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

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.

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.

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

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 algorithm 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 algorithm 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.