3GPP TSG SA WG3 Security — S3#15 S3-000624
12-14 September, 2000
Washington, USA

Source: **Gemplus**

Title: **Comments on CR to 33.102: "Re-transmission of authentication request using the same quintet" in S3-000578**

Gemplus has reviewed the proposed CR in S3-000578 and would like to make some comments :

1) A CR on TS 31.102 will be necessary as a consequence, as some part of the AKA is described in this specification.

2) About adopting a R'99 CR at this very late stage on TS 31.102 :

   a) it would be preferable to keep this new feature as an option. It's an optimization that will save some radio and network resources (by avoiding re-synchronisation). As the USIM is the property of the operator, it's up to the operator to decide what is in a USIM. And so an operator would decide or not to implement this optimization, which is not necessary to make the 3G AKA work.

   b) about the timescale : SAGE has not already delivered the 3G authentication algorithm specifications. So from SC manufacturer point view any internal modification of the AKA mechanism now could be seen as a modification of a not already-implemented algorithm. But this apply only to operators who will go (wait) for the SAGE algorithm.

3) The proposed change implies unusual procedures within the card : deleting the (RAND, AUTN) pair when START is updated implies that we have to modify the UPDATE BINARY command in order to check if it applies to START. Thus it would cause delay in the command execution. And philosophical concerns (e.g. is the command still ISO/IEC 7816 compliant ?)

4) Regarding security, we are concerned that it may be possible to "re-use" these parameters to cause a fake mutual authentication. This would mean that the you would just ask the ME to ask the USIM to use the same parameters as the USIM has stored. If the ME then doesn't make an update for some reasons then these valid parameters could remain for ever. Confirmation would be needed that S3 has looked at this from an attach/eavesdrop point of view.

5) Clarification is needed as to why the USIM shall store 'the corresponding RES'. Why not the corresponding IK and CK, which are as well returned by the authentication algorithm ? IK, CK and RES should be considered the same way, as SQN is not used to compute them. So either the USIM stores RES, IK, CK, or none of them. The last solution seems preferable as it is more secure and requiring less memory resources.

6) What about the SRES and Kc which are generated by the AUTHENTICATE in addition to 3G parameters when service n°27 (GSM access) is supported ?

7) In the CR, it is said that the pair is repeated "when the associated START parameter" is zero. In fact there are two different START values, one for the CS domain, the other for the PS domain. The USIM cannot know which one is associated to the authentication request, because the card doesn't know in which domain the MS is asked to authenticate. Or is it that both START

values should be zero to trigger repetition? Needs clarification in this case.

A proposal was made last week on the S3 email reflector by T-Mobil (S.Puetz) that would solve at least points 3 and 7 above. Gemplus would prefer that solution, should S3 consider that this optimisation is really to be kept mandatory.