NETMANIAS
www.netmanias.com

NMC
CONSULTING GROUP
www.nmcgroups.com

LTE Security I

- LTE Security Concept and LTE Authentication -

August 21, 2012

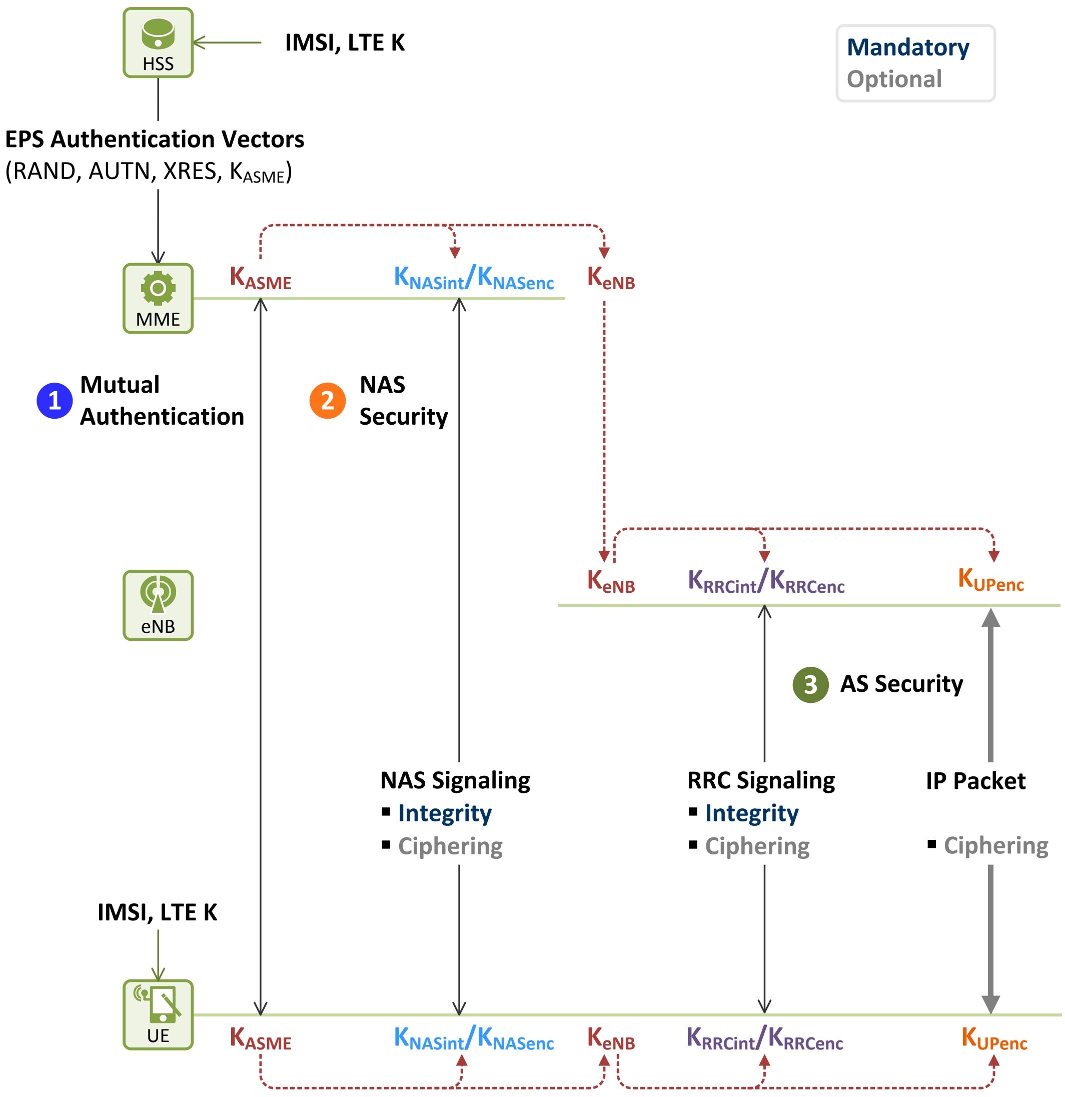
(Last Updated: July 31, 2013)

NMC Consulting Group (tech@netmanias.com)

www.netmanias.com
www.nmcgroups.com

About NMC Consulting Group
NMC Consulting Group is an advanced and professional network consulting company, specializing in IP network areas (e.g., FTTH, Metro Ethernet and IP/MPLS), service areas (e.g., IPTV, IMS and CDN), and wireless network areas (e.g., Mobile WiMAX, LTE and Wi-Fi) since 2002.

Scope and Concept of LTE Security



1 LTE Authentication

- Mutual authentication between UE and LTE network (UE – MME – HSS) using EPS-AKA
  - Base key: **K**
  - Derived key: K_{ASME}

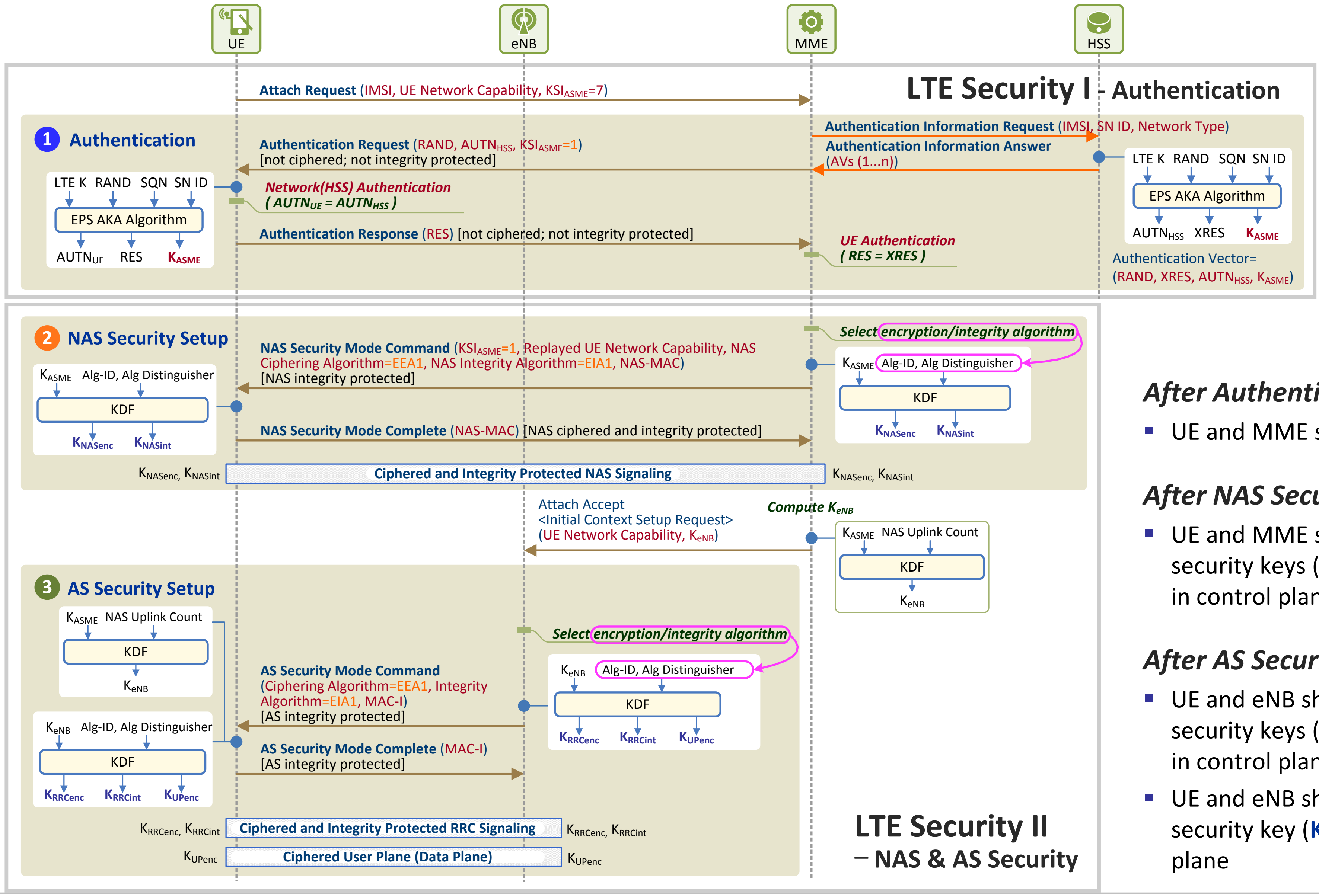
2 NAS Security

- Integrity check (protection/verification) and ciphering /deciphering (or encryption/decryption) for NAS signaling messages between UE and MME
  - Base key: K_{ASME}
  - Derived key: K_{NASint}, K_{NASenc}

3 AS Security

- Integrity check (protection/verification) and ciphering /deciphering (or encryption/decryption) for RRC signaling messages between UE and eNB
  - Base key: K_{eNB}
  - Derived key: K_{RRCint}, K_{RRCenc}
- Ciphering/deciphering (or encryption/decryption) for user IP packets between UE and eNB
  - Base key: K_{eNB}
  - Derived key: K_{UPenc}

Overview of LTE Security



UE eNB MME HSS

LTE Security I - Authentication

Attach Request (IMSI, UE Network Capability, KSI_{ASME}=7)

1 Authentication

Authentication Information Request (IMSI, SN ID, Network Type)

Authentication Information Answer (AVs (1…n))

LTE K RAND SQN SN ID → EPS AKA Algorithm → $AUTN_{HSS}$ XRES K_{ASME}

Authentication Vector= (RAND, XRES, $AUTN_{HSS}$, K_{ASME})

Authentication Request (RAND, $AUTN_{HSS}$, KSI_{ASME}=1) [not ciphered; not integrity protected]

LTE K RAND SQN SN ID → EPS AKA Algorithm → $AUTN_{UE}$ RES K_{ASME}

Network(HSS) Authentication ($AUTN_{UE}$ = $AUTN_{HSS}$)

Authentication Response (RES) [not ciphered; not integrity protected]

UE Authentication (RES = XRES)

2 NAS Security Setup

Select encryption/integrity algorithm

NAS Security Mode Command (KSI_{ASME}=1, Replayed UE Network Capability, NAS Ciphering Algorithm=EEA1, NAS Integrity Algorithm=EIA1, NAS-MAC) [NAS integrity protected]

K_{ASME} Alg-ID, Alg Distinguisher → KDF → K_{NASenc} K_{NASint}

NAS Security Mode Complete (NAS-MAC) [NAS ciphered and integrity protected]

K_{NASenc}, K_{NASint} Ciphered and Integrity Protected NAS Signaling K_{NASenc}, K_{NASint}

Attach Accept <Initial Context Setup Request> (UE Network Capability, K_{eNB})

Compute K_{eNB}

K_{ASME} NAS Uplink Count → KDF → K_{eNB}

3 AS Security Setup

Select encryption/integrity algorithm

K_{eNB} Alg-ID, Alg Distinguisher → KDF → K_{RRCenc} K_{RRCint} K_{UPenc}

AS Security Mode Command (Ciphering Algorithm=EEA1, Integrity Algorithm=EIA1, MAC-I) [AS integrity protected]

AS Security Mode Complete (MAC-I) [AS integrity protected]

K_{RRCenc}, K_{RRCint} Ciphered and Integrity Protected RRC Signaling K_{RRCenc}, K_{RRCint}

K_{UPenc} Ciphered User Plane (Data Plane) K_{UPenc}

LTE Security II – NAS & AS Security

After Authentication

- UE and MME share K_{ASME}

After NAS Security Setup

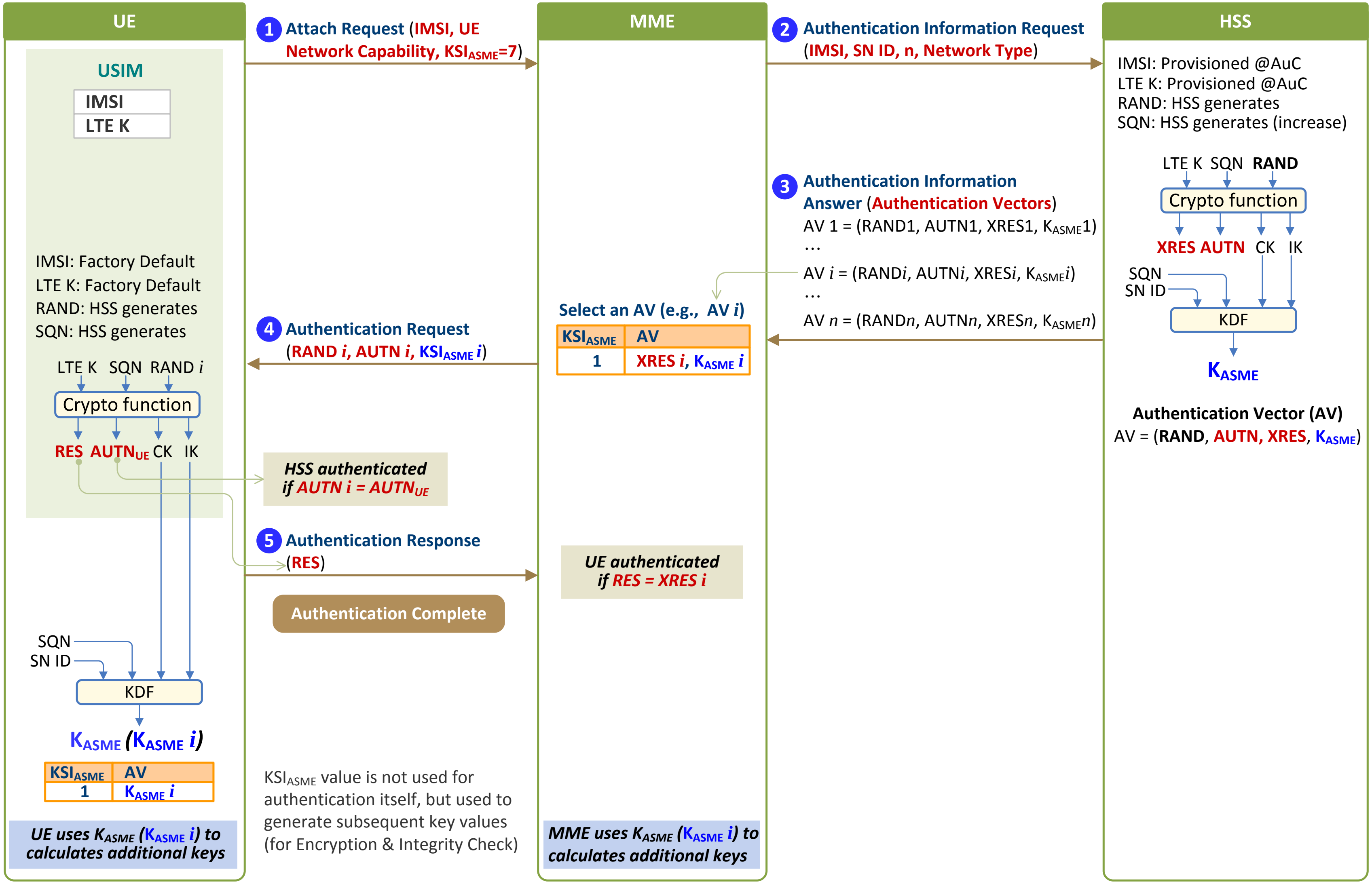
- UE and MME share NAS security keys (**K_{NASenc}, K_{NASint}**) in control plane

After AS Security Setup

- UE and eNB share AS security keys (**K_{RRCenc}, K_{RRCint}**) in control plane
- UE and eNB share a AS security key (**K_{UPenc}**) in user plane

Overview of LTE Authentication Procedure: EPS AKA

EPS AKA (Evolved Packet System Authentication and Key Agreement)



UE

USIM

IMSI
LTE K

IMSI: Factory Default
LTE K: Factory Default
RAND: HSS generates
SQN: HSS generates

LTE K SQN RAND *i* → Crypto function → RES $AUTN_{UE}$ CK IK

SQN, SN ID, CK, IK → KDF → K_{ASME} (K_{ASME} *i*)

KSI_{ASME}	AV
1	K_{ASME} *i*

UE uses K_{ASME} (K_{ASME} i) to calculates additional keys

MME

HSS

1 Attach Request (IMSI, UE Network Capability, KSI_{ASME}=7)

2 Authentication Information Request (IMSI, SN ID, n, Network Type)

IMSI: Provisioned @AuC
LTE K: Provisioned @AuC
RAND: HSS generates
SQN: HSS generates (increase)

LTE K SQN **RAND** → Crypto function → XRES AUTN CK IK

SQN, SN ID, CK, IK → KDF → K_{ASME}

Authentication Vector (AV)
AV = (**RAND**, **AUTN**, **XRES**, K_{ASME})

3 Authentication Information Answer (Authentication Vectors)
AV 1 = (RAND1, AUTN1, XRES1, K_{ASME}1)
…
AV *i* = (RAND*i*, AUTN*i*, XRES*i*, K_{ASME}*i*)
…
AV *n* = (RAND*n*, AUTN*n*, XRES*n*, K_{ASME}*n*)

Select an AV (e.g., AV *i*)

KSI_{ASME}	AV
1	XRES *i*, K_{ASME} *i*

4 Authentication Request (RAND *i*, AUTN *i*, KSI_{ASME} *i*)

HSS authenticated if AUTN i = $AUTN_{UE}$

5 Authentication Response (RES)

UE authenticated if RES = XRES i

Authentication Complete

KSI_{ASME} value is not used for authentication itself, but used to generate subsequent key values (for Encryption & Integrity Check)

MME uses K_{ASME} (K_{ASME} i) to calculates additional keys

LTE Authentication Procedure (1)

- Provisioning Information @HSS/AuC
  - **K**: provisioned to AuC at subscription time
  - **IMSI**: provisioned to HSS & AuC at subscription time
- Storing Information @USIM
  - **K & IMSI**: stored to USIM at manufacturing time

1. Authentication Request from UE

❶ [UE → MME] Request by UE for Network Registration

- UE sends ***Attach Request*** *(IMSI, UE Network Capability, KSI_{ASME}=7)* message to MME
  - **IMSI**: International Mobile Subscriber Identity, a unique identifier associated with the user
  - **UE Network Capability**: security algorithms available to UE
  - **KSI_{ASME}=7**: indicates UE has no authentication key

EEA and EIA in "UE Network Capability" Information [3]

EEA

Algorithm ID	Description
128-EEA0	Null Ciphering Algorithm
128-EEA1	SNOW 3G
128-EEA2	AES
128-EEA3	ZUC (optional)

EIA

Algorithm ID	Description
-	-
128-EIA1	SNOW 3G
128-EIA2	AES
128-EIA3	ZUC (optional)

LTE Authentication Procedure (2)

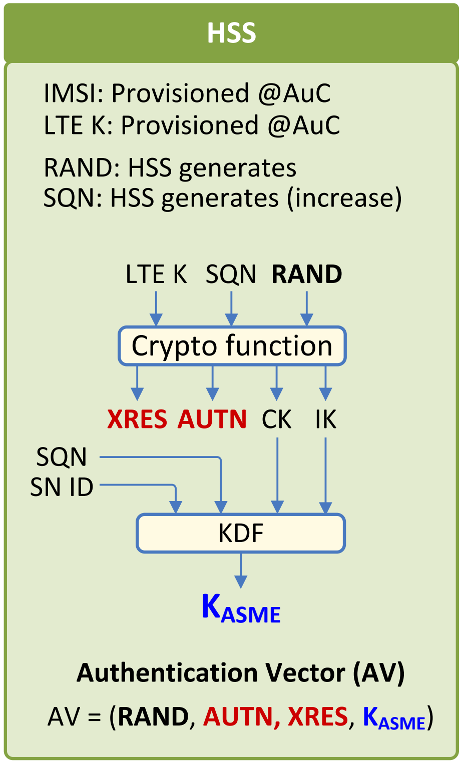
2. Transfer of Authentication Vector(s) from HSS to MME

❷ [MME → HSS] Request by MME for Authentication Data

- MME sends ***Authentication Information Request*** *(IMSI, SN ID, n, Network Type)* message to HSS to request authentication vector(s) for the UE
  - **IMSI**: a unique identifier associated with the user
  - **SN ID**: refers to the network accessed by the user, consists of PLMN ID (MCC+MNC)
  - **n**: number of authentication vectors that MME requests
  - **Network Type**: type of the network accessed by UE (E-UTRAN herein)
- HSS
  - Generates RAND and SQN
  - Calculates XRES, AUTN, CK and IK using AKA Algorithm with inputs, LTE Key (K), SQN and RAND
  - Calculates local master key K_{ASME} using KDF with inputs, CK, IK, SQN and SN ID
  - Constitutes Authentication Vector(s), **AV=(RAND, AUTH, XRES, K_{ASME})**

❸ [MME ← HSS] Response by HSS to the Authentication Data Request

- HSS sends ***Authentication Information Answer*** *(AVs)* message including AVs back to MME
- MME
  - Stores AVs and selects an AV (here the *i*th AV, AV*i*=(RAND*i*, AUTH*i*, XRES*i*, $K_{ASME}i$))



HSS

IMSI: Provisioned @AuC
LTE K: Provisioned @AuC

RAND: HSS generates
SQN: HSS generates (increase)

Authentication Vector (AV)

AV = (**RAND**, **AUTN, XRES**, **K_{ASME}**)

LTE Authentication Procedure (3)

3. Mutual Authentication by UE and MME

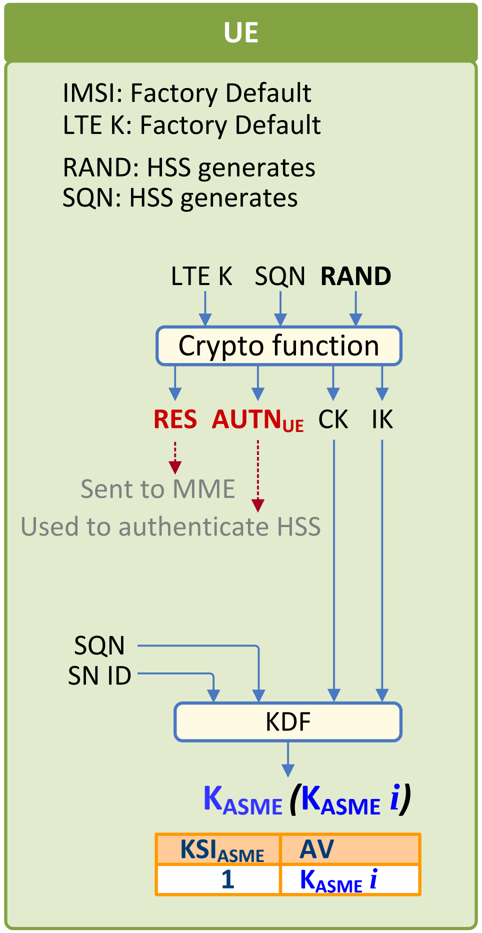
- K_{ASME} : MME Base Key (local master key). Stored only in MME, not delivered to the UE
- UE authenticates the Network (HSS) *by comparing AUTN with* $AUTH_{UE}$
- MME (on behalf of HSS) authenticates the UE *by comparing RES with XRES*

❹ [UE ← MME] Request by MME for User Authentication

- MME sends ***Authentication Request*** *($KSI_{ASME}i$, RANDi, AUTNi)* message to UE
  - Keeps $K_{ASME}i$ and XRESi
  - Allocates $KSI_{ASME}i$ to uniquely identify $K_{ASME}i$ ($KSI_{ASME}i$ is shared in the UE and MME)
  - Sends $KSI_{ASME}i$, RANDi, AUTNi to UE
- UE
  - Calculates Authentication Vector, **AV=(RAND, $AUTH_{UE}$, RES, K_{ASME})** using the same AKA algorithm as in HSS
  - Authenticates the Network (HSS) by comparing **AUTH*i*** with **$AUTH_{UE}$**

❺ [UE → MME] Response by UE to User Authentication

- UE sends ***Authentication Response*** *(RES)* message back to MME
- MME
  - Authenticates the UE by comparing **RES** with **XRES*i***


UE

IMSI: Factory Default
LTE K: Factory Default

RAND: HSS generates
SQN: HSS generates

KSI_{ASME}	AV
1	$K_{ASME}i$

Summary of LTE Security Keys: Authentication

LTE Security Keys related to the LTE Authentication (EPS AKA)

Key	Length	Location	Derived from	Description
K	128 bits	USIM, AuC	-	EPS master key
CK	128 bits	USIM, HSS	K	Cipher key
IK	128 bits	USIM, HSS	K	Integrity key
K_{ASME}	256 bits	UE, HSS, MME	CK, IK	MME base key

References and Abbreviations

[1] Netmanias Technical Document, “LTE Security II: NAS and AS Security”, August 2013, http://www.netmanias.com/bbs/view.php?id=techdocs&no=66

[2] 3GPP TS 24.301, “Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3”.

[3] 3GPP TS 33.401, “3GPP System Architecture Evolution (SAE); Security architecture”.

[4] NMC Consulting Group Confidential Internal Report, “E2E LTE Network Design”, August 2010.

Abbreviations

AES	: Advanced Encryption Standard
AKA	: Authentication and Key Agreement
AS	: Access Stratum
ASME	: Access Security Management Entity
AuC	: Authentication Center
AUTN	: Authentication Token
AV	: Authentication Vector
CK	: Cipher Key
EEA	: EPS Encryption Algorithm
EIA	: EPS Integrity Algorithm
EPS	: Evolved Packet System
HSS	: Home Subscriber Server
IK	: Integrity Key
IMSI	: International Mobile Subscriber Identity
KSI	: Key Set Identifier
LTE	: Long Term Evolution
MCC	: Mobile Country Code
MME	: Mobility Management Entity
MNC	: Mobile Network Code
NAS	: Non Access Stratum
PLMN	: Public Land Mobile Network
RAND	: RANDom number
RES	: Response
RRC	: Radio Resource Control
SN ID	: Serving Network ID
SQN	: Sequence Number
UE	: User Equipment
UP	: User Plane
USIM	: Universal Subscriber Identity Module
XRES	: Expected Response

Netmanias LTE Technical Documents

Visit http://www.netmanias.com to view and download more technical documents.

Index	Topic	Document title	Document presented here
1	Network Architecture	LTE Network Architecture: Basic	
2	Identification	LTE Identification I: UE and ME Identifier	
3		LTE Identification II: NE and Location Identifier	
4		LTE Identification III: EPS Session/Bearer Identifier	
5	**Security**	**LTE Security I: LTE Security Concept and LTE Authentication**	**O**
6		LTE Security II: NAS and AS Security	
7	QoS	LTE QoS: SDF and EPS Bearer QoS	
8	EMM	LTE EMM and ECM States	
9		LTE EMM: User Experience based EMM Scenario and Eleven EMM Cases	
10		LTE EMM Procedure: 1. Initial Attach (Part 1) – Case of Initial Attach	
11		LTE EMM Procedure: 1. Initial Attach (Part 2) – Call Flow of Initial Attach	
12		LTE EMM Procedure: 2. Detach	
13		LTE EMM Procedure: 3. S1 Release	
14		LTE EMM Procedure: 4. Service Request	
15		LTE EMM Procedure: 5. Periodic TAU	
16		LTE EMM Procedure: 6. Handover without TAU (Part 1) – Overview of LTE Handover	
17		LTE EMM Procedure: 6. Handover without TAU (Part 2) – X2 Handover	
18		LTE EMM Procedure: 6. Handover without TAU (Part 3) – S1 Handover	
19		LTE EMM Procedure: 7. Cell Reselection without TAU	
20		LTE EMM Procedure: 8/9. Handover/Cell Reselection with TAU	
21		LTE EMM Procedure: 10/11. Toward Another City	
22	PCC	LTE Policy and Charging Control (PCC)	
23	Charging	LTE Charging I: Offline	
24		LTE Charging II: Online (TBD)	
25	IP Address Allocation	LTE: IP Address Allocation Schemes I: Basic	
26		LTE: IP Address Allocation Schemes II: A Case for Two Cities	

Netmanias Research and Consulting Scope

		99	00	01	02	03	04	05	06	07	08	09	10	11	12	13
Services	eMBMS/Mobile IPTV	□	□	□	□	□	□	□	□	□	□	□	□	□	■	■
	CDN/Mobile CDN	□	□	□	□	□	□	□	□	□	□	□	□	■	■	■
	Transparent Caching	□	□	□	□	□	□	□	□	□	□	□	□	■	■	■
	BSS/OSS	□	□	□	□	□	□	□	□	□	■	■	■	■	■	■
	Cable TPS	□	□	□	□	□	□	□	□	■	■	■	■	■	■	■
	Voice/Video Quality	□	□	□	□	□	□	□	■	■	■	■	■	■	■	■
	IMS	□	□	□	□	□	□	■	■	■	■	■	■	■	■	■
	Policy Control/PCRF	□	□	□	□	■	■	■	■	■	■	■	■	■	■	■
	IPTV/TPS	□	□	□	■	■	■	■	■	■	■	■	■	■	■	■
Mobile Network	LTE	□	□	□	□	□	□	□	□	□	■	■	■	■	■	■
	Mobile WiMAX	□	□	□	□	□	□	□	□	■	■	■	■	■	■	■
	Carrier WiFi	□	□	□	□	□	□	□	□	□	□	□	□	■	■	■
	LTE Backaul	□	□	□	□	□	□	□	□	□	□	□	□	■	■	■
Wireline Network	Data Center Migration	□	□	□	□	□	□	□	□	□	□	□	■	■	■	■
	Carrier Ethernet	□	□	□	□	□	□	□	□	■	■	■	■	■	■	■
	FTTH	□	□	□	□	□	■	■	■	■	■	■	■	■	■	■
	Data Center	□	□	□	□	□	■	■	■	■	■	■	■	■	■	■
	Metro Ethernet	□	□	■	■	■	■	■	■	■	■	■	■	■	■	■
	MPLS	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
	IP Routing	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

Visit http://www.netmanias.com to view and download more technical documents.