Empowered by Innovation NEC

Securing the Next Generation: LTE Security

Anand R. Prasad

<anand@bq.jp.nec.com>

NEC Corporation

Disclaimer: This presentation and opinions presented herein are that of the author and not necessarily that of NEC Corporation

MobiSec 27 May 2010
MI事企画M10-0031

Outline

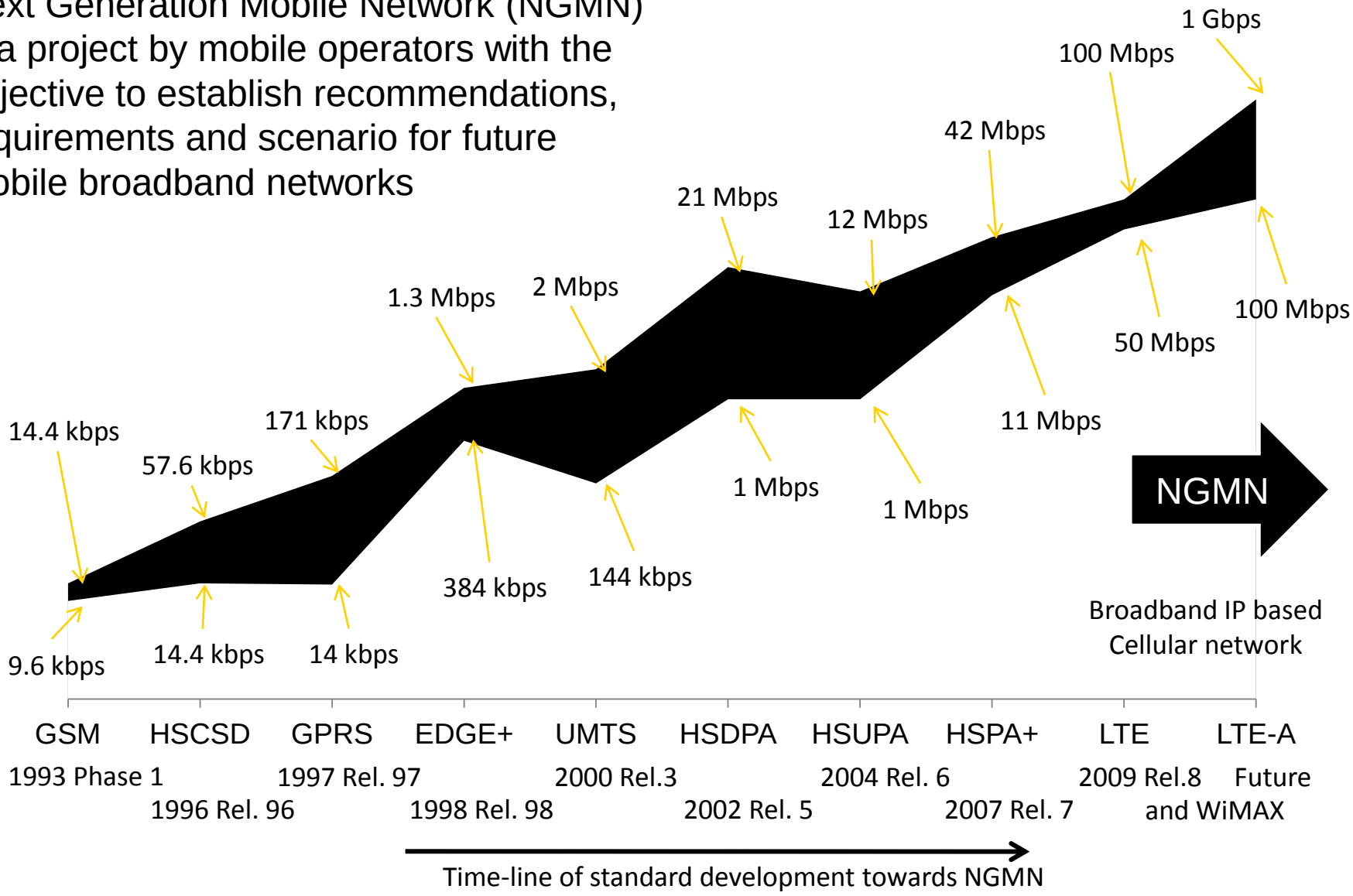
- Background to NGMN & 3GPP
- Evolved packet system (EPS)
- Security in EPS

Empowered by Innovation NEC

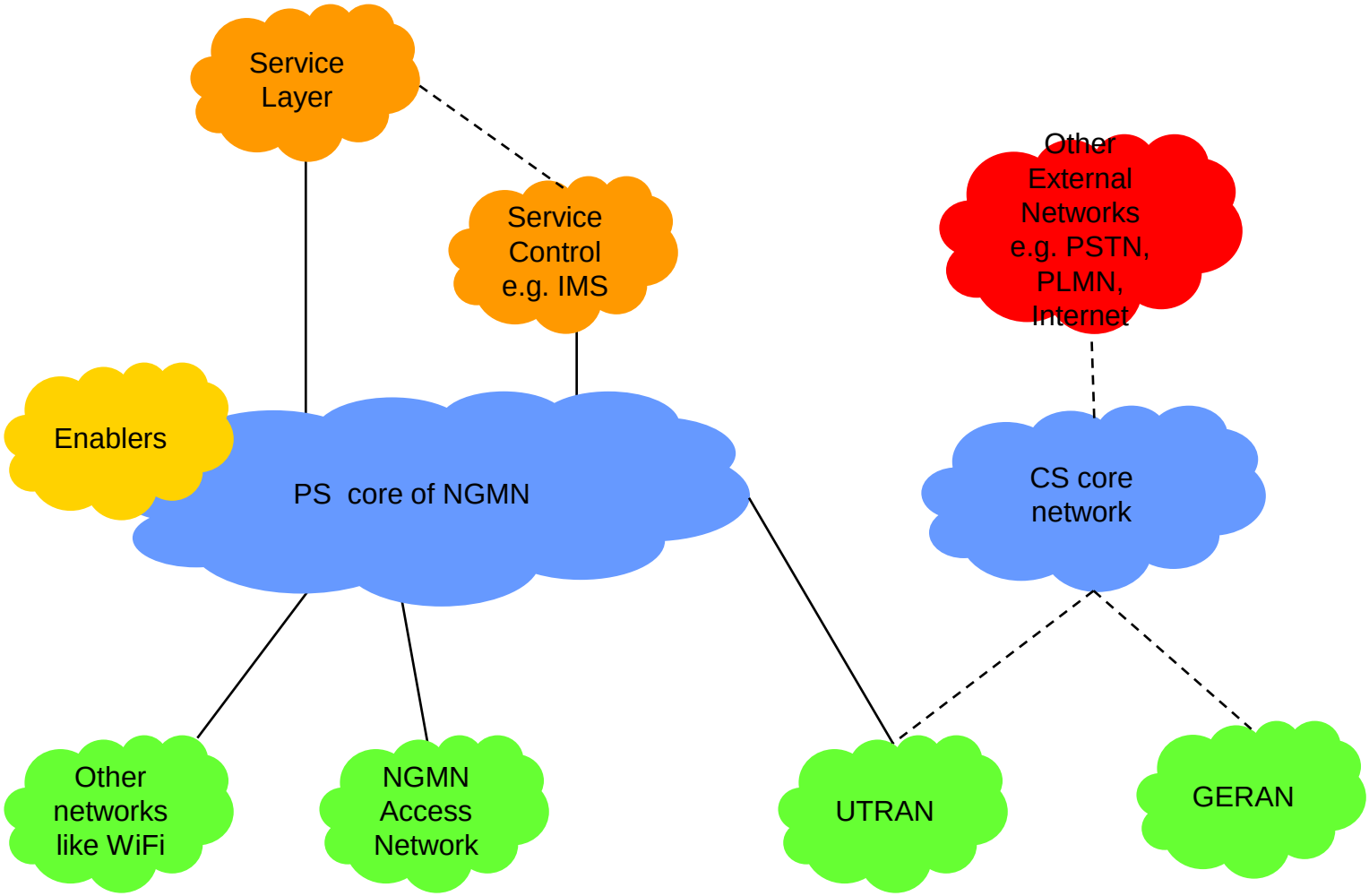
Next Generation Mobile Networks (NGMN) and 3GPP

Towards NGMN

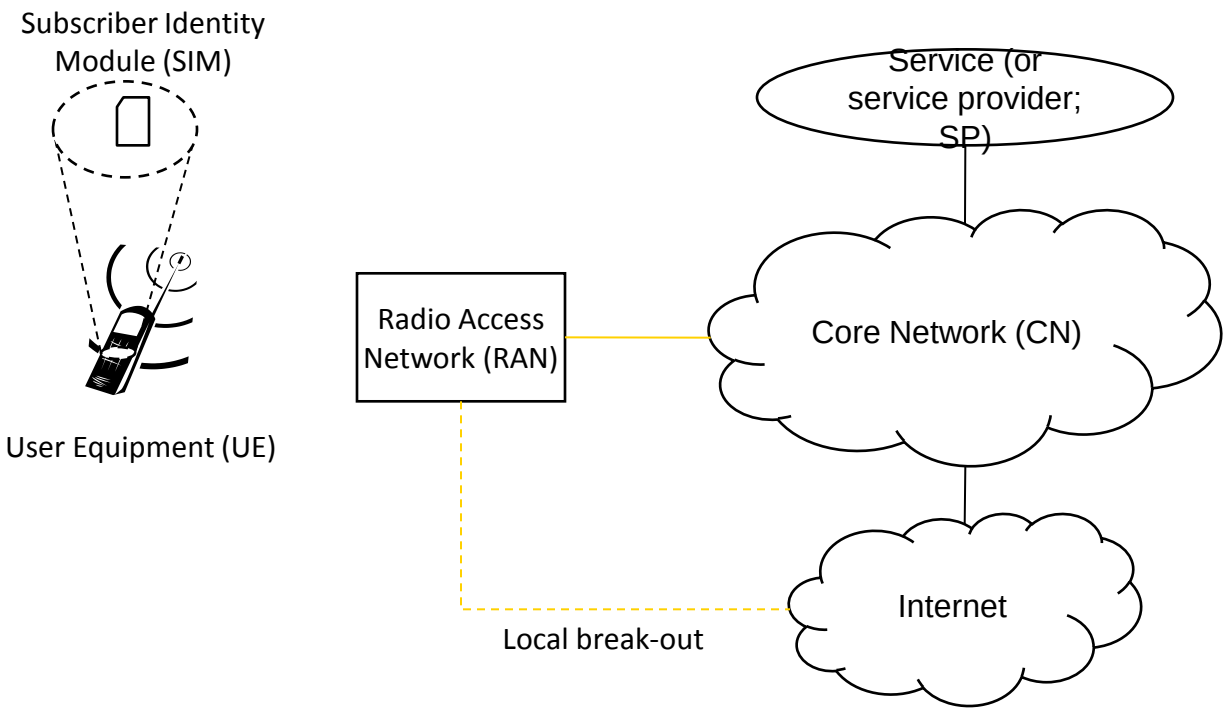
Next Generation Mobile Network (NGMN) is a project by mobile operators with the objective to establish recommendations, requirements and scenario for future mobile broadband networks



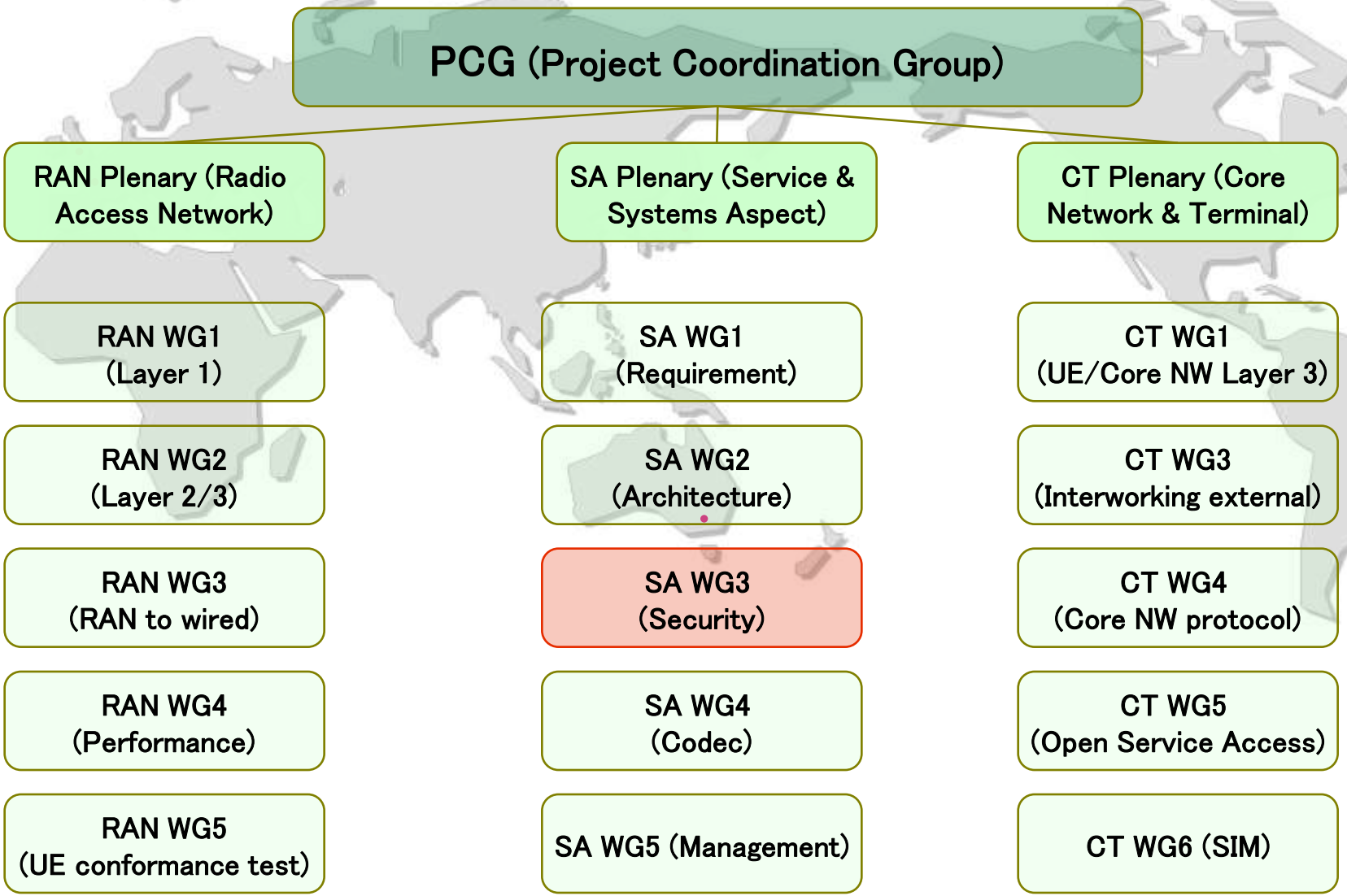
NGMN Architecture



3GPP Basic Network Architecture

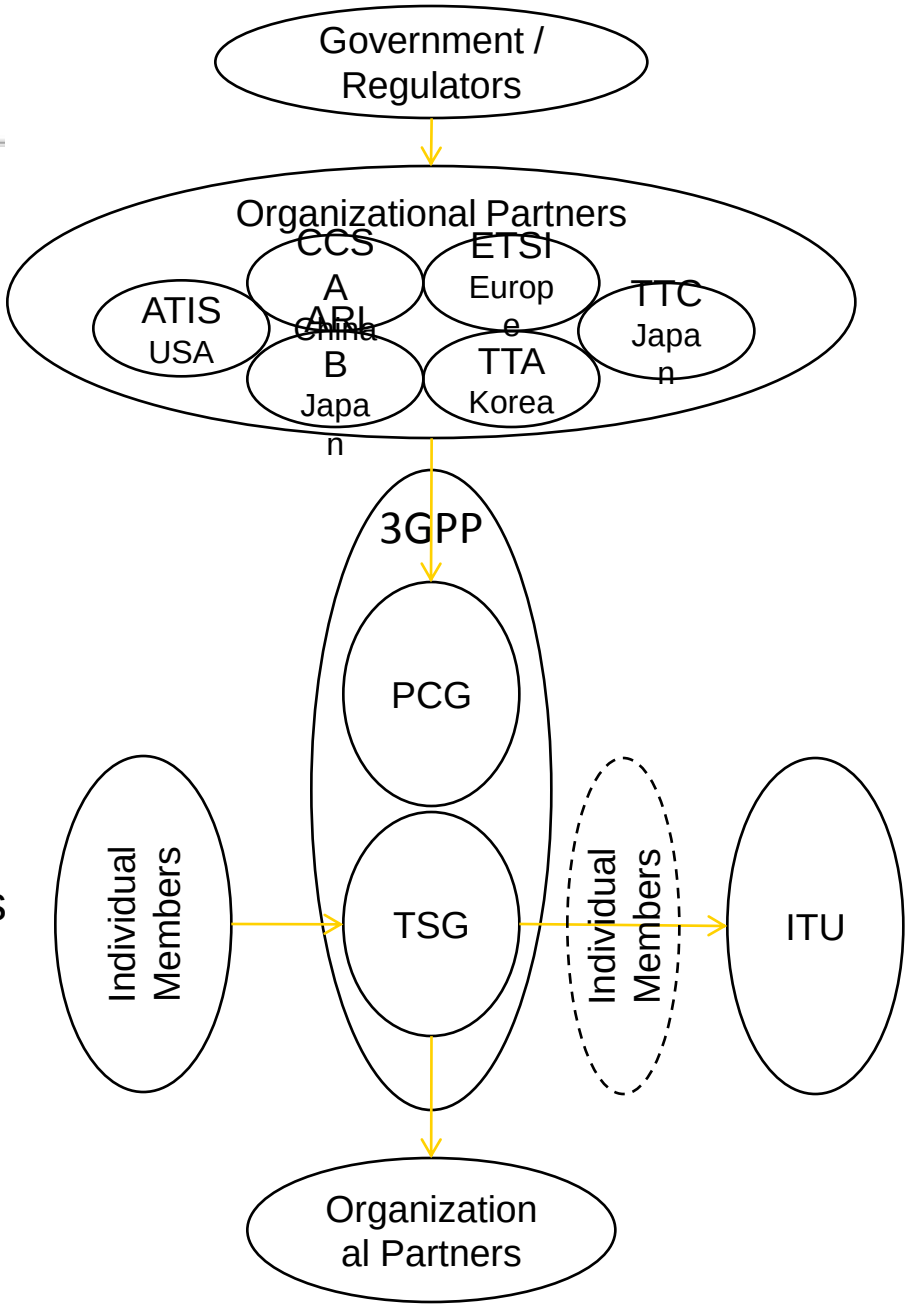


3GPP Overview



This is how it works

- Third Generation Partnership Project (3GPP) develops specification standardized by organizational partners (OPs)
- OPs follow their government / regulatory mandate
- OPs participate in the project coordination group (PCG)
- Individual members are member of at least one of the OPs and provide input to the technical specification group (TSG)
- Result of TSG is a TR or TS that forms specification by OPs
- 3GPP also takes input from ITU and uses its guideline
- Resulting specification from 3GPP TSG is taken to ITU by individual members as specification



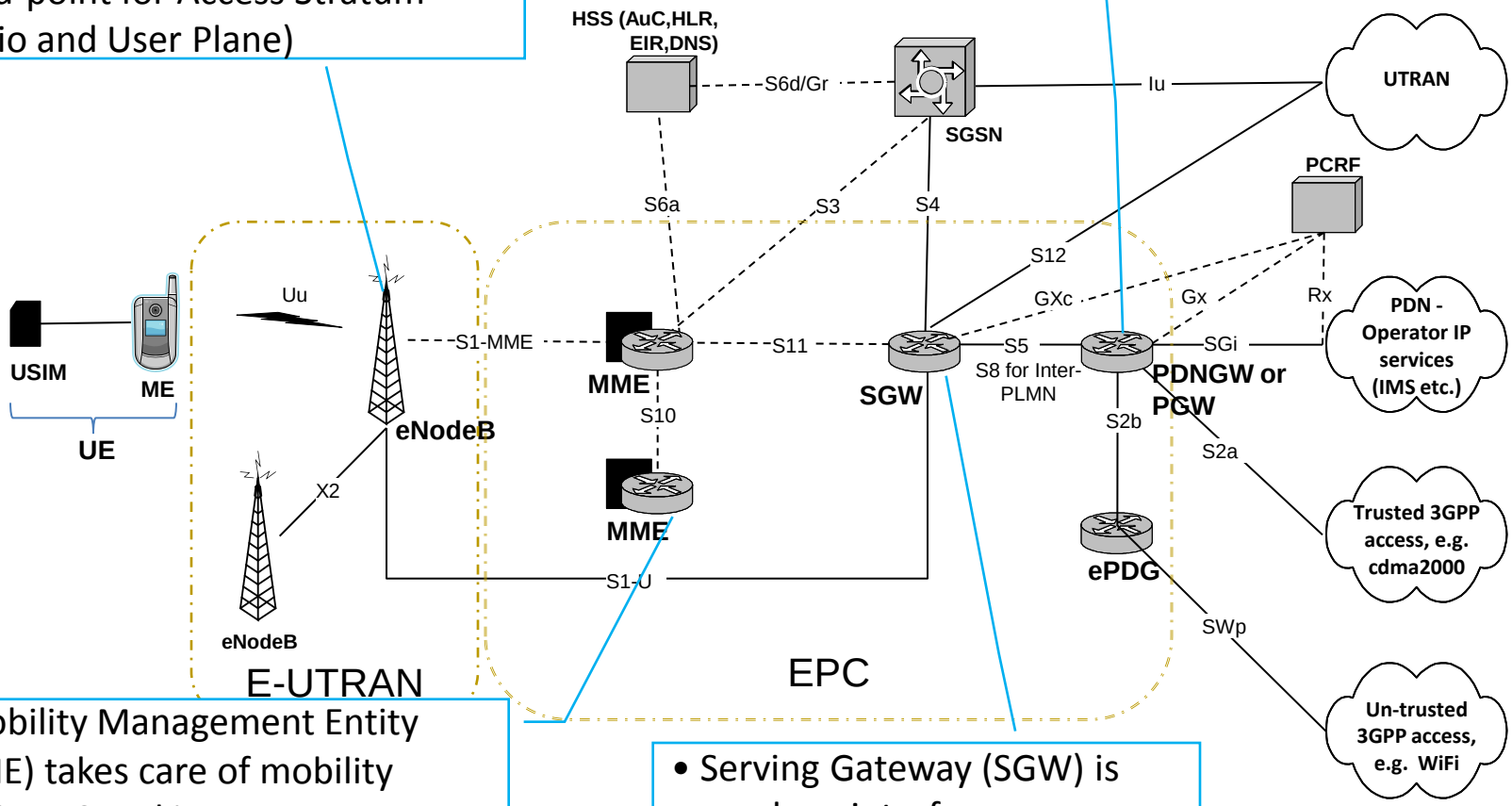
Empowered by Innovation NEC

EPS Overview

Network Overview

• The Packet Data Network Gateway (PDNGW) allocates IP address to the UE.
• Performs user based packet filtering
• Provides accounting for inter-operator charging, packet screening, rate enforcement etc.

• evolved NodeB takes over RNC and NodeB function of UMTS
• End-point for Access Stratum (Radio and User Plane)



• Mobility Management Entity (MME) takes care of mobility within EPS and inter-RAT
• Performs authentication
• End-point for NAS
• Selects gateways for UE

• Serving Gateway (SGW) is user plane interface termination point to eNodeB
• Local mobility anchor between eNodeBs

X2, S1-U, S2a, Rx etc. are reference points between network elements. Protocols are defined for each reference point.
Solid lines between network elements are mainly for user plane traffic as defined by 3GPP while dashed lines are mainly for control plane.

Abbreviations

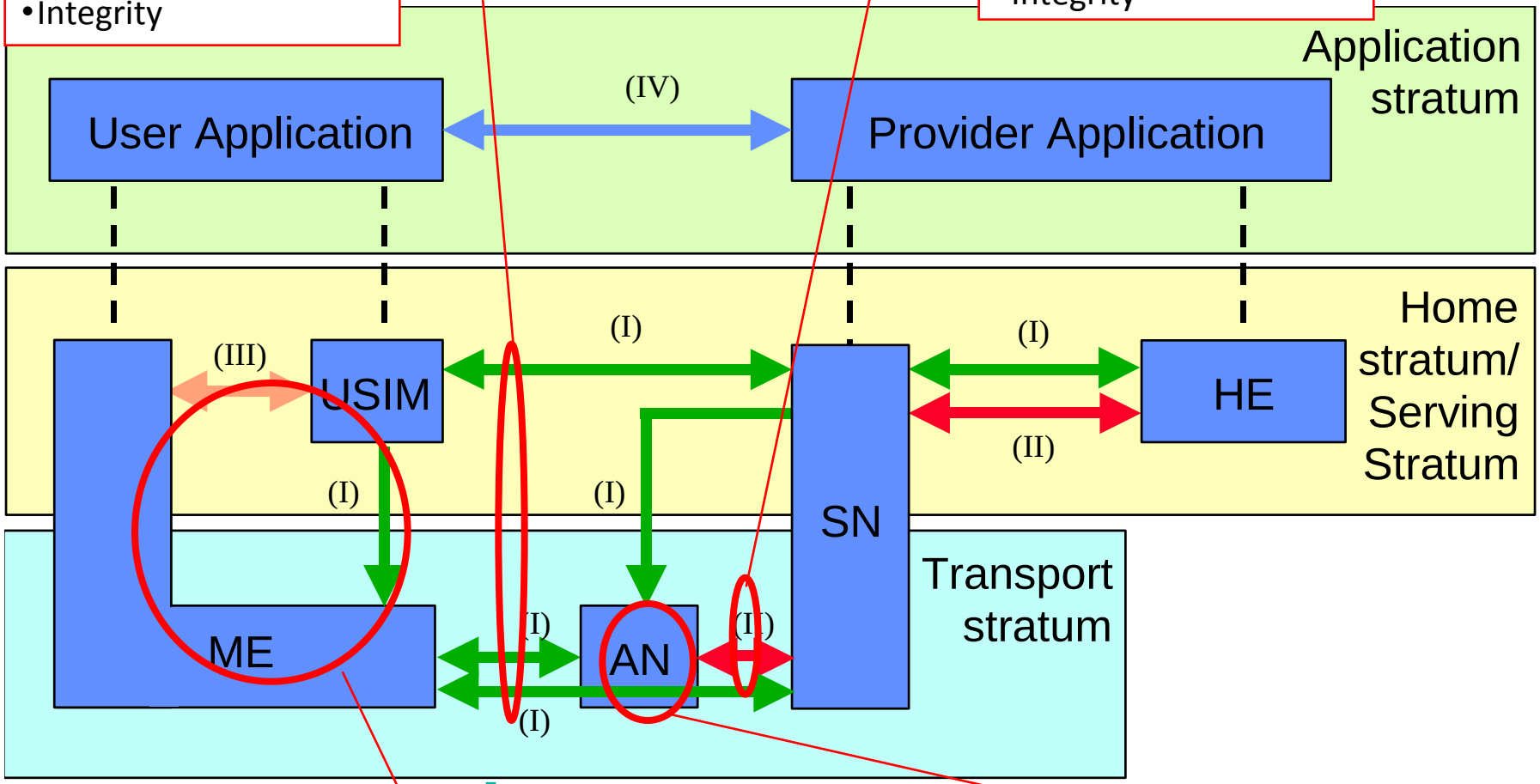
AuC	Authentication Center	MME	Mobility Management Entity
DNS	Domain Name System	PCRF	Policy and Charging Rules Function
EIR	Equipment Identity Register	PDN	Packet Data network
EPC	Evolved Packet Core	PDNGW or PGW	Packet Data Network Gateway
E-UTRAN	Evolved-UTRAN	PLMN	Public Land-Mobile Network
ePDG	evolved Packet Data Gateway	SGSN	Serving GPRS Support Node
GERAN	GSM EDGE Radio Access Network	SGW	Serving Gateway
HLR	Home Location Register	UE	User Equipment
HSS	Home Subscriber Subsystem	USIM	Universal Subscriber Identity Module
ME	Mobile Equipment	UTRAN	UMTS Terrestrial Radio Access Network

EPS Security

Security Overview

- Entity authentication
- Confidentiality
- Integrity

- Authentication
- Confidentiality
- Integrity

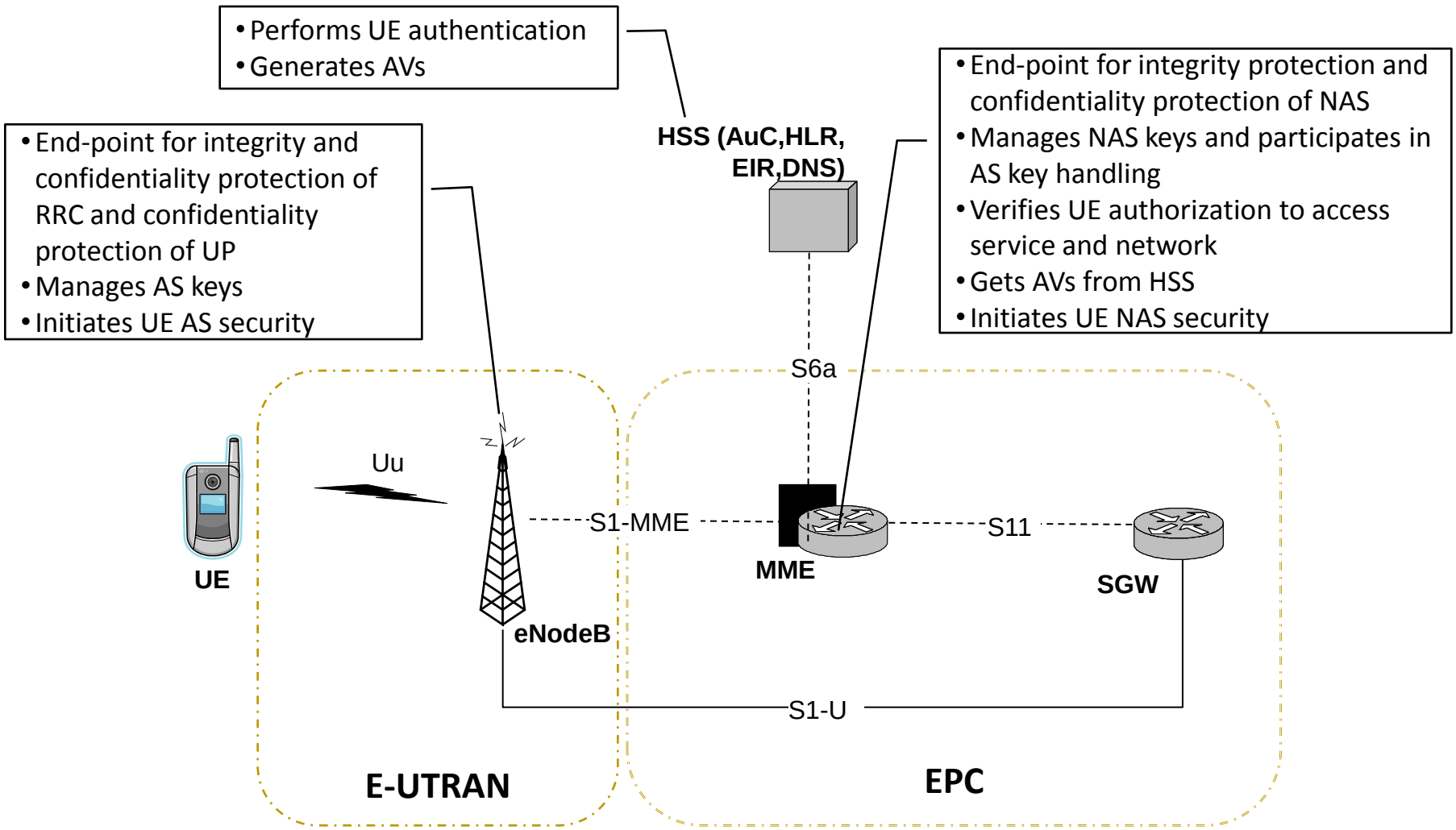


- **Network access security (I)**
- **Network domain security (II)**
- **User domain security (III)**
- **Application domain security (IV)**
- **Visibility and configurability of security (V)**

For UE:
- Privacy: User identity
- Device confidentiality

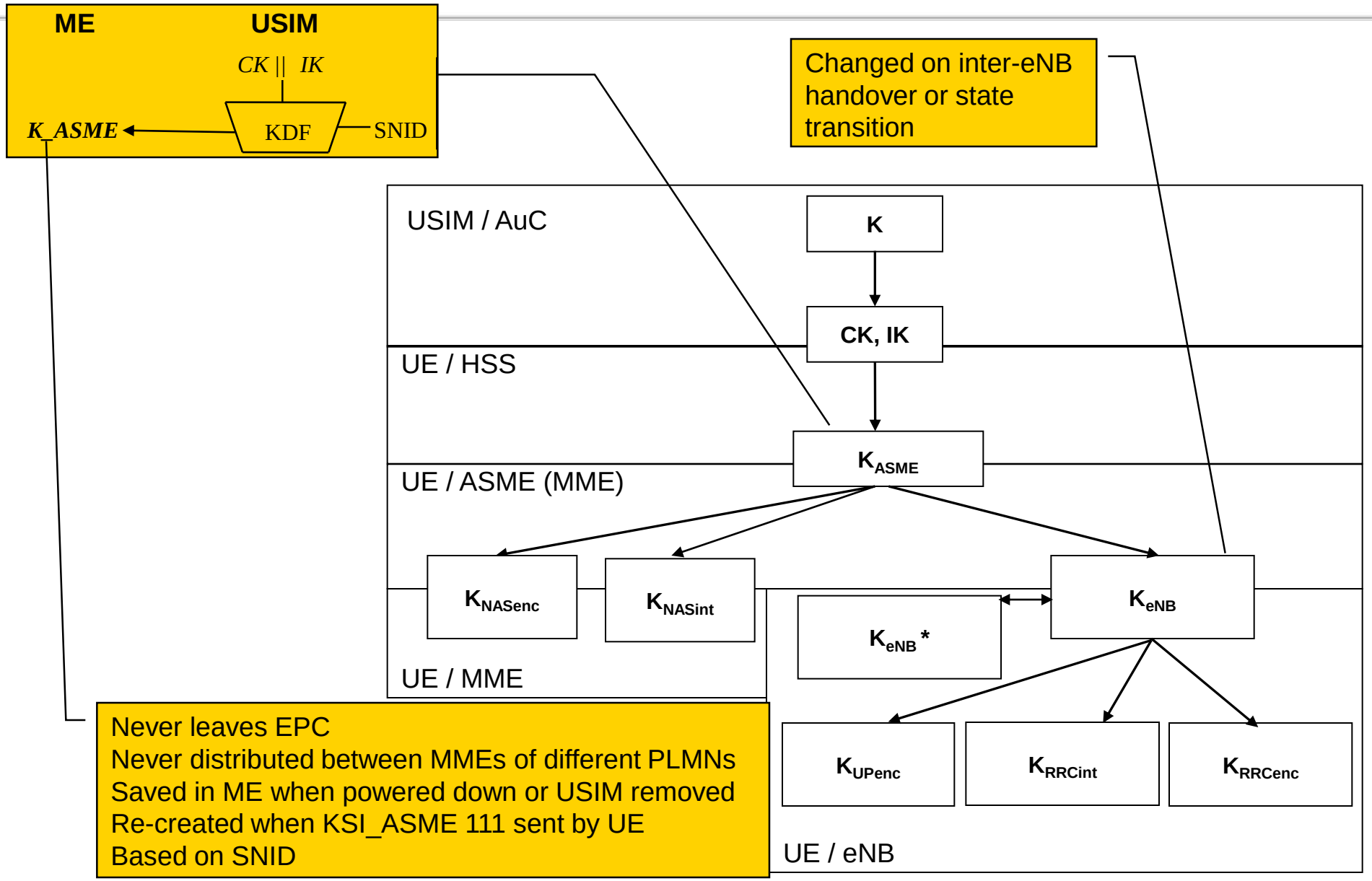
For eNB:
- Requirement on storage
- Handling of keys and data

Network Elements and Security Functions



Confidentiality is optional and integrity protection is mandatory and uses SNOW 3G or AES (or ZUC)

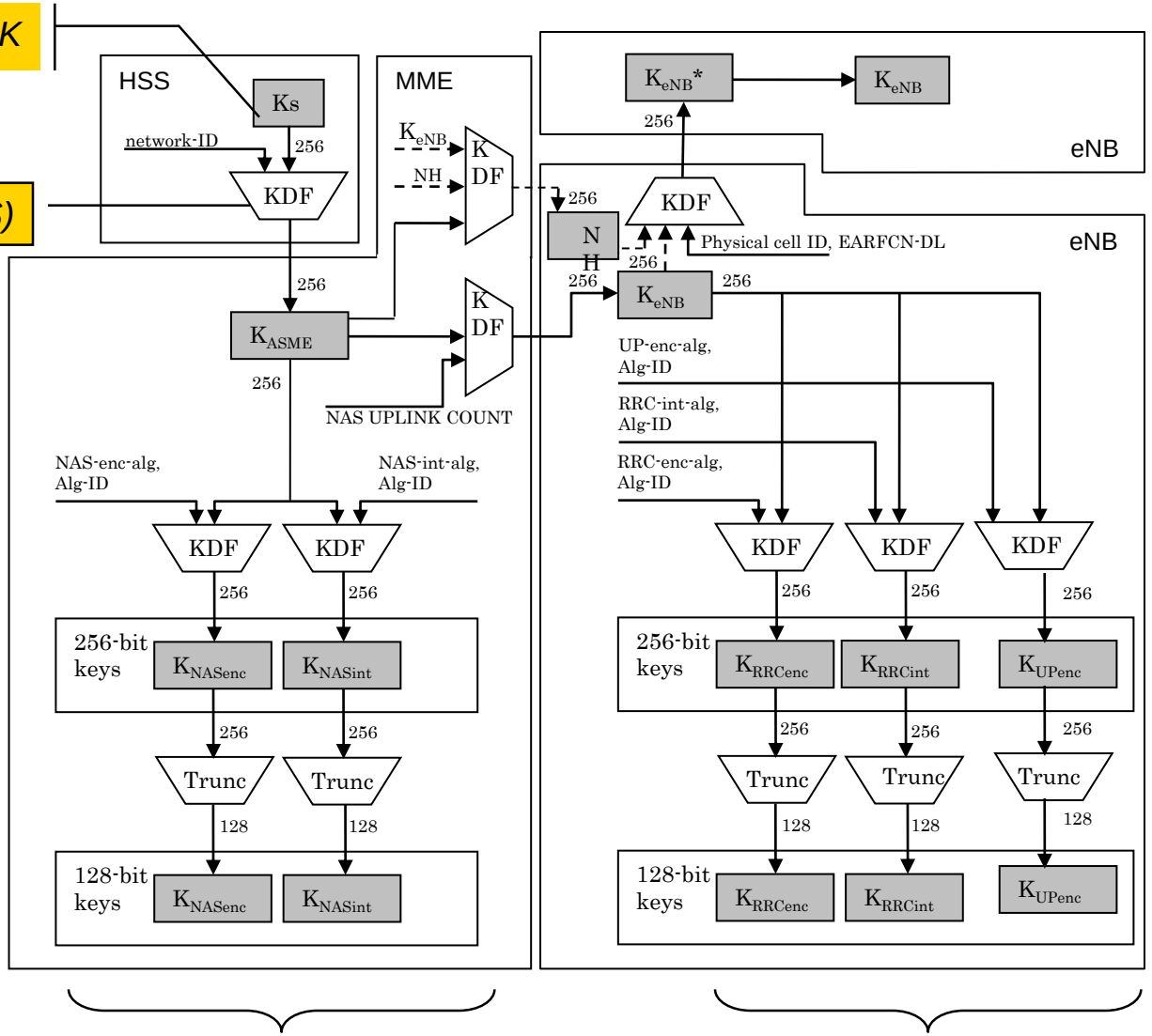
Key Hierarchy



Network: Key Distribution and Derivation

K_s= CK || IK

KDF is HMAC-SHA-256 (Key, S)

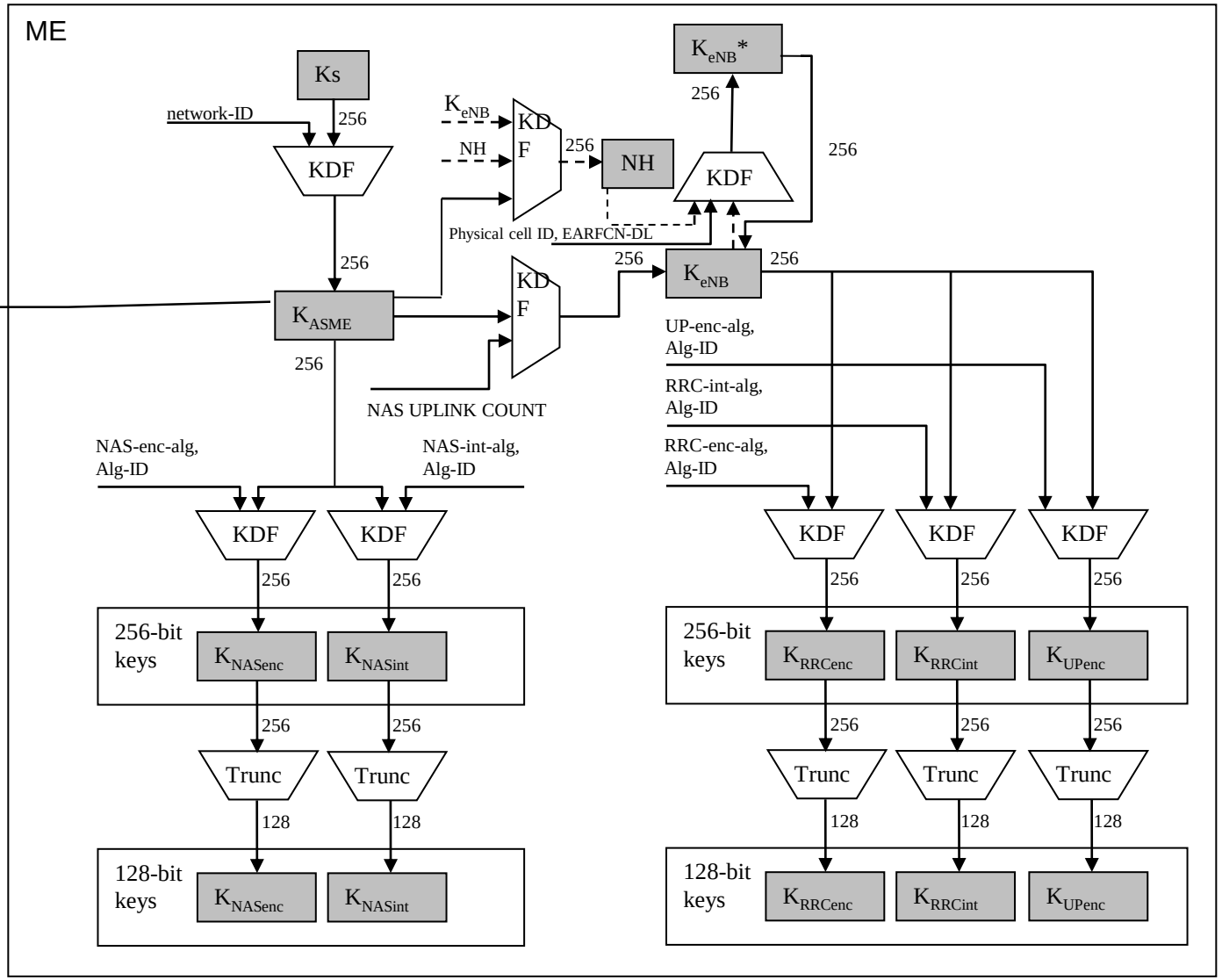


Ciphering is optional. Most NAS msgs. are integrity protected.

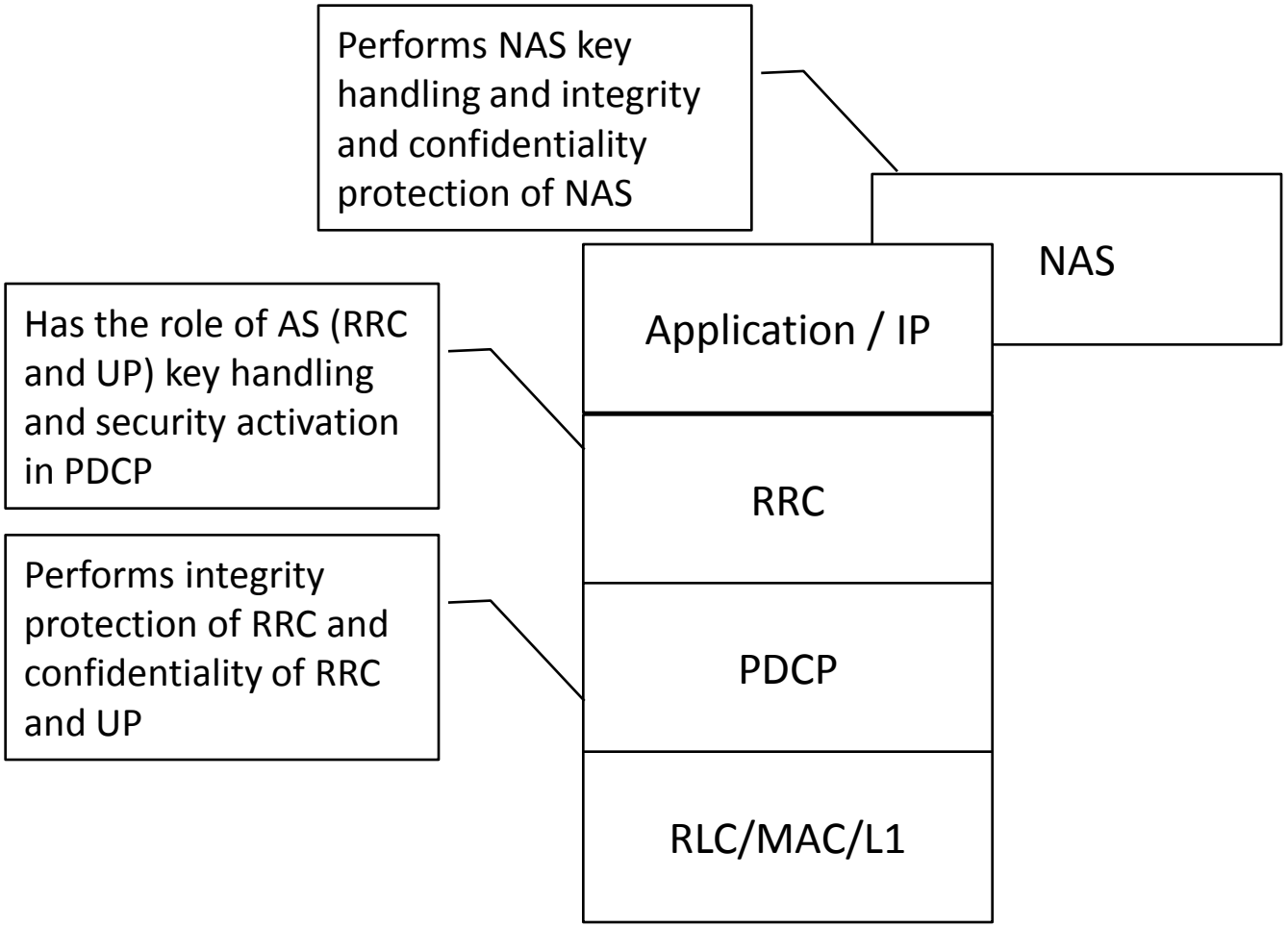
UP and RRC algos. work at PDCP layer. Ciphering is optional

ME: Key Distribution and Derivation

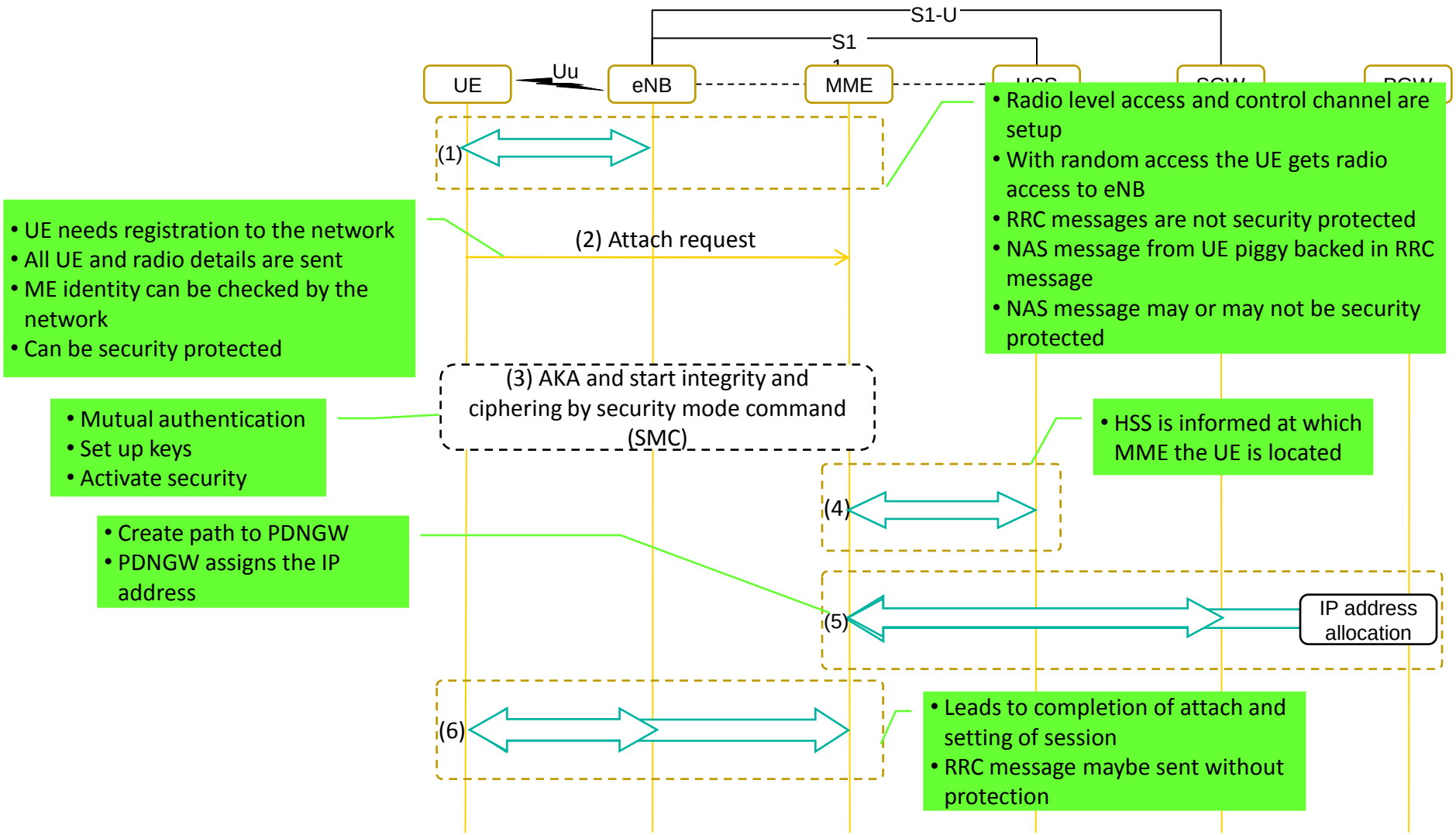
Kasme, KSIasme and uplink/downlink COUNTs stored also when switched off. ME checks for valid USIM / availability of USIM when switch on else deletes all context information



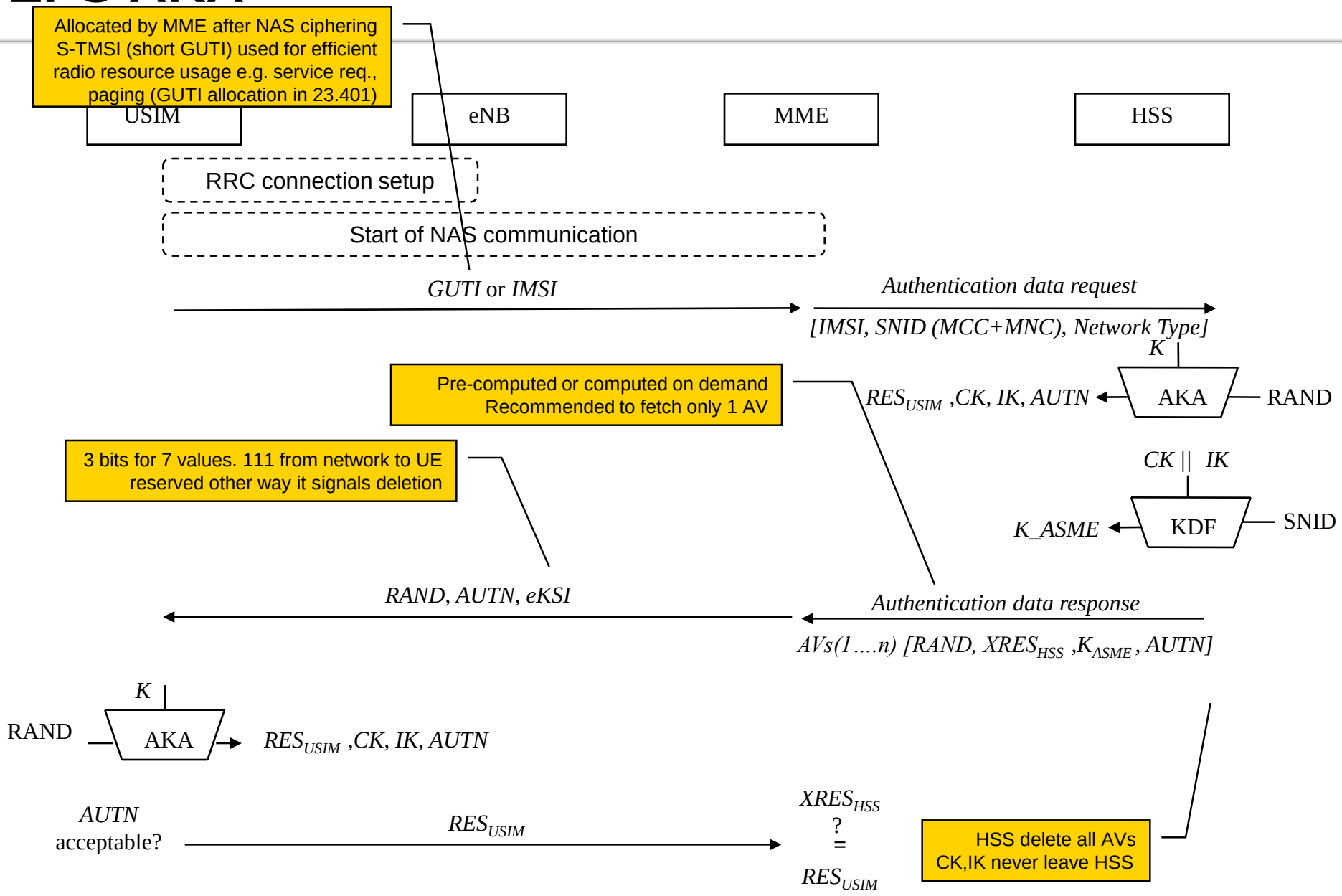
Protocol Layers and Security Functions



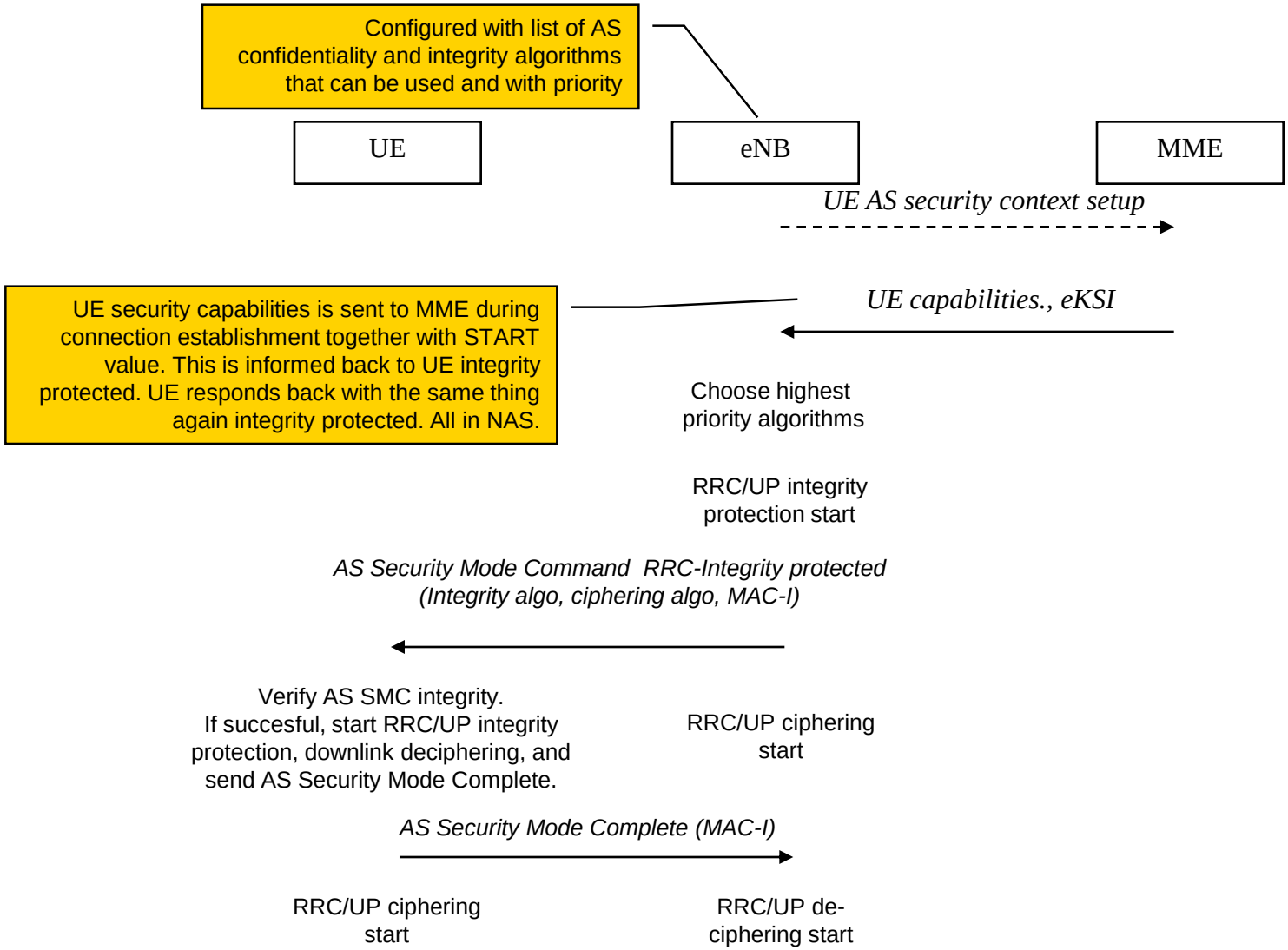
EPS Terminal Start-up and Security



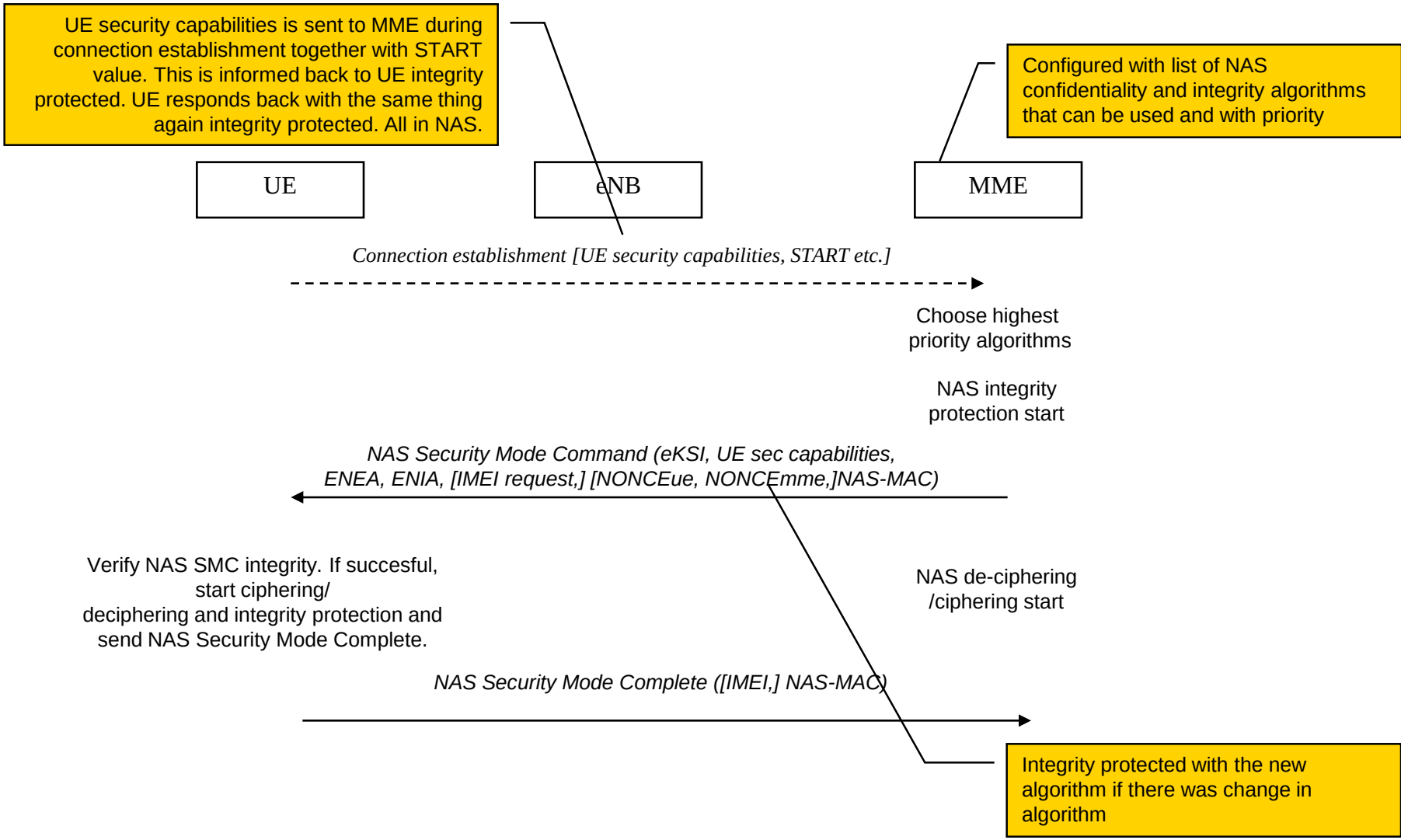
EPS AKA



SMC: AS Algorithm Selection



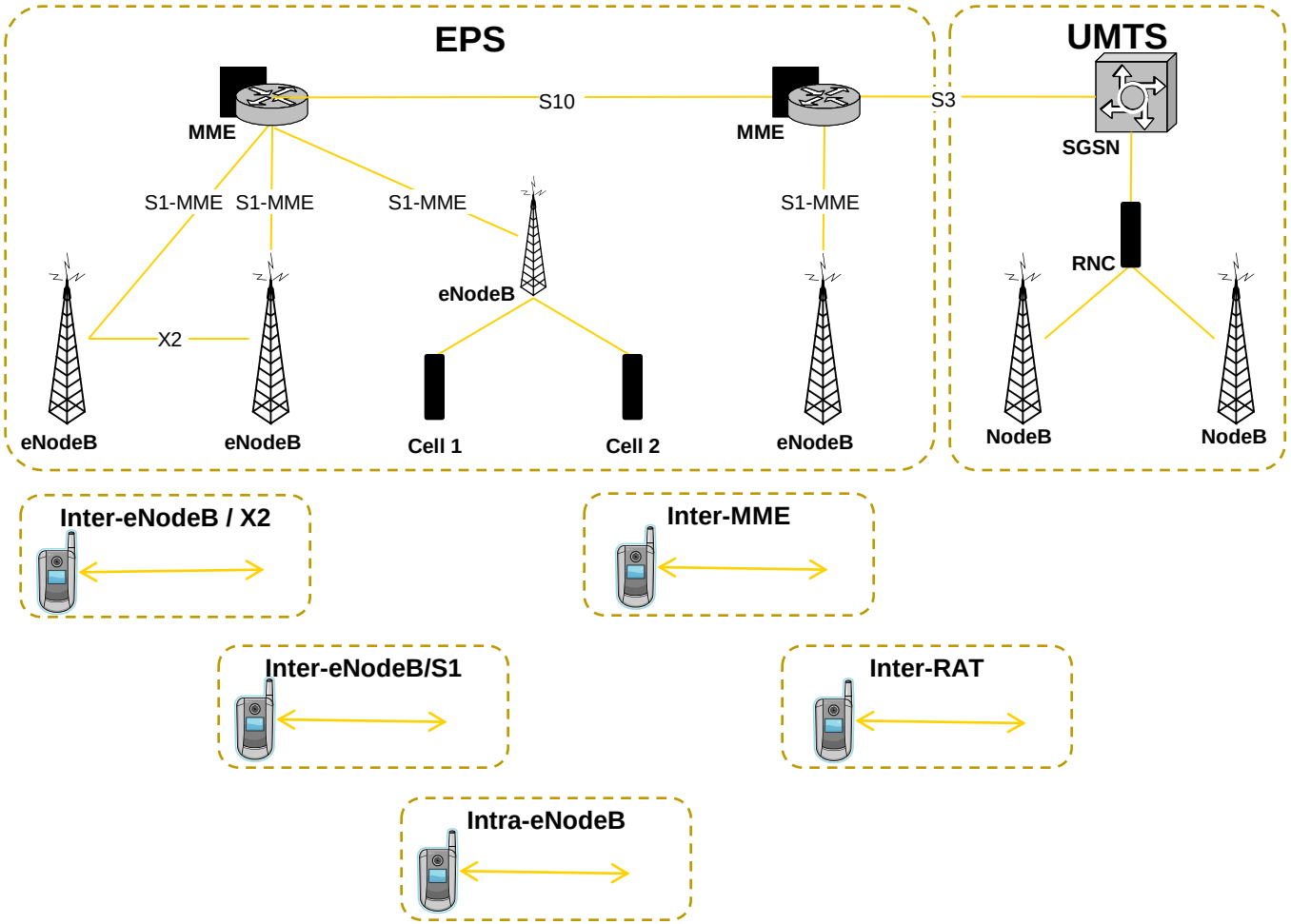
SMC: NAS Algorithm Selection



Security Termination Points

	Ciphering (Usage optional/implementation required)	**Integrity Protection** (Usage & implementation required)
NAS Signalling	Optional and terminated in MME	Mandatory and terminated in MME
U-Plane Data	Optional and terminated in eNB	Not Required
RRC Signalling (AS)	Optional and terminated in eNB	Mandatory and terminated in eNB

Mobility in EPS



Secure Handover in Evolved Packet System (EPS)

Provides forward and backward security

Serving eNB assumed compromised

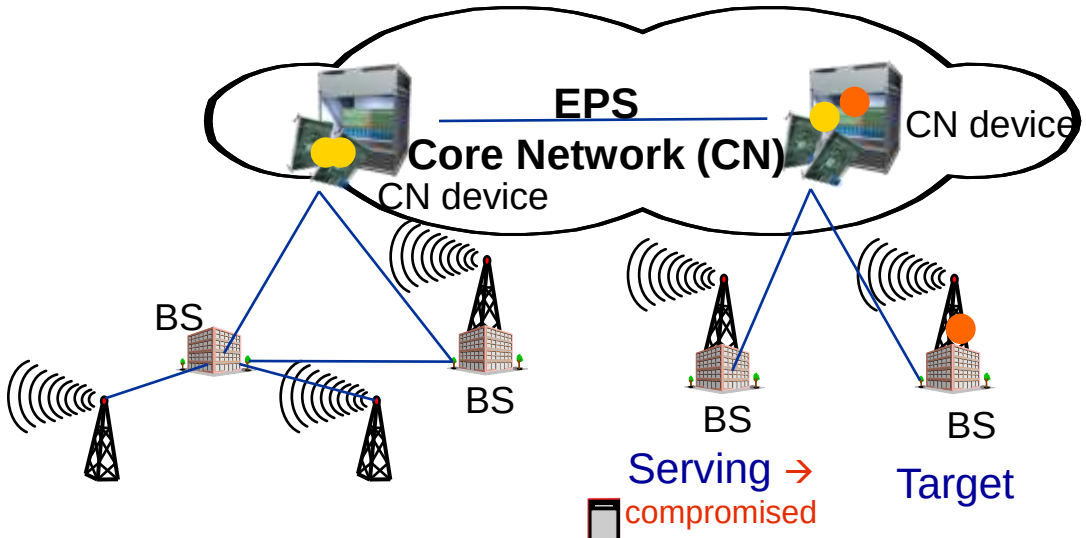
Provide security material before handover → Not good

Provide security material during handover → Not good

Provide security material after handover → Good

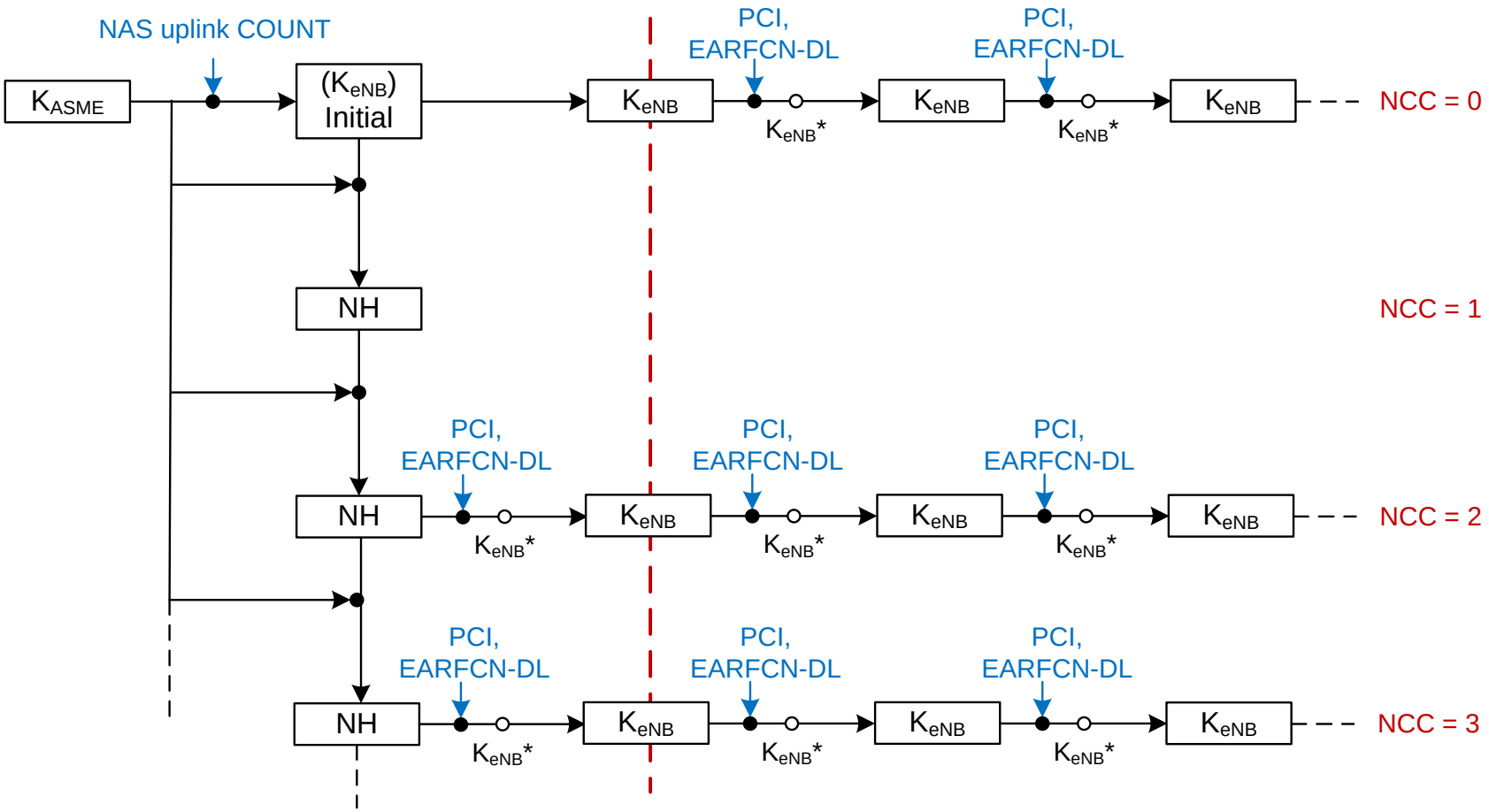
Security material given by BS → Not good

Security material given by core network → Good



If assumption is valid, first hop of handover will not be secure thus next hop security in LTE

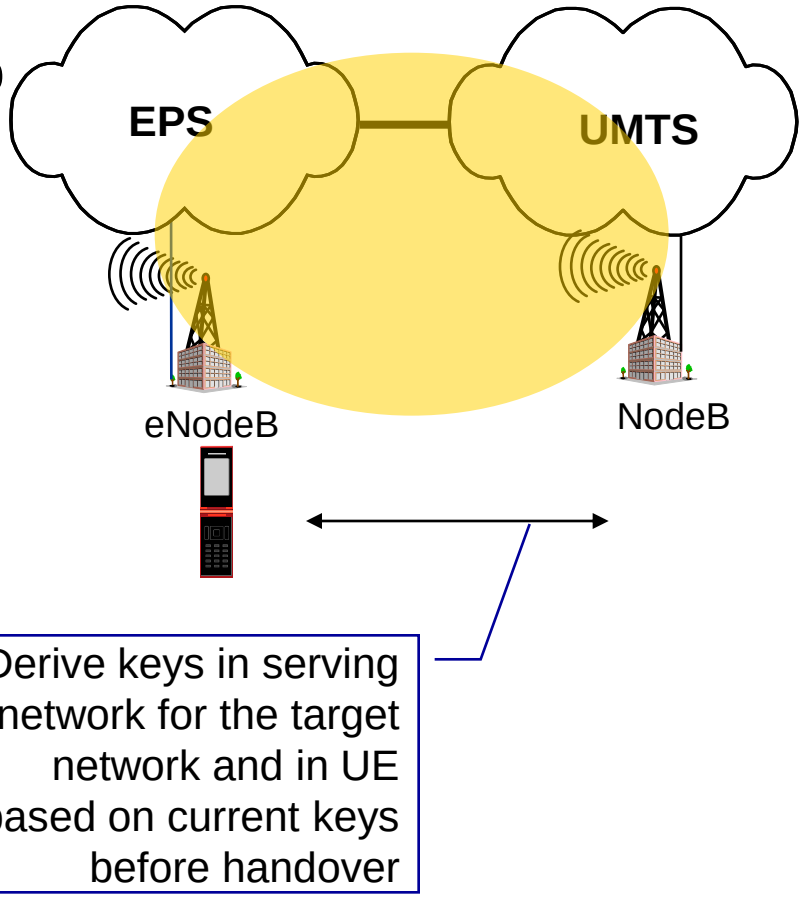
Handover Key Handling



NH: Next Hop
NCC: Next hop Chaining Counter
PCI: Physical Cell Identity

Inter-Technology Handover for EPS

- The idea here is to derive keys both ways from the existing context and do AKA at the earliest possible especially in E-UTRAN
- The keys are named as follows:
  - Mapped context is the one derived from other RAT keys
  - Current context is the context being used
  - Native context is the context of E-UTRAN
- On handover to E-UTRAN mapped context is used although it is recommended that native context should be used as it is considered stronger



Other Security Aspects

Network domain control plane protection

- Protection of IP based control plane will be done using 33.210. If the interfaces are trusted then such protection is not required.
- Thus for S1-MME and X2-C
  - Implement IPsec ESP [RFC 4303 and TS 33.210]
  - IKEv2 certificate based authentication [TS 33.310]
  - Tunnel mode IPsec mandatory on eNB while SEG can be used in core
  - Transport mode is optional

Backhaul link user plane protection

- Protection of user plane will be done using 33.210. If the interfaces are trusted then such protection is not required.
- S1-U and X2-U
  - IPsec ESP as in RFC 4303 and TS 33.210 with confidentiality, integrity and replay protection
  - IKEv2 certificate based authentication [TS 33.310]
  - Tunnel mode IPsec mandatory on eNB while SEG can be used in core
  - Transport mode is optional

Management plane protection

- Same as S1-U and X2-U
- There is no management traffic over X2

More – Conclusions

Conclusions

- Today we took a look at Evolved Packet System (EPS) security – the next generation of mobile communications
  - For more check the 3GPP technical specification: TS 33.401 <http://www.3gpp.org/ftp/Specs/html-info/33401.htm >
- Some of the topics currently 3GPP is working on:
  - Taking care of unsolicited communication
  - Relay node security – IMT-advanced
  - Home(e)NodeB enhancements
- We also spent some time on what the future holds
  - Penetration of security understanding should increase bringing with it more demand on security itself
  - Complete system consideration of security will become even more necessary – Bringing potential change in business arena – providers of service at different layers working together?

Empowered by Innovation