OsmoSGSN - Bug #3193

auth: on GERAN, must allow GSM SRES response even to UMTS AKA challenge

04/21/2018 08:21 PM - neels

Status:	Resolved	**Start date:**	04/21/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

On OsmoSGSN:

```
20180421220155513 DMM INFO gprs_gmm.c:731 MM(901700000014702/e2269155) -> GPRS AUTH AND CIPH RESPO
NSE
20180421220155513 DMM DEBUG gprs_gmm.c:778 MM(901700000014702/e2269155) checking auth: received GS
M SRES = f1 4c b4 f2
20180421220155514 DMM ERROR gprs_gmm.c:714 MM(901700000014702/e2269155) Auth mismatch: expected UM
TS RES = e374fa67087f0318
20180421220155514 DMM NOTICE gprs_gmm.c:651 MM(901700000014702/e2269155) <- GPRS AUTH AND CIPH REJ
ECT
```

On OsmoMSC though it works fine:

```
20180421220150541 DMM DEBUG gsm_04_08.c:617 -> AUTH REQ (rand = cab3375ae19d30bf1550c3da41e55fd5)
20180421220150541 DMM DEBUG gsm_04_08.c:619    AUTH REQ (autn = 4d6215b4eaa900007b24c3d63bc49787)
...
20180421220151472 DRLL DEBUG gsm_04_08.c:3482 Dispatching 04.08 message GSM48_MT_MM_AUTH_RESP (0x5
:0x14)
20180421220151472 DMM DEBUG gsm_04_08.c:996 IMSI:901700000014702: MM GSM AUTHENTICATION RESPONSE (
sres = eb713263)
20180421220151472 DVLR DEBUG vlr.c:1205 VLR_Authenticate(LU:2652801335)[0x6120000132a0]{VLR_SUB_AS
_WAIT_RESP}: Received Event VLR_AUTH_E_MS_AUTH_RESP
20180421220151472 DVLR DEBUG vlr_auth_fsm.c:136 SUBSCR(IMSI:901700000014702) AUTH on GERAN receive
d SRES/RES: eb713263 (4 bytes)
20180421220151472 DVLR INFO vlr_auth_fsm.c:208 SUBSCR(IMSI:901700000014702) AUTH established GSM s
ecurity context
```

Like osmo-msc, we should allow responding with a GSM SRES to a UMTS AKA auth request in OsmoSGSN.

Seen with Ingenico iWL221 (portable electronic payment terminal) on OsmoDevCon 2018.

(This reminds me of osmo-msc #2793 but actually is a bit different -- in osmo-msc, we accepted the SRES but then used the UMTS key for ciphering, here we still need to accept the SRES to begin with)

Related issues:

Related to OsmoSGSN - Bug #3224: verify ciphering after UMTS AKA	**New**	**04/30/2018**

History

#1 - 04/21/2018 08:48 PM - neels

Same behavior observed on Samsung B2100!

Go to menu, select the "globe" symbol and enter a URL, it will then attempt to establish a GMM context.
So fixeria can take the credit card reader back home and we still have a device to reproduce the bug with =)

#2 - 04/30/2018 11:26 PM - neels

- Related to Bug #3224: verify ciphering after UMTS AKA added

#3 - 05/02/2018 09:26 AM - neels

- Status changed from New to Resolved

- % Done changed from 0 to 100

https://gerrit.osmocom.org/7959 merged