ENodeB Interfaces (LTE Security for new user)			
LTE Terminal LTE Network			EventStudio System Designer 6
UE	e Node B	MME	31-Dec-13 14:51 (Page 1)
Generated with EventStu	Idio System Designe	er - http://www.Eventh	lelix.com/EventStudio
We recommend going th http://www.eventhelix.com	rough the following p m/lte/security/lte-sec	presentation for a goc curity-presentation.pdf	d background on LTE keys.
LTE UE is Provis	sioned	I	
UE is powered o	n		
Authentication			
Enable NAS ciphering and integrity protection			
Enable RRC integrity protection and RRC/User Plane ciphering			
Ini	S1AP Initiati	on Message ecurity 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-F	RRC-enc, K-RRC-int keys K-eNB key	s from the	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 Moc AS Encryption Algorithm, AS START for integrity a	S Integrity Algorithm,		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.
RRC Security Mod	de Complete		UE responds with success. This message uses the newly activated keys to encrypt and integrity protect this message.
	S1AP Succes		eNodeB responds back to the MME signaling the successful estblishment of the security context.
Generated with EventStu	idio System Designe	er - http://www.EventH	lelix.com/EventStudio
Copyright (c) EventHelix.	com Inc. 2012 All F	Rights Reserved	
		I	