As presented at NIKSUN WWSMC
July 25-27, 2011 | www.niksun.com

Empowered by Innovation NEC

3GPP SAE/LTE Security

Anand R. Prasad
<anand@bq.jp.nec.com>
NEC Corporation

Disclaimer: This presentation gives views/opinion of the speaker and not necessarily that of NEC Corporation.

NIKSUN WWSMC, 26 July, 2011, Princeton, NJ, USA
MI事企画M11-0043

Outline

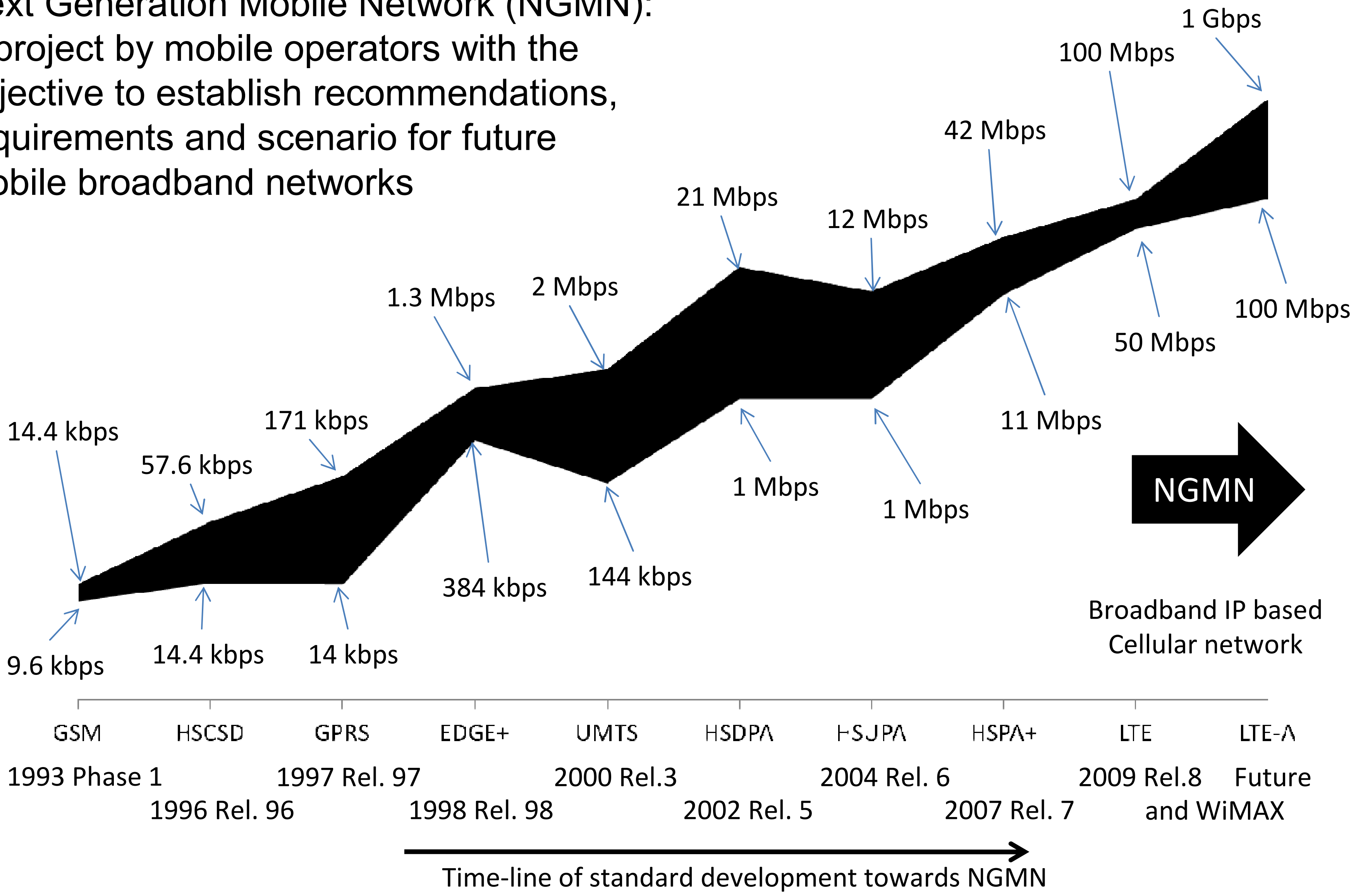
- Background on how this thing came into being:
  - Next Generation Mobile Networks (NGMN) and
  - Third Generation Partnership Project (3GPP)
- Brief overview of Evolved packet system (EPS), i.e., SAE/LTE
- Security in EPS:
  - Requirements
  - Security per network elements and protocol layers
  - Key hierarchy
  - Authentication and key agreement
  - Mobility
- Today and Tomorrow – including current security activities in Global ICT Standardisation Forum for India (GISFI)

For abbreviations check Slide 34

Next Generation Mobile Networks (NGMN) and 3GPP

Towards NGMN

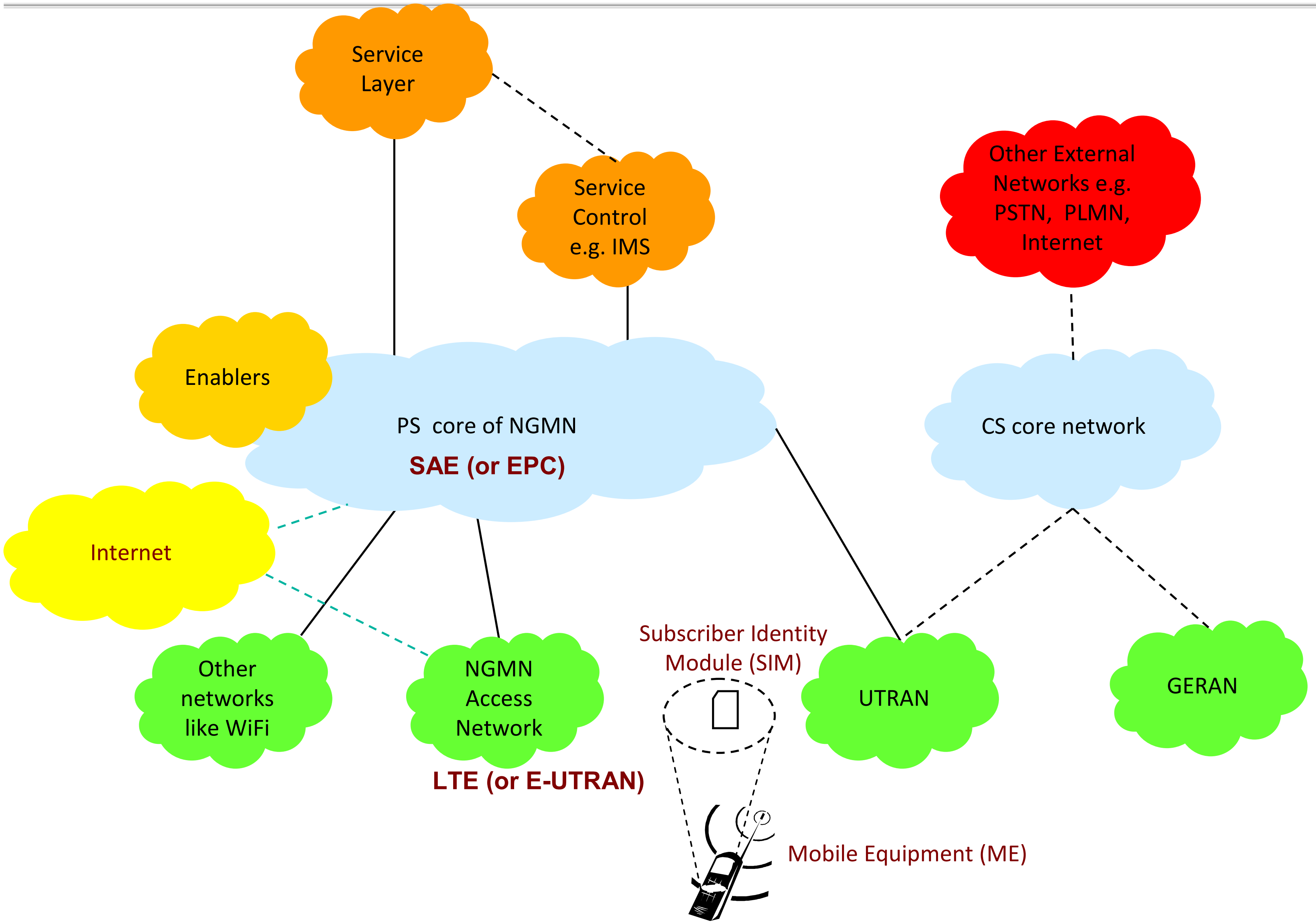
Next Generation Mobile Network (NGMN):
A project by mobile operators with the objective to establish recommendations, requirements and scenario for future mobile broadband networks



Broadband IP based Cellular network

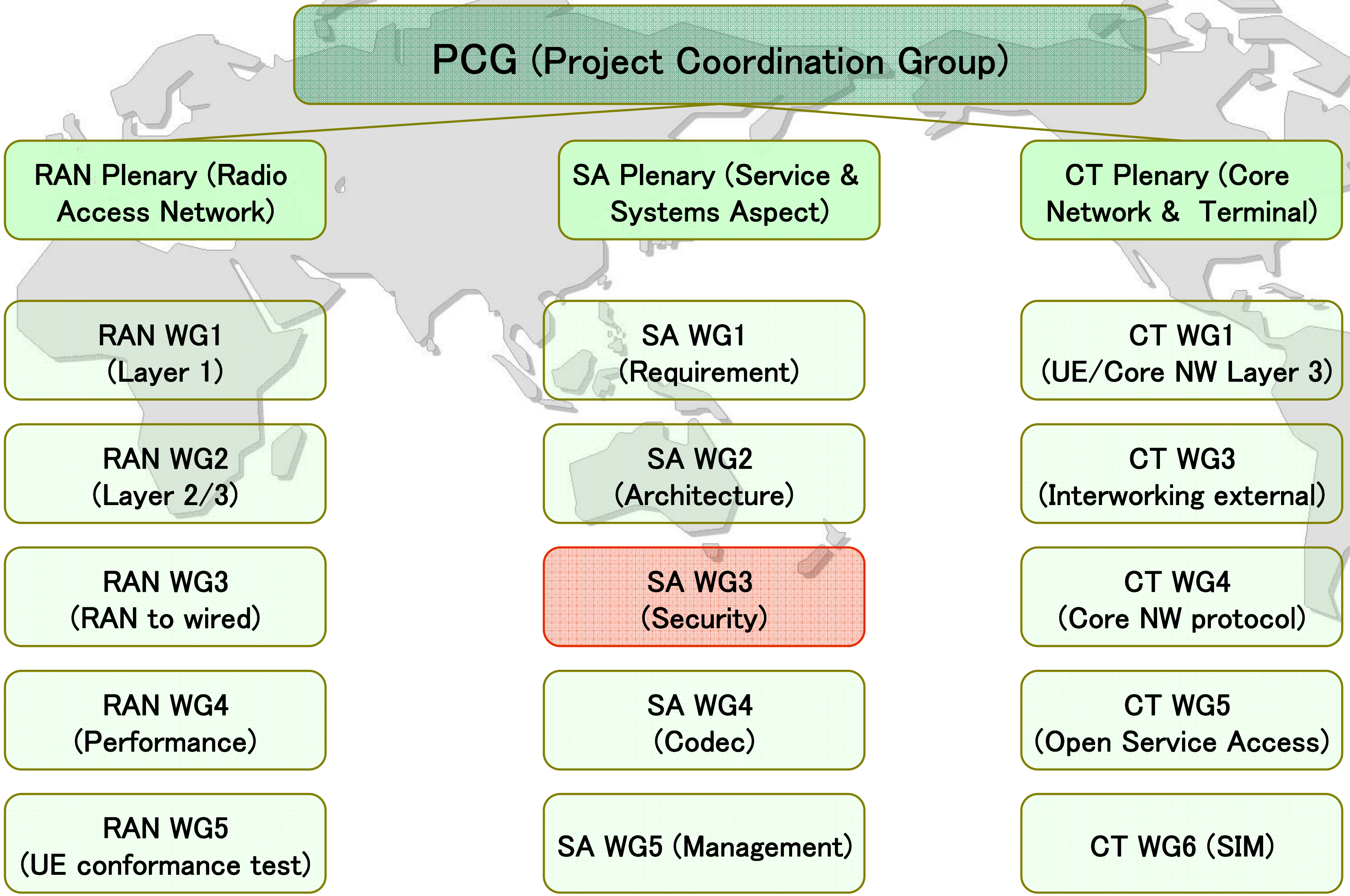
Time-line of standard development towards NGMN

NGMN Architecture 3GPP Basic Architecture



User Equipment (UE)

3GPP Overview



PCG (Project Coordination Group)

RAN Plenary (Radio Access Network)

SA Plenary (Service & Systems Aspect)

CT Plenary (Core Network & Terminal)

RAN WG1 (Layer 1)

RAN WG2 (Layer 2/3)

RAN WG3 (RAN to wired)

RAN WG4 (Performance)

RAN WG5 (UE conformance test)

SA WG1 (Requirement)

SA WG2 (Architecture)

SA WG3 (Security)

SA WG4 (Codec)

SA WG5 (Management)

CT WG1 (UE/Core NW Layer 3)

CT WG3 (Interworking external)

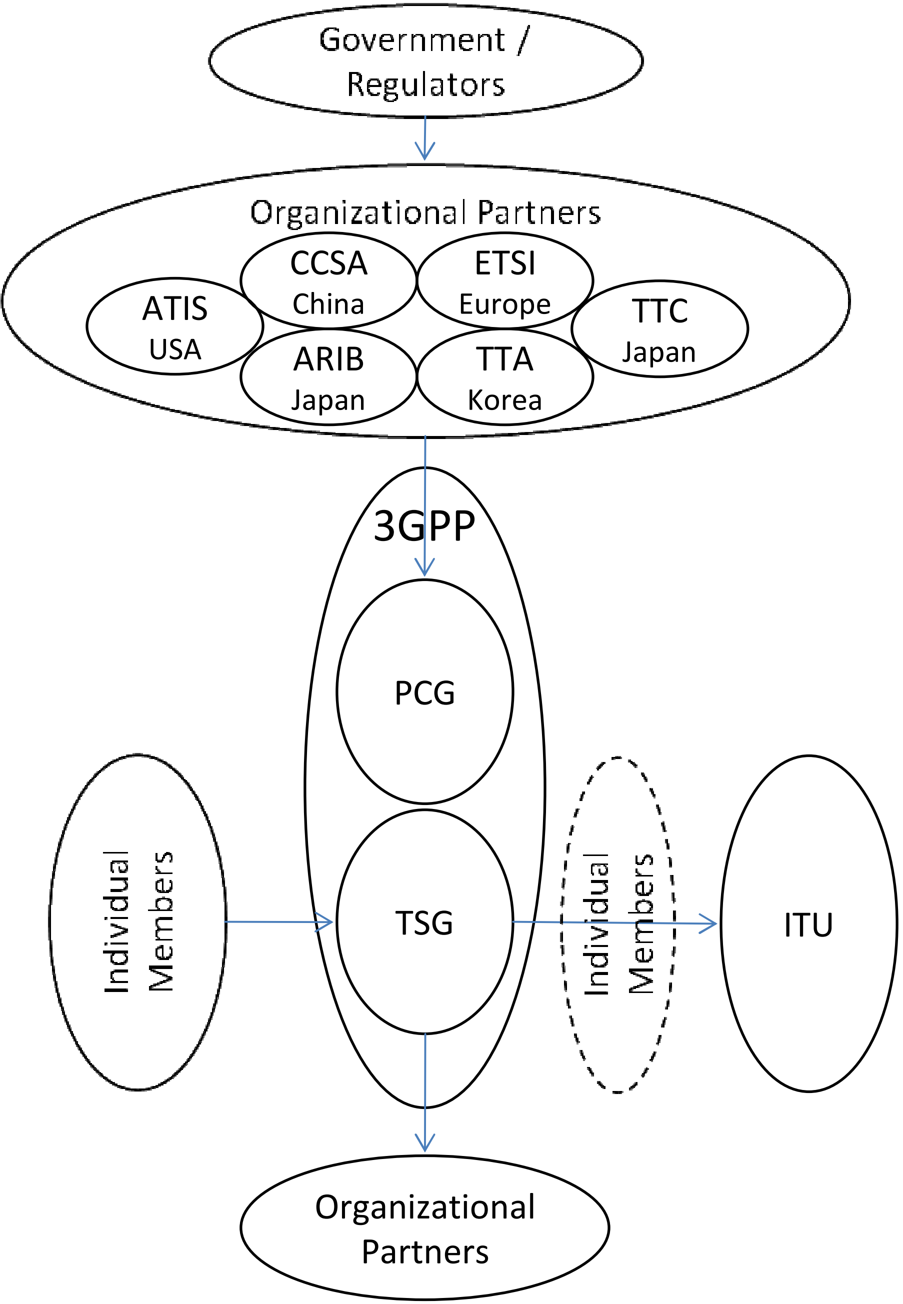
CT WG4 (Core NW protocol)

CT WG5 (Open Service Access)

CT WG6 (SIM)

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 standars 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



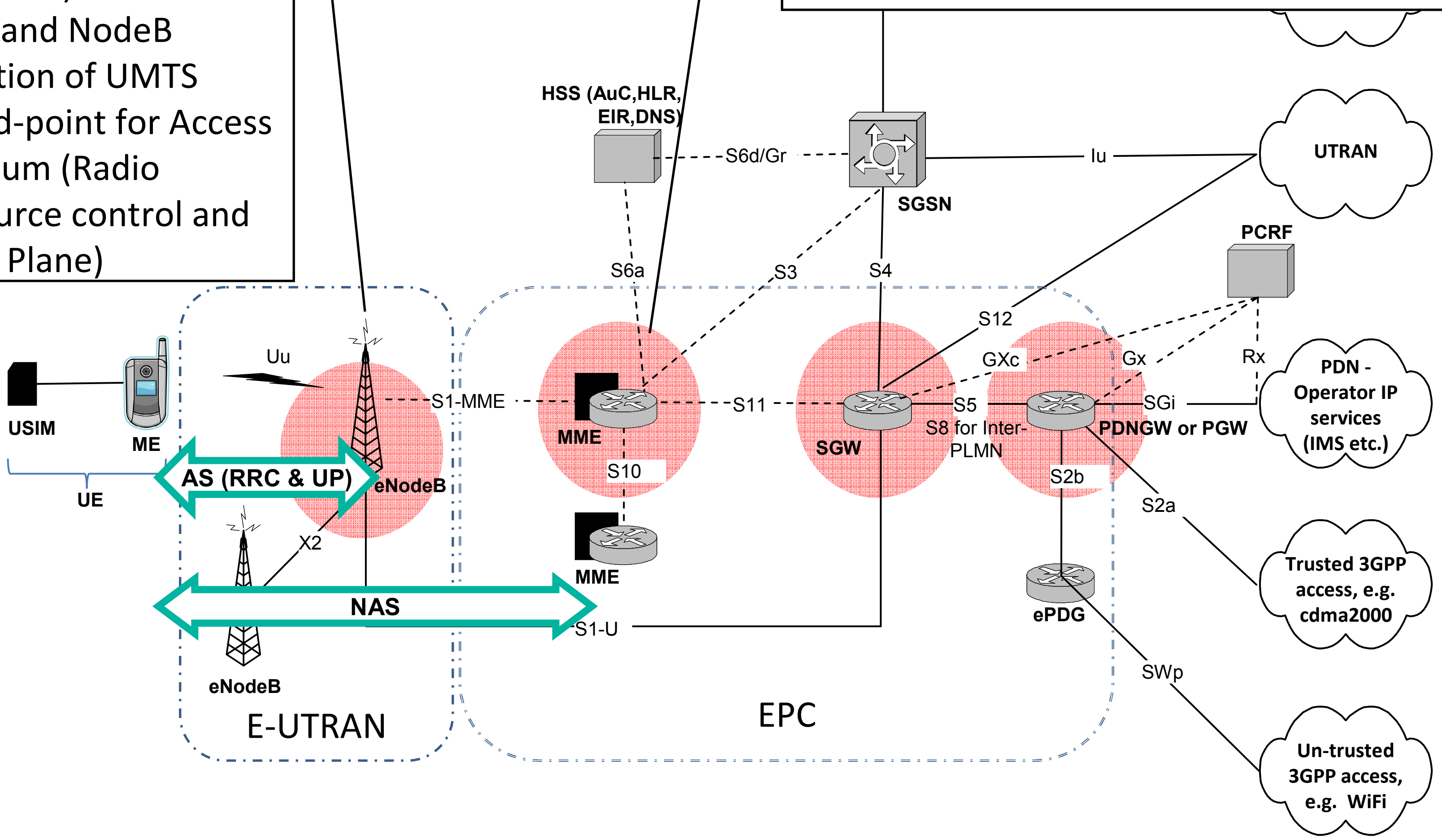
Evolved Packet System (EPS) Overview and Security

- EPS is also know as System Architecture Evolution (SAE) / Long Term Evolution (LTE)
- SAE is also known as Evolved Packet Core (EPC)
- LTE is also known as Evolved UTRAN

Network Overview

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

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



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.
Highlighted network elements are newly introduced network elements in SAE/LTE (EPS). Explanation of network elements related to security are given here.

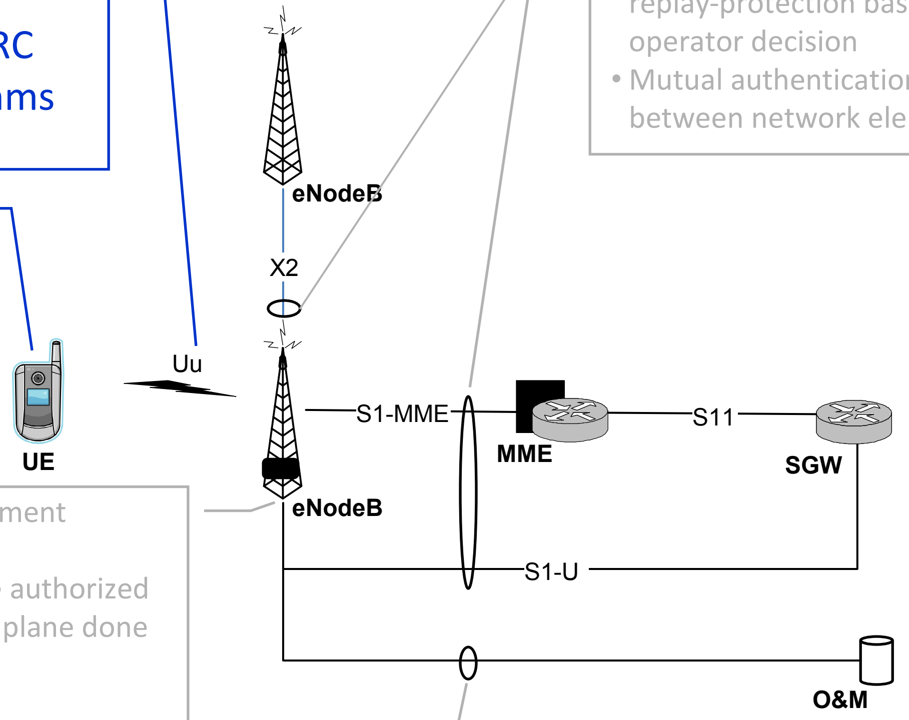
Basic Requirements

- Continued usage of current USIM, i.e., there should not be any change in USIM for accessing EPS network. The USIM that is used in UMTS networks should be thus reusable.
- Security should be at least of the same level or better than that compared to UMTS.

Security Requirements

- Mutual authentication between UE and network
- Optional confidentiality
- Mandatory integrity protection for RRC and NAS and optional for UP (algorithms are SNOW 3G and AES)

- MSIN & IMEI(SV) should be confidentiality protected
- IMEI(SV) should be sent only after NAS security is activated

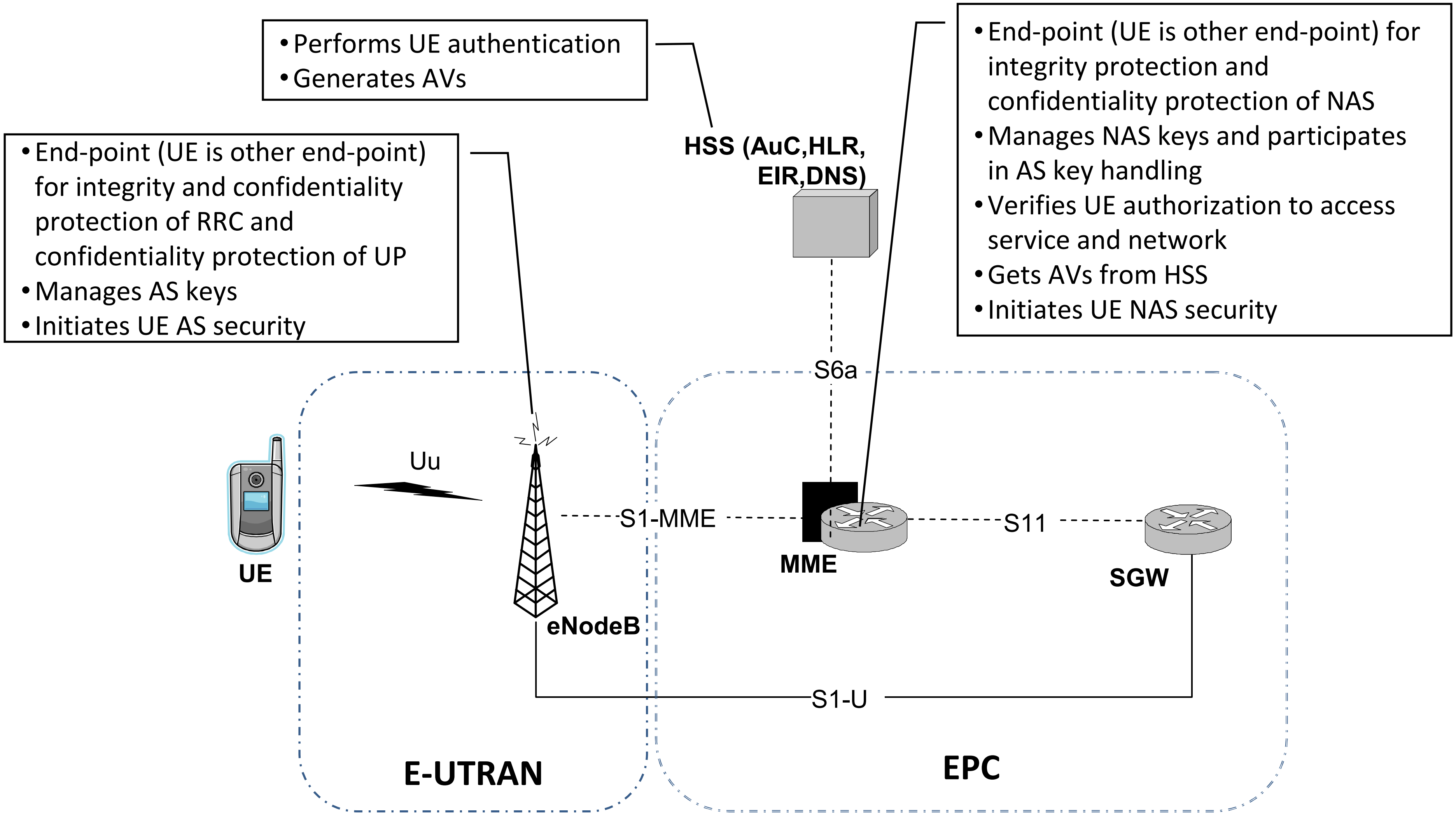


- Integrity, confidentiality and replay-protection based on operator decision
- Mutual authentication between network elements

- Sensitive part of boot-up in secure environment
- Uses authorized data/software
- Ensure data/software change attempts are authorized
- Ciphering /deciphering of control and user plane done in secure environment
- Keys stored in secure environment
- Secure environment integrity ensured
- Sensitive data of secure environment not exposed

- Confidentiality and integrity protection of software transfer
- Mutual authentication between eNB and O&M

Network Elements and Security Functions



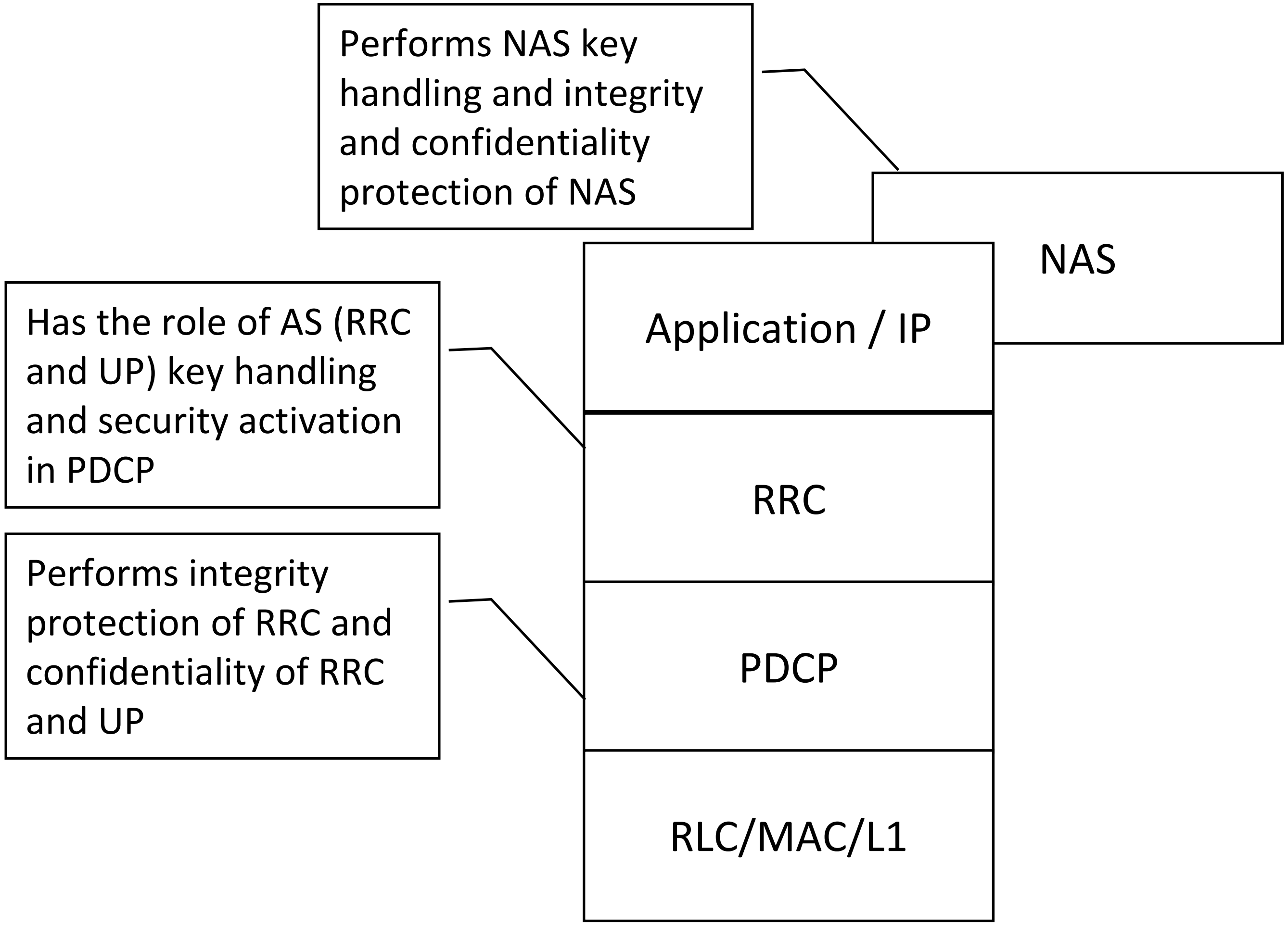
- Performs UE authentication
- Generates AVs

- End-point (UE is other end-point) for integrity and confidentiality protection of RRC and confidentiality protection of UP
- Manages AS keys
- Initiates UE AS security

- End-point (UE is other end-point) for integrity protection and confidentiality protection of NAS
- Manages NAS keys and participates in AS key handling
- Verifies UE authorization to access service and network
- Gets AVs from HSS
- Initiates UE NAS security

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

Protocol Layers and Security Functions

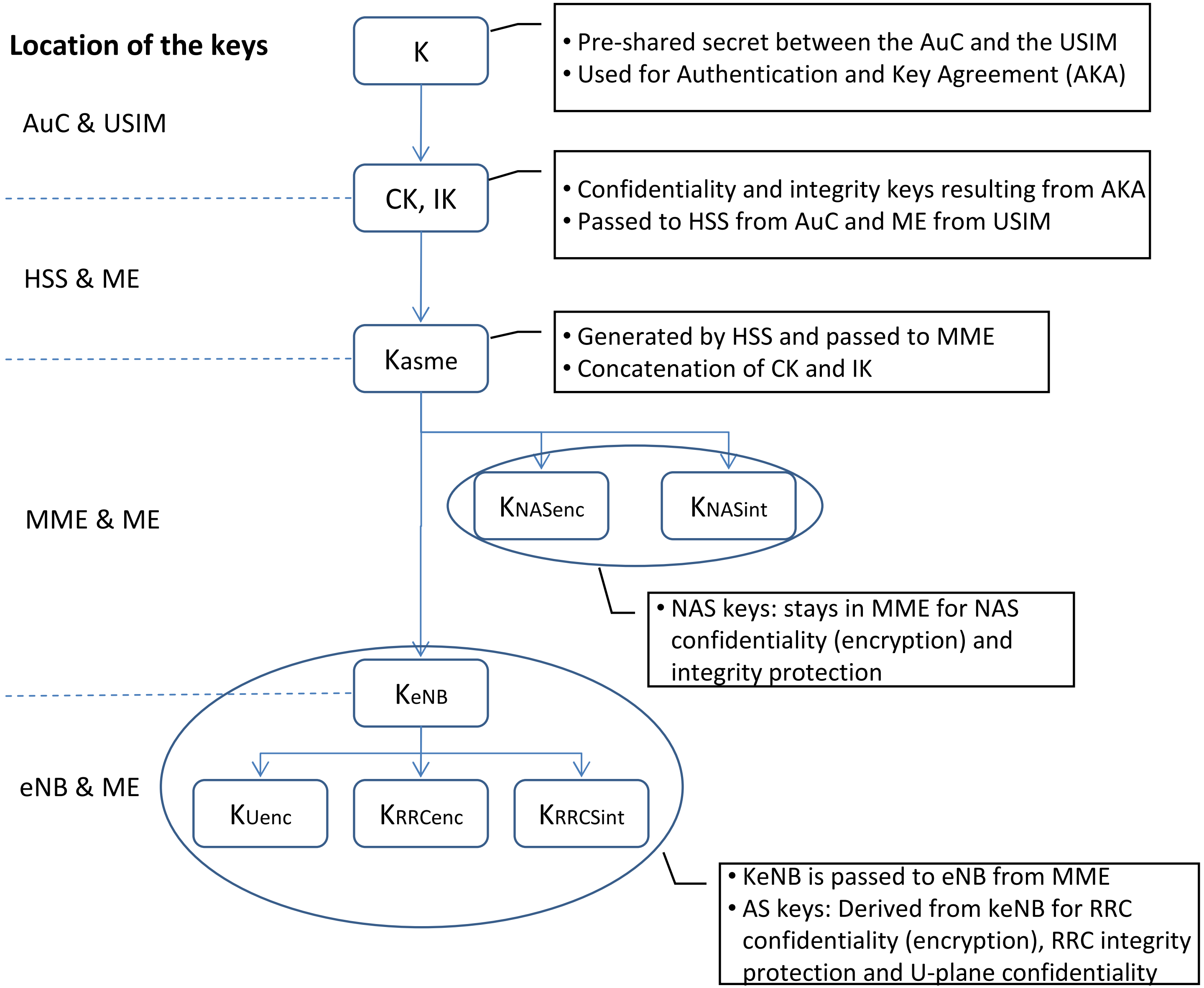


Performs NAS key handling and integrity and confidentiality protection of NAS

Has the role of AS (RRC and UP) key handling and security activation in PDCP

Performs integrity protection of RRC and confidentiality of RRC and UP

Key Hierarchy



Location of the keys

AuC & USIM

HSS & ME

MME & ME

eNB & ME

K

- Pre-shared secret between the AuC and the USIM
- Used for Authentication and Key Agreement (AKA)

CK, IK

- Confidentiality and integrity keys resulting from AKA
- Passed to HSS from AuC and ME from USIM

Kasme

- Generated by HSS and passed to MME
- Concatenation of CK and IK

K_{NASenc} K_{NASint}

- NAS keys: stays in MME for NAS confidentiality (encryption) and integrity protection

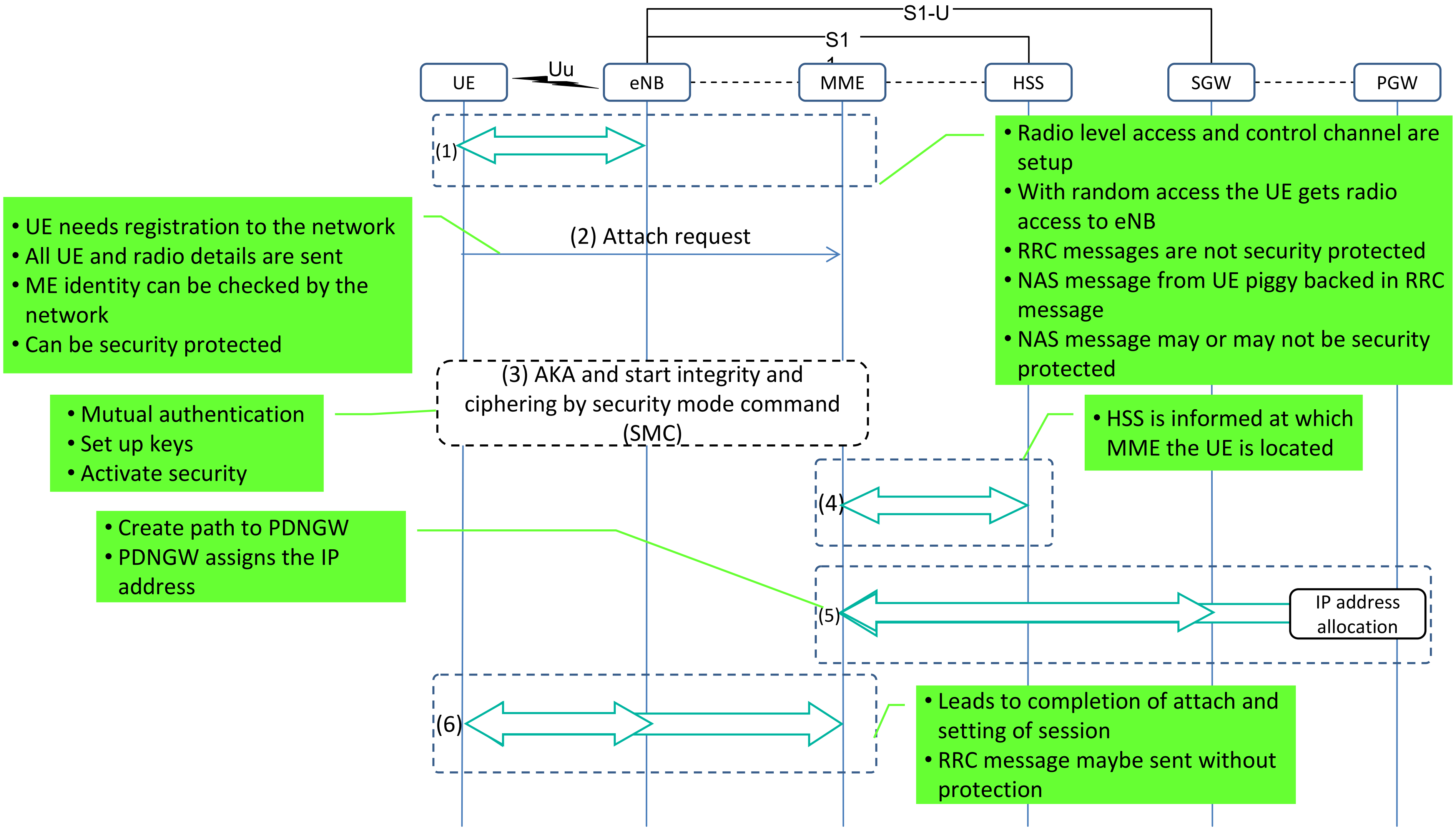
K_{eNB}

K_{Uenc} K_{RRCenc} $K_{RRCSint}$

- KeNB is passed to eNB from MME
- AS keys: Derived from keNB for RRC confidentiality (encryption), RRC integrity protection and U-plane confidentiality

Key separation depending on purpose

EPS Terminal Start-up and Security



- Radio level access and control channel are setup
- With random access the UE gets radio access to eNB
- RRC messages are not security protected
- NAS message from UE piggy backed in RRC message
- NAS message may or may not be security protected

- UE needs registration to the network
- All UE and radio details are sent
- ME identity can be checked by the network
- Can be security protected

(3) AKA and start integrity and ciphering by security mode command (SMC)

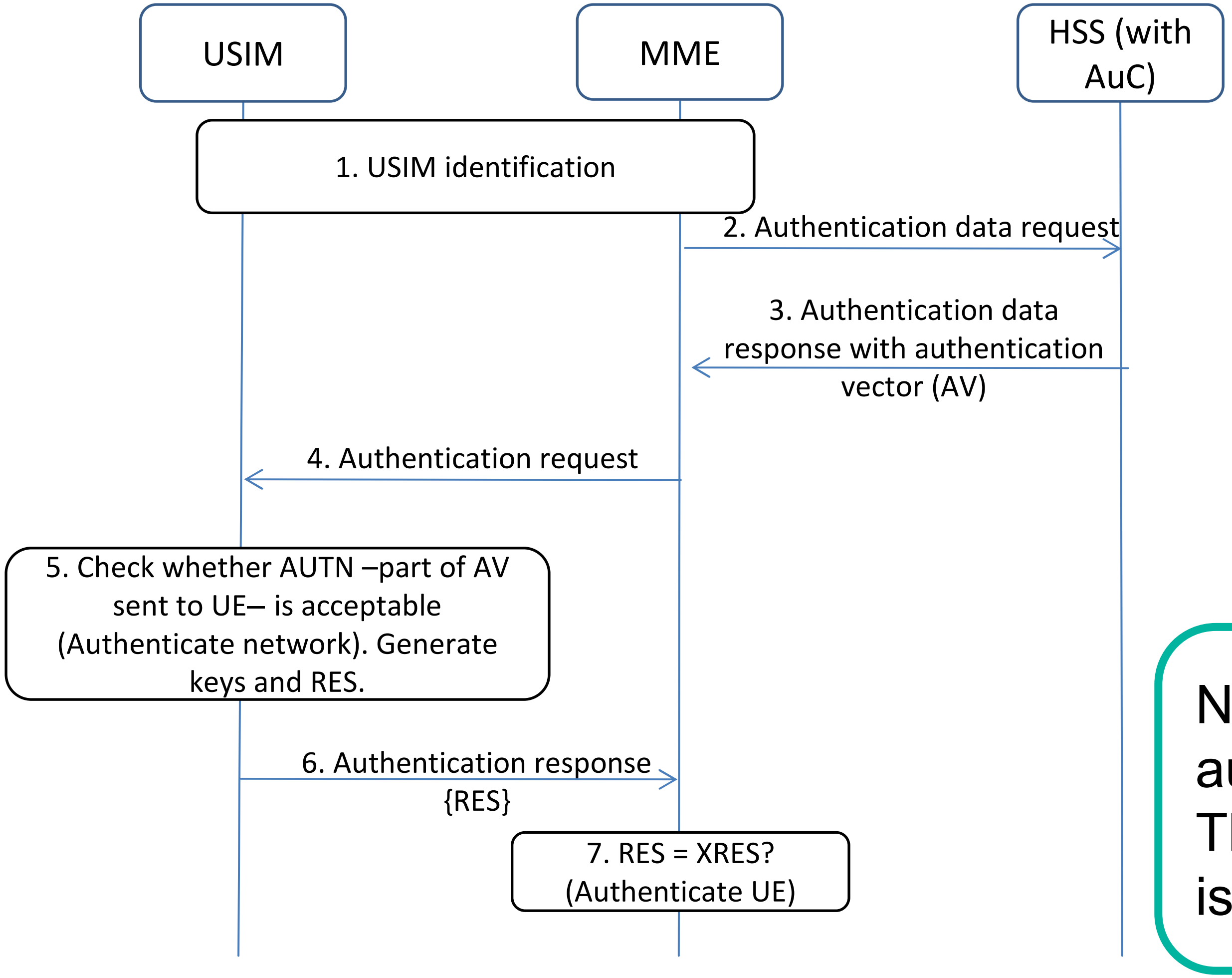
- Mutual authentication
- Set up keys
- Activate security

- HSS is informed at which MME the UE is located

- Create path to PDNGW
- PDNGW assigns the IP address

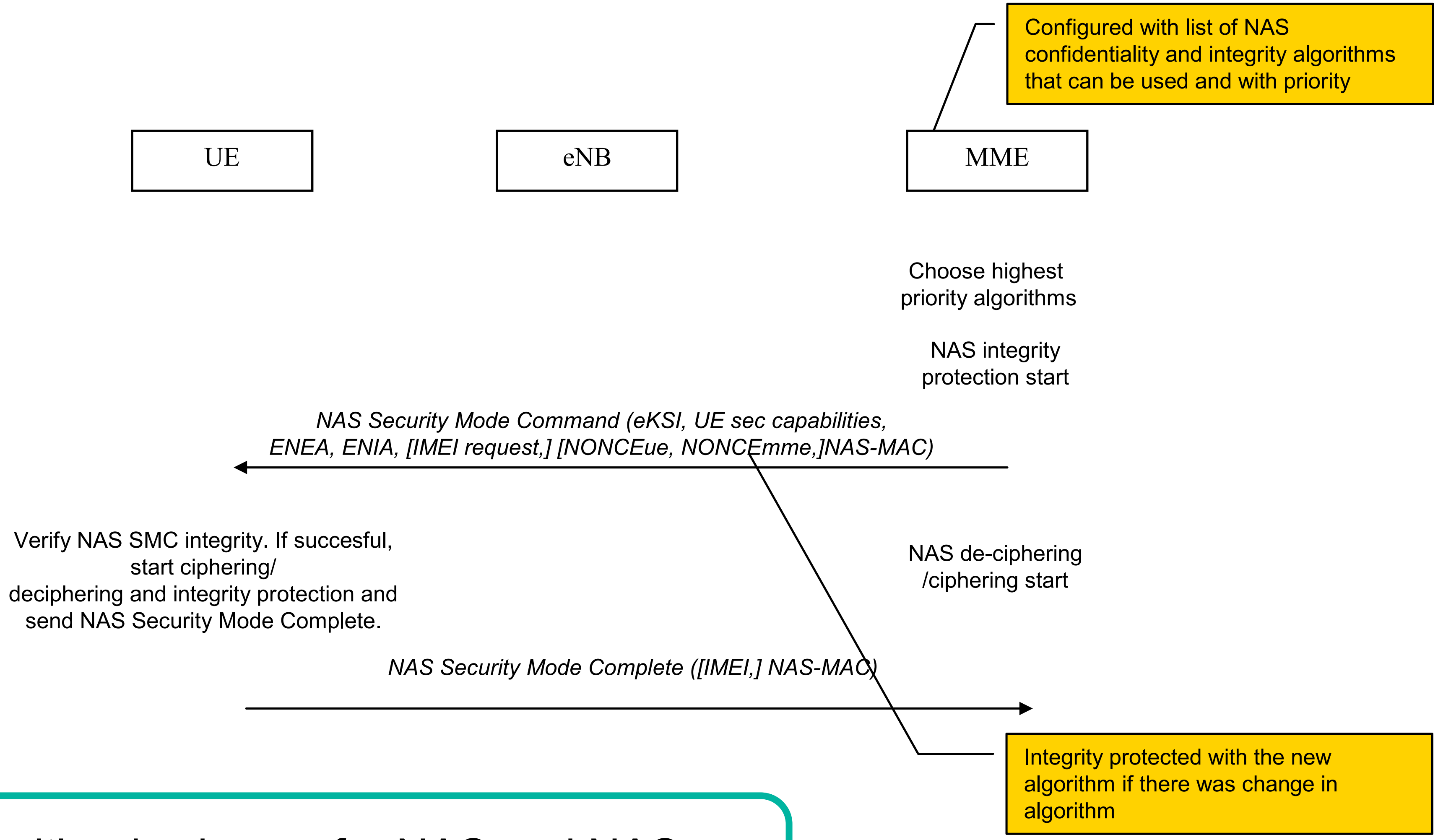
- Leads to completion of attach and setting of session
- RRC message maybe sent without protection

Authentication and Key Agreement (AKA)


USIM
MME
HSS (with AuC)
1. USIM identification
2. Authentication data request
3. Authentication data response with authentication vector (AV)
4. Authentication request
5. Check whether AUTN –part of AV sent to UE– is acceptable (Authenticate network). Generate keys and RES.
6. Authentication response {RES}
7. RES = XRES? (Authenticate UE)

Network and UE are authenticated to each other. The top-level-key (Kasme) is created

SMC: NAS Algorithm Selection



Configured with list of NAS confidentiality and integrity algorithms that can be used and with priority

UE

eNB

MME

Choose highest priority algorithms

NAS integrity protection start

NAS Security Mode Command (eKSI, UE sec capabilities, ENEA, ENIA, [IMEI request,] [NONCEue, NONCEmme,]NAS-MAC)

Verify NAS SMC integrity. If succesful, start ciphering/ deciphering and integrity protection and send NAS Security Mode Complete.

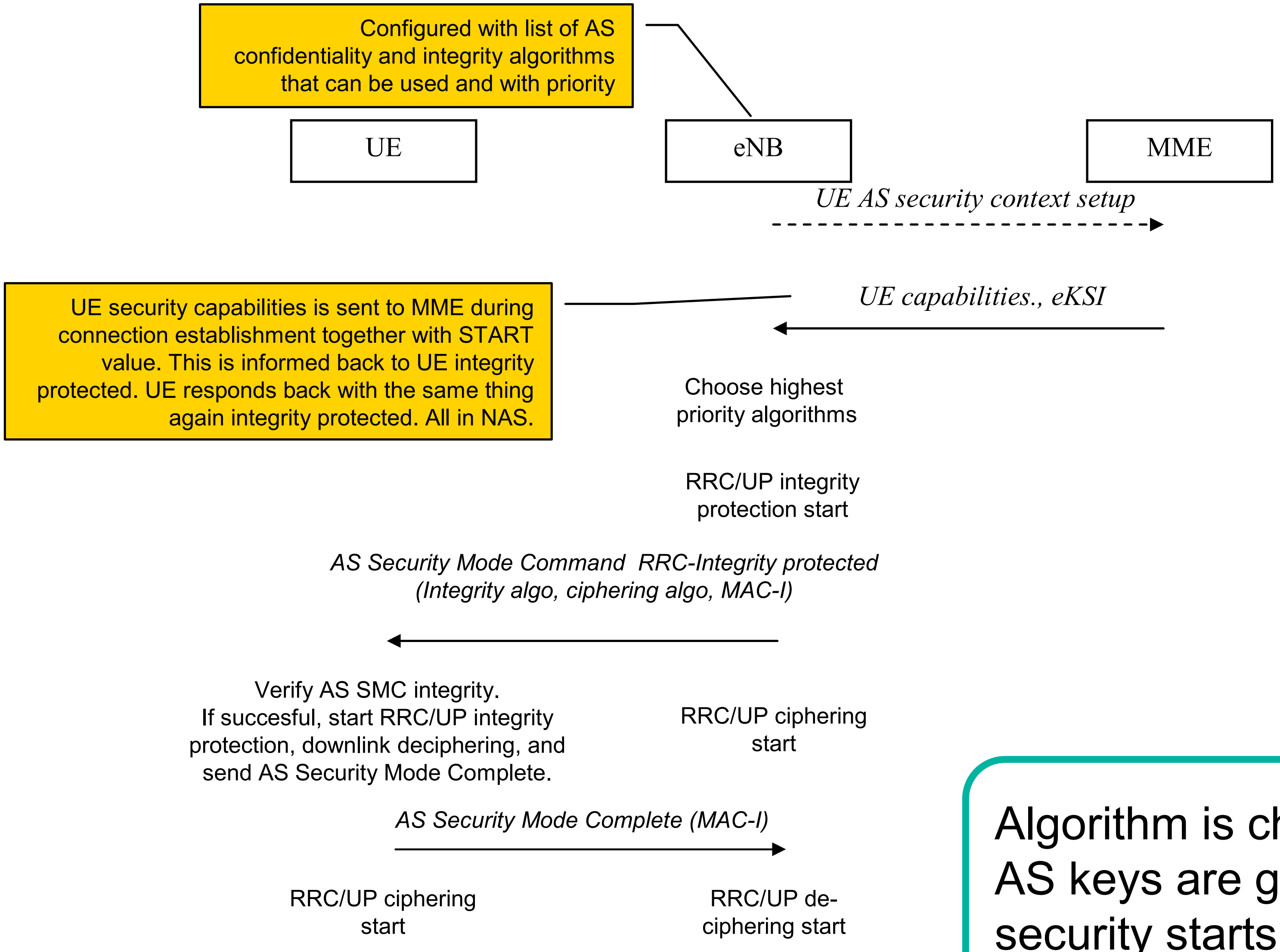
NAS de-ciphering /ciphering start

NAS Security Mode Complete ([IMEI,] NAS-MAC)

Integrity protected with the new algorithm if there was change in algorithm

Algorithm is chosen for NAS and NAS keys are generated. NAS security starts.

SMC: AS Algorithm Selection



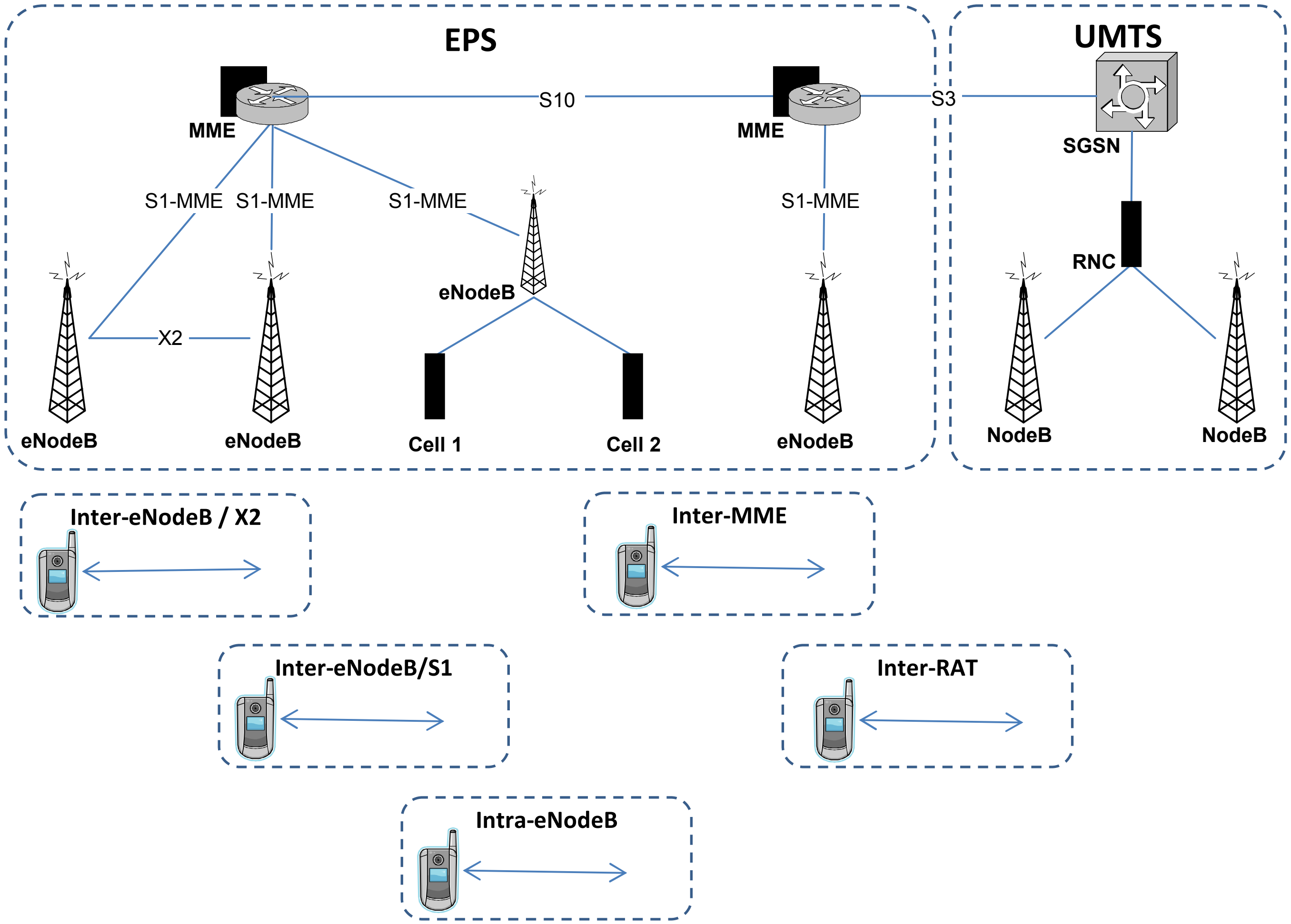
Configured with list of AS confidentiality and integrity algorithms that can be used and with priority

UE security capabilities is sent to MME during connection establishment together with START value. This is informed back to UE integrity protected. UE responds back with the same thing again integrity protected. All in NAS.

UE
eNB
MME
UE AS security context setup
UE capabilities., eKSI
Choose highest priority algorithms
RRC/UP integrity protection start
AS Security Mode Command RRC-Integrity protected (Integrity algo, ciphering algo, MAC-I)
Verify AS SMC integrity. If succesful, start RRC/UP integrity protection, downlink deciphering, and send AS Security Mode Complete.
RRC/UP ciphering start
AS Security Mode Complete (MAC-I)
RRC/UP ciphering start
RRC/UP de-ciphering start

Algorithm is chosen for AS & AS keys are generated. AS security starts.

Mobility in EPS

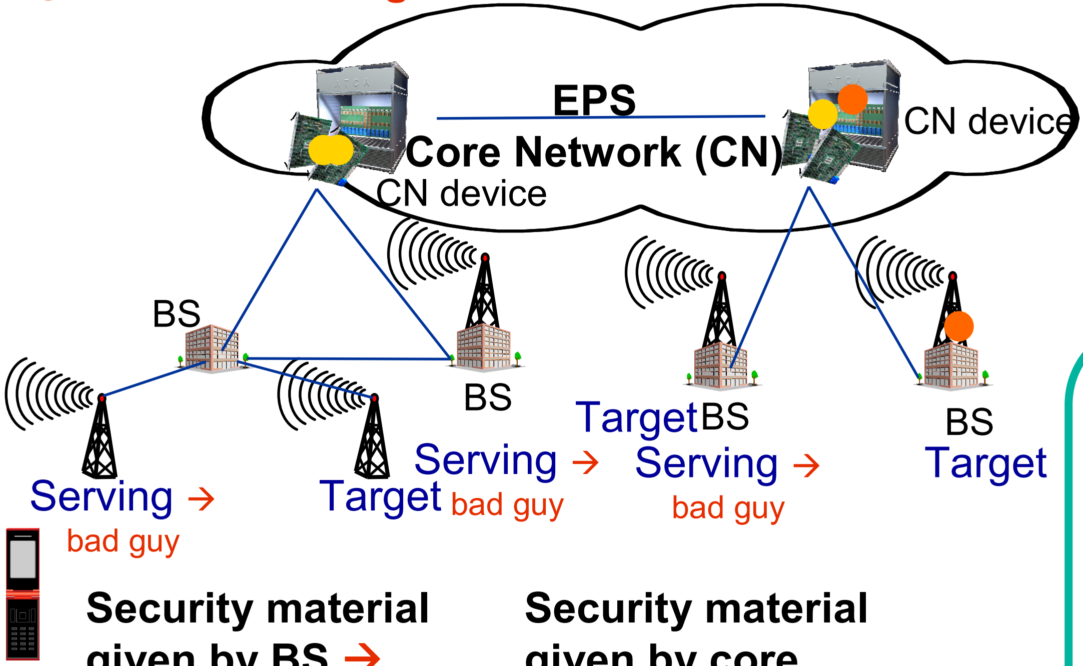


Secure Handover in Evolved Packet System (EPS)

Provide security material before handover → Not good

Provide security material during handover → Not good

Provide security material after handover → Good

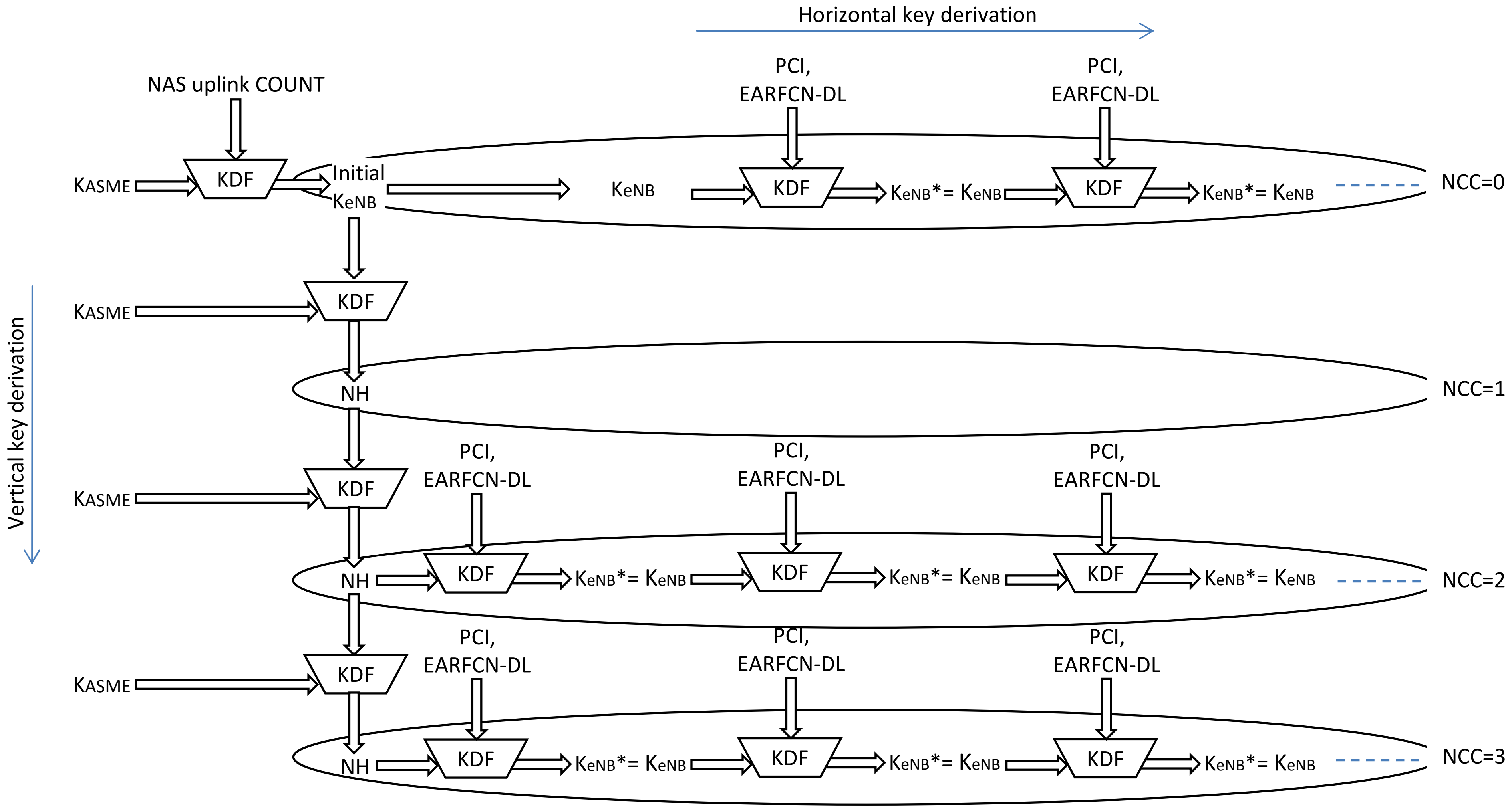


Security material given by BS → Not good

Security material given by core network → Good

- Provides forward and backward security
- Key changed at each handover
- Algorithm can be changed at each handover

Handover and Key Handling

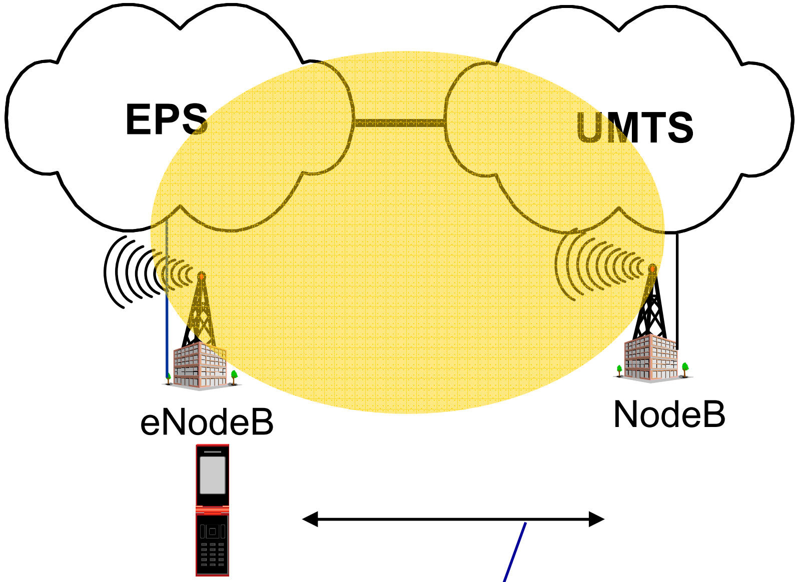


KDF: Key Derivation Function
NH: Next Hop
NCC: Next hop Chaining Counter
PCI: Physical Cell Identity

Detail of key derivation and handling on handover

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

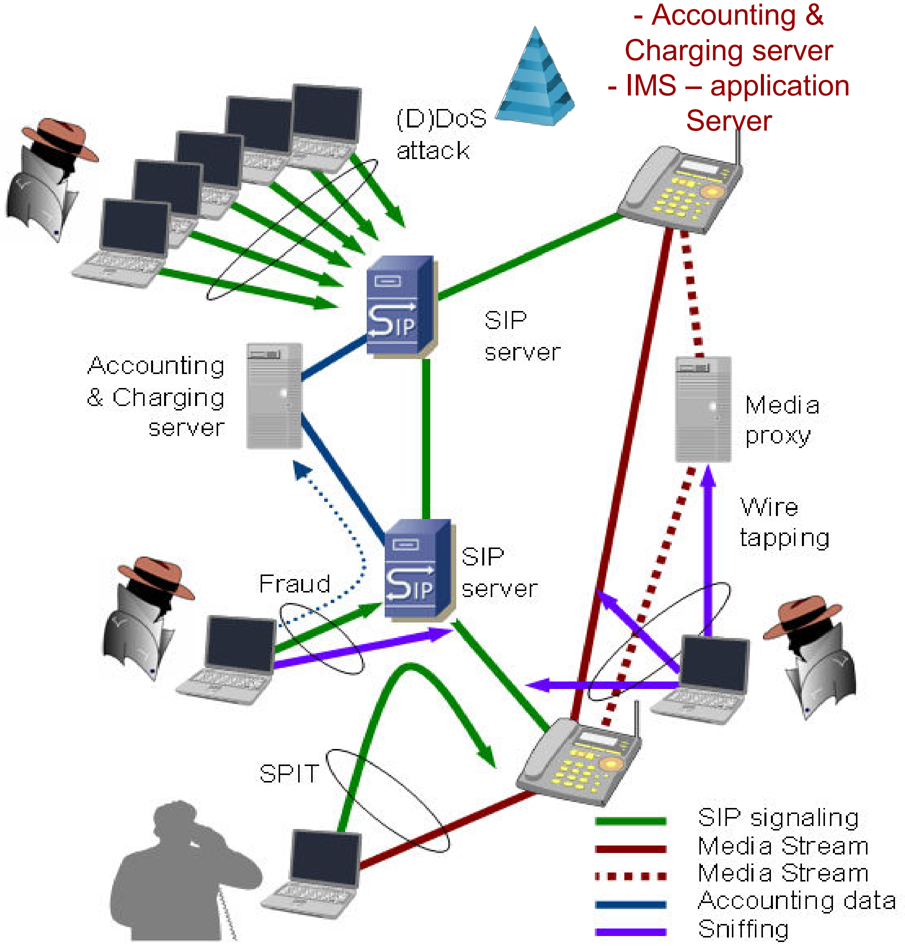


Derive keys in serving network for the target network and in UE based on current keys before handover

Empowered by Innovation NEC

Today to Tomorrow

Protection against Unsolicited Communication in IMS (PUCI)



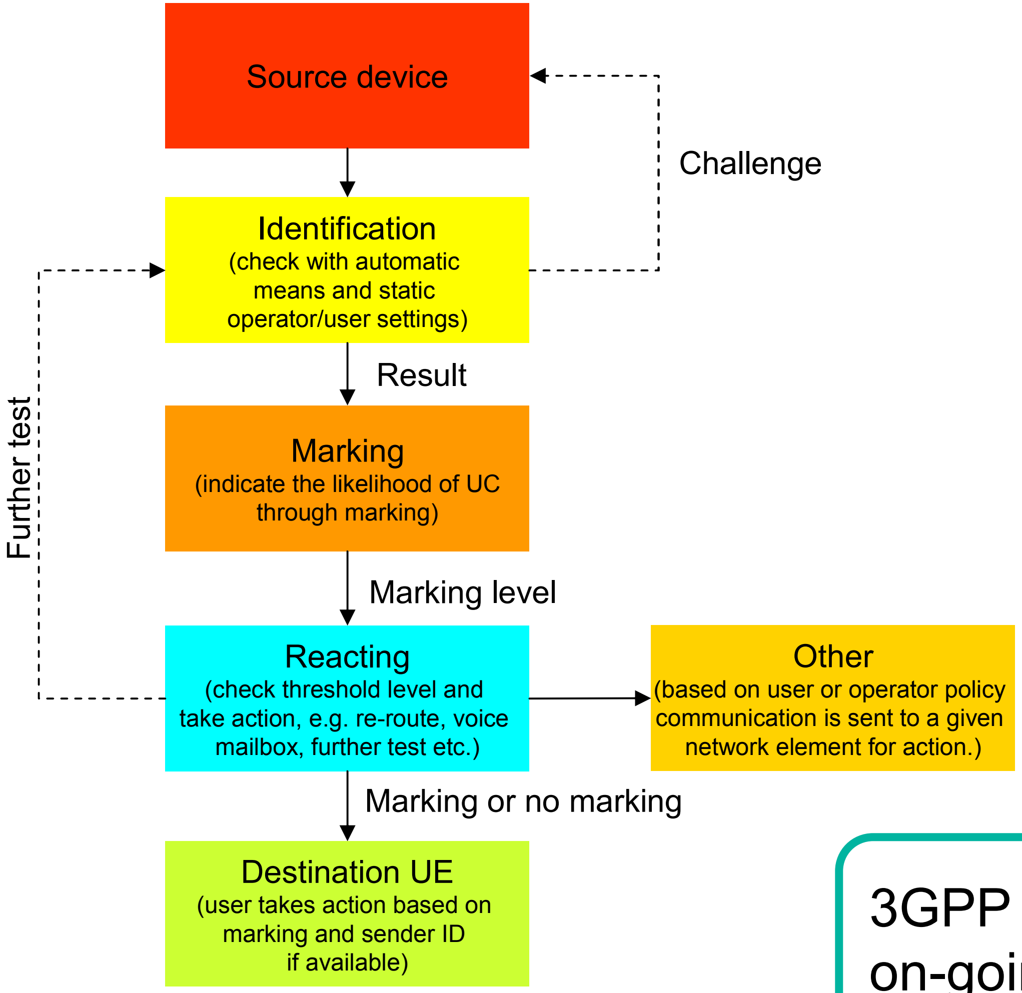
Can lead to SPIT

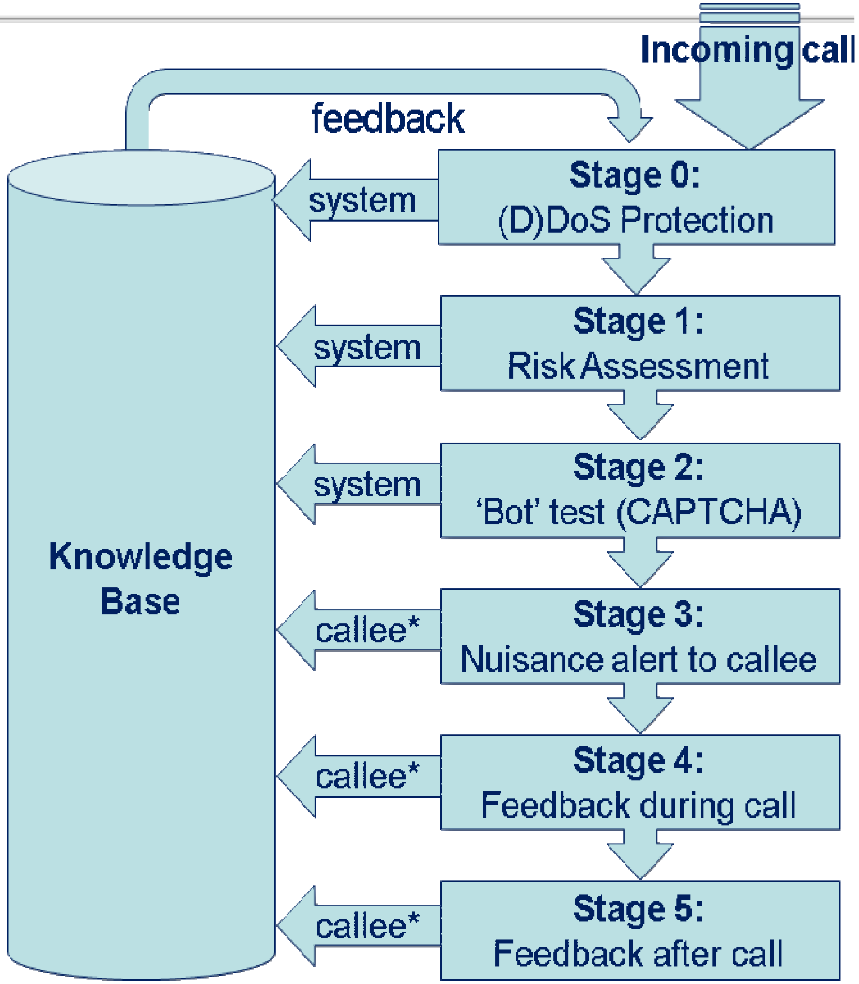
Threats
Data confidentiality
Fraud Activities
Phishing
Denial of Service
Bandwidth Availability
Productivity Loss
Call Quality Degradation
Unauthorized Access
Eavesdropping
SPIT
Customer Satisfaction
Authentication
Re-Routing
Bots, virus etc.
Caller ID Spoofing

There are several VoIP threats that can lead to SPIT

Protection against Unsolicited Communication in IMS (PUCI)

Solve it with Identify, Mark and React


Source device
Challenge
Identification
(check with automatic means and static operator/user settings)
Result
Further test
Marking
(indicate the likelihood of UC through marking)
Marking level
Reacting
(check threshold level and take action, e.g. re-route, voice mailbox, further test etc.)
Other
(based on user or operator policy communication is sent to a given network element for action.)
Marking or no marking
Destination UE
(user takes action based on marking and sender ID if available)



3GPP TR 33.937 available. Further work on-going under SPUCI work-item.

Machine to Machine Communication

- Known as Machine Type Communication (MTC)
- Scenarios are, for example, smart metering or healthcare
- Issues can be from the point of access control to attack on the device itself
- The biggest problem will be the huge number of devices trying to connect to the mobile network and thus overwhelming the network due to high traffic volume

DRINK
DRINK

GISFI Security Activities

- The security activity in Global ICT Standardisation Forum for India (GISFI) provides solution for all the activities being carried out by the standardization forum
- Security SIG also provides input to Indian government
- The activity is still at its early stage, some of the topics covered are:
  - Cyber security and children
  - Cloud security
  - Inter-of-Things (starting from machine-to-machine, M2M, communication)

What is happening today and where will it lead to?

- Some observations of today:
  - Average age of knowledge generation is decreasing with time – data and information in readily available
  - World is slowly but steadily moving towards similar level of life globally – impact on age of population and education level
  - Reachability is at 24 / 7
  - Need for convenience is increasing
  - Computing, telecommunications and networking has converged, if not, the trend has only become faster
  - Openness, free and shared are key words
  - Technology enhancement is moving at a faster pace:
    - Wireless data-rate is catching up with wired
    - Computing power is high and increasing while becoming available to all
  - Human society is maturing
  - Business models are changing very fast: 10 to 2 years to 6 months and now 3 months
  - Operators business: conventional, data only, take a ride

Thoughts: Security?

- Potentially faster cycle for algorithm development
- Need of increased awareness and concern of privacy and security
- Necessity of ever more system security consideration
  - Top-to-bottom
  - End-to-end
- Better privacy control mechanisms
- Choice of level of security
- Fast threat analysis together with proper understanding of risk and input to security solution
- …….

Conclusions

Conclusions

- Today we took a look at Evolved Packet System (EPS) security – the next generation of mobile communications
  - For more: write to me, check my book or 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** (I am the rapporteur in 3GPP)
  - Relay node security – IMT-advanced etc.
- **Global ICT Standardisation Forum for India (GISFI)** is working on several security topics starting from Indian requirements
- Penetration of security understanding should increase which will bring with it more demand on security itself
- **Complete system consideration of security from the beginning** will become even more necessary – Bringing potential changes in **business** arena – providers of service at different layers working together?

….the book

Security in Next Generation Mobile Networks: SAE/LTE and WiMAX

Authors: Anand R. Prasad <http://www.prasad.bz/> and
Seung-Woo Seo

Publisher: River Publishers <http://riverpublishers.com/river_publisher/>

Available: August 2011

ISBN: 978-87-92329-63-9

Table of Contents:

Contact: <anand@bq.jp.nec.com>

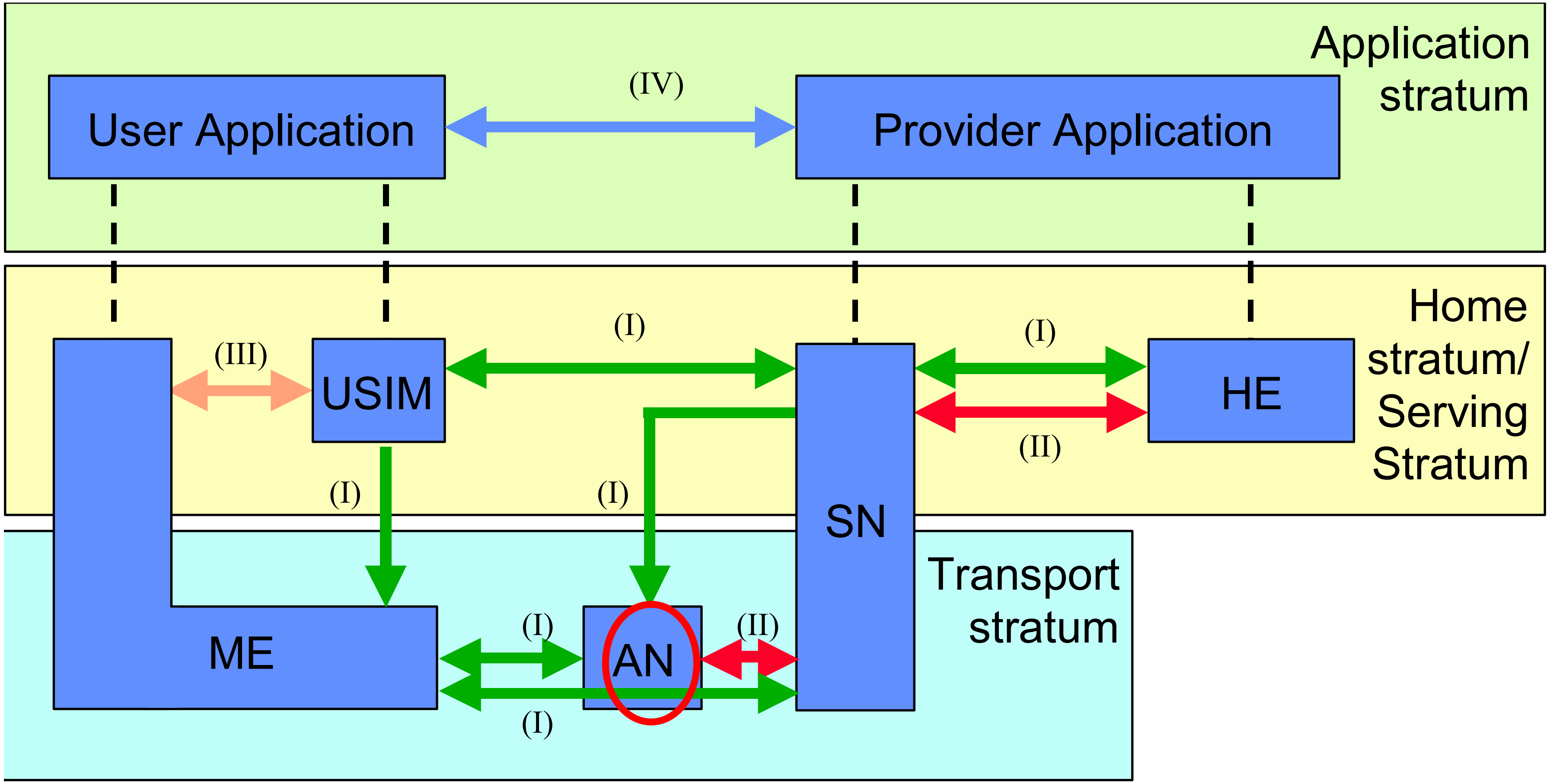
Empowered by Innovation

NEC

Abbreviations

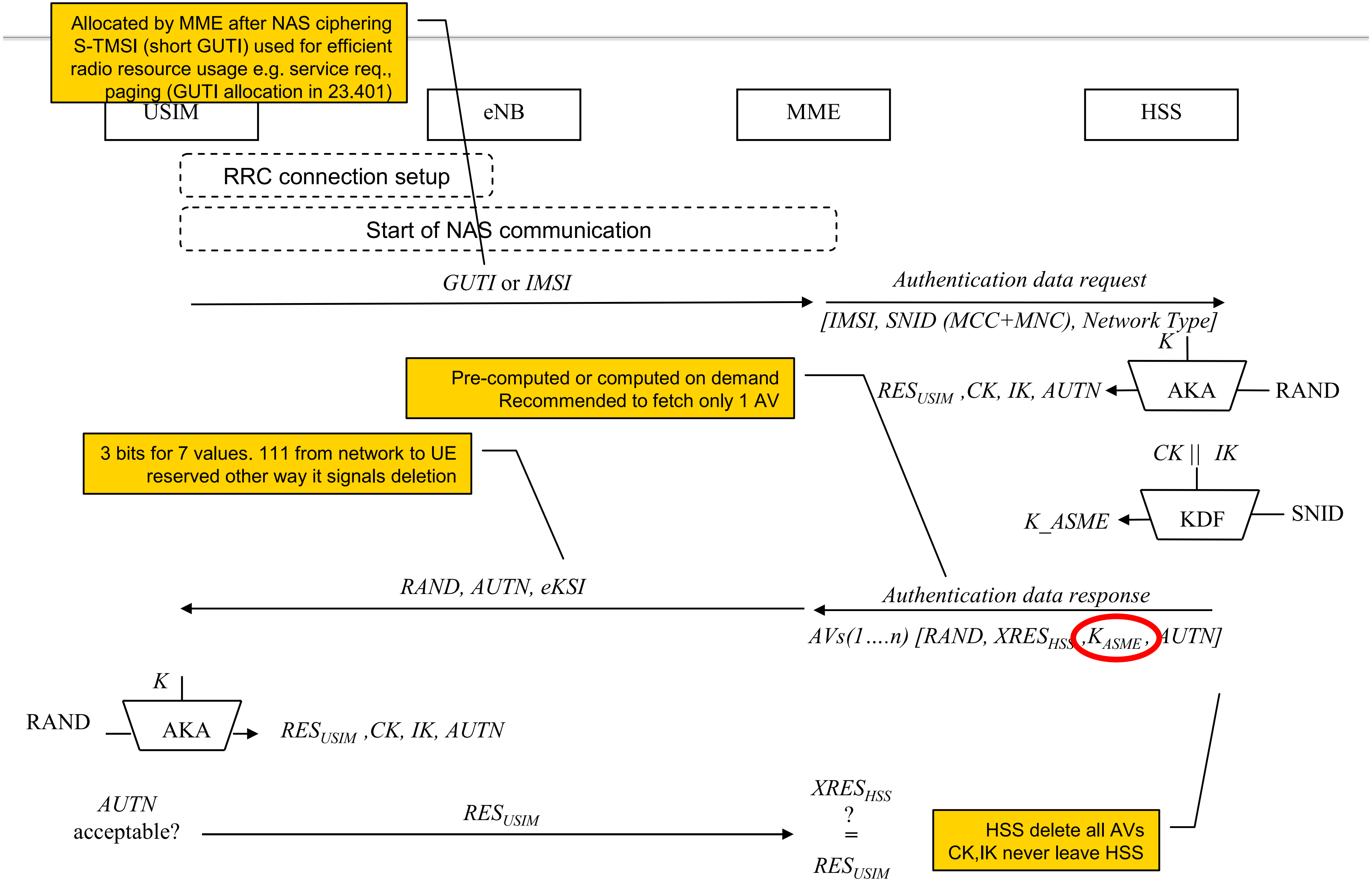
3GPP	Third Generation Partnership Project	NAS	Non Access Stratum
AS	Access Stratum (RRC and UP)	NGMN	Next Generation Mobile Network
AuC	Authentication Center	PCRF	Policy and Charging Rules Function
AV	Autentication Vector	PDCP	Packet Data Control Protocol
DNS	Domain Name System	PDN	Packet Data network
EIR	Equipment Identity Register	PDNGW or PGW	Packet Data Network Gateway
EPC	Evolved Packet Core	PLMN	Public Land-Mobile Network
ePDG	evolved Packet Data Gateway	PUCI	Protection against Unsolicited Communication in IMS
E-UTRAN	Evolved-UTRAN	RAN	Radio Access Network
GERAN	GSM EDGE Radio Access Network	RLC	Radio Link Control
GISFI	Global ICT Standardisation Forum for India	RRC	Radio Resource Control
HLR	Home Location Register	SAE	System Architecture Evolution (or EPC for core network)
HSS	Home Subscriber Subsystem	SPIT	Spam over Internet Telephony
IMS	IP Multemedia Subsystem	SGSN	Serving GPRS Support Node
IP	Internet Protocol	SGW	Serving Gateway
LTE	Long-Term Evolution (or E-UTRAN for	UE	User Equipment
MAC	Medium Access Control	UP	User Plane
ME	Mobile Equipment	USIM	Universal Subscriber Identity Module
MME	Mobility Management Entity	UTRAN	UMTS Terrestrial Radio Access Network

Security Overview



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

EPS AKA



Allocated by MME after NAS ciphering S-TMSI (short GUTI) used for efficient radio resource usage e.g. service req., paging (GUTI allocation in 23.401)

USIM

eNB

MME

HSS

RRC connection setup

Start of NAS communication

GUTI or *IMSI*

Authentication data request

[IMSI, SNID (MCC+MNC), Network Type]

K

AKA

RES_{USIM} *,CK, IK, AUTN*

RAND

Pre-computed or computed on demand
Recommended to fetch only 1 AV

3 bits for 7 values. 111 from network to UE reserved other way it signals deletion

CK || *IK*

KDF

K_ASME

SNID

RAND, AUTN, eKSI

Authentication data response

AVs(1….n) [RAND, $XRES_{HSS}$ *,*K_{ASME}*, AUTN]*

K

RAND

AKA

RES_{USIM} *,CK, IK, AUTN*

AUTN
acceptable?

RES_{USIM}

$XRES_{HSS}$
?
=
RES_{USIM}

HSS delete all AVs
CK,IK never leave HSS

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