libosmocore - Bug #4104

support for KASME generation

07/12/2019 10:14 AM - laforge

Status:	New	**Start date:**	07/12/2019
Priority:	Normal	**Due date:**	
Assignee:	laforge	**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

In an LTE HSS, the normal UMTS AKA is executed up to the point where the vectors/quintuples are generated. However, not the CK+IK is passed back to over Diameter to the MME, but KASME, which is computed from CK+IK, the MCC+MNC of the VPLMN and some other bits.

Let's add support for this to libosmocore

Related issues:

Related to libosmocore - Feature #4105: Support for LTE key derivation functions	**New**	**07/13/2019**

History

#1 - 07/12/2019 10:15 AM - laforge

https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/rd/technical_journal/bn/vol11_3/vol11_3_027en.pdf is a good summary

#2 - 07/13/2019 02:07 AM - laforge

- Related to Feature #4105: Support for LTE key derivation functions added