

Mobile (in)Security - Bug #1479

MTK stack unable to send MO-SMS on TCH/F

02/19/2016 10:51 PM - laforge

Status:	New	Start date:	
Priority:	Normal	Due date:	
Assignee:		% Done:	0%
Category:	MS (Mobile Station)	Spec Reference:	
Target version:			
Resolution:			
Description			
When a phone with MTK chipset (and firmware) wants to send a MO-SMS, it is unable to deliver that SMS if the BTS/BSC assign a TCH/F.			
The MS will respond to the IMMEDIATE ASSIGN with a CM SERVICE ACCEPT, but will never send any CP-DATA. After some time, the BTS/BSC will close the channel again.			
It is well within the authority of the network to decide which channel type to assign to the MS, and there is no technical reason why SMS delivery should not be done over the FACCH.			

History

#1 - 02/21/2016 04:35 PM - laforge

- Assignee deleted (laforge)

#2 - 04/03/2019 09:01 AM - fixeria

there is no technical reason why SMS delivery should not be done over the FACCH.

AFAIR, SMS delivery shall be actually done over SACCH (not FACCH), if a TCH channel is allocated. There should be something about this at the beginning of GSM 04.11.

There was a bug in OsmoBSC, so the MO CP-/RP-messages were being sent on SACCH, while the BSC was responding on FACCH. Maybe, the old OpenBSC was also affected by this bug. Most of the phones I've tested have been working fine despite mixing SACCH and FACCH.