

UE Interfaces (LTE Security for new user)				
LTE Terminal		LTE Network		EventStudio System Designer 6
USIM	UE	e Node B	MME	31-Dec-13 14:51 (Page 1)

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>

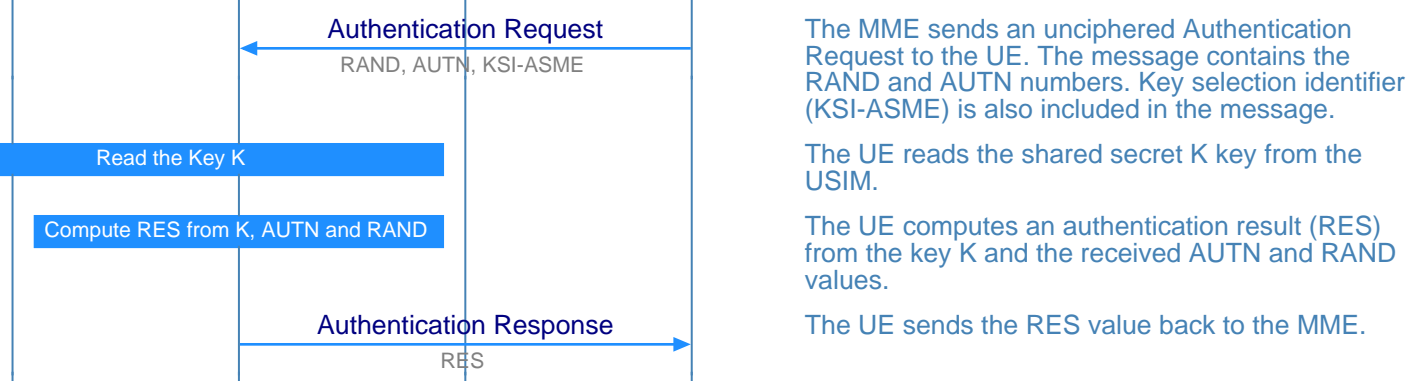
LTE UE is Provisioned

UE is powered on



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

Authentication



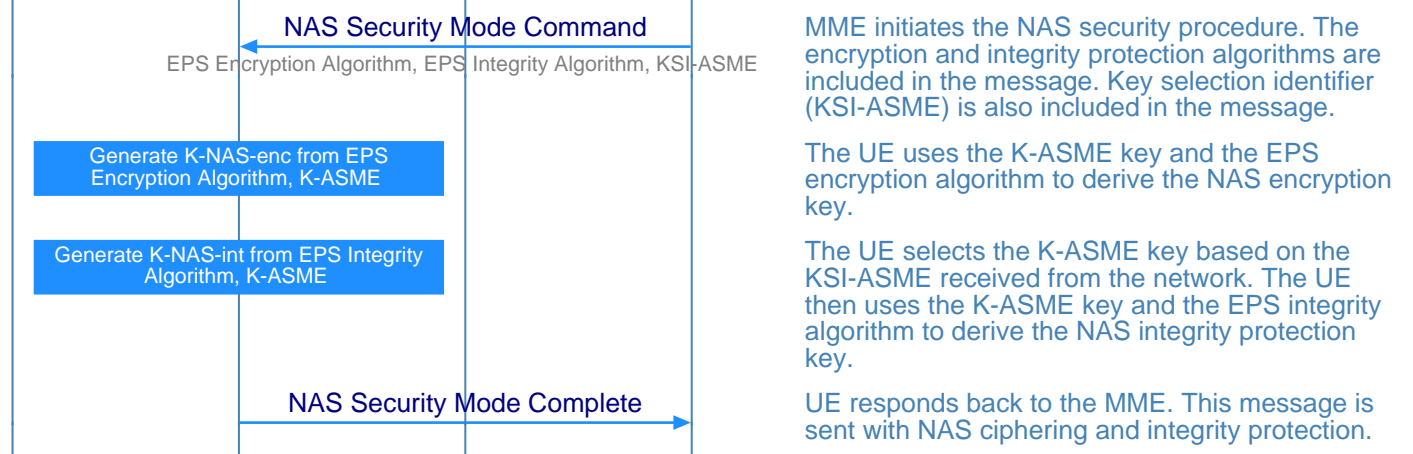
The MME sends an unciphered Authentication Request to the UE. The message contains the RAND and AUTN numbers. Key selection identifier (KSI-ASME) is also included in the message.

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.

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



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

UE Interfaces (LTE Security for new user)				
LTE Terminal		LTE Network		EventStudio System Designer 6
USIM	UE	e Node B	MME	31-Dec-13 14:51 (Page 2)

protect this message.

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

Copyright (c) EventHelix.com Inc. 2012. All Rights Reserved.