3GPP TSG SA WG3 Security — S3#17 **S3-010039**

27 February - 02 March, 2001

Gothenburg, Sweden

TSG-RAN Working Group 2 (Radio L2 and Radio L3) ***R2-010755***
Sophia Antipolis, France, 19th - 23rd February 2001

Source:	**TSG-RAN WG2**
To:	**TSG-SA WG3**
Cc:	**TSG-RAN WG3**
Title:	**LS on Checking the integrity of UE security capabilities**
Contact:	Ainkaran Krishnarajah, Ericsson Email: Ainkaran.Krishnarajah@era.ericsson.se

---

TSG RAN WG2 received a contribution (R2-010574 CR 676r1 to 25.331) based on changes to TS 33.102 in a CR in S3-010729, “Correction on use of GSM MS classmark in UMTS”.

TSG RAN WG2 was at first unsure what to do with the CR to TS 25.331 as TSG RAN WG2 did not know why this change was really needed. TSG RAN WG2 did not receive any LS from TSG SA WG3, indicating:

- the identified scenario of the security threat (to help in understanding the solution proposed)
- the seriousness of such a treat
- and perhaps a request to study the impacts on TSG RAN WG2 protocols

The above points would have been very useful for TSG RAN WG2 and would have aided in the decision making process.

TSG RAN WG2 has tried to study the issue relating to the GSM classmark and would like to inform TSG SA WG3 that there are two ways for the UE to report the GSM CM2 and CM3 information. The first is by the RRC UE CAPABILITY ENQUIRY message (UTRAN → UE) which initiates the RRC UE capability information procedure. The following RRC messages are sent:

UE CAPABILTY INFORMATION (UE → UTRAN): This message contains the “Inter-RAT UE radio access capability” information element.

UE CAPABILTY INFORMATION CONFIRM (UTRAN → UE)

TSG RAN WG2 would like to note that the above three messages are always integrity protected. In such an approach, the requirements on Inter-system handover would need to be taken into consideration. The Inter-RAT UE radio access capabilities can be provided to UMTS by GSM or requested by UMTS (UE CAPABILITY ENQUIRY) when an inter-system handover is made from GSM to UMTS.

The second approach is to send the GSM CM2 and CM3 in the RRC CONNECTION SETUP COMPLETE message. This message is never integrity protected, as the RRC Security mode control procedure would only begin after this procedure has been completed.

TSG RAN WG2 also noticed that in the approved document S3-010729, that the GSM CM2 and CM3 would be sent in the RANAP SECURITY MODE COMMAND. In this case, TSG RAN WG2 does not see the need to have the Inter-RAT UE radio access capability in any RRC procedures and would like to confirm if this assumption is correct.