3GPP TSG SA WG3 Security — S3#16 **S3-000655**

28-30 November, 2000

Sophia Antipolis, France

3GPP T3 Meeting #16 ***Tdoc T3-000631***
Seoul, Korea, 13 - 15 November, 2000

Liaison Statement

From: T3 (Contact: Jeremy Norris, jeremy.norris@eml.ericsson.se)

To: S3

CC: S1, N1

Subject: Re-transmission of authentication request using the same quintet

T3 discussed the impact of 33.102 CR 104r1 (TDoc S3-000578, as approved in SP-000411 at TSG-SA #9) on its specifications and would like to inform S3 of the result.

Though it is technically possible to realise the necessary changes, T3 would like to remark that these have quite an impact on the implementation in the USIM. Not only that the USIM shall store the last challenge/response pair, the AUTHENTICATE command would have to detect a repetition and after checking the "associated start parameter" (which the command currently does not know) react accordingly. Further, an update of EF_{START} would have to trigger the deletion of the stored parameters.

If S3 is of the opinion that the feature should not be implemented in the ME (though this seems to be possible in the opinion of several delegates), then T3 would like to raise the following points for consideration by S3:

- The CR states "The USIM shall store the last (RAND, AUTN) pair as well as the corresponding RES". T3 feels that the need to store RES is unwarranted. This is since the USIM can either re-calculate it from the RAND and AUTN or uses a stored value. The result would be identical. From this it implies that it is up to the USIM how this is performed and therefore it is dependent on the implementation. T3 would like to suggest to S3 to rephrase their requirement in a way to say that the USIM when the (RAND, AUTN) pair is re-transmitted, shall return the same RES as before.

- Do the Cipher Key - CK and the Integrity Key – IK have to be returned as well?.

- In the case that GSM access service is supported by the USIM what should be done with the cipher key Kc?

- T3 would also like S3 to consider the deletion of the stored values from the memory. Shouldn't they be deleted when the UICC is powered down, and when the USIM application session is terminated?

- Clarification is required on the setting of the START value. There seems to be an ambiguity in the current version of TS 33.102. In section 6.4.8, it is stated in the final sentence “During authentication and key agreement the START value associated with the new key set of the corresponding service domain is set to 0 in the USIM and in the ME.” However in section 6.4.5, the fifth bullet point states “The indication of new generated keys implies that the START value to be used shall be reset (i.e. set to zero) at start use of the new keys.” From these there appears to be two differing procedures one is where the START value is zeroed when the keys are used the other is when they are generated. T3 feels it should be when they are used but would like S3 to consider it in detail.

- T3 would also like S3 to consider the potential implication of the circuit switched domain and the packet switched domain authentication parameters. Should both associated (RAND, AUTN) pairs for these domains stored ?

- Finally T3 would like to receive clarification on why exactly the requirement that the stored values have to be deleted immediately upon update of the associated START parameter is necessary. This requirement imposes significant modifications on the USIM interface and the security implications are not really clear to T3.

T3 understands that there is a S3 meeting from Tuesday, 28th to Thursday, 30th of November and proposes to have a joint meeting with S3, preferably either on Monday, 27th or on Tuesday 28th.