3GPP TSG SA WG3 Security — S3#18 **S3-010213**

21 - 24 May, 2001

Phoenix, USA

Report to SA3 on SA#11
Palm Springs, 20th March 2001

I had a very hard time of it at SA#11 – see details below. My presentation is attached.

1. Milenage evaluation report approved. Note that like the other algorithm documents, the report will be published by the individual SDOs.

2. On network domain security, I asked that SA3 be given the opportunity to complete the MAP security items that were scheduled for R-4 in time for the June plenary. I believe this is a better option than postponing everything to R-5, and having to demand that CN remove the features it has already provided in its R-4 specifications. SA agreed to this subject to completion of a formal document explaining what we need to do, what are the consequences of failing to deliver, etc. My understanding is that the work is technically complete (with perhaps a couple of minor problems), but is muddled up with R-5 deliverables and material that is largely tutorial. Assuming this to be the case, we have a major editorial task, and Vodafone will provide a resource to help accelerate the work. My understanding is that automated key management is not in the agreed R-4 deliverable.

3. On the IMS security, some concern was expressed by CN1 that what we were doing was not aligned with their SIP protocol work. This apparently emerged at the joint SA3/SA2 meeting – which the SA2 chair confirmed was very useful. I was surprised by this, and agreed we would have a joint meeting with CN1, probably around our May meeting. We are expected to provide the IMS security specification for the June meeting of SA.

4. SA2 requested another joint meeting with us. I agreed in principle to this being at our ad hoc meeting in Madrid organised for the 26th April. I know this will eat into time we have set aside for our IMS work, but if we have done our 'homework' before the meeting, we can use SA2 as a very useful sounding board to check our security solution. Can I have your views on this proposal. Could we extend our ad hoc to the 29th?

5. There was wide criticism that SA3 does not liaise properly with other groups – one way or another SA1, RAN and CN1 all said this.

6. The CR's were handled as follows:
   - CR to 03.25 1ST – approved
   - CR135, 136, 137, 140, 141, 142 to 33.102 – all approved
   - CR 143 – correction to mechanism for protecting GSM ciphering – approved, but see below
   - CR138, 139 to 33.102 – approved

- CR013 to 33.105 – approved
- CR016, 017, 018 to 33.105 – approved
- CR's on LI approved except that to R-5 which was withdrawn.

7. The CR on handling algorithm identifiers in class marks caused me a lot of trouble – I was attacked by RAN and others for us having failed to properly inform them and involve them in the solution. I don't know what happened here, but it must not happen again.

8. The new work item on 'end-to-end security' was accepted – I look forward to contributions. It was recognised that this could have a lot of implications for RAN, GERAN and CN, etc. and we must keep them informed of what we are proposing.

Michael Walker
Chairman SA3
20th March 2001