NETMANIAS
www.netmanias.com

NMC CONSULTING GROUP
www.nmcgroups.com

LTE Security I: LTE Security Concept and LTE Authentication

Table of Contents

The LTE Security technical document consists of two companion documents: this first document (Part I, LTE Security I) and the second document (Part II, LTE Security II) that follows. These documents will cover the following three topics: LTE authentication (in Part I) and NAS security and AS security (in Part II). In Part I, an overview of LTE security explaining the concept of the three topics and the relationship among them will be given, followed by a detailed description of LTE authentication procedure.

July 31, 2013

(Initial Released: May 23, 2011)

www.netmanias.com

NMC Consulting Group (tech@netmanias.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.

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 Identifiers	
3		LTE Identification II: NE and Location Identifiers	
4		LTE Identification III: EPS Session/Bearer Identifiers	
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		Eleven EMM Cases in an EMM Scenario	
10		LTE EMM Procedure 1. Initial Attach - Part 1. Cases 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 and Cell Reselection with TAU	
21		LTE EMM Procedure 10 & 11. Move to Another City and Attach	
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	

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
eNB	Evolved Node B
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
HSS	Home Subscriber Server
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
KDF	Key Derivation Function
KSI	Key Set Identifier
LTE	Long Term Evolution
MAC-I	Message Authentication Code for Integrity
MCC	Mobile Country Code
MME	Mobility Management Entity
MNC	Mobile Network Code
NAS	Non Access Stratum
NAS-MAC	Message Authentication Code for NAS for Integrity
PDCP	Packet Data Convergence Protocol
PLMN	Public Land Mobile Network
RAND	RANDom number
RES	Response
RRC	Radio Resource Control
SN ID	Serving Network IDentity
SQN	Sequence Number
UE	User Equipment
UP	User Plane
USIM	Universal Subscriber Identity Module
XRES	Expected Response
ZUC	Zu Chongzhi

I. Introduction

Wireless communication, in its nature, is always at a risk of eavesdropping or manipulation because data originally sent from/to a user may be received and unlawfully used by an unintended user. Locations or traveling routes of a user can also be easily tracked by tracing to which cells the user is connected or through which cells the user is travelling. And this can result in privacy infringement. Mobile communication networks provide security features to ensure data transferred over radio links is not manipulated, prevent unauthorized access by an unintended user to the data received, and protect the privacy of users

The LTE Security document describes basic security features offered by LTE networks, including LTE authentication, NAS (Non Access Stratum) security and AS (Access Stratum) security. LTE authentication is the process of determining whether a user is an authorized subscriber to the network that he/she is trying to access, while NAS security and AS security are features required to securely deliver user data that travels over LTE radio links at NAS and AS levels.

The LTE Security document consists of the following two companion documents: Part I, LTE Security I, and Part II, LTE Security II. Part I will explain the concept of LTE security and the detailed procedure of LTE authentication, and Part II will discusses NAS and AS security setup.

Part I is organized as follows: In Chapter II, the scope of these two companion documents will be defined and a conceptual overview will be given. Chapter III will focus on the detailed procedure of LTE authentication and Chapter IV will summarize the LTE authentication and the LTE authentication-related keys.

II. LTE Security Concept

2.1 Scope and Concept of LTE Security

Figure 1 below shows the scope and overall concept of the LTE Security documents. The scope of these documents will include the following three areas:

1. LTE Authentication: performs mutual authentication between a UE and a network.
2. NAS Security: performs integrity protection/verification and ciphering (encryption/decryption) of NAS signaling between a UE and an MME.
3. AS Security
   - performs integrity protection/verification and ciphering of RRC signaling between a UE and an eNB.
   - performs ciphering of user traffic between a UE and an eNB.

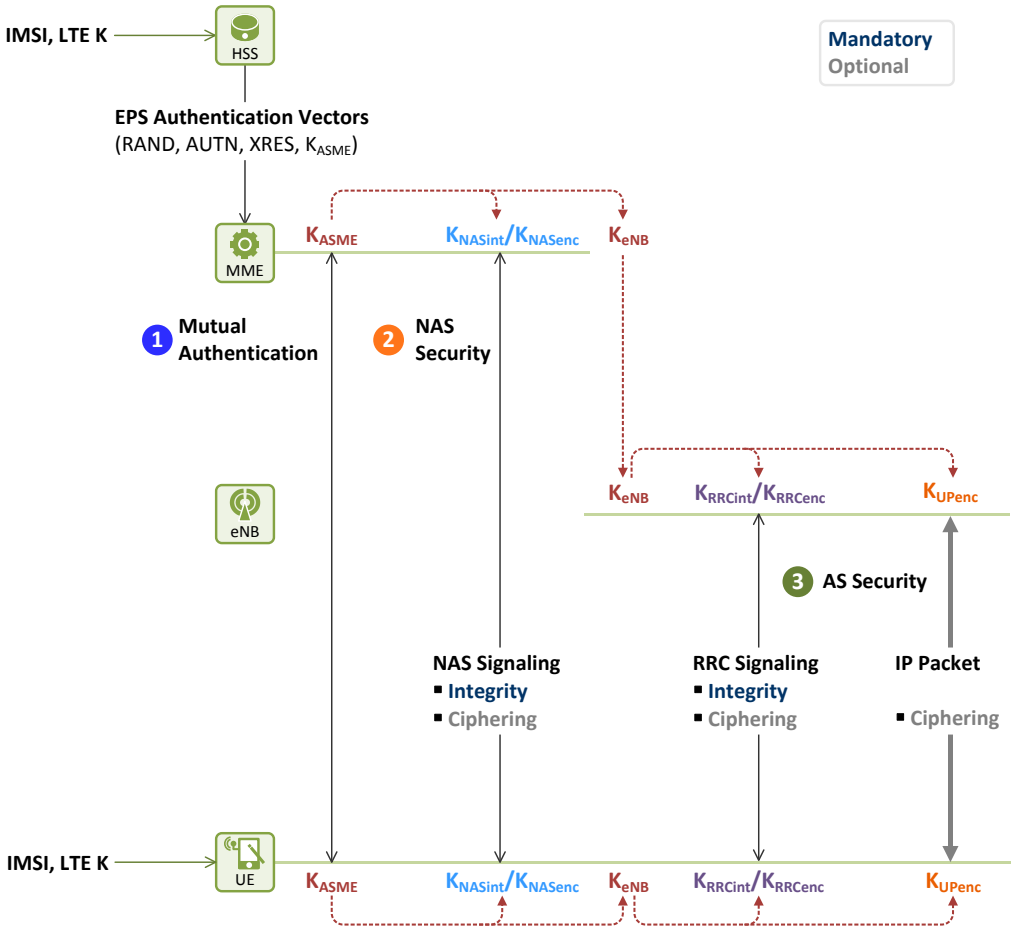


Figure 1. Scope and concept of LTE security

LTE Authentication

In mobile communication networks, authentication refers to the process of determining whether a user is an authorized subscriber to the network that he/she is trying to access. Among various authentication procedures available in such networks, EPS AKA (Authentication and Key Agreement) procedure is used in LTE networks for mutual authentication between users and networks.

The EPS AKA procedure consists of two steps. First, an HSS (Home Subscriber Server) generates EPS authentication vector(s) (RAND, AUTN, XRES, K_{ASME}) and delivers them to an MME. Then in the second step, the MME selects one of the authentication vectors and uses it for mutual authentication with a UE and shares the same authentication key (K_{ASME}) each other. Mutual authentication is the process in which a network and a user authenticate each other. In LTE networks, since the ID of the user's serving network is required when generating authentication vectors, authentication of the network by the user is performed in addition to authentication of the user by the network.

ASME (Access Security Management Entity) is an entity that receives top-level key(s), from an HSS, to be used in an access network. In EPS, an MME serves as ASME and K_{ASME} is used as the top-level key to be used in the access network. The MME, on behalf of an HSS, conducts mutual authentication with a UE using K_{ASME}. Once mutually authenticated, the UE and MME get to share the same K_{ASME} as an authentication key.

To avoid any possible eavesdropping or manipulation of data over radio links, K_{ASME} is not delivered to the UE via E-UTRAN. Instead, the MME delivers part of authentication vector to the UE, which uses it to authenticate

the network and generates K_{ASME} as the HSS does.

NAS Security

NAS security, designed to securely deliver signaling messages between UEs and MMEs over radio links, performs integrity check (i.e., integrity protection/verification) and ciphering of NAS signaling messages. Different keys are used for integrity check and for ciphering. While integrity check is a mandatory function, ciphering is an optional function. NAS security keys, such as integrity key (K_{NASint}) and ciphering key (K_{NASenc}), are derived by UEs and MMEs from $K_{ASME.}$

AS Security

AS security is purposed to ensure secure delivery of data between a UE and an eNB over radio links. It conducts both integrity check and ciphering of RRC signaling messages in control plane, and only ciphering of IP packets in user plane. Different keys are used for integrity check/ciphering of RRC signaling messages and ciphering of IP packets. Integrity check is mandatory, but ciphering is optional.
AS security keys, such as K_{RRCint}, K_{RRCenc} and K_{UPenc}, are derived from K_{eNB} by a UE and an eNB. K_{RRCint} and K_{RRCenc} are used for integrity check and ciphering of control plane data (i.e., RRC signaling messages), and K_{UPenc} is used for ciphering of user plane data (i.e., IP packets). Integrity check and ciphering are performed at the PDCP (Packet Data Convergence Protocol) layer.

A UE can derive K_{eNB} from K_{ASME}. However, since K_{ASME} is not transferred to an eNB, an MME instead generates K_{eNB} from K_{ASME} and forwards it to the eNB.

2.2 Overview of LTE Security Procedure

Figure 2 shows the overview of LTE security procedure. 1 displays LTE authentication procedure while 2 and 3 demonstrate security setup procedures for NAS and AS respectively. A brief description of each procedure will be given below first. Then, a detailed explanation on the LTE authentication procedures and NAS and AS security setup procedures will be given in Chapter III hereof and again in Part II, LTE Security II, that follows.

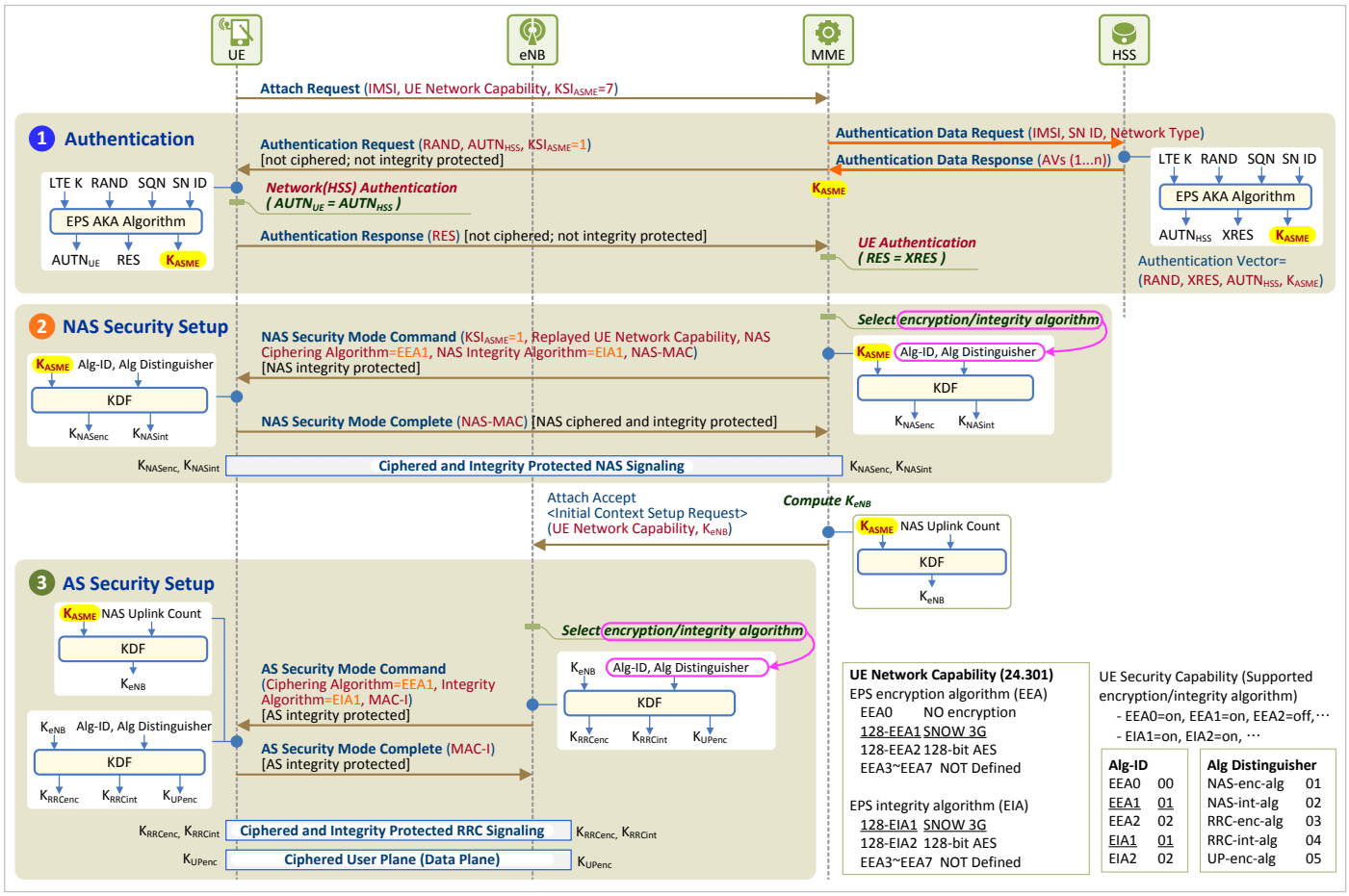


Figure 2. Overview of LTE security procedure

1 LTE Authentication

When a user requests for access to a LTE network, mutual authentication between the user and the network is conducted using EPS AKA procedure. An MME, upon receipt of such request, identifies the user using his/her IMSI and requests authentication vector(s) (AVs) from an HSS[1]. The HSS then generates AV(s) using EPS AKA algorithm, AV={RAND, XRES, $AUTN_{HSS}$, K_{ASME}}, and forwards them to the MME.

After storing the AVs, the MME selects one of them and uses it to perform mutual authentication with the UE[2]. The MME forwards RAND and $AUTN_{HSS}$ to the UE, which then computes RES, $AUTN_{UE}$ and K_{ASME} using EPS AKA algorithm. The UE now compares its own $AUTN_{UE}$ and $AUTN_{HSS}$ received from the MME for network authentication. Once authenticated, RES is forwarded to the MME, which then compares the XRES received from the HSS and the RES received from the UE for user authentication. If the UE and network have authenticated each other, they share the same key K_{ASME} (K_{ASME} is not transferred between UE and MME, though).

[1] MME may request for more than one authentication vectors.

[2] In general, UE consists of USIM and ME. USIM handles mutual authentication and ME delivers authentication information between MME and USIM. Once the network is successfully authenticated, USIM calculates CK and IK and delivers them to ME, which then calculates K_{ASME} based on them. USIM and ME are collectively referred to as UE herein for the sake of convenience unless it is required to refer to USIM specifically.

2 NAS Security

Once the UE and MME have authenticated each other and the same key K_{ASME} is shared, NAS security setup procedure begins. In this procedure, NAS security keys to be used when delivering NAS signaling messages are derived from K_{ASME} for secure delivery of these messages. This procedure consists of a round trip of NAS signaling messages (**Security Mode Command** and **Security Mode Complete** messages), and begins when the MME delivers a **Security Mode Command** message to the UE.

First, the MME selects NAS security algorithms (Alg-ID: Algorithm ID) and uses them to create an integrity key (K_{NASint}) and a ciphering key (K_{NASenc}) from $K_{ASME.}$ Then, it applies K_{NASint} to the **Security Mode Command** message to generate an NAS message authentication code (NAS-MAC, Message Authentication Code for NAS for Integrity). The MME then delivers the **Security Mode Command** message including the selected NAS security algorithms and the NAS-MAC to the UE. As the UE does not know the selected encryption algorithm yet, this message is integrity protected only but not ciphered.

Upon receiving the **Security Mode Command** message, the UE verifies the integrity thereof by using the NAS integrity algorithm selected by the MME and uses NAS integrity/ciphering algorithm to generate NAS security keys (K_{NASint} and K_{NASenc}) from K_{ASME}. Then it ciphers the **Security Command Complete** message with K_{NASenc} and generates a message authentication code, NAS-MAC with K_{NASint} to the ciphered message. Now it forwards the ciphered and integrity protected message to the MME with the NAS-MAC included.
Once the MME successfully verifies the integrity of the received **Security Mode Complete** message and has them decrypted using the NAS security keys (K_{NASint} and K_{NASenc}), the NAS security setup procedure is completed.

Once the NAS security is set up, NAS signaling messages between the UE and the MME are ciphered and integrity protected by the NAS security keys and then securely delivered over radio links.

3 AS Security

After NAS security setup is finished, AS security setup procedure between a UE and an eNB begins. In this procedure, AS security keys to be used when delivering RRC signaling messages and IP packets are derived from K_{eNB} for secure delivery of these data. This procedure consists of a round trip of RRC signaling messages (**Security Mode Command** and **Security Mode Complete** messages), and begins when an eNB delivers **Security Mode Command** message to the UE.

First, the MME calculates K_{eNB} from K_{ASME} and delivers it to the eNB, which uses it to perform the AS security setup procedure. The eNB selects AS security algorithms (Alg-ID: Algorithm ID) and uses them to create an integrity key (K_{RRCint}) and a ciphering key (K_{RRCenc}) from K_{eNB} to be used for RRC signaling messages, and a ciphering key (K_{UPenc}) to be used in the user plane. Then, it applies K_{RRCint} to the **Security Mode Command** message to generate a message authentication code (MAC-I, Message Authentication Code for Integrity). The eNB now delivers the **Security Mode Command** message including the selected AS security algorithms and the MAC-I to the UE.
Upon receiving the **Security Mode Command** message from the eNB, the UE verifies the integrity thereof by using the AS integrity algorithm selected by the eNB and uses AS integrity/ciphering algorithm to generate AS security keys (K_{RRCint}, K_{RRCenc} and K_{UPenc}). Then it generates a message authentication code, MAC-I, with the RRC integrity key to the **Security Command Complete** message, and then forwards the

message including the MAC-I to the eNB.

When the eNB successfully verifies the integrity of the received **Security Mode Complete** message by using the AS integrity key, the AS security setup procedure is completed.

After the AS security is set up, RRC signaling messages between the UE and the eNB are ciphered and integrity protected by the AS security keys, and user IP packets are encrypted and then securely delivered over radio links.

III. LTE Authentication Procedure

The LTE authentication procedure briefly described in Chapter II will be further discussed below. Figure 3 shows the EPS AKA-based LTE authentication procedure that is performed when a UE attaches to the LTE network. On the USIM and in the HSS/AuC are stored a permanent key, LTE key (K), and IMSI[3]. These LTE key (K) and IMSI are stored on the USIM card when a UE is being manufacturing, and provisioned in the HSS/AuC when a user begins subscription to his/her operator's network.

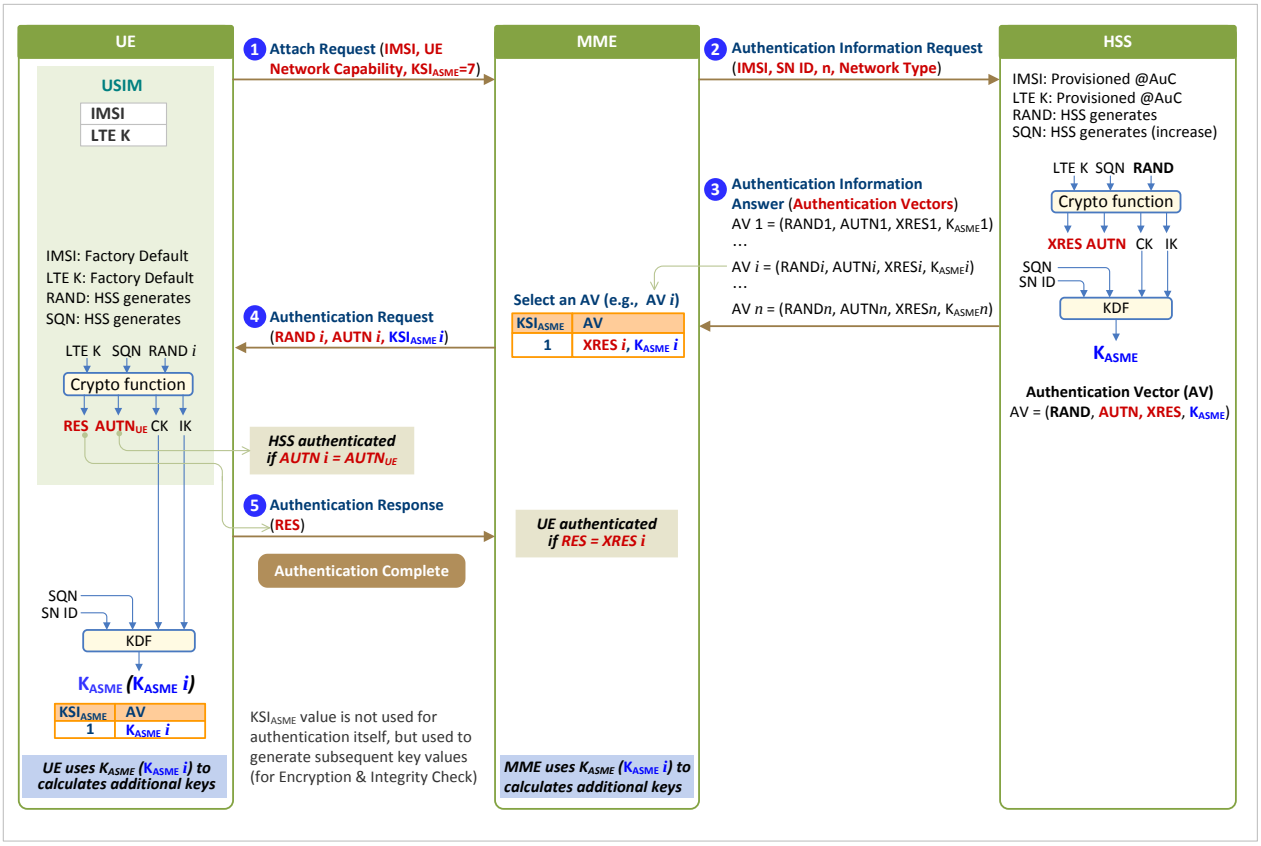


Figure 3. LTE authentication procedure

[3] LTE key (K) is stored in AuC (Authentication Center) in operator's network and in USIM in UE. In Figures herein, AuC and HSS are collectively referred to as HSS, and USIM and ME as UE for the sake of convenience.

3.1 Authentication Request by UE

❶ [UE → MME] Request by UE for network registration

When a UE attempts to access the network for initial attach, it delivers **Attach Request** (IMSI, UE Network Capability, KSI_{ASME}=7) message to an MME. And this triggers EPS AKA procedure. The following information elements are included in the **Attach Request** message:

- **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

UE network capability informs the MME of what kinds of capability the UE has related to EPS, and indicates which NAS and AS security algorithms, i.e., EPS Encryption Algorithms (EEA) and EPS Integrity Algorithms (EIA) are supported by the UE. Each of them has a value of 1 bit that is presented as on (supported) or off (not supported) (e.g. EEA0=on, EEA1=on, EEA2=off, …, EIA1=on, EIA2=on, …). Table 1 lists some of UE network capability information, specifically ciphering and integrity protection algorithms defined in [3].

Table 1. UE network capability information – EEA and EIA [3]

EEA		EIA	
EEA0	Null ciphering algorithm	EIA0[4]	Null integrity protection algorithm
128-EEA1	SNOW 3G	128-EIA1	SNOW 3G
128-EEA2	AES	128-EIA2	AES
128-EEA3	ZUC	128-EIA3	ZUC

KSI_{ASME} identifies KSI_{ASME} for the UE and the MME. It is 3 bits and has values ranging from 0 ('000') to 7 ('111'), where 7 ('111') indicates the UE has no K_{ASME} available.

3.2 Authentication Data Exchange between MME and HSS

❷ [MME → HSS] Request by MME for authentication data

The MME recognizing the UE has no K_{ASME} available initiates LTE authentication procedure to get new authentication data by sending an **Authentication Information Request** (IMSI, SN ID, n, Network Type) message to the HSS. Message parameters used for this purpose are as follows:

- **IMSI**: a unique identifier associated with the user
- **SN ID (Serving Network ID)**: refers to the network accessed by the user, consists of PLMN ID (MCC+MNC)
- **n (number of Authentication Vectors)**: number of authentication vectors that MME requests
- **Network Type**: type of the network accessed by UE (E-UTRAN herein)

Upon receipt of the **Authentication Information Request** message from the MME, the HSS generates RAND and SQN, and creates XRES, AUTN, CK and IK using EPS AKA algorithm with LTE key (K), SQN and RAND. Thereafter, using CK, IK, SQN and SN ID, it derives a top-level key (K_{ASME}) of the access network, from Key

[4] EIA0 is allowed in an unauthorized emergency call only.

Derivation Function (KDF), to be delivered to the MME. KDF is a one-way has function. Since SN ID is required when deriving K_{ASME}, K_{ASME} is derived again if the serving network is changed. After K_{ASME} is derived, the HSS forms authentication vectors AV_i = ($RAND_i$, $AUTN_i$, $XRES_i$, K_{ASMEi}), i = 0 … n-1.

❸ [MME ← HSS] Response by HSS to the authentication data request

The HSS forms as many AVs as requested by the MME and then delivers an **Authentication Information Answer** (AVs) message to the MME.

3.3 Mutual Authentication by UE and MME

The MME stores the AVs received from the HSS, and selects one of them to use in LTE authentication of the UE. In Figure 3, the MME selected *i*th AV (AV_i). K_{ASME} is a base key of MME and serves as a top-level key in the access network. It stays within EPC only and is not delivered to the UE through E-UTRAN, which is not secure. The MME allocates $KSI_{ASME,}$ an index for K_{ASME}, and delivers it instead of K_{ASME} to the UE so that the UE and the MME can use it as a substitute for K_{ASME} (in Fig. 3, KSI_{ASME}=1).

❹ [UE ← MME] Request by MME for user authentication

The MME keeps K_{ASMEi} and $XRES_i$ in AV_i but delivers KSI_{ASMEi}, in substitution for K_{ASMEi}, $RAND_i$ and $AUTN_i$ as included in the **Authentication Request** (KSI_{ASMEi}, $RAND_i$, $AUTN_i$) message to the UE. $XRES_i$ is used later in ❺ when authenticating the user.

The UE, upon receiving the **Authentication Request** message from the MME, delivers $RAND_i$ and $AUTN_i$ to USIM. USIM, using the same EPS AKA algorithm that the HSS used, derives RES, $AUTN_{UE}$, CK and IK with the stored LTE key (K) and $RAND_i$ and SQN generated from the HSS[5]. The UE then compares $AUTN_{UE}$ generated using EPS AKA algorithm and AUTN received from MME ($AUTN_i$ in Fig. 3) to authenticate the LTE network (the serving network).

❺ [UE → MME] Response by UE to user authentication

Once the UE completes the network authentication, it delivers an **Authentication Response** (RES) message including RES generated using EPS AKA algorithm to the MME. If the network authentication using AUTN fails in ❹, the UE sends an **Authentication Failure** (CAUSE) message that contains a CAUSE field stating reasons for such failure.

When the MME receives the **Authentication Response** message from the UE, it compares RES generated by the UE and $XRES_i$ of the AV received from the HSS to authenticate the user.

USIM delivers CK and IK to the UE after its network authentication is completed. The UE derives K_{ASME} using Key Derivation Function (KDF) with CK, IK, SQN and SN ID and stores it using KSI_{ASME} received from the MME as its index. Thereafter, KSI_{ASME} is used instead of K_{ASME} during the NAS security setup between the UE and the MME.

[5] SQN is concealed in $AUTN_i$.

IV. Closing

We have discussed the LTE authentication, one of the LTE security topics. As seen so far, LTE authentication is mutual authentication performed by and between a user and a network based on EPS AKA procedure. An MME in the serving network performs mutual authentication with a UE on behalf of an HSS, and as a result, K_{ASME} is shared by the UE and the MME. Table 2 summarizes the LTE authentication-related keys covered herein. In Part II, LTE Security II, that follows, NAS and AS security setup procedures based on K_{ASME} discussed herein will be further explained.

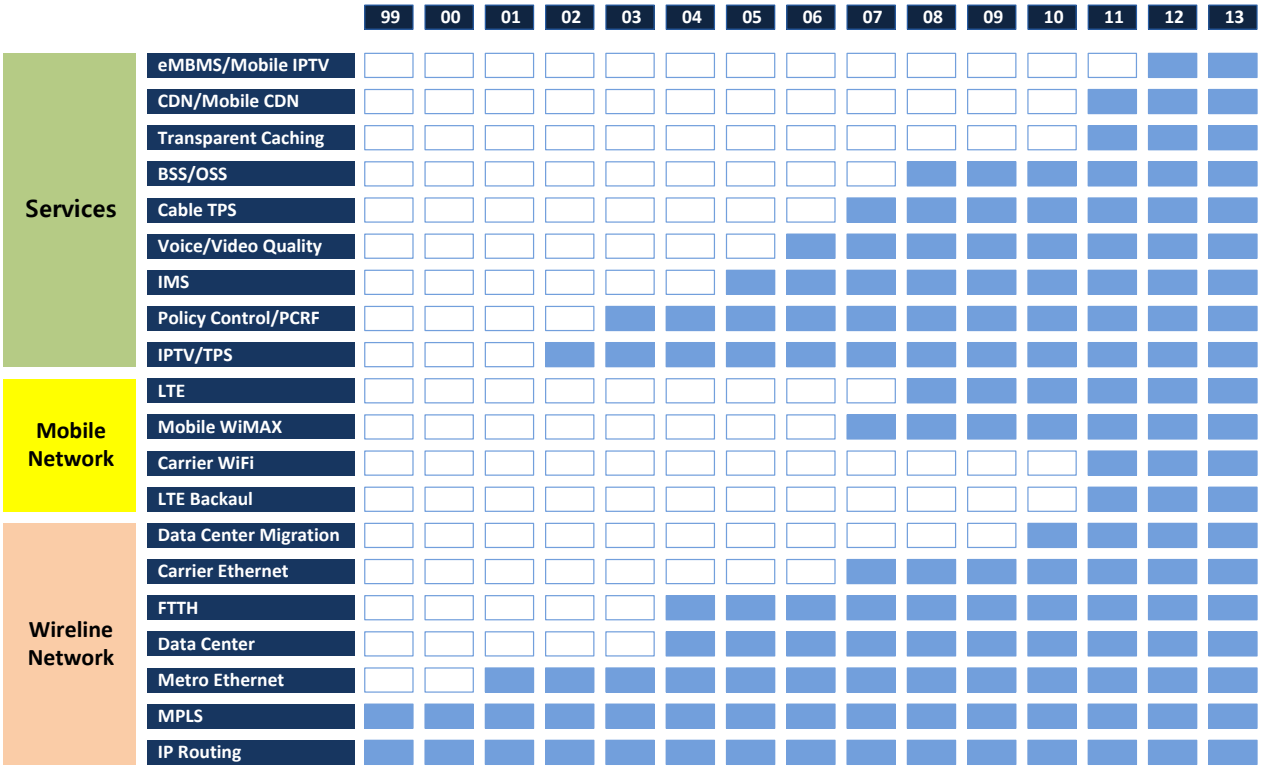
Table 2. LTE security keys: Authentication

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

References

[1] Netmanias Technical Document, “LTE Security II: NAS and AS Security”, August 2013, http://www.netmanias.com/en/?m=view&id=techdocs&no=5903.
[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.

Netmanias Research and Consulting Scope



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