

OsmoSGSN - Bug #3224

verify ciphering after UMTS AKA

04/30/2018 11:07 PM - neels

Status: New	Start date: 04/30/2018
Priority: Normal	Due date:
Assignee: lynxis	% Done: 0%
Category: lu interface	
Target version:	
Spec Reference:	
Description	
Depending on whether UMTS or GSM AKA was established, ck or kc must be used as ciphering key. In osmo-sgsn, I cannot find any bit of code that would use the UMTS ck. All I can find is: osmo-sgsn/src/gprs/gprs_llc.c:	
<pre>if (llme->cksn != mm->auth_triplet.key_seq && mm->auth_triplet.key_seq != GSM_KEY_SEQ_INVALID) { memcpy(llme->kc, mm->auth_triplet.vec.kc, gprs_cipher_key_length(mm->ciph_algo)); }</pre>	
Verify in practical tests that ciphering works with UMTS AKA. Also verify that when the MS responds with GSM AKA to a UMTS AKA challenge, the GSM AKA key is used. (The same issue has been solved in the MSC not too long ago.)	
Related issues:	
Related to OsmoSGSN - Bug #3193: auth: on GERAN, must allow GSM SRES response...	Resolved 04/21/2018
Related to OsmoSGSN - Bug #2857: No automatic testing of luPS interface	Stalled 01/23/2018 01/23/2018

History

#1 - 04/30/2018 11:26 PM - neels

- Related to Bug #3193: auth: on GERAN, must allow GSM SRES response even to UMTS AKA challenge added

#2 - 06/23/2018 07:42 PM - laforge

- Related to Bug #2857: No automatic testing of luPS interface added

#3 - 08/20/2018 04:09 PM - neels

- Assignee set to lynxis

assigning to lynxis -- is this resolved by your osmo-sgsn patches?

#4 - 08/20/2018 06:04 PM - lynxis

no. it's not. There is still no ciphering (yet) implemented.

#5 - 04/15/2019 07:30 AM - laforge

- Category set to lu interface