Generated with EventStudio System Designer - http://www.EventHelix.com/EventStudio

We recommend going through the following presentation for a good background on LTE keys.
http://www.eventhelix.com/lte/security/lte-security-presentation.pdf

LTE UE is Provisioned

Program the secret key K

LTE security is based on a shared secret key. The USIM is programmed with a secret key K.

Provision the user with secret key K

The secret key K is also provisioned on the HSS.

USIM and HSS have a shared secret key K

UE is powered on

Initial NAS Message

UE Security Capabilities, Supported ciphering and integrity protection algorithms

The UE establishes an RRC connection and sends a Initial NAS Message to the MME.

Check if security tuples exist for the UE

This is a new session. No security tuples are cached on the MME.

DIAMETER Authentication

Information Request

The MME uses the DIAMETER protocol to request security tuples from the NME.

Find the key for UE

Compute K-ASME, AUTN, XRES and RAND from the key K

The HSS derives K-ASME, AUTN (Authentication token), XRES (Expected Authentication Result) and RAND (A random number) from the shared secret key K.

DIAMETER Authentication

Information Response, K-ASME, AUTN, XRES, RAND

HSS passes the security tuple to the MME containing K-ASME, AUTN, XRES and RAND.

Generate keys K-NAS-enc, K-NAS-int and K-eNB from K-ASME

The MME derives the K-NAS-enc (NAS layer encryption key), K-NAS-int (NAS layer intergrity protection key) and K-eNB (Key for eNodeB).

Authentication

Authentication Request

RAND, AUTN, KSI-ASME

The MME sends an unciphered Authentication Request to the UE. The message contains the RAND and AUTN numbers. Key selection identifier (KSI-ASME) is also included in the message.

Read the Key K

The UE reads the shared secret K key from the USIM.

Compute RES from K, AUTN and RAND

The UE computes an authentication result (RES) from the key K and the received AUTN and RAND values.

Authentication Response

RES

The UE sends the RES value back to the MME.

Compare RES and XRES

The MME compares the RES value received from the UE with the XRES value specified by the HSS. Matching of the two values authenticates the UE. In this

scenario, the values match and the MME proceeds with NAS security procedure.

Enable NAS ciphering and integrity protection

NAS Security Mode Command
EPS Encryption Algorithm, EPS Integrity Algorithm, KSI-ASME

MME initiates the NAS security procedure. The encryption and integrity protection algorithms are included in the message. Key selection identifier (KSI-ASME) is also included in the message.

Generate K-NAS-enc from EPS Encryption Algorithm, K-ASME

The UE uses the K-ASME key and the EPS encryption algorithm to derive the NAS encryption key.

Generate K-NAS-int from EPS Integrity Algorithm, K-ASME

The UE selects the K-ASME key based on the KSI-ASME received from the network. The UE then uses the K-ASME key and the EPS integrity algorithm to derive the NAS integrity protection key.

NAS Security Mode Complete

UE responds back to the MME. This message is sent with NAS ciphering and integrity protection.

Enable RRC integrity protection and RRC/User Plane ciphering

S1AP Initiation Message
Initial Context Setup, UE Security Capabilities, K-eNB

MME now initiates a security context setup with the eNodeB. The UE security capabilities and the K-eNB is sent to the eNodeB.

Generate K-RRC-enc, K-RRC-int keys from the K-eNB key

eNodeB derives the RRC encryption and integrity protection keys from the K-eNB key.

Generate K-UP-enc keys from the K-eNB key

eNodeB derives the user plane encryption key from the K-eNB key.

RRC Security Mode Command
AS Encryption Algorithm, AS Integrity Algorithm, START for integrity and encryption

The eNodeB initiates the security mode command to the UE. The message contains the AS integrity protection and encryption algorithms. The START parameters are also included in the message.

Generate K-RRC-enc and K-UP-enc keys from the AS Encryption Algorithm and K-ASME

The UE uses the K-ASME and the AS Encryption algorthm to determine the RRC and User Plane encryption keys.

Generate K-RRC-int key from the AS Integrity Algorithm and K-ASME

The UE uses the K-ASME and the AS Integrity algorthm to determine the RRC integrity protection key.

RRC Security Mode Complete

UE responds with success. This message uses the newly activated keys to encrypt and integrity protect this message.

S1AP Successful Outcome
Initial Context Setup

eNodeB responds back to the MME signaling the successful estblishment of the security context.