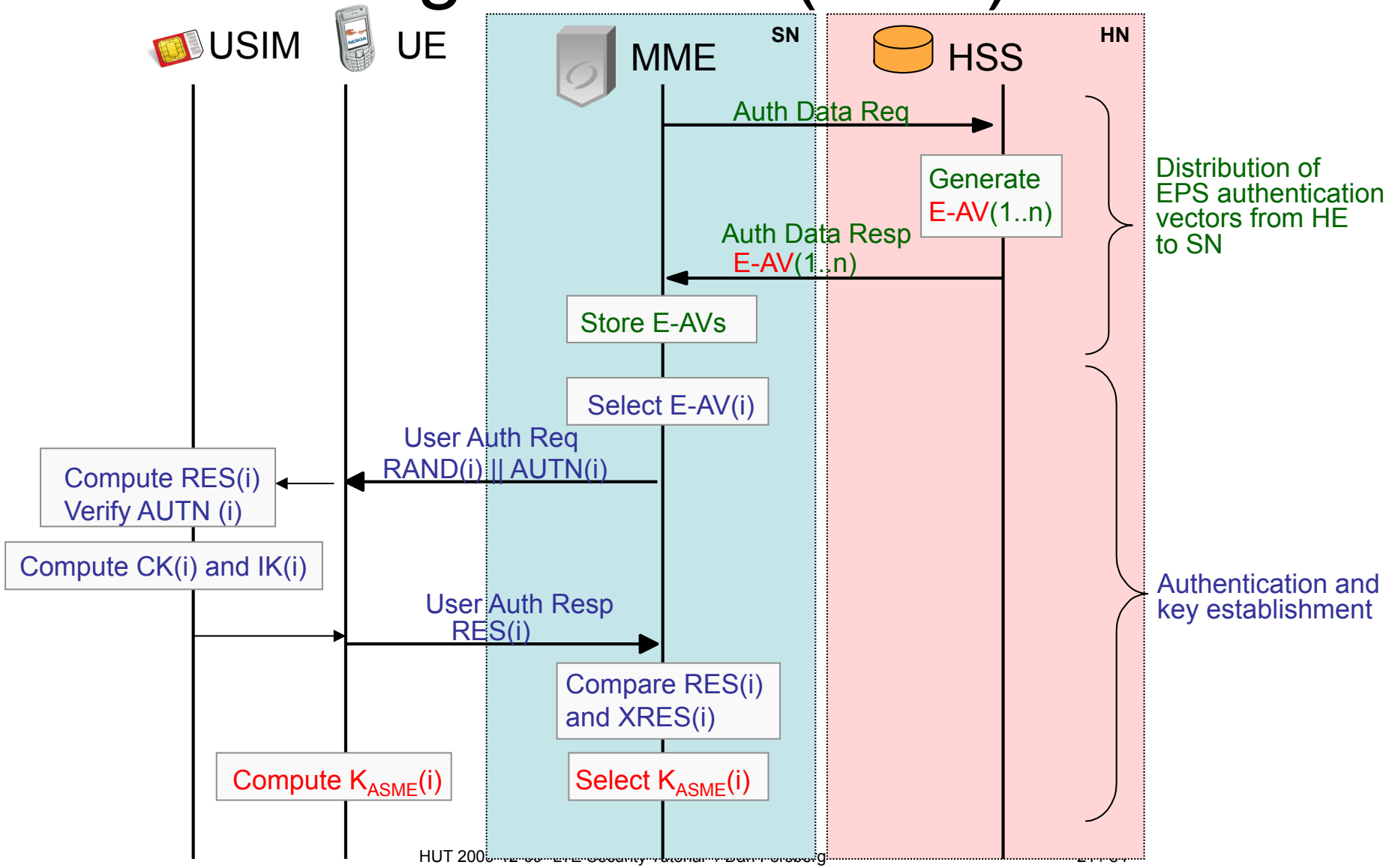
- Network tries to find out user context based on GUTI
  - If not found requests IMSI from the UE



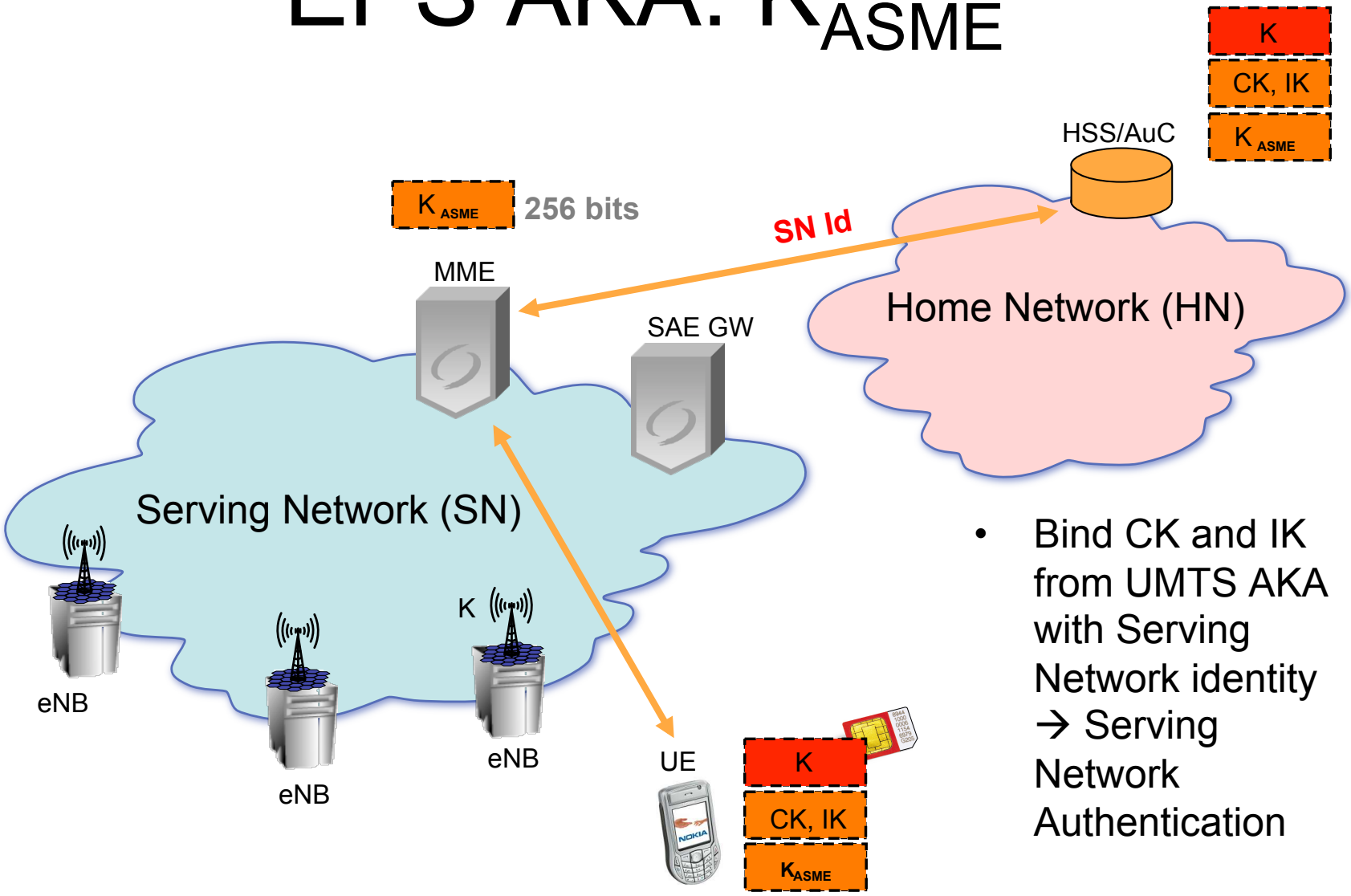
UMTS Authentication and Key Agreement (AKA)



EPS Authentication and Key Agreement (AKA)

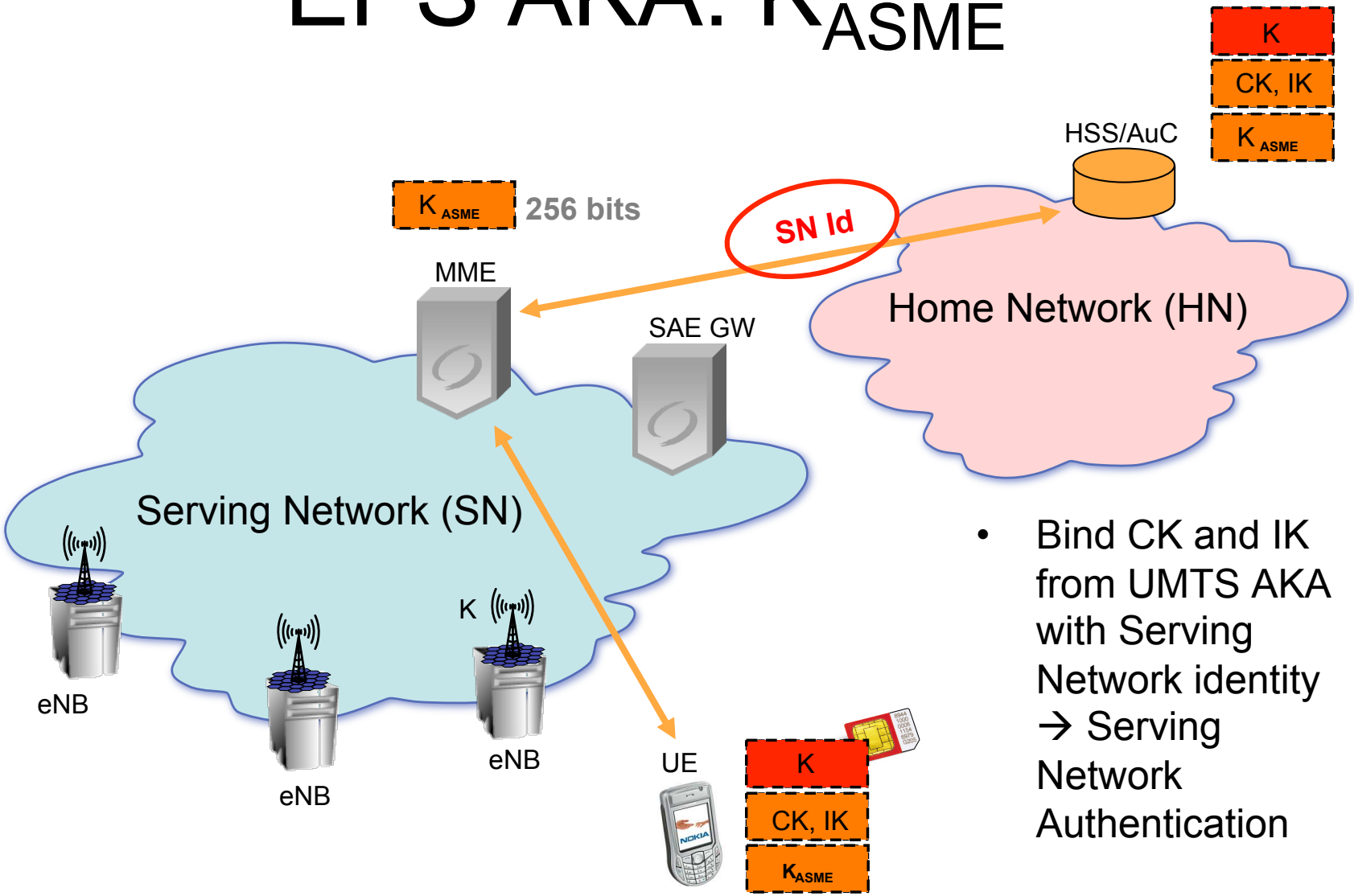


EPS AKA: K_{ASME}



- Bind CK and IK from UMTS AKA with Serving Network identity → Serving Network Authentication

EPS AKA: K_{ASME}



- Bind CK and IK from UMTS AKA with Serving Network identity → Serving Network Authentication

Key Separation and Freshness

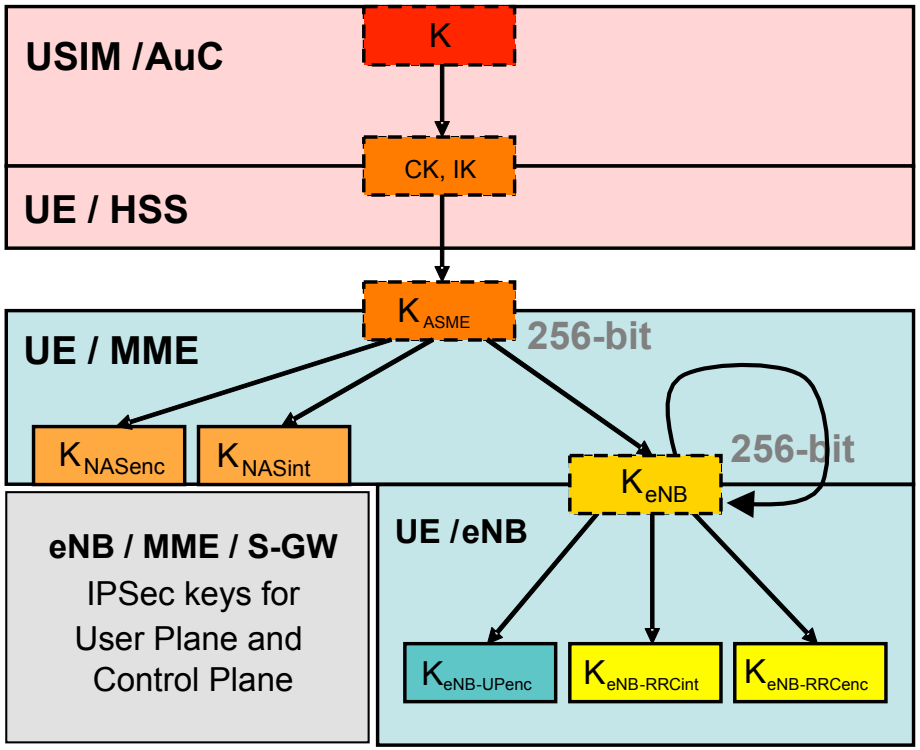
- Key separation:
  - Separate keys for control (CP) and user planes (UP)
  - Separate keys for access (AS) and core connectivity (NAS)
  - Separate keys for integrity and ciphering
  - Separate keys for different algorithms (algorithm id binding)

- Key freshness:
  - New AS keys in every idle to active state transition
  - New keys AS+NAS in intersystem handovers (except cached keys)
  - New AS keys during handovers
  - New keys with EPS AKA
  - New keys before COUNT wraps around

Key Lengths

- System design allows longer future key lengths: keys that are transported toward the crypto endpoints are 256-bit
  - K_{eNB}
  - K_{ASME}
- Actual AS and NAS protection keys are 128-bit
  - K_{NASInt}
  - K_{NASEnc}
  - K_{RRCEnc}
  - K_{RRCInt}
  - K_{UPEnc}

Basic Key Hierarchy



Home Network (HN)

Serving Network (SN)

Security Algorithms

- Two different mandatory 128-bit EPS ciphering and integrity algorithms for CP an UP from day one
  - Snow3G (UMTS based, UIA2 and UEA2) and
  - AES (by US NIST, FIPS standard 197) algorithms

- Algorithm-id:
  - "0000" 128-EEA0 NULL ciphering algorithm
  - "0001" 128-EEA1 SNOW 3G
  - "0010" 128-EEA2 AES
  - "0001" 128-EIA1 SNOW 3G
  - "0010" 128-EIA2 AES

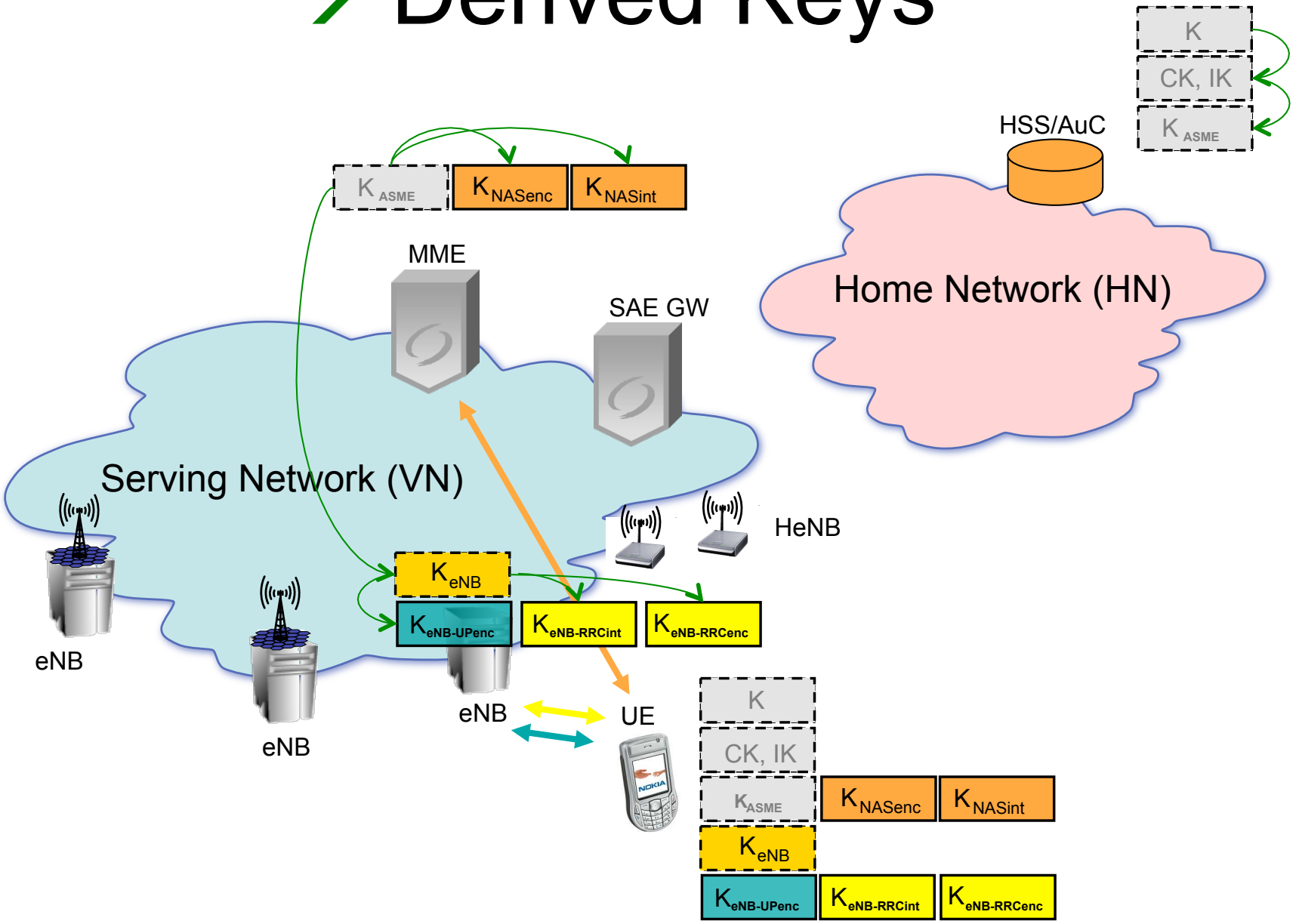
Basic Key Derivations

- KDF = Key Derivation Function, a one way hash function (SHA256)
- K_{ASME} = KDF(CK, IK, PLMN Id, SQN $\oplus$ AK)
- K_{eNB} = KDF(K_{ASME}, $COUNT_{NAS\text{-}UL}$)

- NAS Keys
  - K_{NASInt} = KDF(K_{ASME}, NAS-int-alg, algorithm-id)
  - K_{NASEnc} = KDF(K_{ASME}, NAS-enc-alg, algorithm-id)

- AS Keys
  - K_{RRCInt} = KDF(K_{eNB}, RRC-int-alg, algorithm-id)
  - K_{RRCEnc} = KDF(K_{eNB}, RRC-enc-alg, algorithm-id)
  - K_{UPEnc} = KDF(K_{eNB}, UP-enc-alg, algorithm-id)

→ Derived Keys



Ciphering Algorithm Inputs

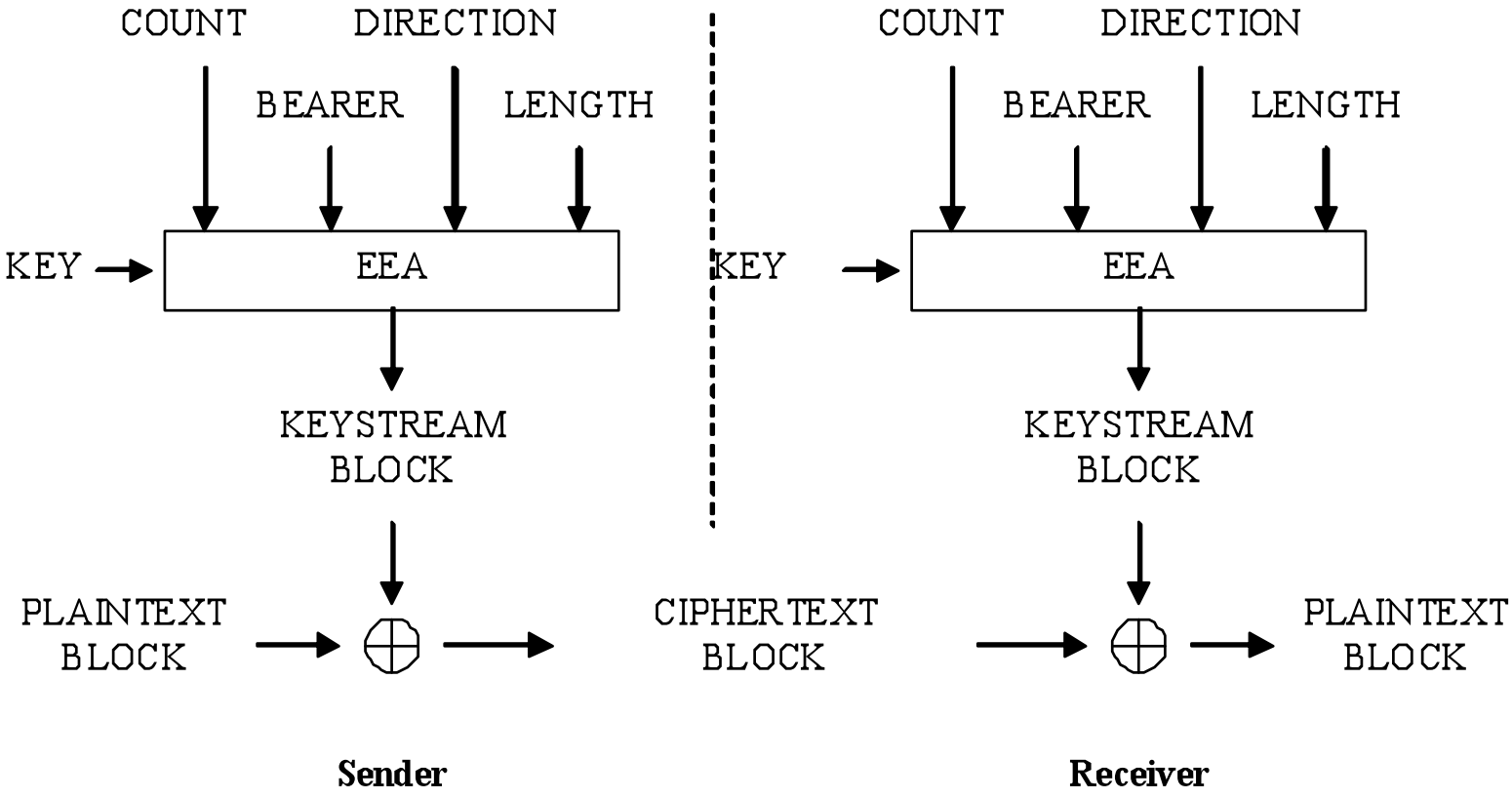


Figure B.1-1: Ciphering of data [TS33.401]

Integrity Algorithm Inputs

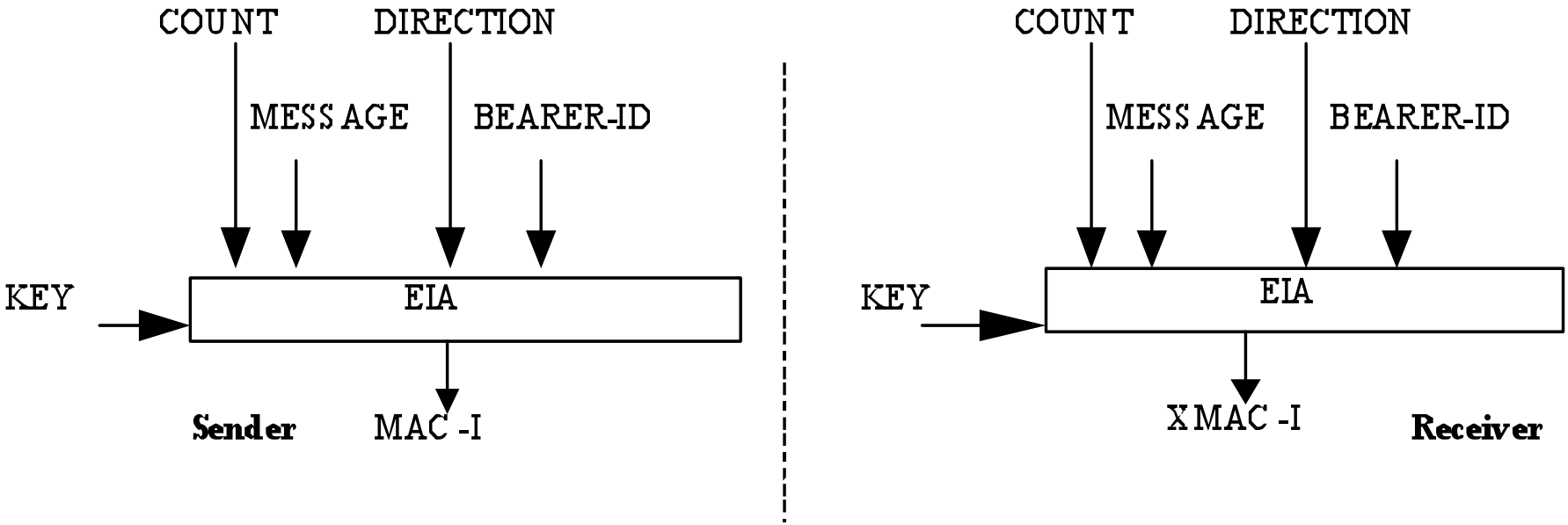
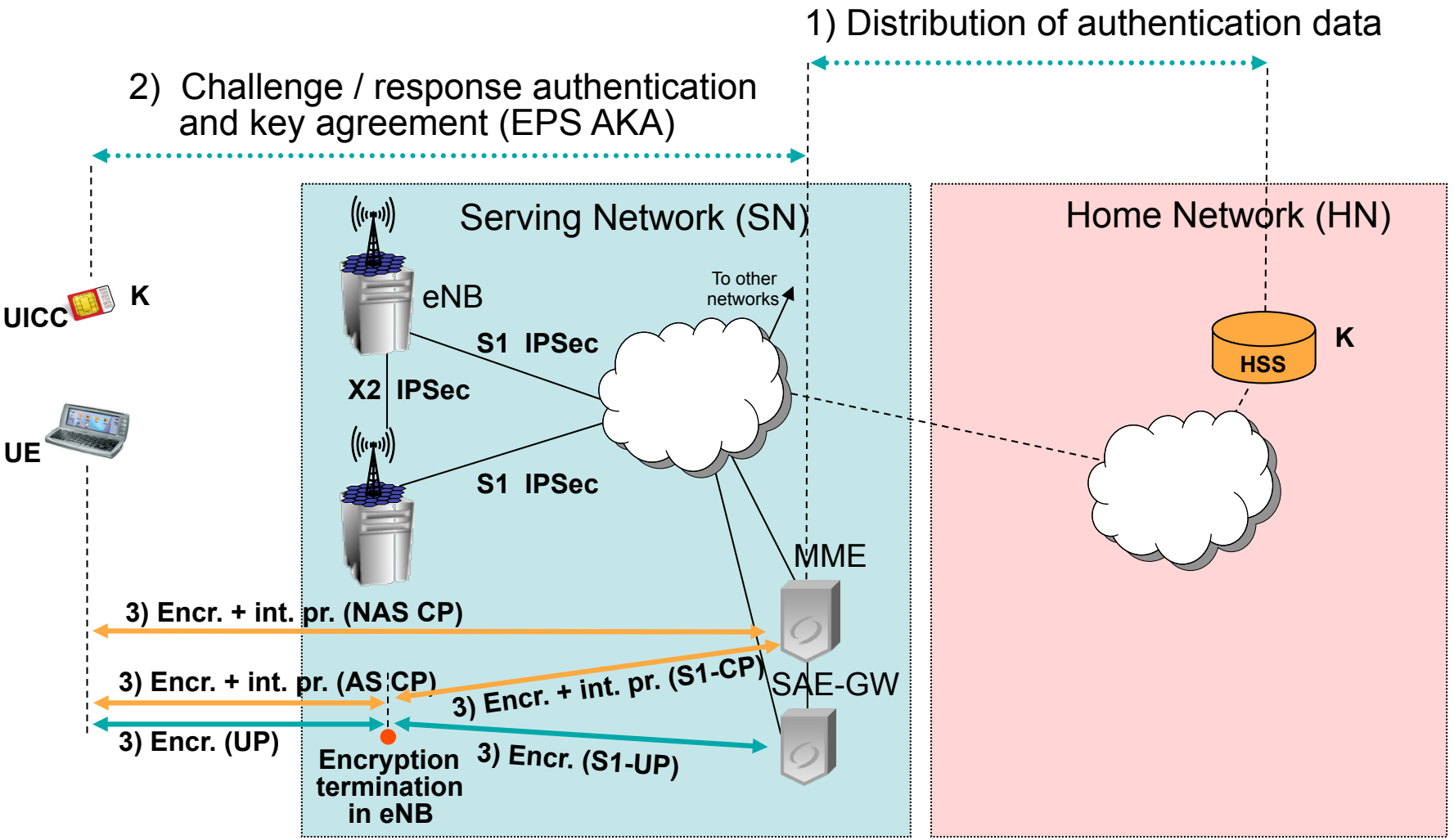


Figure B.2-1: Derivation of MAC-I (or XMAC-I) [TS33.401]

Summary: Security Architecture



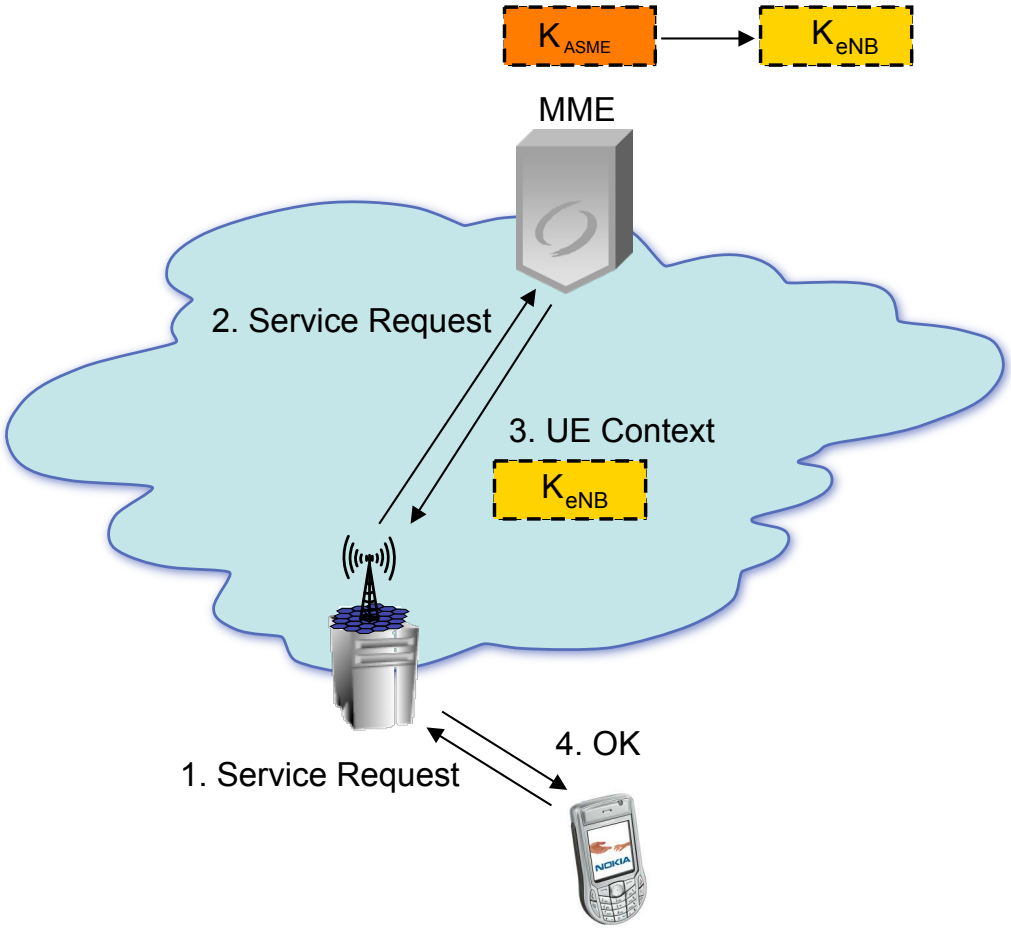
4. Intra-LTE Mobility Security

Terminology

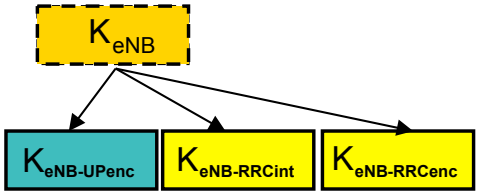
- **Refresh of K_{eNB}**
  - Derivation of a new K_{eNB} from the same K_{ASME} and including a freshness parameter
- **Re-keying of K_{eNB}**
  - Derivation of a new K_{eNB} from a new K_{ASME} (i.e., after an AKA has taken place)
- **Re-derivation of NAS keys**
  - Derivation of new NAS keys from the same K_{ASME} but including different algorithms (and no freshness parameter)
- **Re-keying of NAS keys**
  - Derivation of new NAS keys from a new K_{ASME}
- **KDF** – Key Derivation Function
  - One way hash function like SHA256

- **Chaining of K_{eNB} - "K_{eNB}*"**
  - Derivation of a new K_{eNB} from another K_{eNB} (i.e., at cell handover)
- **Key Separation**
  - Keys are cryptographically not directly related
- **Forward Key Separation**
  - New key can not be deduced from the old key
- **Backward Key Separation**
  - Old key can not be deduced from the new key
- **NH** - Next Hop Key
  - Cryptographically separate key from K_{eNB} (from MME to the eNB)
- **NCC** - Next Hop Chaining Count
  - Short round robin key derivation (NH) index
- **{NH, NCC} pair**
  - NH/K_{eNB} and NCC are always carried together

Idle to Active State Transition



- Fresh K_{eNB} is derived from K_{ASME} and NAS uplink COUNT value
- eNB selects security algorithms (AES or SNOW 3G)
- No need for EPS AKA



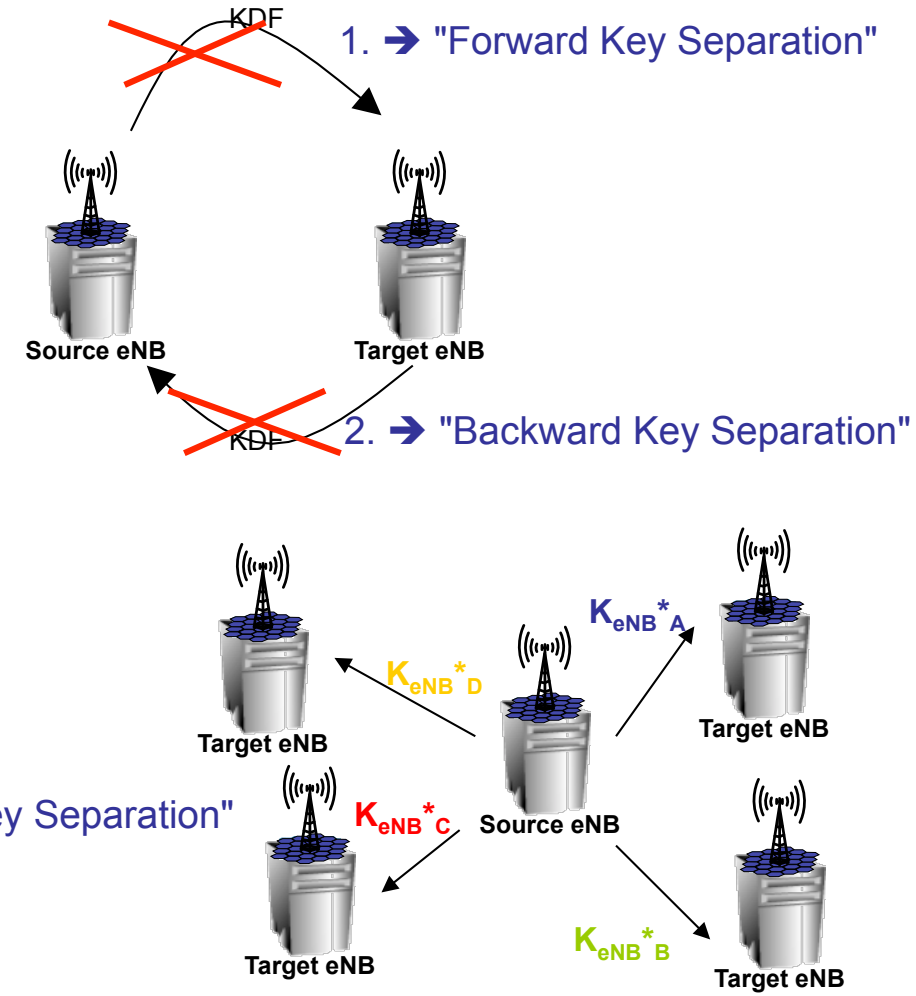
Keys in Mobility

- In case of handover new keys (K_{eNB}) are derived
  - fast key derivation

- Intersystem mobility (handled in more details on next chapter)
  - Security context transfer in handover to/from UTRAN and GERAN
  - Handover from UTRAN and GERAN may be followed by key change on the fly in active state

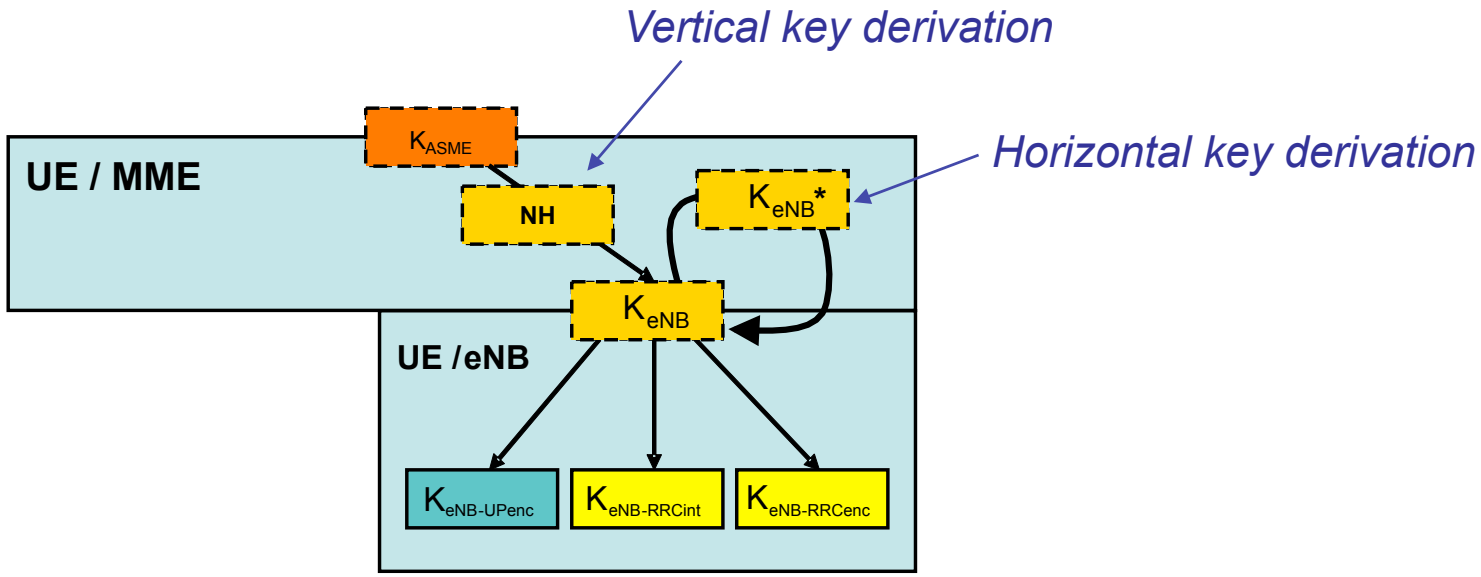
Keys in LTE Handovers (HO)

- LTE Security reduces the key scope and lifetime to minimize the threat of key compromise
  1. Forward key separation
     - New K_{eNB} key (called NH) from MME
  2. Backward key separation
     - Key chaining with one way hash function
  3. Key separation for different target eNBs/cells
     - Phycal cell id (PCI) and frequency bindings

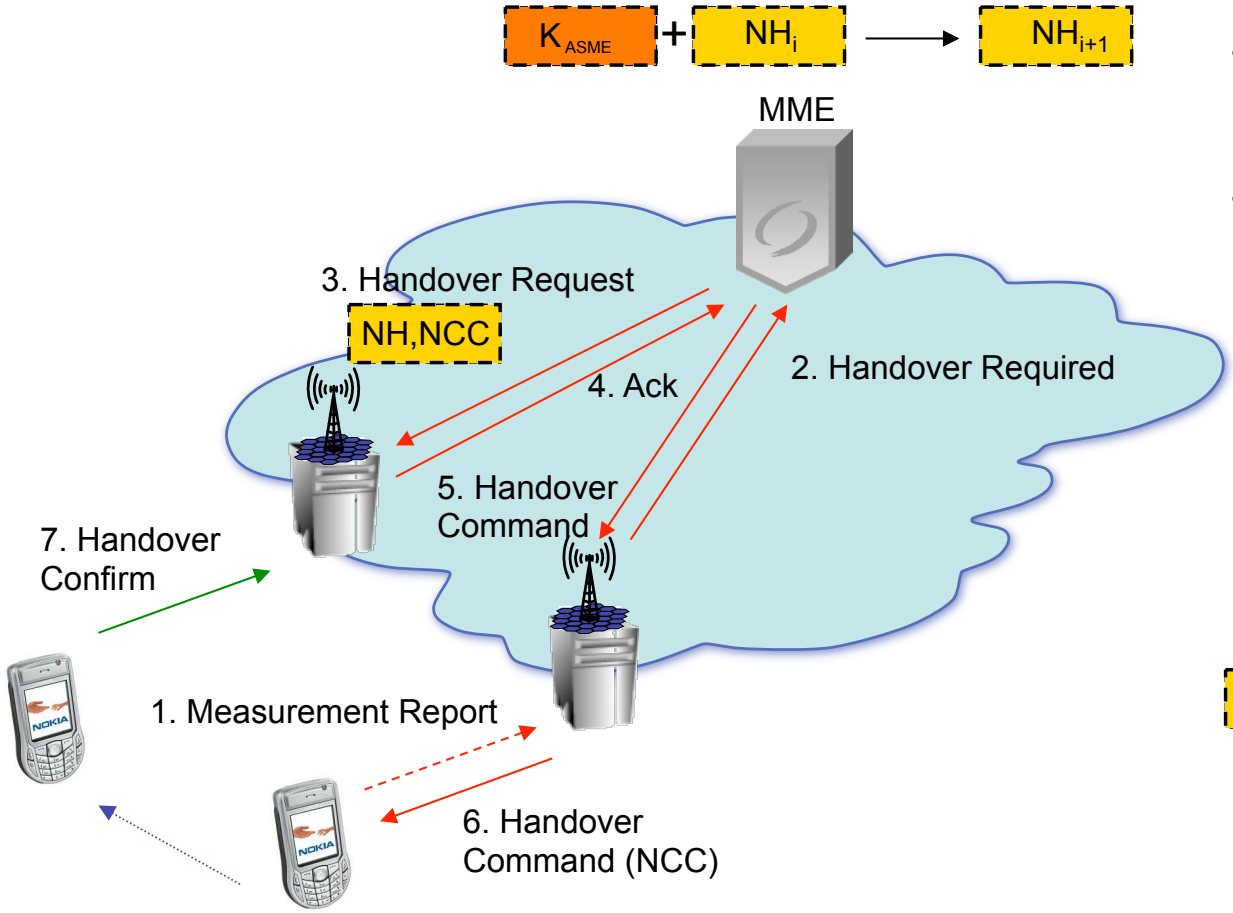


Handover: Next Hop (NH) Key

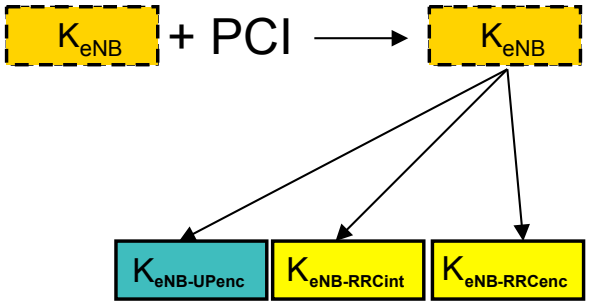
- K_{eNB0} = KDF(K_{ASME}, NAS uplink COUNT)
- NH_0 = KDF(K_{ASME}, K_{eNB0})
- NH_{NCC+1} = KDF(K_{ASME}, NH_{NCC})
- Derived in MME and delivered to the eNB as K_{eNB}



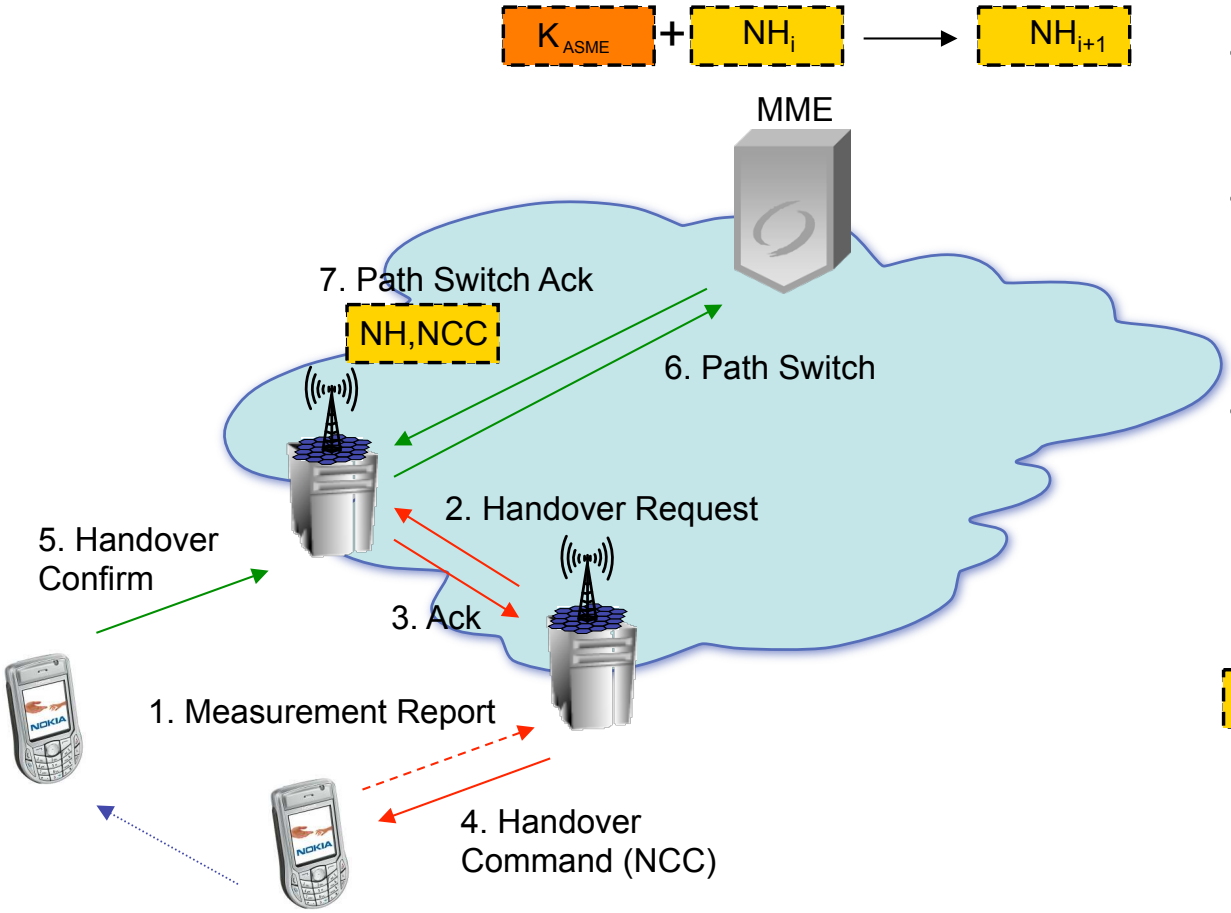
S1 Handover - "Vertical Key Derivation"



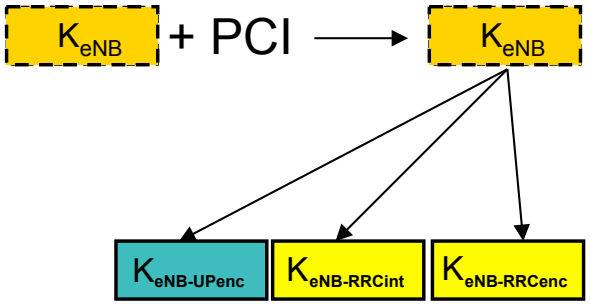
- Fresh K_{eNB} is derived from NH and K_{ASME}
- eNB selects security algorithms (AES or SNOW 3G)



X2 Handover - "Horizontal Key Derivation"



- Fresh K_{eNB} is derived from previous K_{eNB}
- MME provides fresh NH for target eNB <u>after HO</u>
- eNB selects security algorithms (AES or SNOW 3G)

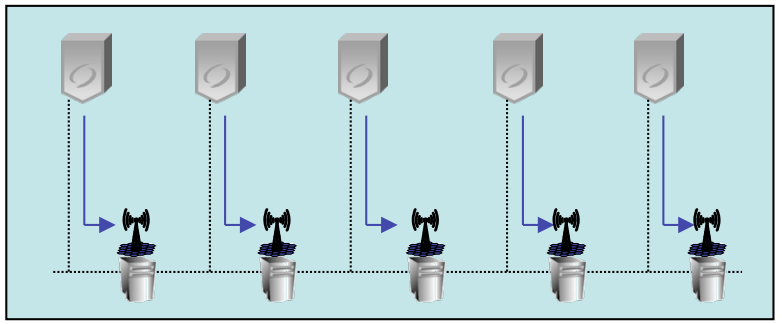


Intra-LTE HO Key Derivations

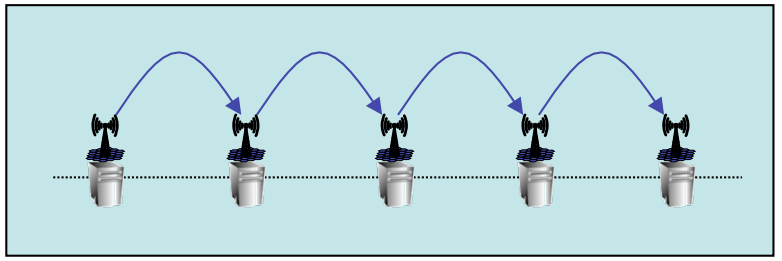
- Initial
  - K_{ASME} = KDF(…)
  - K_{eNB0} = KDF(K_{ASME}, $COUNT_{NAS-UL}$)
  - NH_0 = KDF(K_{ASME}, K_{eNB0})

1. With full key separation - vertical key derivation:
   - NH_{NCC+1} = KDF(K_{ASME}, NH_{NCC})
   - …
   - K_{eNB}* = KDF(NH_{NCC}, PCI)

2. With key chaining - horizontal key derivation:
   - K_{eNB}* = KDF(K_{eNB}, PCI)

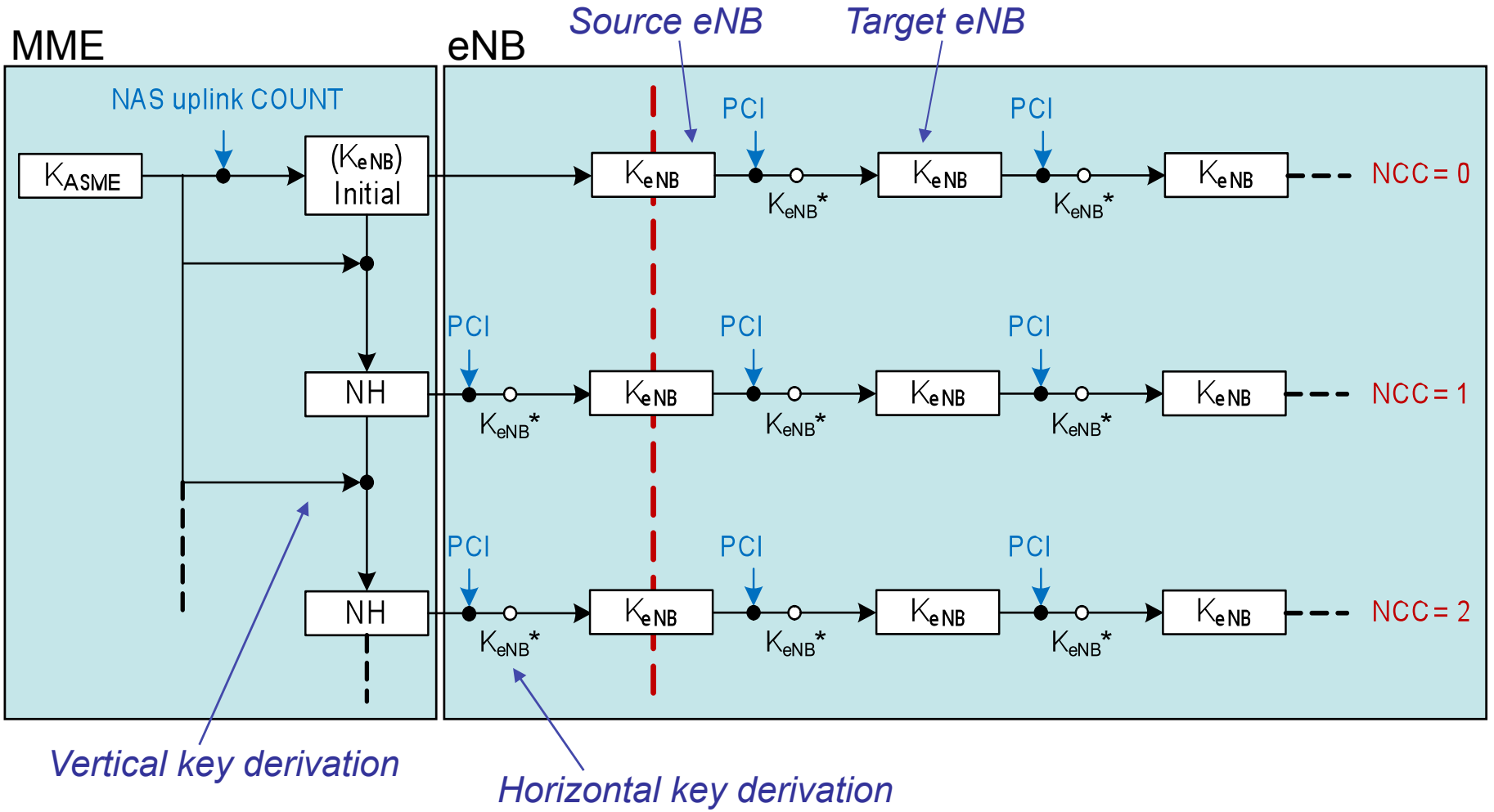


1. Vertical key derivation – forward key separation



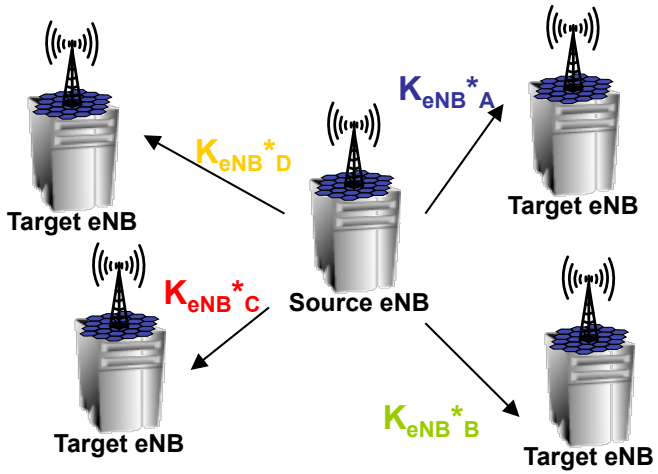
2. Horizontal key derivation – backward key separation

K_{eNB} Key Derivations



Token Calculation for Radio Link Failures (RLF)

- Source eNB prepares target eNB(s) beforehand
  - “make-before-break"
- For error situations the "HO Command" may be lost
  - How to fast authenticate the UE to the new and prepared eNB without selected algorithm for the target eNB?
- Solution: Create token in source eNB and UE – "shared secret"



5. Intersystem Mobility Security

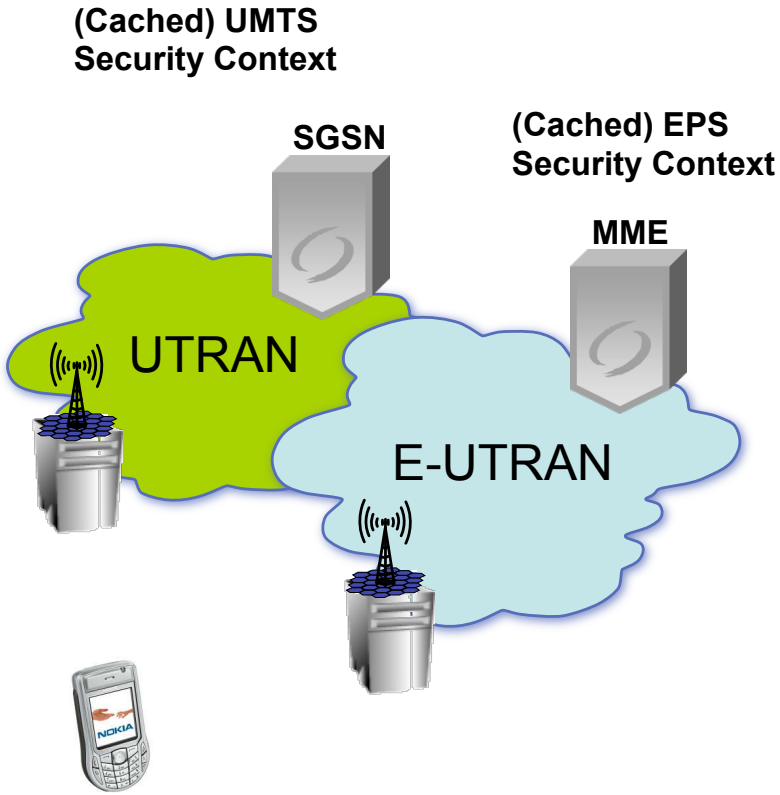
Terminology

- **EPS security context**
  - Includes EPS NAS and AS security context
- **UE Security capabilities**
  - The set of identifiers corresponding to the ciphering and integrity algorithms implemented in the UE. This includes capabilities for E-UTRAN, and includes capabilities for UTRAN and GERAN if these access types are supported by the UE.
- **EPS AS security context**
  - The cryptographic keys at AS level with their identifiers
  - The identifiers of the selected AS level cryptographic algorithms
  - Counters used for replay protection.
  - Exists only when the UE is in ECM-CONNECTED state

- **EPS NAS security context**
  - K_{ASME} with the associated key set identifier (KSI_{ASME})
  - NAS keys: K_{NASint} and K_{NASenc},
  - UE security capabilities,
  - Algorithm identifiers of the selected NAS integrity and encryption algorithms
  - Uplink and downlink NAS COUNT values
  - The distinction between cached and mapped EPS security contexts also applies to EPS NAS security contexts. For EMM-ACTIVE mode UEs, the EPS NAS security context shall also include the Next Hop parameter NH, and the Next Hop Chaining Counter parameter NCC.
- **Native security context**
  - A security context that was created for a given system during prior access
- **Current security context**
  - The security context which has been taken into use by the network most recently
- **Legacy security context**
  - A security context which has been established according to TS 33.102 [4].
- **Mapped security context**
  - Security context created by converting the current security context for the target system in inter-system mobility, e.g., UMTS keys created from EPS keys.

NEW in LTE: ISR & Cached (native) Security Context

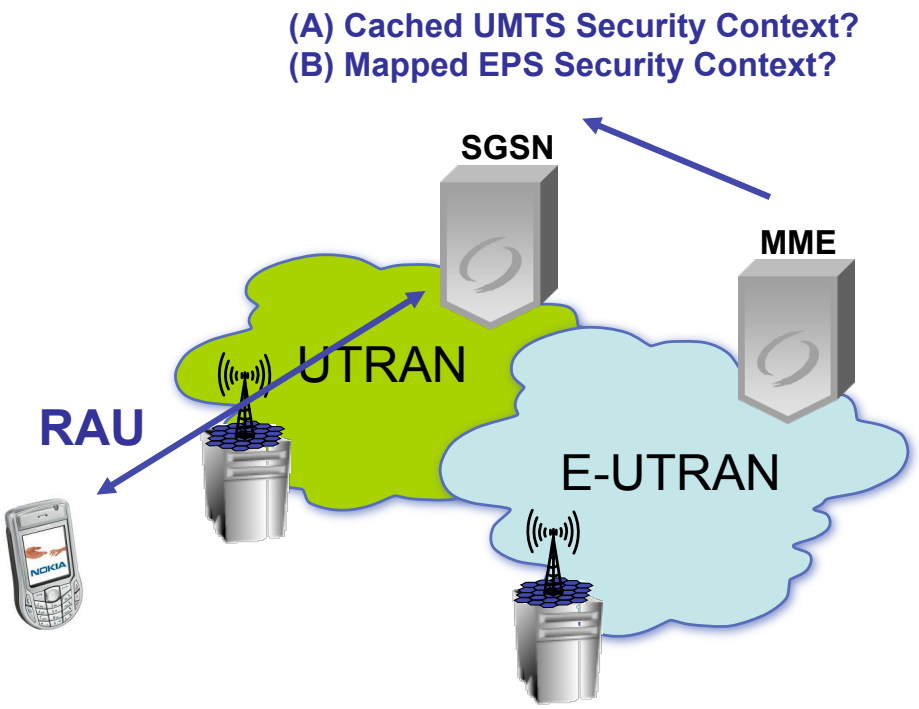
- Idle State Reduction (ISR) mechanism keeps the UE registered in UMTS SGSN and LTE MME at the same time
- Both SGSN and MME have valid security context, but..
  - What context to use during idle mode mobility?
  - What context to use during intersystem handovers?
  - How to ensure fresh keys?
- LTE MME needs to select from mapped context or cached context



IDLE: E-UTRAN → UTRAN

(LTE → UMTS)

- Use (A) cached or (B) mapped context in UTRAN depending on content of "old P-TMSI" in Routing Area Update (RAU) request
  - Valid P-TMSI (A) or GUTI (B)
- NAS downlink COUNT value used for freshness of mapped keys CK', IK'
  - CK', IK' = KDF (K_{ASME}, NAS downlink COUNT)
- UE sends NAS-token in the RAU request
  - MME verifies the NAS-token and corresponding NAS downlink COUNT value
  - Similar to "P-TMSI Signature"

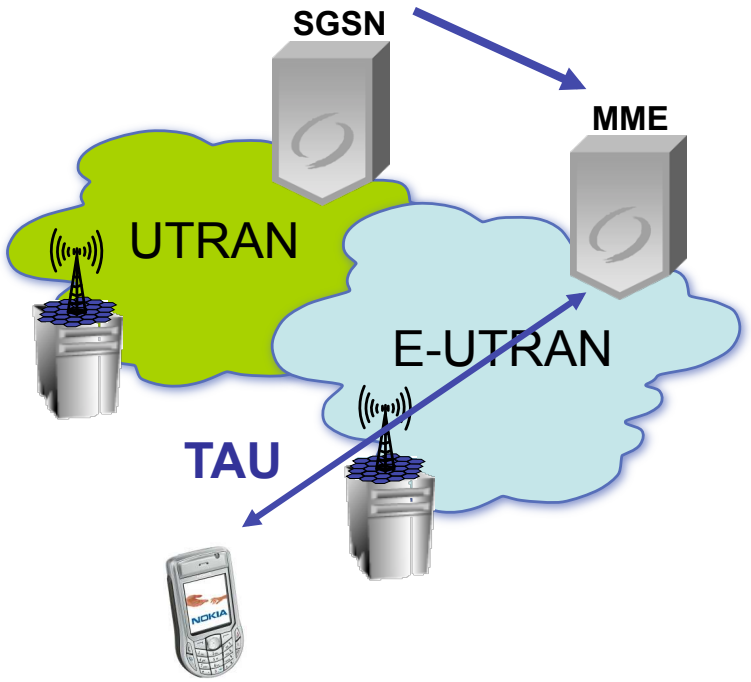


IDLE: UTRAN → E-UTRAN with Mapped Context (UMTS → LTE)

- TAU (Tracking Area Update) request is not integrity-protected

- Nonce exchange:
  - $Nonce_{UE}$ is included in TAU request
  - MME includes $Nonce_{UE}$ and $Nonce_{MME}$ in SM Command sent after receiving TAU request and before sending TAU accept

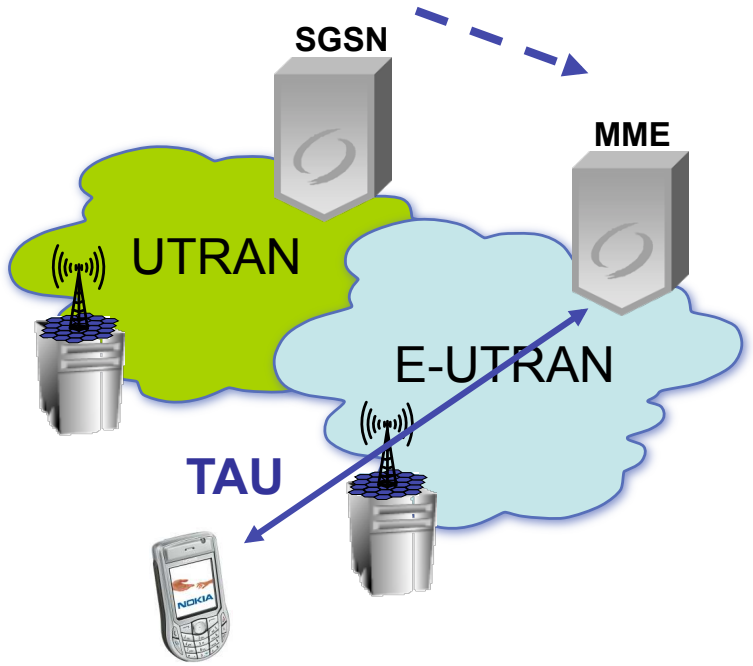
- K_{ASME} is refreshed based on $Nonce_{UE}$ and $Nonce_{MME}$



IDLE: UTRAN → E-UTRAN with Cached Context (UMTS → LTE)

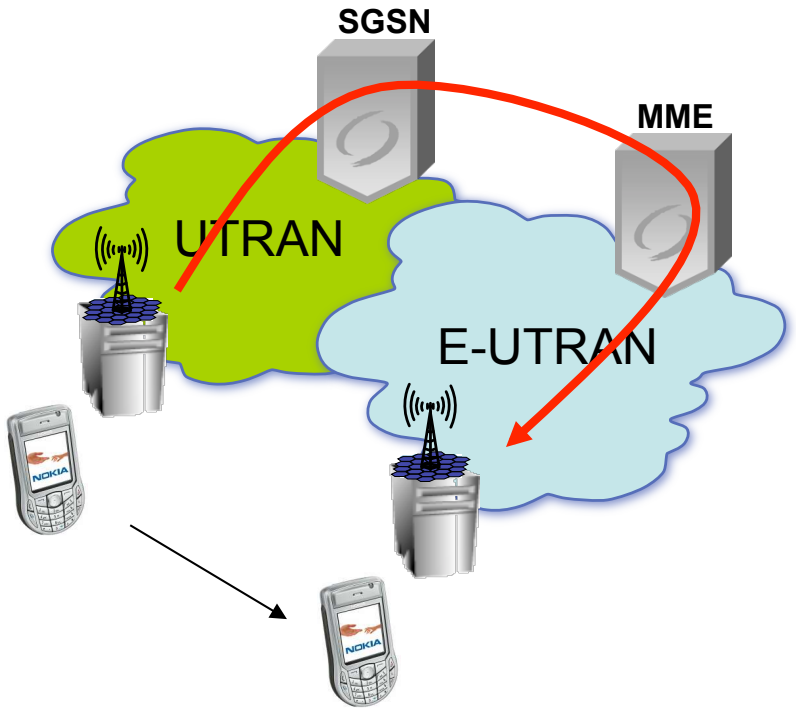
- TAU Request is integrity protected with cached keys

- $Nonce_{UE}$ is included in TAU Request
  - Allow fallback to mapped context

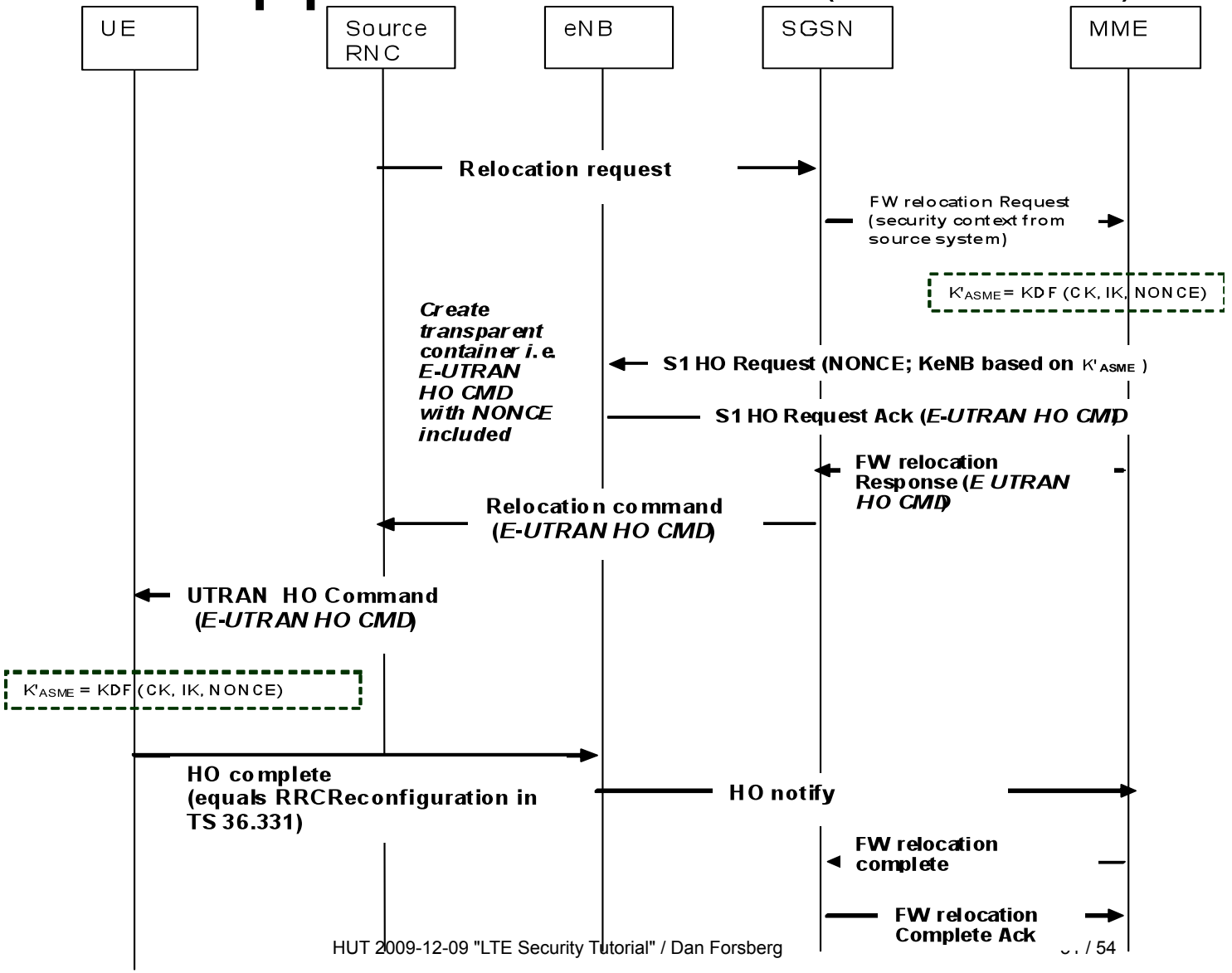


HO: UTRAN to E-UTRAN with Mapped Context (UMTS → LTE)

- Always uses mapped context, but activation of cached context some time after HO is possible
  - "key-change-on-the-fly"
- K_{ASME} is refreshed by deriving it from CK, IK and $Nonce_{MME}$
- The TAU request following the handover is integrity-protected, not ciphered, with a NAS key derived from a fresh K_{ASME}

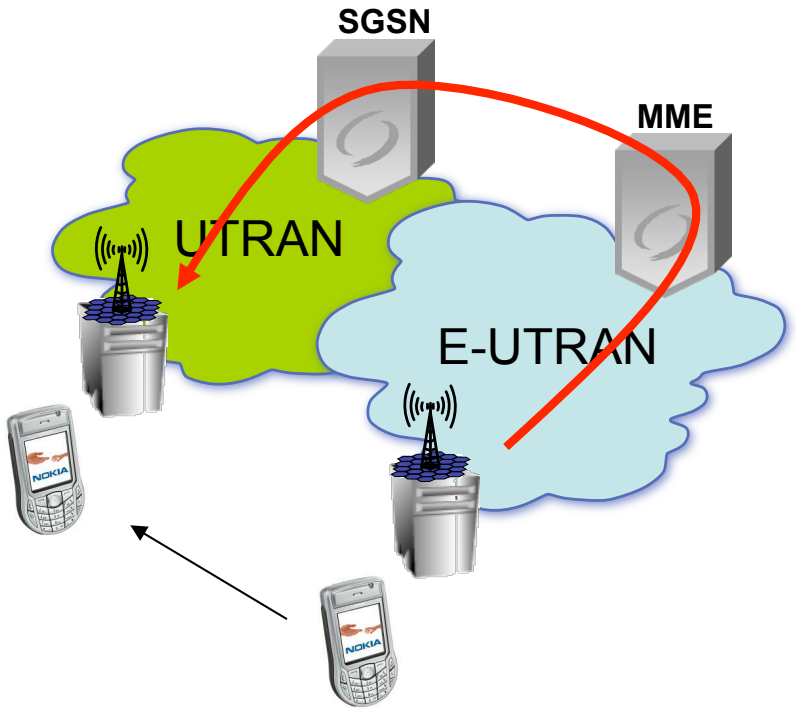


HO: UTRAN to E-UTRAN with Mapped Context (UMTS → LTE)



HO: E-UTRAN to UTRAN with Mapped Context (LTE →UMTS)

- Always uses mapped context
- HO Command include NAS downlink COUNT value
- CK, IK are derived from NAS downlink COUNT and K_{ASME}



Summary

Summary: Changes compared to UMTS

- Security at different protocol layers
- Termination point for air interface security
- New key hierarchy
- Cryptographic network separation, key binding – serving network authentication
- Key separation in intra-LTE handovers
- Use of trusted base station platforms (implementation)
- Two strong security algorithms and algorithm extensibility for future proofness from Day One
- Key separation in intersystem mobility
- Homogeneous security concept for connecting heterogeneous access networks (not handled in this presentation)

References

[TS33.401] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security architecture; (Release 9)

[TS33.402] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses; (Release 9)

[TS33.102] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 8)

[TS23.401] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 9)