3GPP TSG SA WG3 Security — S3#17 **S3-010118**

27 February - 02 March, 2001

Gothenburg, Sweden

Title: **(Draft) LS on UE ciphering capabilities**

Source: **TSG SA WG3**
To: **TSG RAN**
Cc: **TSG RAN WG 2; TSG SA**
Contact Person: **valtteri.niemi@nokia.com**

A mechanism for protection of UE's GSM ciphering capabilities was approved to the security architecture of UMTS in December 2000. A companion CR to 25.331 was proposed to RAN2 and the attached LS was sent to S3. In this LS, S3 addresses the concerns raised by RAN2 in the attached LS. Also, the role of the feature in the context of the whole 3G security is discussed.

Based on these arguments, S3 would like to ask whether RAN could consider the inclusion of the proposed CR (R2-010574 CR 676r1 to 25.331) into R99 specifications. In that case, S3 presents a corrective CR to 33.102 for SA plenary (to put the stage 2 and stage 3 specifications fully in line with each other). In the case time frames do not allow the inclusion of the feature to R99 specifications the CRs should be included into R4 specifications.

As mentioned, the CR to 25.331 was postponed in RAN2 because there was enough information about the security threat involved. We describe a threat scenario and emphasize the importance of implementing the mechanism in R99.

An example threat scenario is the following. There is a "man-in-the-middle" node between UE and the network which acts as a simple relay but occasionally tries to modify messages in such way that some unfortunate situation occurs. In UTRAN, the man-in-the-middle cannot modify those messages that are integrity protected. However, for instance, the first RRC signalling messages are not integrity protected since the keys are not yet in place.

The object of the man-in-the-middle in our scenario is to convince the network that the UE has weaker ciphering capabilities that it actually has. Assume the network asks for the GSM classmarks CM2 and CM3 in the RRC CONNECTION SETUP message. The man-in-the-middle blocks out this question in downlink and, thus, UE does not know that it should send the classmarks. Subsequently, in the uplink message RRC CONNECTION SETUP COMPLETE, the man-in-the-middle adds classmarks with downgraded ciphering capability information. An alternative way is to simply modify the classmarks in uplink signalling.

The impacts of the threat will increase with the introduction of the A5/3 ciphering algorithm. Indeed, part of the terminal base will support this stronger algorithm while the rest support only A5/1 and A5/2. As integrity protection is in use in UTRAN it is useful to extend the protection also to GSM part to cover handovers from UTRAN to GSM.

What is proposed in RAN2 is to add the GSM ciphering capability (7 bits) to the RRC: SECURITY MODE COMMAND (just as UTRAN security capability is added in the same message to protect it from the man-in-the-middle attack). The UE checks the correctness of this information.

Another way to protect the GSM ciphering classmarks would be to use the specific (integrity protected) RRC UE capability information procedure referred to in the LS from RAN2 . However, this cannot be mandatory (prior to inter-system handover) since the other method to obtain the classmarks (in RRC connection establishment) was introduced to decrease the signalling load. Hence, this latter method should also be protected.

Let us now discuss what are the consequences if the change is postponed to later releases. In that case, if either the UE is R99 or the network is R99 the protection mechanism does not work: either the network does not send the capability information downlink or the UE does not check the

correctness of the information. Consequently, for instance, a R99 network cannot protect the A5/3 capability in the UE when handover to a GSM BSS (which supports A5/3) occurs. Furthermore, the man-in-the-middle would typically pretend to be R99 (e.g. R99 UE towards the network) in order to avoid the protection mechanism.

On the other hand, it is clear that the mechanism only protects GSM ciphering capabilities in the case where the connection is originally established on the UTRAN and handed over to GSM. If the connection is on GSM side from the beginning, the capabilities cannot be protected this way. However, if there is still an opportunity to make this enhancement in the R99 RAN2 specifications then it should be taken.

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.