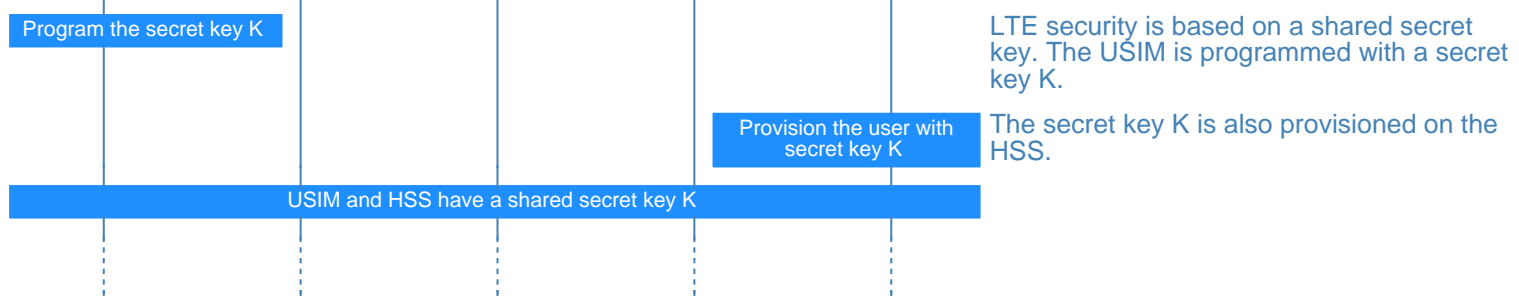


Generated with EventStudio System Designer - <http://www.EventHelix.com/EventStudio>

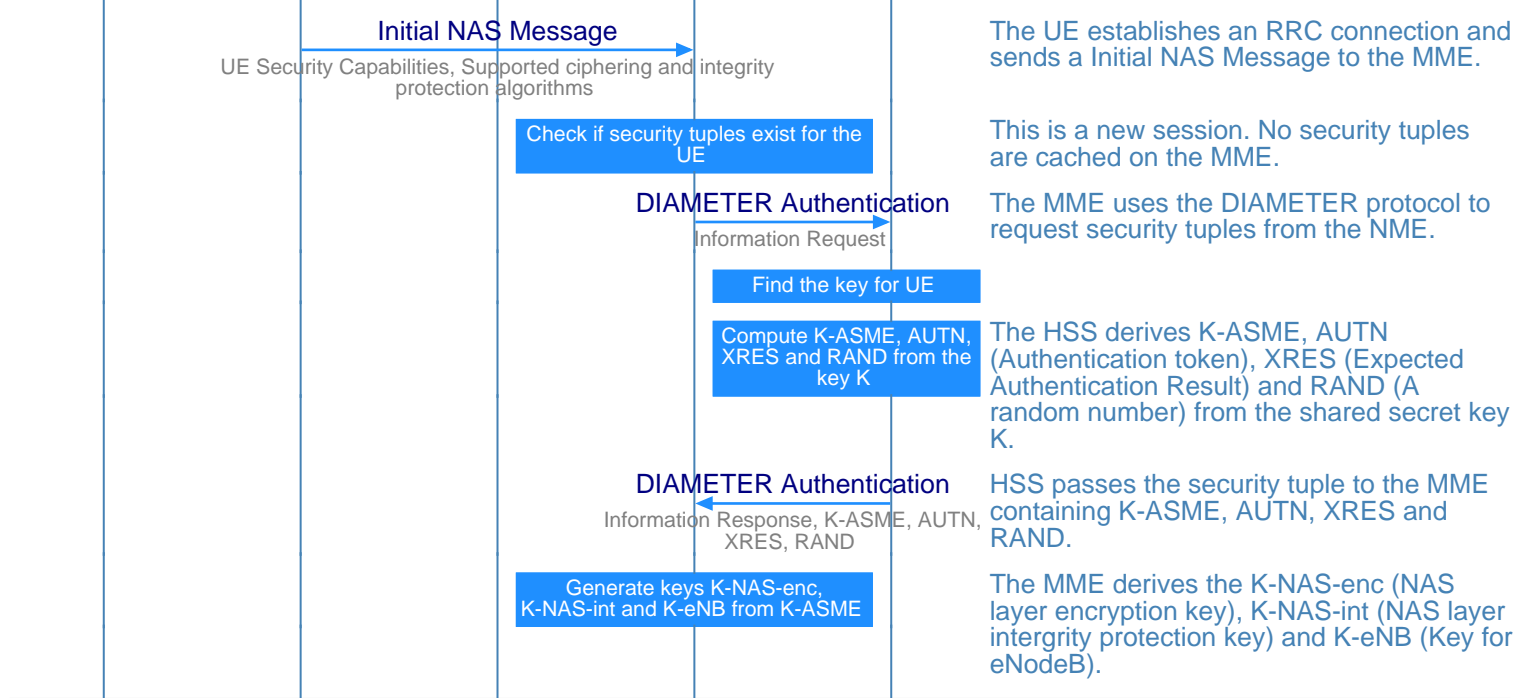
We recommend going through the following presentation for a good background on LTE keys.
<http://www.eventhelix.com/lte/security/lte-security-presentation.pdf>

LTE UE is Provisioned



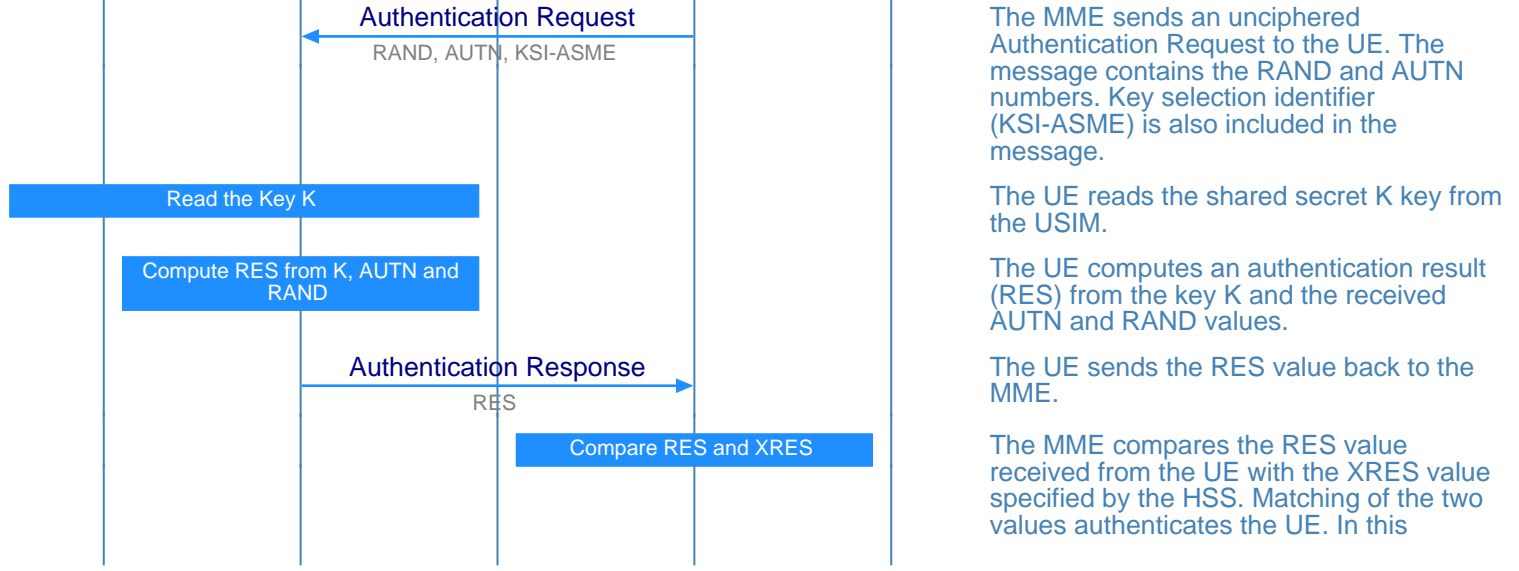
LTE security is based on a shared secret key. The USIM is programmed with a secret key K.
 The secret key K is also provisioned on the HSS.

UE is powered on



The UE establishes an RRC connection and sends a Initial NAS Message to the MME.
 This is a new session. No security tuples are cached on the MME.
 The MME uses the DIAMETER protocol to request security tuples from the HSS.
 The HSS derives K-ASME, AUTN (Authentication token), XRES (Expected Authentication Result) and RAND (A random number) from the shared secret key K.
 HSS passes the security tuple to the MME containing K-ASME, AUTN, XRES and RAND.
 The MME derives the K-NAS-enc (NAS layer encryption key), K-NAS-int (NAS layer integrity protection key) and K-eNB (Key for eNodeB).

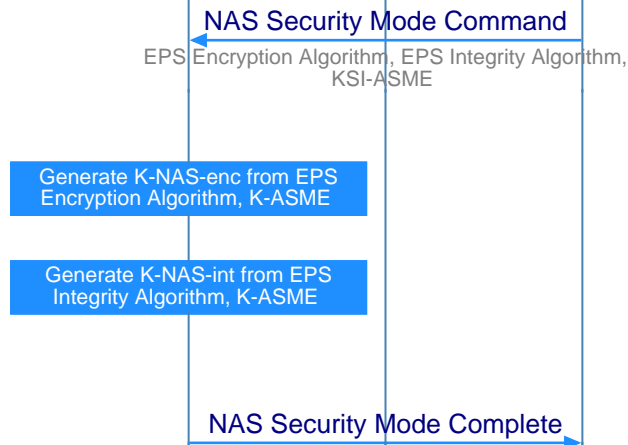
Authentication



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.
 The UE reads the shared secret K key from the USIM.
 The UE computes an authentication result (RES) from the key K and the received AUTN and RAND values.
 The UE sends the RES value back to the MME.
 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



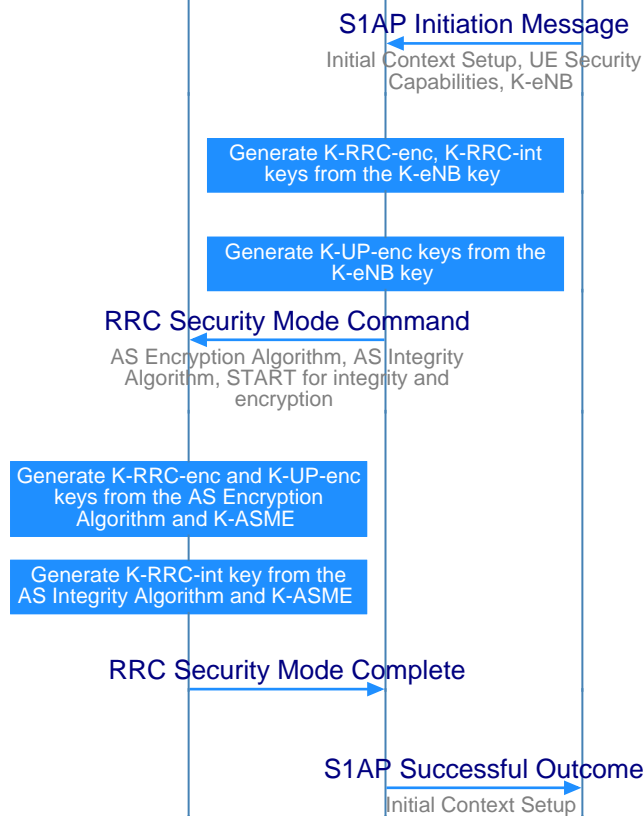
MME initiates the NAS security procedure. The encryption and integrity protection algorithms are included in the message. Key selection identifier (KSI-ASME) is also included in the message.

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

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.

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



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

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

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

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.

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

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

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

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