MME Interfaces (LTE Security for new user)					
LTE Terminal UE	LTE Network e Node B MME HSS			ПСС	EventStudio System Designer 6
			_		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 power	ed on [']		ı	1	
	nitial NAS Messa	ae			The UE establishes an RRC connection and sends
UE Security Capabilitie	es, Supported cipherir algorithms	ng and integrity			a Initial NAS Message to the MME.
	Chec		oles exist for th		This is a new session. No security tuples are cached on the MME.
		DIA	METER Au ^a Information F		The MME uses the DIAMETER protocol to request security tuples from the NME.
		DIA Information	METER Au Response, K-A RAND	ASME, AUTN, XR	HSS passes the security tuple to the MME RES, containing K-ASME, AUTN, XRES and RAND.
	Gener	ate keys K-NA K-eNB fror	S-enc, K-NAS- n K-ASME	int and	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					
	uthentication Req				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.
Au	thentication Resp	onse			The UE sends the RES value back to the MME.
		Compare RE	S 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					
	Security Mode Co porithm, EPS Integrity		-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.
NAS	Security Mode Co	omplete			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					
		ation Messa	ge		MME now initiates a security context setup with the eNodeB. The UE security capabilities and the K-eNB is sent to the eNodeB.
	S1AP Succ				eNodeB responds back to the MME signaling the successful estblishment of the security context.
Generated with Ev		'	http://www	.EventHelix.co	om/EventStudio
Copyright (c) EventHelix.com Inc. 2012. All Rights Reserved.					
Copyright (c) Even	itHelix.com Inc. 2	J12. All Rig	nts Reserve	d.	